Cybersecurity Culture: An Ill-Defined Problem

Noluxolo Gcaza, Rossouw Von Solms

Cybersecurity Culture: An ill-defined Problem

Noluxolo Gcaza[1] and Rossouw von Solms[2]

[1]Nelson Mandela Metropolitan University, Port Elizabeth, South Africa & CSIR, Pretoria, South Africa
S208045801@live.nmmu.ac.za
[2]Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
rossouw@nmmu.ac.za

Abstract. Cybersecurity necessitates the development of a solution that encourages acceptable user behaviour in the reality of cyberspace. Nowadays, users are considered to be the weakest link in the security chain – due to their insecure behaviour and their lack of awareness. However, even users who possess more cybersecurity awareness are reported to behave no differently from those who lack any form of cybersecurity awareness. Therefore, cultivating a cybersecurity culture is regarded as the best approach for addressing the human factors that weaken the cybersecurity chain. Research focusing on defining and measuring the cybersecurity culture is considered to be lacking. Additionally, there is an apparent lack of widely accepted key concepts that further delimits the culture. Both these assertions suggest that cybersecurity culture is an ill-defined problem. Therefore, this paper will attempt to confirm that cybersecurity culture is an ill-defined problem by means of content analysis. Classifying cybersecurity culture as an ill-defined problem can guide future researchers in what problem-solving processes to employ when addressing the problem of cybersecurity culture.

Keywords: Cybersecurity; culture; cybersecurity; content analysis; ill-defined problems

1 Introduction

Cybersecurity needs the development of a cybersecurity culture that encourages acceptable user behaviour in the reality of cyberspace. [1]. Cultivating a cybersecurity culture is regarded as the best approach for addressing the human factors that weaken the cybersecurity chain [2]. It has been found that even users who possess more cybersecurity knowledge can behave no differently from those who lack any form of cybersecurity awareness [3]. Regardless, of the fact that the awareness level of the user positively affects the user behaviour, there is still an apparent gap between the user awareness levels and their respective practices and behaviour [4]. Thus, according to van Niekerk [5], in order for a culture to effectively counter the effects of the human factor, user knowledge (awareness and education) and behaviour need to be addressed. Thus, it can be accepted that two of the pillars of cybersecurity culture are awareness and education [6].

While the role of cultivating a culture in pursuing cybersecurity is well-appreciated, research focusing intensely on defining and measuring cybersecurity culture is still in its infancy [7]. Furthermore, studies conducted by Reid and van Niekerk [8], [9] revealed that there are no widely accepted key concepts that delimit a cybersecurity culture. Nevertheless, due to the relationship between information security and cybersecurity, it is reasonable to make the assumption that what describes an information security culture should also apply to the cybersecurity culture [10].

It should be noted that there is profound difference information security and cybersecurity. However some authors use cybersecurity interchangeably with information security. Ried and Van Niekerk [8] argue that the fundamental difference is that information security aims to ensure the continuity of business and to limiting the impact of security incidents, in order to minimize business damages. As such, information security is primarily concerned with preserving the information in an organizational context. Cybersecurity, however, extends far beyond the borders of a business, considering that information is shared and disclosed in cyberspace. Therefore, even though a close association exists between information security and cybersecurity, there are aspects that fall outside the scope of information security [8].

Nevertheless, Schein [11] defines information security culture as a "pattern of shared basic assumptions that the group learned; as it solved its problems of external adaptation and internal integration, which have worked well enough to be considered valid; and therefore, to be taught to new members, as the correct way to perceive, think, and feel in relation to those problems". Similarly, in information security, Schlienger and Teufel [12] refer to the culture within the organization as that which "should support all [the] activities, in such a way that information security becomes a natural aspect in the daily activities of every employee. Security culture helps to build the necessary trust between the different actors." Both the latter and former information security culture definitions deal with altering the behaviour of users, by instilling a certain way to "naturally behave" in daily life, a way that conforms to certain information security assumptions.

The assertion that research focusing on defining and measuring cybersecurity culture is lacking, as well as a lack of the apparent widely accepted key concepts that delimit the culture, both suggest that cybersecurity culture is an ill-defined problem. With ill-defined problems, the following is true: The information needed to solve the problem is often incomplete or inconsistent; no standard criteria exist to confirm the solutions; and it is uncertain which elements make up the problem, or the solution to the problem [13], [14].

This paper seeks to test the claims that imply that cybersecurity culture an ill-defined problem. In doing so, future researchers addressing cybersecurity culture can be guided in the selection of the problem-solving processes. Hence, this paper reviews the existing literature, focusing specifically on cybersecurity culture, in order to determine the following:

- Does the existing literature acknowledge the need for a cybersecurity culture?
- Does a generally accepted definition of cybersecurity culture exist?
- Does a widely accepted approach for cultivating a cybersecurity culture exist?

- What are the elements that describe a cybersecurity culture?

This paper will attempt to address these questions by means of content analysis. The following section provides a discussion on ill-defined problems. Thereafter, a section entailing the research methodology employed to conduct the content analysis can be found. The section following the research methodology will provide an account of the content analysis on cybersecurity culture; and this is followed by a discussion on the findings. Finally, concluding remarks will be provided.

2 Ill-defined problems

The terms "ill-defined" and ill-structured" are used interchangeably in the literature. To eliminate confusion, this study will adopt the term "ill-defined". Problems are regarded as ill-defined, when "essential concepts, relations, or solution criteria are unspecified or under-specified, open-textured, or intractable, requiring a solver to frame or re-characterize it. This re-characterization, and the resulting solution, [is] subject to debate" [15]. Re-characterization is the process of decomposing the problem into sensible representations. Notably, re-characterization is often inherent in ill-defined problems [15]. In addition to re-characterization, a criterion exists to determine the 'defined' level of a problem [14], [15]. It includes vaguely defined number of goals; incomplete and inaccurate or ambiguous uncertain information; inconsistent relationship between concepts, rules, and principles among cases based on context; multiple solutions, solution paths, or no solution at all; and no one universal agreement on the appropriate solution.

A vaguely defined number of goals relates to the fact that ill-defined problems do not have defined end-states. Moreover, it is often challenging to find all the necessary information that is needed to solve the problem. Ill-defined problems exhibit inconsistency, when considering the concepts and principles that delimit the problem and the rules govern the problem-solving process. Often, there is no standard solution for such problems. Perhaps that is due to the fact that each problem solver re-characterizes the problem from his own unique standpoint and suggests a solution based on that unique perspective. Hence, ill-defined problems lack a single universal solution.

The task of designing a house can be used as an example of an ill-defined problem, particularly in a scenario were the architect is required to be creative and not to use a pre-existing design. In this scenario, the architect is not informed on what the client wants the house to look like on completion. The problem space is ill-defined (referring to the structural elements of the house), the specification of the elements that make up the problem space are unknown (referring to the type of structural elements). Nevertheless, the task of designing a house can easily move to the well-defined end of the problem continuum; if the client makes known the desired end-state of the house. Specifications, such as the number of rooms, the structural specifications, such as a wooden house or brick garage. In this scenario, it can be seen that based on the information that is available, the problem can be rendered ill-defined or well-defined.

Thus, an analysis of the existing information can confirm that the cybersecurity culture can be seen as an ill-defined problem.

It can be gathered that what is true for ill-defined problems is in contrast to that of well-defined problems. On the contrary, well-defined problems exhibit characteristics that include a known goal state; a well-defined initial state; and a constrained logical state; constraint parameters; and single correct, convergent answer to reach a satisfactory final solution [14]. Unlike ill-defined problems, well-defined problems have a known end-state. Consequently, a problem-solver approaches the problem with a clear end-goal in mind. Additionally, a well-defined problem has an elaborate initial stage; since all the information about the problem is available to the problem-solver. Furthermore, there is a constraint in all the concepts, rules and cases that form part of the problem space. Lastly, a well-defined problem has a widely acceptable solution [14].

The pursuit to identify a problem as well-defined, or ill-defined, is crucial; because the problem-solving process differs for problems on the different ends of the continuum [16]. According to Voss and Post[17] as well as Sinnott [18] in solving ill-defined problems, a unique problem-solving process is used, compared with that used to address well-defined problems. Simon [14] seems to disagree with this notion; and this author suggests that the question of being ill-defined does not lie on the problem, but rather in the problem-solver. Simon [14] adds that it is the experience of a problem-solver that leads to a problem being deemed well-defined or ill-defined. On the contrary, many authors [17]–[19] support Reitman [16] in the notion that ill-defined problems require a unique problem-solving process. Generally, when solving a well-defined problem the best solution is selected by anticipating the logical consequences of each [20], [21]. On the contrary, with ill-defined problems the selection of the best solution is guided by the solver's perception of the problem constraints. Thus when solving problems from opposite ends of the continuum – is different the problem solving process differs. Additionally, different techniques are used to solve ill-defined and well-defined problems. For well-defined problems, the techniques are quantitative in nature; whilst for ill-defined problems, the techniques are rather qualitative [22]. Therefore, it is essential for the problem-solver to know the type of problem s/he is dealing with, in order to follow the correct problem-solving process [22].

This section has provided a discussion on ill-defined problems. Additionally, it has contrasted ill-defined and well-defined problems. It has motivated why it is important to categorise a problem as either ill-defined, or well-defined. The following section discussed the methodology that will be used to confirm that cybersecurity culture is indeed an ill-defined problem.

3 Methodology

A content analysis is defined as "a research technique for making replicable and valid inferences from texts (or other meaningful matter) within the context of their use" [23]. Downe-Wambolt [24] describes content analysis as a "research method that provides a systematic and objective means to make valid inferences from verbal, vis-

ual, or written data, in order to describe and quantify specific phenomena". The purpose of content analysis is to establish and gather meaning from the text, in order to draw realistic conclusions from the data collected. In the context of this paper, the nature of the analysis will be qualitative; because the data will be presented in words; and the interpretation thereof will be drawn solely from the words [25]. Generally, a three-step process is followed, when conducting a qualitative content analysis. This process includes planning, a data collection, and the data analysis [25].

The qualitative content analysis on cybersecurity culture was carried out in a manner that aligns with the process explained above, with the application thereof being discussed as follows.

Planning. Five elements should be taken into consideration in the planning phase. In the context of the cybersecurity culture analysis, these elements were applied as follows:

Aim. The aim of this content analysis is to confirm that cybersecurity culture is an ill-defined problem.

Sample and unit of analysis. This paper reviewed the literature that explicitly focuses on the cybersecurity culture. For a qualitative content analysis, one to thirty sources are considered sufficient [26]. However, the information needs of the study should govern the number of sources [27]. In the case of this study, however, only thirteen articles were deemed relevant.

The choice of data collection method. The data were collected from online digital libraries. Table 1 below has an exhaustive list of the databases that were used.

Method of analysis. A qualitative content analysis was performed because of the nature of the problem addressed in the paper, namely, a cybersecurity culture.

Ethical considerations. The choice of the data collection method determines whether ethical issues should be considered. This is most likely in methods, such as interviews, focus group and questionnaires. However, in the case of freely available literature, the ethical aspects are not a concern. As such, this issue is not applicable in this inquiry.

The Data Collection. The data were collected from online digital libraries that include CSIR worldcat, Primo central, IEEE, Scopus, Emerald, Springer and EbscoHost. Table 1 contains the search strategies were employed to gather the information.

Table 1. Search Strategy

List of sources searched:	Search strategy used, including any limits	Total number of results found
1. CSIR worldcat	"cyber security culture"	24 *(3 relevant)*
2. Primo central	"cyber security culture"	9 *(information security)*
3. IEEE	cybersecurity culture	30 *(4 relevant)*
4. Scopus / Science Direct	(TITLE-ABS-KEY (cyber) AND TITLE-ABS-KEY (security) AND TITLE-ABS-KEY (culture))	3
5. Emerald	("Cyber security" W/5 culture)	2
6. Springer	("Cyber security" W/5 culture)	8
7. EbscoHost	"cyber security culture"	3

From the results recorded in the table, in total, only thirteen articles were deemed relevant; because some were duplicated in the sources that were searched. Previously, it was mentioned that only literature that explicitly focuses on cybersecurity culture would be considered. The literature on information security culture, or other related studies were ignored; because if the related studies were included, the sample unit would give a false impression regarding the extent of knowledge that currently exists on the topic at hand. Only peer-reviewed journals and conference articles were considered. The year of publication was not constrained because the aim was to retrieve as much existing information on the topic to date. Additionally, no disciplines were eliminated because the aim was to get information from different contexts.

Data Analysis. This study was deductive in nature; since it is based on a predetermined hypothesis. The hypothesis is that cybersecurity culture is an ill-defined problem. Additionally, the analysis will be based on what is written by the authors – instead of the underlying meaning in the text; thereby, it becomes a manifest analysis.

Report Findings. Sections 4 and 5 provide an account of the findings.

This section discussed the research methodology, the following section provides a review of the existing literature on cybersecurity culture.

4 Cybersecurity culture content analysis

Da Veiga [7] focuses on defining cybersecurity culture, in order to be able to measure and quantify the culture. The paper suggests that a cybersecurity culture should ideally be fostered in all levels, including individual, organizational, national and international levels. The author draws insight from the IT discipline, together with industrial psychology, to define cybersecurity culture as "the intentional and unintentional manner, in which cyberspace is utilized from an international, national, organizational or individual perspective in the context of the attitudes, assumptions, beliefs, values, and knowledge of the cyber user.

The cybersecurity culture that emerges becomes the way things are done when interacting in cyberspace; and this can either promote or inhibit the safety, security, privacy, and civil liberties of individuals, organizations or governments." This definition features the description of organizational culture, which is "the way things are done here". Additionally, the paper proposes a cybersecurity culture research methodology (CSeCRM) with the aim to ensure that the culture can be measured. According to the author, the proposed methodology can be potentially used to assist in identifying which actions need to be taken, in order to change and direct a cybersecurity culture.

Malyuk and Miloslovsaya [28] focus on integrating cybersecurity culture in IT professional training courses. The authors argue IT professionals can no longer be predominantly centred on technical cybersecurity measures. According to Malyuk and Miloslovsaya [28] human factors necessitate the integration of cybersecurity culture in the IT profession. Although the paper focuses on the 'cybersecurity' culture, the authors attempted to define 'information' security instead.

Banks [29] studied the impact of leadership on cybersecurity practices in an organizational setting. The paper identifies leadership from senior management as the key to implementing a culture of cybersecurity amongst employees. Banks [29] argues that poor leadership is the weakest link of the cybersecurity chain in organizations; therefore, senior management should be an example and "practise what they preach". According to Banks [29], senior management can demonstrate their leadership by means of security policies and cybersecurity awareness and education programs.

Tziarras [30] focuses on cultivating cybersecurity culture on a global level through multi-levelled collaboration. The paper argues that for a global cybersecurity culture to be formed, there is a need for a multi-levelled management of cybersecurity. As such, Tziarras [30] proposes a framework for the multi-levelled management of cybersecurity culture. The study goes into great depth to evaluate the international cybersecurity implementation. It furthermore attempts to define cybersecurity culture from the concept of strategic culture. According to Tziarras [30], strategic culture only implicates members of a specific nation; therefore it is limited when compared with cybersecurity culture. Even so, the paper draws principles from strategic culture to describe a culture of cybersecurity as "a body of collective – i .e., non-state, subnational, and national attitudes, patterns of behavior, beliefs, as well as conceptions of (cyber) security, based on the need to secure multiple referent objects against various cyber threats, which would influence [the] cybersecurity strategies."

Reid and van Niekerk [31] sought to discern information security culture from a cybersecurity culture. A literature review on both domains was done, in order to expose any seeming similarities and differences. The authors reported that cybersecurity culture was under researched. The authors suggest that due to the relationship between information security and cybersecurity, insights from an information security culture could be extrapolated to define a cybersecurity culture. As such, the authors discuss cybersecurity culture by using the same principles that delineate information security. However, Reid and van Niekerk [31] argue that the context of information security and cybersecurity differ; therefore, practical implementation would also differ when applying some of the extrapolated principles.

Kortjan and von Solms [32] focus on establishing a national cybersecurity culture in a South African context. Firstly, the paper discusses what constitutes a cybersecurity culture from international sources that include the ITU and OECD. From these sources, the authors reason that awareness and education are key instruments in establishing the culture. Hence, the study proposes cybersecurity awareness and education guidelines that are drawn from an existing campaign in SA.

Reid and van Niekerk [9] examine how education can be used to foster a cybersecurity culture. The aim of the paper is to establish a standard approach in structuring a culture fostering an education campaign. The authors address the aim by reviewing an existing campaign in SA. The study revealed the following four lessons. Firstly, the manner in which educational material is distributed impacts how/if the message is received. Secondly, the involvement of teachers with the cybersecurity campaign is crucial; as it encourages the participation of learners. Thirdly, for a campaign to be reliable and memorable to its intended target audience, official and age-appropriate

branding is necessary. Finally, the content of the campaign should be appropriate and continuously improved.

Luiijf, Basseling and Graaf [33] study and compare nineteen national cybersecurity strategies from eighteen different nations across the globe. The paper reveals the differences and the similarities found in how nations address cybersecurity. From the analysis, a list of recommendations are made to assist other nations in developing national cybersecurity strategies. Amongst other things that can be gathered from the analysis, there is the fact that only three national strategies: from Uganda, South Africa and Romania, explicitly list cultivating a cybersecurity culture, as a strategic objective. Primarily, the contribution of the paper is a basic structure for developing a cybersecurity policy.

Hall [34] examines the importance of humans in the cybersecurity process in an organizational setting. This author identifies employees as the "greatest source of weakness in the cybersecurity effort [or] plan". The author emphasizes that in any cybersecurity plan, organizations should take cognizance of the vulnerabilities that employees bring about. The paper advocates a culture of cybersecurity amongst all the employees. According to Hall [34], the culture will, over time, create an environment where employees implement cybersecurity practices without resentment.

Kritzinger and S. von Solms [35] attempt to address the major cyber safety concerns in the African continent. According to these authors, the major cybersecurity concerns are the lack of focused research on cybersecurity, the lack of a legal framework and policies, the lack of cybersecurity awareness and the lack of technical security measures. With these four concerns in mind, the paper proposes a framework that consists of four dimensions. These dimensions entail a combination of all possible solutions to the cybersecurity concerns. The authors suggest that the proposed framework is crucial in enhancing a cybersecurity culture in Africa.

Ghernouti-Hélie [36] analyses the "characteristics and issues related to the deployment of a national cybersecurity strategy in an interconnected world". The paper reviews the components of cybersecurity national strategies. It emphasizes the importance of operational structures to support the deployment of such strategies. Additionally, the paper stresses the importance of a cybersecurity culture in supporting a cybersecurity strategy. The author identifies education and awareness as "pillars of a cybersecurity culture". From an educational point of view, the paper focuses on formal education to build human capacities. From an awareness point of view, the author focuses on end-users, policy-makers, and on the professionals in various disciplines.

Adelola, Dawson and Batmaz [37] have attempted to establish the need for an Internet security awareness programme in Nigeria. The authors examine Internet security awareness programmes in developed countries for the purpose of deducing principles that can be used by Nigeria in establishing a cybersecurity awareness and education campaign. These countries include the US and the UK; additionally, the authors review the existing guidelines that aid the development of an awareness programme. The paper gives an extensive account of a framework developed by the National Institute of Standards and Technology (NIST). According to the authors, this campaign should enable a cybersecurity culture in Nigeria amongst all the cyberspace users.

Batteau [38] studies safety culture and corporate culture in defining a cybersecurity culture in an organizational context. The article suggests that critical to such a culture is the concept of trust, in relation to identification and authentication. The article goes to great length to motivate that trust is essential in cultivating a culture; because those who subscribe to a particular culture are linked by the perception and belief that "they are in this together". Additionally, the lack of trust amongst people (referring to the confidence in the actions and intentions of others) leads to compromised security in an organization. With trust in mind, the author describes cybersecurity culture as follows: "A culture of cybersecurity is a complex amalgamation of generalized transactional and strategic trust relationships. This culture cannot be designed, in the sense that an engineer designs a complex piece of machinery; but it can be cultivated, in the sense that a gardener cultivates a flower garden".

5 Summary of the results

This section provides the results of the qualitative content analysis in Table 2. The results are analysed using the research questions stated in section 1. Thus the coding scheme for the analysis is extrapolated from research questions.

Table 2. Content Analysis Summary

Study	Mentions Importance of Cybersecurity Culture	Provides a definition of Cybersecurity Culture	Proposes an approach to Cultivate Cybersecurity Culture	Delimits the elements that make up a cybersecurity culture
Da Veiga [7]	✓	✓		
Malyuk and Miloslovsaya [28]	✓		✓	
Banks [29]	✓		✓	
Tziarras [30]	✓	✓	✓	
Reid and van Niekerk [8]	✓			
Kortjan and von Solms [32]	✓		✓	
Reid and van Niekerk [9]	✓		✓	
Luiijf, Basseling and Graaf [33]	✓			
Hall [34]	✓			
Kritzinger and S. von Solms [35]	✓			
Ghernouti-Hélie [36]	✓			✓
Adelola, Dawson and Batmaz [37]	✓		✓	
Batteau [38]	✓	✓		

A total of thirteen sources were included as part of the content reviewed in this paper. Table 2 above presents a summary of the results. The results show that all of the included sources acknowledge the importance of cultivating a cybersecurity culture. Additionally, only three of the reviewed sources define cybersecurity culture. The definitions all differ; because they are established from different concepts that were

deemed fitting for each author, i.e. security culture and/or corporate culture, as well as strategic culture. Only six sources proposed an approach to cultivate cybersecurity culture. The sources regard one, or a combination of the following measures, as the means to cultivate the culture: Awareness Programs; Formal Education; Cybersecurity Policies; Collaboration. Furthermore, only one source delimits the elements that potentially make up a culture. The source identifies Awareness and Education, as the pillars of the culture.

From the results presented above, six observations can be made. Firstly, judging from the number of articles that explicitly focus on cybersecurity culture, it can be confirmed that research in this area is currently lacking. Secondly, the need for a cybersecurity culture is well appreciated. Thirdly, even though there is acknowledgment of the need for a cybersecurity culture, there is no single standard solution for cultivating the culture. Fourthly, no criteria to measure the validity of the proposed approaches can be found. Fifthly, the definition of cybersecurity culture is subject to the authors' context of application; and it is established from a range of relevant concepts, according to the authors' perspective. This approach, when defining a subject, is known as re-characterization, which is inherent in ill-defined problems. Finally, the elements that make up a cybersecurity culture are still to be defined.

According to the primary objective of this paper, the first and last observation confirm the assertions that research focusing on defining and measuring cybersecurity culture is considered to be lacking. Additionally, there is an apparent lack of widely accepted key concepts that delimit the culture. It was suggested that these claims indicate that cybersecurity culture is still an ill-defined problem. The findings from the analysis show that research focusing specifically on cybersecurity culture is currently lacking, this observation relates to incomplete and uncertain information as per the characteristics of ill-defined problems. Additionally, the findings show that there is no single standard solution for cultivating the cybersecurity culture, as such this relates to the lack of a universal agreement on the appropriate solution. Furthermore, the fact that the definition of cybersecurity culture is subject to the authors' perspective and context of application illustrates that there are inconsistent relationships between concepts, rules, and principles among cases based on context. Thus, when contrasting the observations against the characteristics of an ill-defined problem, it may be concluded that a cybersecurity culture can be classified as an ill-defined problem.

6 Conclusion

To effectively ensure cybersecurity, a supplementary method to complement the technical measures is required. Such a method should holistically address the human factors. This approach is recognized as a cybersecurity culture. Cultivating a culture is acknowledged as a paramount effort in ensuring cybersecurity; however, what defines a cybersecurity culture is still unclear in the research community. Thus, this study sought to classify cybersecurity culture as an ill-defined problem by means of qualitative content analysis.

It was said that classifying cybersecurity culture as ill-defined would contribute to future research by guiding future researchers in what problem-solving processes to employ, when addressing the problems of a cybersecurity culture.

The study is limited; in that it does not suggest suitable problem-solving processes for cybersecurity culture. However, it does hint on some qualitative approaches. The study is part of a large research project that ultimately attempts to define the cybersecurity security culture problem space; and it proposes an inclusive approach for cultivating the culture.

References

1. International Telecommunication Union, "Global Security Report," 2008.
2. J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 2010, pp. 476–486, Jun. 2010.
3. Y. Al-shehri, "Information Security Awareness and Culture," *Br. J. Arts Soc. Sci.*, vol. 6, no. 1, pp. 61–69, 2012.
4. S. Furnell, "End-user security culture: a lesson that will never be learnt?," *Comput. Fraud Secur.*, no. April, 2008.
5. J. Van Niekerk and R. Von Solms, "Understanding Information Security Culture: A Conceptual Framework," *Proc. ISSA 2006*, pp. 1–10, 2006.
6. N. Kortjan and R. Von Solms, "A conceptual framework for cybersecurity awareness and education in SA," *South African Comput. Journal, 52, 29-41.*, vol. 2014, no. 52, pp. 29–41, 2014.
7. A. da Veiga, "A cyber- security culture research philosopy and approach to develop a valid and reliable measuring instrument," in *SAI Computing Conference 2016*, 2016, p. 10.
8. R. Reid and J. van Niekerk, "From Information Security to Cyber Security Cultures Organizations to Societies," in Information Security for South Africa (ISSA), 2014, 2014, pp. 1–7.
9. R. Reid and J. van Niekerk, "Towards an Education Campaign for Fostering a Societal , Cyber Security Culture," in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, 2014, pp. 174–184.
10. N. Gcaza, R. Von Solms, and J. Van Vuuren, "An Ontology for a National Cyber-Security Culture Environment," in *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, 2015, pp. 1–10.
11. E. Schein, *Organizational culture and leadership. 2nd ed. Jossey- Bass; 1992*, 2nd Editio. San Francisco: Jossey-Bass, 1992.
12. T. Schlienger and S. Teufel, "Information security culture – from analysis to change," in *In Security in the Information Society*, 2002, pp. 191–201.
13. K. P. Wood, "Inquiring Systems and Problem Structure: Implications for Cognitive Development," *Hum. Dev.*, vol. 26, pp. 249–265, 1983.
14. H. A. Simon, "The structure of ill- structured problems," *Artif. Intell.*, vol. 4, no. 1973, pp. 181–201, 1973.
15. C. Lynch, K. D. Ashley, N. Pinkwart, and V. Aleven, "Concepts, Structures, and Goals: Redefining Ill-Definedness," *Int. J. Artif. Intell. Educ.*, vol. 19, no. 3, pp. 253–266, 2009.
16. W. Reitman, *Cognition and thought*. New York: Wiley Publishing, 1965.
17. J. Voss and T. Post, "On the solving of ill-structured problems," in *The nature of expertise*, New Jersey: Lawrence Erlbaum, 1988.

18. J. D. Sinnott, *A model for solution of ill-structured problems: Implications for everyday and abstract problem solving*. New York: Praeger, 1989.
19. K. P. Wood, "A secondary analysis of claims regarding the reflective judgment interview: Internal consistency, sequentially and intra-individual differences in ill- structured problem solving," in *Annual Meeting of the American Educational Research Association*, 1994.
20. J. Bransford and B. Stein, *The IDEAL problem solver: A guide for improving thinking, learning, and creativity*. New York: W. H. Freeman, 1983.
21. A. Newell and H. a. Simon, "Human problem solving," vol. 104, no. 9, 1972.
22. N. Shin Hong, "Well-structured and Ill-structured," The Pennsylvania State University, 1998.
23. K. Krippendor, *Content Analysis: An introduction to its methodology*. SAGE Publications, 2004.
24. B. Downe-Wambolt, "Content analysis: method, applications and issues," *Health Care Women Int.*, vol. 13, pp. 313–321, 1992.
25. M. Bengtsson, "How to plan and perform a qualitative study using content analysis," *NursingPlus Open*, vol. 2, pp. 8–14, 2016.
26. B. Fridlund and C. Hildingh, "Health and qualitative analysis methods," in *Qualitative research, methods in the service of health*, Lund: Studentlitteratur, 2000, pp. 13–25.
27. M. Q. Patton, *Qualitative, research & evaluation methods*. California: SAGE Publications, 2002.
28. A. Malyuk and N. Miloslavskaya, "Cybersecurity culture as an element of IT professional training," in *3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, DIPDMWC 2016*, 2016, pp. 205–210.
29. N. Banks, "Practise what you preach," *Comput. Fraud Secur.*, vol. 2016, no. 4, pp. 5–8, 2016.
30. Z. Tziarras, "The Security Culture of a Global and Multi-levelled Cybersecurity," *Cyber-Development, Cyber-Democracy Cyber-Defense Challenges, Oppor. Implic. Theory*, vol. 9781493910, pp. 113–116, 2014.
31. R. Reid and J. van Niekerk, "From Information Security to Cyber Security Cultures Organizations to Societies," in *Information Security for South Africa (ISSA), 2014*, 2014, pp. 1–7.
32. N. Kortjan and R. von Solms, "Fostering a cyber security culture: a case of South Africa," in *Proceedings of the 14th Annual Conference on World Wide Web Applications*, 2012, no. November.
33. E. Luiijf, K. Besseling, and P. De Graaf, "Nineteen national cybersecurity strategies," *Int. J. Crit. Infrastructures*, vol. 9, no. 1–2, pp. 3–31, 2013.
34. M. Hall, "Why people are key to cybersecurity," *Netw. Secur.*, vol. 2016, no. 6, pp. 9–10, 2016.
35. E. Kritzinger and S. von Solms, "A Framework for Cyber Security in Africa," *J. Inf. Assur. Cybersecurity*, vol. 2012, no. 2012, pp. 1–10, Jan. 2012.
36. S. Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture," in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 370–373.
37. T. Adelola, R. Dawson, and F. Batmaz, "The urgent need for an enforced awareness programme to create internet security awareness in Nigeria," *Proc. 17th Int. Conf. Inf. Integr. Web-based Appl. &Services - iiWAS '15*, pp. 1–7, 2015.
38. A. W. Batteau, "Creating a culture of enterprise cybersecurity.," *Int. J. Bus. Anthropol.*, vol. 2, no. 2, pp. 36–47, 2011.