Using an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa

JC Jansen van Vuuren[1], L Leenen[1], JJ Zaaiman[2]

[1] Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[2] University of Venda
jjvvuuren@csir.co.za
lleenen@csir.co.za

Abstract: Many developing countries are particularly vulnerable to cyber security threats due to an enormous growth in Internet connectivity rates over the past decade. The South African government approved a draft version of its National Cybersecurity Policy Framework in March 2012. Although implementation of this policy has been initiated in a few isolated instances, a holistic approach is lacking. Due to the cybersecurity environment not being clearly bounded and defined, it is very difficult to put forward a National Cybersecurity Policy Framework that is easy to understand and implement.

In this paper, the authors motivate that an ontology can assist in defining a model that describes the relationships between different stakeholders and cybersecurity components that are relevant in the policy implementation. An ontology is a technology that enables an encoded, shareable vocabulary and domain model and it has powerful automated reasoning abilities. This methodology can contribute to a more holistic approach for the implementation of the South African National Cybersecurity policy. The Extended Cyber Security Toolkit (XCyberST) (Jansen van Vuuren, Leenen, Phahlamohlaka, & Zaaiman 2013) as the basis for mapping cybersecurity entities to functions, was the initial attempt to model the national cybersecurity policy environment in South Africa. The authors proposed the use of an ontological model for the cybersecurity policy implementation in a previous paper (Grobler, van Vuuren, & Leenen 2012), and this model is now presented. The model is partially based on information in the XCyberST and implemented in Protégé, an ontology editor. Although this model has been developed for the South African cybersecurity environment, it can easily be adapted to be used in other countries.

Keywords: Cybersecurity, Policy Implementation, Ontology, South Africa, Cybersecurity Toolkit.

1. Introduction

Similar to many other developing nations, South Africa has focused more on increasing Internet connectivity than establishing cybersecurity in the past decade. This country currently experiences a high incidence of cyber attacks, in fact, in 2011 South Africa ranked third in the world in terms of the number of cyber attacks a country encountered (Amit 2011). Since the approval of its draft Cybersecurity Policy in 2012 (SA Goverment Gazette 2010), there has been no holistic approach from the South African government to implement the policy. The authors of this paper proposed an Extended Cyber Security Toolkit (XCYBERST) in 2013 that proposes a government structure and an implementation model to adopt for the implementation of the Cybersecurity Policy. The XCYBERST is discussed in Section 3.

An ontology is a technology that provides a way to exchange semantic information between people and systems. It provides a common vocabulary and depicts all the concepts and inter-concept relations in a formal logic representation. An ontological model for the Cybersecurity Policy implementation environment will capture the complexities of the numerous stakeholders, their responsibilities and functions, and their inter-relationships. Ontologies and their benefits are discussed in Section 4. Our cybersecurity policy ontology is also described in this section.

2. Background

South Africa published its first draft Cybersecurity policy in 2010 (SA Goverment Gazette 2010). This was followed by the National Cybersecurity Policy Framework (NCPF) in 2012 (Dube 2012). With the approval of this document, South Africa has acknowledged that it does not have a coordinated approach in dealing with Cybersecurity. Various structures have since been established but to have an efficient cyber security strategy there is a need for a partnership between business, government and civil society. South Africa's efforts to ensure a secured cyberspace could be severely compromised without this holistic approach. Although several efforts are made to implement this NCPF it is still not available to the public. However, some of the information is available from media statements. Mrs Stella Ndabeni-Abrahams, Minister of Communication in South Africa, commented that as government they have adopted the National Cyber Security Policy Framework to provide measures to build confidence and trust in the secure use of Information and Communications Technologies (ITCs) (Moyo & Kayle 2012). The first structure to be established is the Cybersecurity Hub that will pull together public and private sector threat information for the purposes of processing and disseminating such information to relevant stakeholders. This process has already started (De Kock 2013).

Given the current status of the NCPF in South Africa, as the overarching strategy that must guide cybersecurity, there is not enough emphasis on using a holistic approach for the implementation of such a policy. One of the methodologies with which the cybersecurity policy can be analysed is the description of Jablonsky (1997) for national power. Jablonsky defines national security in terms of natural and social determinants of national power (Jansen van Vuuren, Phahlamohlaka, & Brazzoli 2010). The Cybersecurity toolkit, CyberSAT, (Phahlamohlaka, Jansen van Vuuren, & Coetzee 2011) developed with the South African environment in mind, is based on the policy elements as described in the Draft Cybersecurity Policy of South Africa (SA Government Gazette, 2010). The CyberSAT has adapted to the Extended Cyber Security Toolkit (XCyberST) to include the NCPF (Jansen van Vuuren et al. 2013). This XCyberST framework (with minor adjustments) is used to develop an initial ontology that can be used as a guide for a holistic approach towards the implementation of the NCPF.

3. Analysis

The XCyberST for national security is presented in Table 1 *(Jansen van Vuuren et al 2013)*. In the first column are the elements of the policy, while the second column represents the philosophical position of each element. The third column is divided into the five social determinants of national power elements. Whilst the toolkit is based on the policy elements from the South African environment, the determinants of national power are generic, and thus the toolkit could be adopted for Cybersecurity implementations by other countries when national security considerations are pertinent.

Note that minor changes have been made to the XCyberST as published previously*:* some modifications to the Stakeholders and to some of the functions have been made. The capacity to deal with Cyber Warfare is not addressed. This should become an additional policy element and it will be fully explored in future work.

Table 1: *The Extended Cyber Security Toolkit for National Security (XCyberST)*

	Philosophical Position	**Social Determinants of National Power**					**Stake-holders**
Policy Elements		**Economic**	**Political**	**Military**	**Psychological**	**Informational**	
Structures in support of cybersecurity	*Cybersecurity breaches will happen regardless of the structures established*	Establish commercial and financial response structures e.g. sector CSIRTs	Establish a National security level institutional arrangement on cybersecurity	Establish structures to protect Critical Infrastructure	Build confidence in the response capacity of established institutions	Establish national CSIRTS Let the public to trust in the security of communication channels and systems	SSA DOC DOD SABRIC ISP
Reduction of cybersecurity threats and vulnerabilities	*Threats and vulnerabilities will always be there, reduction thereof is a key goal*	Develop various economic breaches monitoring tools and techniques	Send regular political signals that cyber security is a priority	Develop monitoring tools and techniques on an on-going basis	Effectively communicate the benefits of paying attention to threats and vulnerabilities	Effectively communicate that cyber security is a priority	DOC SSA SABRIC ISP DOD
Cooperation and coordination between government and private sector	*Partnerships and cooperation across all sectors and society are critical*	Build business confidence that continued ICT use is a competitive advantage rather than a liability.	Build public confidence that the political leadership will take care of their personal information	Create reasonable civil-military interactions within broader government framework	Spell out clear lines of accountability and expected behaviours that could contribute to trust and confidence building	Build confidence in the public that its political leadership will take care of their personal information	DOC DOD SSA
International cooperation on cybersecurity	*No country can do it alone*	International partnerships and shared global spaces are necessary tools	Leaders need to develop relationships that extend across borders	Define standards of conduct in cyberspace	Establish reasonable precautions in relation to balancing secrecy and information sharing are necessary	Promote information sharing	SSA DOC DOD
Research and capacity building	*Focus internally on research on threats and education of public*	Focus on public education and research initiatives for prevention of individual to become victim of cybercrime	Government wide support for cybersecurity awareness initiatives and skills development to win the Cybersecurity battle	Research and understanding of Cybersecurity threats and set up of protection systems against attacks	Research and understanding of Cybersecurity threats enhance better cyber behaviour of individual users	Focus on public education and research agenda	DST DOE DOC CSIR DOD
Promote culture of cybersecurity	*Focus internally on the creation of awareness on the risks in cyberspace*	Focus on public awareness	Articulate coordinated national information and communications infrastructure objectives	Protection of citizen & enhancement of ethical behaviour is an important part of the cybersecurity battle	It is the behaviour of individual users that is the single most important part of the cybersecurity battle	Focus on public awareness of cyber risks and solutions	DOE DOC ICASA
Legal framework and compliance with technical	*Effectual legal system and active participation in creation of*	Define standards of conduct in cyberspace.	Articulate coordinated national information and communicatio	Protection of citizens with effectual legal framework adherence	Legal adherence of citizens to cyber policy guidelines and	Articulate coordinated national information & communica-	SABS DOJ DOC SAPS

and operational cybersecurity standards	*international standards*		ns infrastructure objectives, standards and legal framework	and defining of standards of conduct in cyberspace	standards of conduct in cyberspace.	tions infrastructure objectives	

- ***Structures in support of cybersecurity:*** *Cybersecurity breaches will happen regardless of the structures established.* With this policy element and the accompanying philosophical position, one could develop toolsets appropriate for each social determinant of national power. For instance a military Computer Security Incident Response Team (CSIRT) could be established as a structure in support of cyber security in the military as a social determinant of national power.
- ***Reduction of cybersecurity threats and vulnerabilities:*** *Threats and vulnerabilities will always be there; reduction thereof is a key goal.* Monitoring tools and techniques across the five dimensions could be developed aimed at reducing the threats and vulnerabilities
- ***Cooperation and coordination between government and private sector:*** *Partnerships and cooperation across all sectors and society are critical.* Guided once more by the five social determinants, toolsets in support of public private partnership could be developed. Knowing whom to call when an incident occurs is very critical, irrespective of where the capability might be housed within the state.
- ***International cooperation on cybersecurity:*** *No country can do it alone.* Tools to support international cooperation across borders could be developed, enabling leaders to develop relationships of trust
- ***Research and capacity building:*** *Focus internally and on the basics. Insider threats are more than external threats.* Development of research, recruitment and retention strategies to build expertise.
- ***Promote culture of cybersecurity:*** *Focus internally on research on threats and education of public* Promotion of a national program so that the general population across all sectors secure their own parts of cyberspace
- ***Legal framework and compliance with technical and operational cybersecurity standards:*** *Actively Participate in the creation of international standards.* Defining the standard of conduct in cyberspace and legal adherence is critical for a safe society.

The major stakeholders that are presented in the table, are the stakeholders presented in the ontology: the State Security Agency (SSA), the Justice, Crime Prevention and Security Cluster (JCPS), the Department of Communications (DOC), the Department of Justice and Constitutional Development (DOJ), the Department of Science and Technology (DST), the Department of Education (DOE), the Communications Authority of SA (ICASA), the South African Police Services (SAPS), the Department of Defence (DOD), the South African Bureau of Standards (SABS), the Council for Scientific and Industrial Research (CSIR), the South African Banking Risk Information Centre (SABRIC), and Internet Service Providers (ISPs).

4. The Cybersecurity Implementation Ontology

The main benefit of the ontology is the availability of a formal, encoded description of the cyber security strategic environment: that is, all the entities, their attributes and their inter-relationships will be defined and represented. There will be a single shareable model of the environment, agreed-upon by subject experts. During the implementation of the South African cyber security policy, the ontology will be used to map relevant aspects of the strategy to actors and functions as described in the ontology.

Subsection 1.1 gives an overview of ontologies and Subsection 1.2 presents the Cybersecurity Policy Implementation Ontology (CPIO).

1.1 What is an Ontology?

An ontology is 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. Grüber (1993) defines an ontology as *"formal, explicit specification of a shared conceptualisation"*. A formal ontology is a machine-readable domain model defining entities and their inter-entity relationships. It also has an automated reasoning facility enables the derivation of new information from the facts contained in an ontology.

Noy and McGuinness defined an ontology as: "…. *a common vocabulary for researchers who need to share information in a domain …. includes machine-interpretable definitions of basic concepts in the domain and relations among them.*"(Noy & McGuinness 2001).

Ontologies provide the following benefits:

- Sharing a common understanding of the structure of information
- Facilitate reuse of domain knowledge
- Make domain assumptions clear
- Separate domain knowledge from operational knowledge
- Analyse domain knowledge

Noy and McGuinness describe an ontology as a formal explicit description of concepts of discourse classes, with the properties of each class describing various attributes of the concepts (slots) and their restrictions. Classes are the focal point of ontologies, and can be divided into subclasses which represent more detailed concepts. The information in an ontology is expressed in an ontology language (a logic-based language) that has a well-defined semantics and powerful reasoning tools. The web ontology language (OWL) 2.0 is the official Semantic Web ontology language. OWL was designed to provide a common way to process the content of web information instead of displaying it. It is intended to be interpreted by computer applications and not to be read by people (OWL 2 Web Ontology Language, 2012). In this research, OWL was used to interpret the ontological model developed for the cyber security strategic domain.

1.2 A Domain Ontology for the Cyber Security Environment

The XCyberST in Table 1 maps various activities, functions and responsibilities on the five practical aspects (i.e. Social Determinants of National Power) as proposed for international cyber security policy implementation to the stakeholders. The implementation of the policy will involve a significant number of entities and functions. Due to the increasing complexity, the authors proposed in a previous paper that an ontological model can support the process (Grobler et al. 2012). This proposed model has now been refined, extended and implemented in this paper.

Ontologies have been used previously to define policy frameworks and instantiate policies (Bradshaw et al. 2003); (Cuppens-Boulahia, Cuppens, Autrel, & Debar 2009); (Kagal, Finin, & Joshi 2003)). Kagal et al. argue that policy languages are often bound to specific domains and cannot be applied across domains. In cases where policies cover different domains and systems a more flexible language is required. The use of ontologies is growing rapidly in a variety of application areas, and is the underlying technology driving the Semantic Web initiative ((Berners-Lee, Hendler, & Lassila 2001)). A semantic language such as an ontology language allows flexibility and sharing of information. Ontologies should therefore be a valuable contribution to the final implementation of a cyber security policy in South Africa. An ontological model supports communication and sharing of information between role players during the implementation of a policy.

The proposed cyber security strategy environment ontology is implemented in Protégé, a free, open-source platform that provides a suite of tools to construct domain models and knowledge-based applications with ontologies (Protégé_ontology_editor 2013). The reasoning facility of Protégé is used to pose questions to the ontology and to extract information.

A part of the CPIO is depicted in Figure 1.

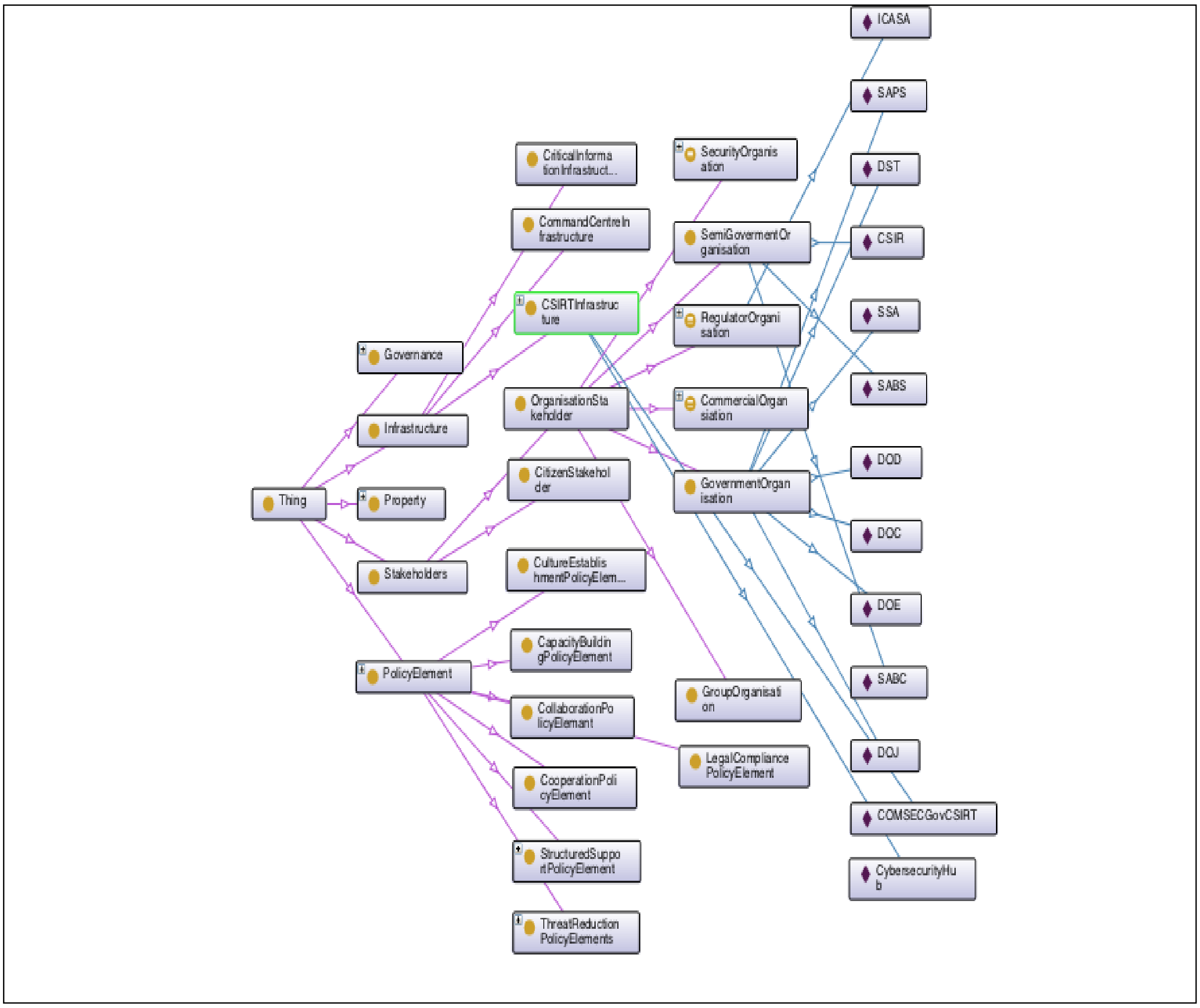


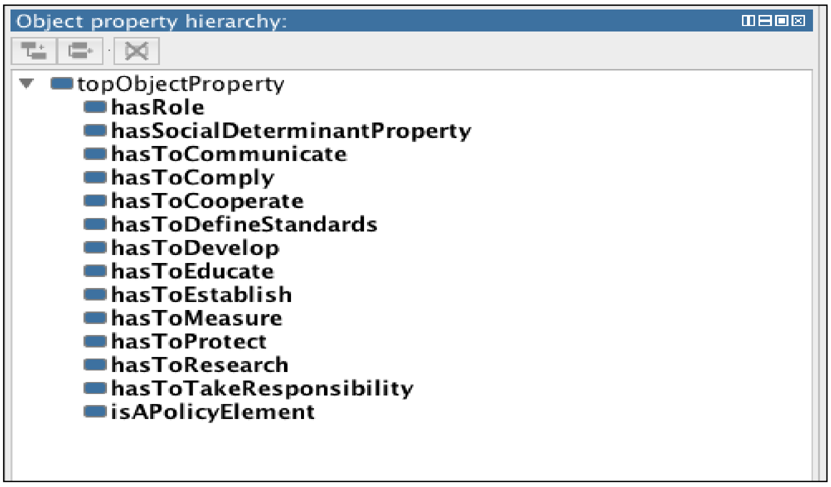
Figure 1: Part of the Cybersecurity Policy Implementation Ontology

This figure shows a part of the class structure but not all the relationships between classes. The main classes are *Stakeholders*, *PolicyElement*, *Governance*, *Property* and *Infrastructure*, and can be seen in the second column from the left side. Some of the subclasses of the main classes are shown in the third column from the left:

- The *Infrastructure* class has subclasses *CriticalInfrastructure, CommandCentreInfrastructure* and *CSIRTInfrastructure.*
- The *Stakeholders* class has subclasses *OrganisationStakeholder* and *CitizenStakeholder.*
- The *PolicyElement* class has subclasses *StructureSupportPolicyElement, CapacityBuildingPolicyElement, ThreatReductionPolicyElement, CollaborationPolicyElement, CooperationPolicyElement, LegalCompliancePolicyElement,* and *CulturePolicyElement.*

In the fourth column from the left we show the subsets of the *OrganisationStakeholder*, and in the last column all the individuals (i.e. the stakeholders as shown in the last column of Table 1) are shown. For each of the individual stakeholders we have added specific responsibilities and functions in the ontology via object properties (i.e. relationships). Some of these object properties are shown in Figure 2. An example is that the "*SAPS hasToProtect* some *LegalCompliancePolicyElement".* For each of the stakeholders a number of functions or responsibilities are represented in the ontology.

With the concepts (classes) and the relationships between the classes (object properties) the automated reasoner plug-in of Protégé can reason over the ontology. Some of the questions that can be posed and the answers that are produced are shown in Figure 3 to Figure 5.

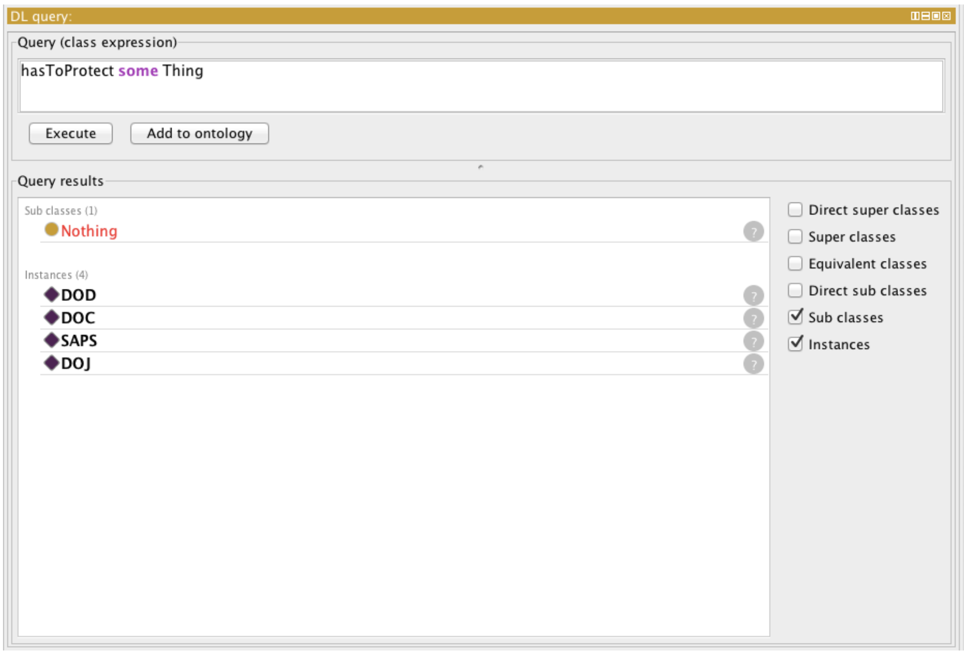


Object property hierarchy:

- topObjectProperty
  - hasRole
  - hasSocialDeterminantProperty
  - hasToCommunicate
  - hasToComply
  - hasToCooperate
  - hasToDefineStandards
  - hasToDevelop
  - hasToEducate
  - hasToEstablish
  - hasToMeasure
  - hasToProtect
  - hasToResearch
  - hasToTakeResponsibility
  - isAPolicyElement

Figure 2: Object Properties

In Figure 3, the question "*hasToProtect some Thing*" which appears in the top rectangular window, requests all the individuals that have the responsibility to protect something or someone. The answer can be seen in the larger window at the bottom: the DOD, DOC, SAPS and DOJ.



Query (class expression)

```
hasToProtect some Thing
```

Query results

Sub classes (1)
- Nothing

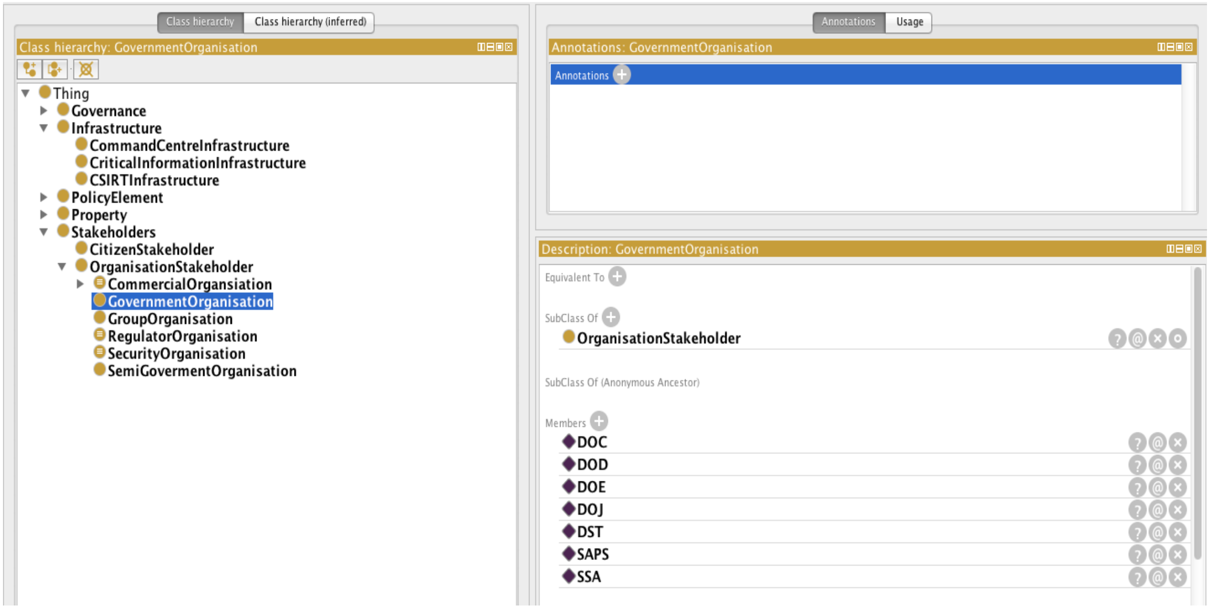
Instances (4)
- DOD
- DOC
- SAPS
- DOJ

☐ Direct super classes
☐ Super classes
☐ Equivalent classes
☐ Direct sub classes
☑ Sub classes
☑ Instances

Figure 3: A Query with Answer

In Figure 4, the class hierarchy can be seen in the window on the left side, with the *OrganisationStakeholder* class expanded. One of its subclasses, the *GovernmentStakeholder* class is highlighted. In the window on the bottom right side, the individuals that belong to the latter subclass are shown. These seven organisations were entered into the ontology as individuals that are members of this subclass.

In Figure 5, the *SecurityOrganisation* subclass of the *OrganisationStakeholder* class is highlighted in the window on the left side. In the window on the bottom right side, three individual organisations are indicated to be members of this subclass: the DOD, SAPS and SSA. Note that these three individuals are highlighted; this is because the reasoner has inferred that they are *also* members of the *SecurityOrganisation* subclass. This inference could be made due to the logical statement "*OrganisationStakeholder and (hasRole some SecurityRole)*" (also visible higher up in the same window) that all members of the *SecurityStakeholder* subclass must satisfy – every member of the latter subclass must be a member of the *OrganisationStakeholder* class and perform some security role. Each of these individuals has been entered with the latter property, i.e. "*hasRole some SecurityRole*".



Class hierarchy: GovernmentOrganisation

```
Thing
  Governance
  Infrastructure
    CommandCentreInfrastructure
    CriticalInformationInfrastructure
    CSIRTInfrastructure
  PolicyElement
  Property
  Stakeholders
    CitizenStakeholder
    OrganisationStakeholder
      CommercialOrgansiation
      GovernmentOrganisation
      GroupOrganisation
      RegulatorOrganisation
      SecurityOrganisation
      SemiGovermentOrganisation
```

Annotations: GovernmentOrganisation

Annotations

Description: GovernmentOrganisation

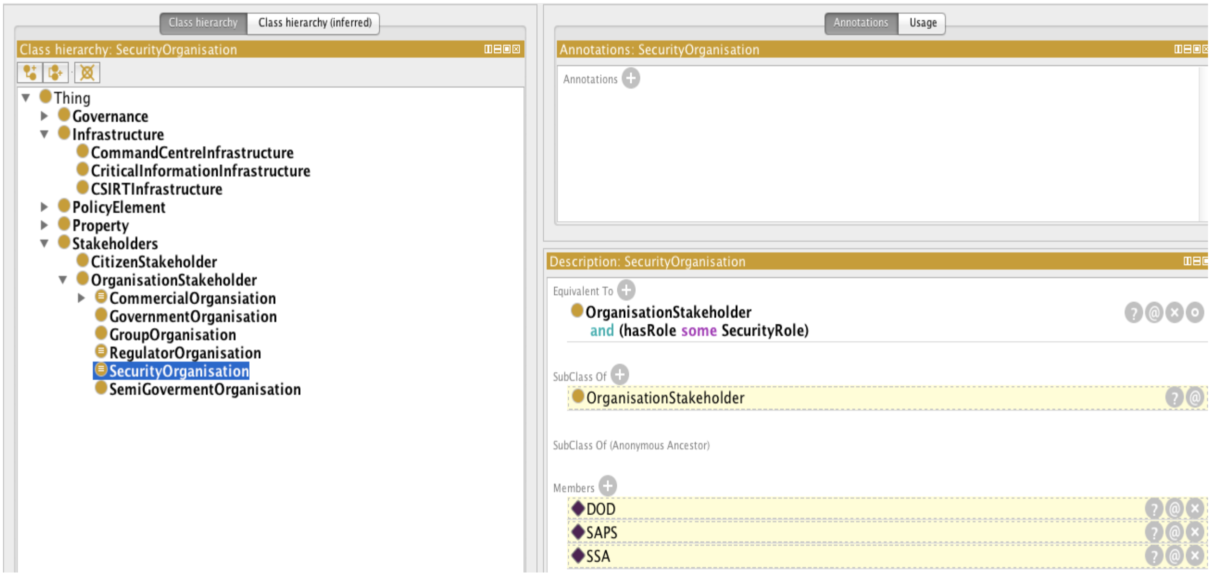
Equivalent To

SubClass Of
OrganisationStakeholder

SubClass Of (Anonymous Ancestor)

Members
DOC
DOD
DOE
DOJ
DST
SAPS
SSA

Figure 4: Individual Stakeholders



Class hierarchy: SecurityOrganisation

```
Thing
  Governance
  Infrastructure
    CommandCentreInfrastructure
    CriticalInformationInfrastructure
    CSIRTInfrastructure
  PolicyElement
  Property
  Stakeholders
    CitizenStakeholder
    OrganisationStakeholder
      CommercialOrgansiation
      GovernmentOrganisation
      GroupOrganisation
      RegulatorOrganisation
      SecurityOrganisation
      SemiGovermentOrganisation
```

Annotations: SecurityOrganisation

Annotations

Description: SecurityOrganisation

Equivalent To
OrganisationStakeholder
and (hasRole some SecurityRole)

SubClass Of
OrganisationStakeholder

SubClass Of (Anonymous Ancestor)

Members
DOD
SAPS
SSA

Figure 5: Inference made: Individuals that are also security organisations

It is clear from these examples that the ontology can be queried on the roles and relationships between entities and concepts, and that it also can derive facts that has not been entered. In a complex domain, the ontology can fulfil a role as a single source of information regarding all the entities, roles and relationships that exist.

5. Conclusion and Future Work

This paper presents an ontological model to support the implementation of the Cybersecurity Policy for South Africa. Although a draft version of this policy has been approved by the government in

2012, very few steps have been taken to implement it. The model has been implemented as an ontology in Protégé, an ontology editor.

In the future, the ontology will be extended and updated as the implementation of the policy is rolled out: more stakeholders and tasks will be identified. The authors will involve domain experts to evaluate the contents of the ontology.

6. References

Amit, I. I. (2011). Information Security Intelligence Report: A recap of 2010 and prediction for 2011. Retrieved 5 February, 2011, [online]
www.Security-Art.com

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The semantic web. *Scientific american, 284*(5), 28-37.

Bradshaw, J., Uszok, A., Jeffers, R., Suri, N., Hayes, P., Burstein, M., et al. (2003). *Representation and reasoning for DAML-based policy and domain services in KAoS and Nomads.* Paper presented at the Proceedings of the second international joint conference on Autonomous agents and multiagent systems.

Cuppens-Boulahia, N., Cuppens, F., Autrel, F., & Debar, H. (2009). An ontology-based approach to react to network attacks. *International Journal of Information and Computer Security, 3*(3), 280-305.

De Kock, N. (2013). Deputy Minister of Communications commends CSIR on progress with national cybersecurity. Retrieved October 10, 2013, [online]
http://www.csir.co.za/news/2013/10/national_cybersecurity.html

Dube, B. (2012). *Statement on the approval by Cabinet of the Cyber Security Policy Framework for South Africa*. Retrieved 5 April 2012. from http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794.

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

Grüber, T. 1993*. A translation approach to portable ontology specifications.* Knowledge Acquisition, 5. pages 191-220*.*

Jansen van Vuuren, J., Leenen, L., Phahlamohlaka, J., & Zaaiman, J. (2013). *Development of a South African cybersecurity policy implementation framework*.

Jansen van Vuuren, J., Phahlamohlaka, J., & Brazzoli, M. (2010). The Impact of the Increase in Broadband Access on National Security and the Average citizen. *Journal of Information Warfare, 5*, 171-181.

Kagal, L., Finin, T., & Joshi, A. (2003). *A policy language for a pervasive computing environment.* Paper presented at the Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on.

Moyo, A., & Kayle, A. (2012). DOC calls for collaboration, security innovation. Retrieved 9 October, 2012, [online]
http://www.itweb.co.za/index.php?option=com_content&view=article&id=54874

Noy, N. F., & McGuinness, D. L. (2001). Ontology development 101: A guide to creating your first ontology: Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report SMI-2001-0880.

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. (2011). *Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation*. Paper presented at the SACSAW.

Protégé_ontology_editor. (2013). Retrieved July, 24, 2013, [online]
http://protege.stanford.edu/

SA Goverment Gazette. (2010). South African National Cyber Security Policy.