An Ontology for a National Cyber-Security Culture Environment

N. Gcaza[1], R. von Solms[1] and J. van Vuuren[2]

[1] PO Box 77000, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa
[2]Council for Scientific and Industrial Research, Meiring Naude Road, Pretoria, 0001 South Africa
e-mail: {Noluxolo.Gcaza; Rossouw.VonSolms}@nmmu.ac.za; jjvvuuren@csir.co.za

Abstract

The modern-day use of cyberspace has created a world that is increasingly relying on online services to operate. Nevertheless, cyberspace has a 'dark side'; as there are many risks associated it. This 'dark side' has called for safety and security measures to be implemented through cyber security. As such, cultivating a supportive culture is perceived to be an important contributing factor to cyber security. For this reason, many nations aspire to cultivate a culture of cyber security amongst all the users of cyberspace. However, what is lacking currently is a well-defined and delineated definition of the cyber-security culture domain. To define this domain, this paper proposes a national cyber-security culture ontology.

Keywords

Cyber Security, Cyber-Security Culture, Ontology

1. Introduction

At the inception of cyberspace, "…no one, perhaps, could have clearly foreseen that and how the Internet would someday become a veritable platform for globalized criminal activities" (Moses-Òkè 2012, p.1). Nowadays, cyberspace is a 'playground' for criminal activities, such as cybercrime, fraud, identity theft, phishing and more. A report compiled by the RSA (RSA 2014) on criminal activities, reported that in the year 2013, organisations lost about $5.9 billion to phishing attacks. The RSA foresees more sophisticated and pervasive cybercrime trends in future, which include mobile threats and malicious software.

Such security implications of cyberspace called for the establishment of cyber-security measures. Von Solms and van Niekerk (2013, p.5) define cyber security as "…the protection of cyberspace itself, the electronic information, the [Information and Communication Technologies] ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace".

Cyber security came into the spotlight in 2007, when Estonia became one of the first countries to experience a cyber-attack on its national assets (Dlamini et al. 2011). This attack called for national attention, owing to the high level of dependence of the Estonian government services on cyberspace. As a result, Estonia drafted a cyber-security policy, in order to avoid future incidents of the same kind (Dlamini et al. 2011).

As it is, over 50 nations, such as the United States (US), the United Kingdom (UK) and Australia have followed suit by drafting and implementing strategies and policies that outline how each nation intends to approach cyber security (Klimburg 2012). According to Pfleeger (2012), cyber security is the prevention and protection of cyber attacks by means of both technology and a human-centred approach. However, for a long time, technology-centred solutions such as anti-virus software, encryption, firewalls and more have been used in isolation. Up until it was acknowledged that in isolation, such solutions are not sufficient to mitigate the cyber-security risks. One of the reasons for this was that many users perceive these security measures as an obstacle (Pfleeger & Caputo 2012).

This user perception is often attributed to the difficulty of the security measure, and/or mistrust and misinterpretation of the security measure (Virginia Tech 2011). Additionally, a user-resistant behaviour was observed in a study that revealed that when users are prompted to change their passwords, the prompt was ignored or delayed; since the users perceived this security measure as being a waste of time (Pfleeger & Caputo 2012). Users often lack the awareness of cyber-security risks, making them easy targets for exploitation. Furthermore, humans are deemed as a threat not only to themselves, but also to others – and to national security at large (Dlamini & Modise 2012).

Due to the above-mentioned observations concerning the human factor, a more human-centred approach (i.e. a cyber-security culture) to cyber security is an imperative. Van Niekerk and von Solms (2010, p.476) view the establishment of a culture as the "…key to managing the human factor". However, what is lacking currently is a well-defined and delineated definition of the cyber-security culture domain. Therefore, the primary objective of this paper is to propose an ontological approach for formally defining a national cyber-security culture domain.

2. Cyber Security

The International Telecommunications Union (ITU) regards the creation of a cyber-security culture as an essential approach to cyber security (International Telecommunication Union, 2008). Recognizing this, many developed nations, such as the US, the UK and Canada are striving to cultivate such a culture amongst their respective citizens (Kortjan & von Solms 2014). South Africa (SA), in particular, has outlined the creation of a culture of cyber-security as a major objective of its draft cyber-security policy framework (SA Government gazette 2011).

One of the pillars of such a culture comprises awareness and education (Ghernouti-Hélie 2010). However, it is found that even users who possess more cyber-security knowledge do not necessarily act differently to those who lack any form of cyber-security awareness (Al-shehri 2012). Regardless, of the fact that the awareness level of the user positively affects the user behavior, there is still an apparent gap between the user awareness levels and respective practices and behavior (Furnell et al. 2008). Therefore, "cyber security needs the development of a cyber-security culture and acceptable user behaviour in the new reality of cyberspace..." (High-Level Experts Group (HLEG) 2008, p.103).

Having realized the role of cultivating a culture in pursuing cyber security it is important to formally and precisely define what is meant by a cyber-security culture. Even though the concept of fostering a cyber-security culture is used extensively, research that focuses particularly on cyber security culture is still at its infancy, and knowledge on the subject is not clearly bounded and defined. However, because of the relationship between information security and cyber security, it is reasonable to make the assumption that what applies in information security culture may also apply to cyber security culture.

Schein (1992, p.17) 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, that has 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 (2002) refer to the culture within the organization as that which "should support all activities in such a way that information security becomes a natural aspect in the daily activities of every employee".

Both the latter and former information security culture definitions deal with altering the behavior of users by instilling a certain way to "naturally behave" in daily life, a way that subscribes to certain information security assumptions. This is precisely the ultimate aim of the envisaged cyber security culture. A security culture considers the social, cultural, ethical aspects of a user in order to change the overall security behavior. Moreover, such a culture is cultivated over time and is evident in the behavior of users (Schlienger & Teufel 2002). There is, however, a lack of a clear definition of a security culture. Even though research that promotes the benefits of cultivating a security culture exists, supportive literature is lacking (da Veiga et al. 2007).

Consequently, in an attempt to formally define and represent a national cyber security culture domain, an ontological approach is proposed in this paper. Through such an approach, the aim is to better formalise cyber security culture, from a national point of view. Further details on this ontology are provided in the following section.

3. An Ontology for Knowledge Representation

The definition most cited of an ontology in the context of computer science was proposed by Gruber who defined an ontology as: "an explicit specification of a conceptualization" (Gruber 1993, p17). An ontology enables one to conceptualize a specific subject in a formal and explicit manner (Gruber 1993). It is also defined as "a technology that provides a way to exchange semantic information between people and systems. It consists of an encoded, common domain vocabulary and a description of the meaning of terms in the vocabulary" (Grobler et al. 2012, p.220). An ontology can be used to define and formalize a domain that is not explicitly defined (Fenz et al. 2009). Moreover, with this approach, the existing knowledge can be mapped together, in order to present a holistic view of a particular domain (Fenz & Ekelhart 2009). For these reasons, an ontological approach is appropriate for defining and formalizing the domain of a cyber-security culture.

In general, an ontology consists of two components: a descriptive component and a reasoning component (Grobler et al. 2012). The descriptive component captures the domain from the perspective of the domain experts; and it presents the domain information in a manner that is comprehensible to humans, and one that can be processed by computers. The reasoning component enables the ontology to make new deductions from the existing facts. From the descriptive angle, an ontology generally uses the following terms (Noy & McGuinness 2001):

- A domain – the subject area that is modelled by the ontology.
- Classes and subclasses – concepts embodied in the domain.
- Individuals – those typical of the class.
- Properties – it defines the relationships between two classes.
- Restrictions – a feature used to define and describe a class that is based on the relationships among the class participants.

From the perspective of ontology, Davis, Shrobe and Szolovits (1993, p.17), argued that if something is a surrogate (a substitute), it enables one to "determine [the] consequences by thinking rather than acting, that is, by reasoning about the world rather than taking actions". As such, with the use of ontology, one can draw inferences and reason about the world – without having to act. Additionally, the authors acknowledge that a surrogate is not immune to errors. Nevertheless, the main goal of knowledge representation is not perfection; but rather it is to create an ontology that fulfils its purpose, one which has the least amount of errors (Davis et al. 1993).

To develop such an ontology, it is important for one to have a clear understanding of the domain of interest, the classes, the individuals, the properties and restrictions. Such information can be acquired with the aid of the existing body of knowledge. Brinson, Robinson and Rogers (2006) attempted to define and formalize the cyber-forensic domain. These authors studied the existing knowledge on traditional forensics; and they argued towards a formal curriculum for cyber forensics. Another instance of an ontological approach is that of Wali, Chun and Geller (2013). These

authors maintain that online cyber-security-educational resources are scattered; and this makes it difficult for users to locate the right learning resources at the right time. Consequently, they developed a cyber-security ontology with the aid of the existing cyber-security textbooks and security ontologies.

Likewise, Grobler, van Vuuren and Leenen (2012) also developed an ontology in their attempt to define and formalize a conceptualization of the cyber-security strategic environment domain. According to these authors, the use of an ontology for the cyber-security strategic environment could contribute to the development, implementation and roll out of a national cyber-security policy in SA. Furthermore, Fenz and Ekelhart (2009) also used an ontology in their attempt to formalize and holistically present information-security knowledge. According to these authors, they were driven by the apparent lack of any unified and well-defined information-security-risk-management process. In developing this ontology, the existing information-security best practices and standards were considered.

From the above-cited instances, it is evident that an ontological approach can be used to define, formalize and holistically present the knowledge of a domain that is rather poorly defined. Noy and McGuiness (2001) summarise the reasons for developing an ontology, as follows: To share a common understanding of the structure of information among people or software agents; to enable the re-use of domain knowledge; to make domain assumptions explicit; to distinguish domain knowledge from the operational knowledge; and to analyze this domain knowledge.

In the context of this study, an ontological approach would contribute to formalizing a national cyber-security culture domain. It could assist in eliminating the vagueness of the vocabulary that exists in the domain of cyber security. It could further ensure the integration and interoperability of concepts in the domain at hand. It would play a fundamental role in ensuring the complete and holistic conceptualization of the domain of a cyber-security culture. The following section will discuss this proposed ontology for the domain of a national cyber-security culture.

4. A National Cyber-Security Culture Domain

The previous section provided an overview of ontology; this section will introduce the proposed ontology for a national cyber-security culture domain. It will provide an overview of the knowledge base represented by the ontology; and it will further provide a brief on the development of the ontology.

4.1. Knowledge Base

As an initial attempt to model a national cyber-security culture domain, a study on cyber-security culture, focusing on awareness and education, was used as a foundation. This study was published in 2013 as an academic dissertation in fulfilment of the requirements for the Master of Technology degree (Kortjan 2013); and it was also published in a journal (Kortjan & von Solms 2014). Furthermore,

additional sources were consulted, in order to gather additional information regarding the other constituents of a cyber-security culture.

In summary, in the above-mentioned academic dissertation, it was reasoned that a cyber-security culture has pillars; one of these pillars comprises awareness and education. This pillar was delineated in three forms: Awareness Campaigns; Formal Education; and Workforce Education. In terms of the Awareness campaigns, which were the main focus of the study, a national cyber-security awareness and education campaign entitled *iWiseMzansi* was suggested for SA. The name *iWiseMzansi* suggests an informative SA, hence the 'i', and a cyberwise SA, and hence the name 'wise'. "Mzansi" is an accepted name that refers to SA. It was further proposed that *iWiseMzansi* could reach the people of SA through sub-campaigns and initiatives that should include the following:

- *iWiseMzansi* Month – an annual cyber security-centred event aimed at all South African citizens.
- *iWiseMzansi* Community Outreach – an initiative intended to give everyone an opportunity to lend a helping hand and to participate in spreading cyber-security awareness and education to communities.
- *iWiseMzansi:* For All – an all-encompassing cyber-security educational website for the general public of SA.
- *iWiseMzansi:* For Schools – aimed at learners in primary and secondary schools, to ensure that cyber security forms part of the school curriculum.

It was further reasoned that for this pillar to stand, it has to be resourced, with a delineated target audience; and finally, it must have dedicated role-players with active roles. As previously mentioned, additional sources were consulted, in order to gather additional information on the other constituents of a cyber-security culture. Along with other useful deductions from these sources, additional cyber-security pillars were extrapolated, such as: Research and Development; Cyber-Security Measures; and Capacity Development (Wamala 2011; High-Level Experts Group (HLEG) 2008; Klimburg 2012).

The aforesaid pillars basically depict the following: to cultivate a cyber-security culture amongst users. Over and above the need for basic awareness and education, there has to be a strong component of research and development in order to be able to determine the current behavioural norms and other related factors. Additionally, as with information security, clear cyber-security assumptions and related measures need to be in place. Finally, the necessary capacity and various capabilities also need to be considered.

The information modelled in the proposed ontology for a national domain of a cyber-security culture is described in this section. Accordingly, the subsequent subsection presents this proposed ontology.

4.2. The Ontology

Reflecting on the existing knowledge, as previously discussed, the ontology was developed and implemented by using Protégé, an open-source ontological editor. Figure 1 presents the proposed ontology.

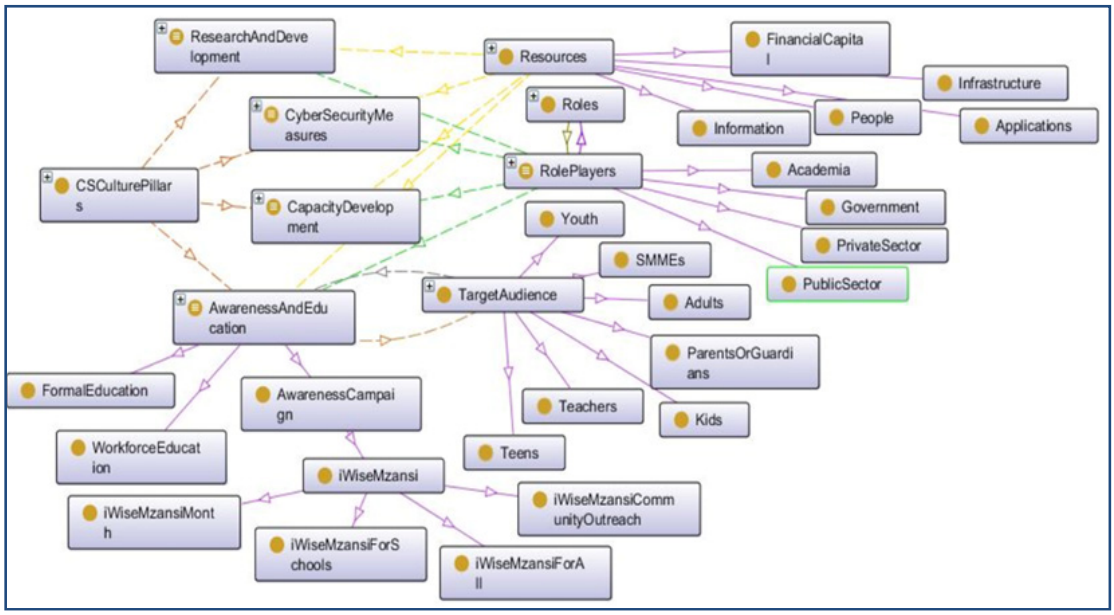

Figure 1: National Cyber-Security Culture Domain

Figure 1 presents the proposed high-level ontology model for a national cyber security culture domain. The concepts and relationships presented in the ontology will be elaborated in the development phases, in order to highlight the ontology model. The development the proposed ontology included the following phases that were adapted from Noy and McGuinness (2001): Defining classes in the ontology; arranging the classes in a taxonomic (subclass–superclass) hierarchy; defining the properties (relationships); and describing the permissible values for these slots; and defining individuals. These phases will be expanded further in the following subsections.

4.2.1. Classes and Taxonomic hierarchy

As previously mentioned, the domain at hand is that of a national cyber-security culture. The main classes of the domain are: *CSCulturePillars* (CS = Cyber Security), *ResearchandDevelopment*, *CyberSecurityMeasures, CapacityDevelopment, AwarenessandEducation, Resources*, *RolePlayers, Roles, and TargetAudience.* In the ontology these classes are arranged in a taxonomic hierarchy. Therefore some of these main classes have subclasses, which have further subclasses as well, as listed below:

- The *AwarenessandEducation* class has subclasses *AwarenessCampaigns*, *FormalEducation* and *WorkforceEducation.*

- The subclass *AwarenessCampaigns* also has a subclass *iWiseMzansi.*
- The subclass *iWiseMzansi* also has subclasses *iWiseMzansiMonth*, *iWiseMzansi*CommunityOutreach, *iWiseMzansiforAll* and *iWiseMzansiForSchools.*
- The *Resources* class has subclasses: *People, Information, Applications, Infrastructure* and *FinancialCapital*.
- The *RolePlayers* class has subclasses: *Academia, Government, PrivateSector, and PublicSector.*
- The *TargetAudience* class also has subclasses: *Kids, Teenagers, Youth, ParentsorGuardians, Adults, Teachers* and *SMMEs* (Small, Medium and Micro-sized Enterprises).

4.2.2. Relationships

It can be observed in Figure 1 that all the classes have a particular link to some or other class within the ontology. This link represents the relationships (properties) in which each class participates. These relationships are shown in Figure 2 below.

Figure 2: Defined Object Properties

As previously mentioned, an ontology has reasoning abilities. As such, the automated reasoner in Protégé can make inferences in the ontology by using the classes defined, as well as the properties in Figure 2.

4.2.3. Individuals

The last phase in the development of an ontology model is the identification of the individuals, as the instances of a class. The individuals that can be created in this proposed ontology are those of *the iWiseMzansi* class, i.e. iWiseMzansi Week, iWiseMzansi Community Outreach, iWiseMzansi: For All and iWiseMzansi: For Schools.

At this stage, the proposed ontology for the national cyber-security culture domain is still a high-level ontology that has only presented the descriptive components of the domain. Even so, it can be said that from a descriptive point of view, an explicit and formal conceptualization of the domain has been presented. Following are some concluding remarks and future plans from the study.

5. Conclusion and Future Work

It has come to the attention of many nations that although cyberspace offers many positive benefits, it also brings with it a number of safety and security implications. In recognition of this, implementing a culture of cyber-security is increasingly becoming a global pursuit. However, what is lacking currently is a well-defined and delineated definition of the cyber-security culture domain itself. Accordingly, this paper has proposed an ontology whereby this environment can now be formally defined.

In the future, further data on a cyber-security culture will be gathered in order to add depth to the ontology. A general morphological analysis (GMA), which is "simply an ordered way of looking at things" (Ritchey 2011, p.7), will be employed, in order to obtain more insights on the cyber-security culture from the relevant experts. The GMA will take place early in 2015. This technique is employed to define, the structure, and to analyze the complex issue of the policy driven, such as a cyber-security culture (Ritchey 2011). As such, the reasoning end of the ontology will be incorporated when the lower levels of the ontology have been added.

6. References

Al-shehri, Y., 2012. Information Security Awareness and Culture. *British Journal of Arts and Social Sciences*, 6(1), pp.61–69.

Brinson, A., Robinson, A. & Rogers, M., 2006. A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*, 3(2006), pp.37–43.

Davis, R., Shrobe, H. & Szolovits, P., 1993. What is in a Knowledge Representation? *AI Magazine*, p.21.

Dlamini, I.Z., Taute, B. & Radebe, J., 2011. Framework for an African Policy Towards Creating Cyber-Security Awareness. *Security*, pp.15–31.

Dlamini, Z. & Modise, M., 2012. Cyber-security awareness initiatives in South Africa: a synergy approach. In *7th International Conference on Information Warfare and Security*. USA: Academic Conferences International.

Fenz, S. & Ekelhart, A., 2009. Formalizing information security knowledge. *4th International Symposium on Information, Computer, and Communications Security - ASIACCS '09*, p.183.

Fenz, S., Pruckner, T. & Manutscheri, A., 2009. Ontological mapping of information security best-practice guidelines. Lecture Notes in Business Information Processing, 21, pp.49–60.

Furnell, S., Tsaganidi, V. & Phippen, A., 2008. Security beliefs and barriers for novice Internet users. *Computers & Security*, 27(7-8), pp.235–240.

Ghernouti-Hélie, S., 2010. A National Strategy for an Effective Cybersecurity Approach and Culture. In *2010 International Conference on Availability, Reliability and Security*. Ieee, pp. 370–373.

Grobler, M., van Vuuren, J. & Leenen, L., 2012. Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward. *ICT Critical Infrastructures and Society*, pp.215–225.

Gruber, T.R., 1993. A Translation Approach to Portable Ontology Specifications by a Translation Approach to Portable Ontology Specifications. *Knowledge Acquisition*, 5(April), pp.199–220.

High-Level Experts Group (HLEG), 2008. *ITU Global Cybersecurity Agenda High-Level Experts Group (HLEG) Global Strategic Report*, Geneva, Switzerland.

International Telecommunication Union, 2008. *Global Security Report*.

Klimburg, A., 2012. National cyber security framework manual 1st ed. Alexander Klimburg, ed., Tallinn: NATO CCD COE Publications.

Kortjan, N., 2013. *A Cyber Security Awareness and Education Framework for South Africa*. Nelson Mandela Metropolitan University.

Kortjan, N. & Von Solms, R. 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal, 52, 29-41.*, 2014(52), pp.29–41.

Moses-Òkè, R., 2012. Cyber capacity without cyber security: A case study of Nigeria's national policy for information technology (NPFIT). *The Journal of Philosophy, Science & Law*, 12, pp.1–14.

Van Niekerk, J.F. & Von Solms, R., 2010. Information-security culture: A management perspective. *Computers & Security*, 29(2010), pp.476–486.

Noy, N.F. & McGuinness, D.L., 2001. Ontology Development 101 : A Guide to Creating Your First Ontology, Available at: http://protege.stanford.edu/publications/ontology_development/ontology101.pdf.

Pfleeger, S.L. & Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber-security risk. *Computers & Security*, 31(2012), pp.597–611.

Ritchey, T. 2011. General Morphological Analysis (GMA). In Risk, Governance and Society (Vol. 17, pp. 7–19).

RSA, 2014. *The current state of cybercrime: An Inside Look at the Changing Threat Landscape*, Available at: www.emc.com/rsa.

SA Government gazette, 2011. Draft National Cybersecurity-Policy Framework for South Africa. , p.33. Available at: http://www.cyanre.co.za/national-cybersecurity-policy.pdf.

Schein, E., 1992. *Organizational culture and leadership. 2nd edn. Jossey- Bass; 1992* 2nd Edition, San Francisco: Jossey-Bass.

Schlienger, T. & Teufel, S., 2002. Information security culture – from analysis to change. In *In Security in the Information Society*. US: Springer, pp. 191–201.

Von Solms, R. & van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, (2013), pp.1–6.

Da Veiga, A., Martins, N. & Eloff, J.H.., 2007. Information security culture – validation of an assessment instrument. *Southern African Business Review*, 11(1), pp.147–166.

Virginia Tech, 2011. When users resist. *Pamplin: College of Business Magazine*. Available at: http://www.magazine.pamplin.vt.edu/fall11/passwordsecurity.html [Accessed Nov 11, 2014].

Wali, A., Chun, S.A. & Geller, J., 2013. A Boot-strapping Approach for Developing a Cyber-security Ontology, Using Textbook-Index Terms., *2013 International Conference on Availability, Reliability and Security*, pp.569–576.

Wamala, F., 2011. *ITU National Cybersecurity Strategy Guide*, Geneva, Switzerland.