An Ontological Model for a National Cyber-Attack Response in South Africa

Aphile Kondlo[1], Louise Leenen[1,2] and Joey Jansen van Vuuren[3]
[1]University of the Western Cape, South Africa
[2]Centre for AI Research, South Africa
[3]Tshwane University of Technology, South Africa
3579632@myuwc.ac.za
lleenen@uwc.ac.za
jansenvanvuurenjc@tut.ac.za

Abstract: South Africa is increasingly targeted by cyber criminals and is often ranked under the top five countries suffering the most cyber-attacks. In an initiative to counter these attacks, the South African government has initiated various measures such as a National Cybersecurity Policy Framework Policy (NCPF) and a Cybercrimes Act. However, the structures and policies that follow from these measures have not been fully implemented yet. Although the government published the NCPF in 2015 and enacted the Cybercrimes Act in May 2021, there is still a gap in terms of interoperability and shared understanding within the environment. In addition, numerous new structures have been established and others are still being planned. One example of a new structure is the Cybersecurity Hub, the national CSIRT, that is mandated to co-ordinate attack information and provide support for cyber incidents. In addition, the Hub must also implement a national Cybersecurity Awareness program. This paper presents a model for the Cybersecurity Hub in the event of a cyber incident in South Africa. The model is based on different attack scenarios and depicts the complex interoperability problem of the various roles, responsibilities, and interactions of role players when there is a cyber incident. One of the scenarios is an attack on critical infrastructure. The model is a prototype of a semantic knowledge base (an ontology) which will help with planning and decision making. Core queries that should be answered concern the critical role players during and after a cyber event; the communication activities that have to take place; and the response actions and the skills required to handle the event.

Keywords: cybersecurity governance, ontology, national critical infrastructure protection, national cybersecurity, cyber-attack

1. Introduction

The rapid development of information and communication technologies (ICT) has a major impact on the future, and digital transformation is one of the most significant societal changes. Many nations are driving initiatives to connect their citizens to the internet. The South African government, for example, introduced an initiative called SA Connect in 2013 as part of its National Broadband Policy (Alison, Onkokame, & Rademan, 2018). This initiative has two main goals; the first one was to deliver widespread broadband access to 90 percent of the country's population by 2020, and the second to deliver widespread broadband access to 100 percent of the country's population by 2030 (Alison, Onkokame, & Rademan, 2018). When comparing South Africa to the rest of Africa in terms of the percentage of the population that has access to the internet, South Africa is only ranked 13th in Africa with a percentage internet penetration of 59,8%, while countries such as Kenya and Libya have above 80% penetration (Statistica, n.d.). Although increased connectivity has many positive impacts ranging from economic growth to providing improved communication platforms, citizens and the private and government sectors also become increasingly vulnerable to cyber threats. Cybersecurity is a growing concern for governments across the world but especially in developing countries where governments are mostly not investing sufficiently in cybersecurity.

Many developing countries are struggling to provide national cybersecurity and are vulnerable to cyber-attacks on critical infrastructures. South Africa is one of the countries that suffer the most cyber-attacks and is thus very vulnerable; the Global Cyber Index placed SA sixth on its list of countries targeted most by cyber-attacks (Gavaza, 2021). Although South Africa has managed to make good progress in terms of cyber legislation and national cyber governance, the country still has a great deal of work to do in this regard. On 7 March 2012, the South African Cabinet approved the National Cybersecurity Policy Framework (NCPF) (State Security Agency, 2015) which had been developed over a number of years. The NCPF is a government policy document which recognises that the state is charged with implementing a government led, coherent and integrated cybersecurity approach. The NCPF was intended to provide a holistic approach to promote a cybersecurity implementation plan to be developed by the Justice, Crime Prevention and Security (JCPS) Cluster in consultation with relevant

stakeholders, identifying roles and responsibilities, timeframes, specific performance indicators, and monitoring and evaluation mechanisms. The JCPS cluster consists of the Departments of Police, Defence, Home Affairs, and Justice and Correctional Services, and is responsible for the co-ordination of interdepartmental crime prevention initiatives across the criminal justice system. The JCPS works in consultation with other Government clusters to oversee the implementation of the policy framework, with the aim to ensure centralised coordination of cybersecurity issues. (State Security Agency, 2015).

The implementation of the NCPF led to various structures being developed and to the enactment of Cybercrimes Act 19 of 2020, in 2021 (RSA Government, 2021). An early draft of the Act was initially introduced to the National Assembly on 9 December 2016 as the Cybercrimes and Cybersecurity Bill (RSA Governmemnt, 2016). This Bill was revised to become the Cybercrimes Bill in 2017 (Parliamentary Montoring Group (PMG), n.d.) and then became Cybercrimes Act after going through some changes over the following four years until it was finalised in 2020, and enacted on 1 June 2021. The objective of the Cybercrimes Act is to consolidate legislation relating to cybercrime in a single act by addressing offences that are relevant to cybercrimes and to criminalise offences related to data, messages, computers and networks. It also regulates the investigation and prosecution of cybercrimes. (RSA Government, 2021).

It is interesting to note that the NCPF and the initial draft of the Cybersecurity Act, the Cybercrimes and Cybersecurity Bill, prescribed the establishment of a number of new structures required for national cybersecurity. These structures have been omitted from the Cybercrimes Act but are expected to be contained in a new Cybersecurity Bill which is apparently still to be drafted. In this paper, we adhere to the description of these structures contained in the NCPF, because the NCPF is still a valid policy. One of these structures is the Cybersecurity Hub[1], South Africa's National Computer Security Incident Response Team (CSIRT). The Hub was established in 2015 and strives to make Cyberspace an environment where all residents of South Africa can safely communicate, socialise, and transact in confidence[1]. It works with stakeholders from government, the private sector, civil society and the public to identify and counter cybersecurity threats. A few examples of other structures that have been established or are under development include a Point of Contact centre[2] operated by the South African Police Service (SAPS), a Cyber Security Centre operated by the South African National Defence Force (SANDF), a Cybersecurity Response Committee (CRC) operated by the State Security Agency, and a National Cyber Security Advisory Council (NCAC). (Sutherland, 2017).

This paper describes research to support the Cybersecurity Hub during its response to cyber incidents; specifically the development of an ontological model that will map the complexity of the interactions required between national cyber structures to respond during a cyber-attack. This first phase of the research focuses on a scenario where a National Critical Infrastructure (NCI) is attacked. The protection of National Critical Infrastructure (NCI) is discussed in Section 2. Section 3 provides a short introduction to ontologies and considers research on the use of ontologies in support of cyber governance. A scenario depicting a cyber-attack on an NCI in South Africa is presented in Section 4, as well as a model depicting the main role players and their interactions. The last two sections of the paper contain a brief evaluation of the initial model and the conclusion.

2. The protection of national critical infrastructure

The protection of NCIs against cyber-attacks is a critical aspect of national cybersecurity. Most developed and developing countries consider sectors ranging from telecommunications, energy, transport, water supply, health, finance, and other infrastructures that 'allow a nation to function' as their critical infrastructure, even though national security and military systems form significant components of critical national infrastructure (Cyber Infrastructure & Security Agency, 2019). Cyber-attacks on these infrastructures can cripple a country's economy and cause national emergencies. For example, on 23 December 2015, Ukraine Kyivoblenergo, a regional electricity distribution company experienced a cyber-attack that resulted in a power outage which left approximately 225 000 customers without power (Shehod, 2016). The attackers reportedly re-used a decade-old Trojan, BlackEnergy, to gain access to the company's network. Another incident occurred in December 2014 with a cyber-attack on the Korea Hydro & Nuclear Power Company, which operates nuclear power plants in the Republic of Korea (ROK) (Lee & Lim, 2016). The cyber-attack emerged as a national security threat and triggered

[1] https://www.cybersecurityhub.gov.za/

[2] Note that the establishment of the Point Of Contact centre is prescribed in the Cybercrimes Act. The NCFP prescribed two structures to be operated by SAPS but these have been replaced by the Point Of Contact.

a response from ROK society, which up until then had been sensitive to security incidents (Lee & Lim, 2016). Even though the cyber-attack did not result in loss of human life or the destruction of facilities, it showed that there is a need to pay attention to such incidents because it highlighted the inadequacies of the existing cybersecurity systems for critical infrastructure.

The protection of critical infrastructure and national crisis management is likely to increase cybersecurity's strategic significance for national security. Ensuring the safety of critical infrastructure is actually a matter of national security with or without a cyber aspect (Tatar, Calik, Celik, & Karabacak, 2014). One challenge highlighted by Tatar et al. is the fact that a significant part of critical infrastructures (CI) in liberal market economies are run by the private sector although they are deemed to be an integral part of national security. Consequently, governmental assistance is required for these service providers because most countries regard the protection of CIs to be a governmental responsibility. The risk of cyber-attacks on critical infrastructure and data fraud or theft is a constant concern for business leaders globally (ENISA, 2021). According to the World Economic Forum's Global Risks Report 2020 (World Economic Forum, 2021), the risk of cyber-attacks on critical infrastructure and data fraud or theft ranked in the top ten of risks most likely to occur, while the recent COVID-19 Risk Outlook identified cyber-attacks as the third greatest concern due to the current and sustained shift to digital work patterns.

A cyber-attack on entities that are part of critical infrastructure can have a debilitating impact on national security, and the risk increases significantly for electricity grids, nuclear installations, and telemetry or command and control networks of space assets (Samuel & Sharma, 2016). The US Department of Homeland Security identifies 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the US that their incapacitation or destruction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof (Samuel & Sharma, 2016).

The financial sector has been a consistent target for hackers. The banking industry increasingly warn their customers of the risks of cyber fraud and has to prevent the possibility of criminals imitating their employees. An article released on the South African Banking Risk Information Centre (SABRIC) website, states that in the year 2017, 13 438 incidents occurred across banking apps, online banking and mobile banking, and cost the industry more than R250 000 000 in gross losses (SABRIC, 2017). Even though the financial sector may seem to be the most consistently targeted by hackers, power provision is a critical vulnerability for any nation, and the loss of power creates cascading damage in other critical sectors (Samuel & Sharma, 2016). In this paper, we describe an attack on a power utility as a use case.

According to Kyung-bok and Jong-in, malware attacks such as the Stuxnet and Dragonfly, which were capable of causing physical damage, were detected worldwide, and the cybersecurity of critical infrastructure resurfaced as a security issue among advanced countries. The U.S. issued Executive Order 13636 to improve and reinforce critical infrastructures cybersecurity, and Presidential Policy Directive 21 to address the role of government agencies in order to ensure the effective implementation of this order (Lee & Lim, 2016). The UK is establishing a "cybersecurity hub" for threat-information sharing with CI operators, and it has also formed a joint communique that regulates joint training and information sharing pertaining to CI cyber threats.

The consistent cyber-attacks on national critical infrastructure have become a major issue for various countries. It is clear that a cybersecurity strategy plan is a requirement for all countries that have a connection to the internet in their national critical infrastructures. This research builds on existing research on national cybersecurity in South Africa and addresses requirements to enable relevant new structures to become effective once they have been implemented.

3. The use of ontologies in cyber governance

An ontology is a semantic technology that provides a way to exchange semantic information between people and systems (Jansen van Vuuren, Leenen, & Zaaiman, 2014). A formal definition of an ontology is given by Gruber (1993): "…a formal, explicit specification of a shared conceptualisation". An ontology allows a formal, shared representation of the key concepts of a specific domain and it provides a way to attach meaning to the terms and relations used in describing the domain. The main advantages of an ontology is a semantic search ability, provision of a common shared vocabulary, the ability to share domain knowledge, and enablement of semantic integration and interoperability between various knowledge sources.

Although a number of ontologies have been developed for the cybersecurity domain, the use of ontologies to model the complexities of cyber governance in particular, has received limited attention in the research community. Greiman (2018) considered how ontological research methodologies contribute to the understanding of cyber governance at the global level. One of the numerous motivations she highlights for using an ontology to model the complexity of the cyber governance environment, is the ability of an ontology to formally define a vocabulary for the domain. Greiman found that although there have been a number of research endeavours on the development of cybersecurity ontologies (Obrst, Chase, & Markeloff, 2021), there are very few investigations on the use of ontological development to support the interoperability of cyber governance at the international level. Greiman explored an ontological approach to analyse cyber governance with the motivation that ontological models can provide insight into the entities, attributes and processes in this domain. She mentioned the following research publications in which ontologies were developed to support cyber governance:

1. Gcaza et al. (2015) developed an ontology to foster a national cybersecurity culture.
2. Jansen van Vuuren, et al. (2014) developed an ontological model for the implementation of the national cybersecurity policy framework for South Africa.

Talib et al. (2018) presented preliminary results of a project to develop an ontology that captures different national cybersecurity policies in Saudi Arabia. The aim of this ontology is to ensure an implementable national cybersecurity approach by mapping the different relevant policies with functions and responsibilities. In addition, the ontology will clarify the complexity of the necessary structures and provide a formal, shared description of the environment before implementation can succeed.

4. Critical infrastructure attack scenario and model

Veerasamay et al. highlight the use of scenario planning to deal with the numerous uncertainties that exist when strategic planning is done for cyber incident response (Veerasamy, Mashiane, & Pillay, 2019). Based on informal guidance received from the Cybersecurity Hub, results from Veerasamy et al.'s research and cybersecurity frameworks such as the popular NIST framework[3], the authors describe a high-level NCI cyber-attack scenario for South Africa. The next step was to develop an ontological model to map the numerous role players and their roles. Due to the fact that cyber measures and structures in South Africa are not yet mature, the coordination of national assistance will benefit from a model that depicts the relevant role players and their roles.

Our scenario depicts a cyber-attack on a South African NCI with national impact and describes the response from the Cybersecurity Hub's (the national CSIRT) perspective. Multiple entities must collaborate and communicate – the focus is on high-level role players, and not on the internal structures of any such entity. This first phase of modelling remain at a high-level of abstraction and will be expanded in the future. The scenario captures focal points with respect to the stakeholders, the response to an incident, the skills required and the communication amongst involved parties.

The government departments directly engaged in cybersecurity in South Africa (RSA Government, n.d.) are State Security, Justice and Constitutional Development, Defence, and Telecommunications and Postal Services - they all belong to the same cluster, the Justice, Crime Prevention and Security (JCPS) Cluster. Other departments will be engaged as required. The cyber structures that are involved in a response to an attack on NCI in South Africa are listed below (Phahlamohlaka & Hefer, 2019):

3. The JCPS's *Cybersecurity Response Committee* (CRC) has the responsibility to formulate strategy and decision-making in the national cyber domain and is chaired by the Director-General of State Security, and hosted by the SSA. The CRC is supported by the SSA's Cyber Security Centre.
4. The *Cybersecurity Hub*, or national CSIRT, will coordinate general cyber security activities in the private sector;
   inform Private Sector CIRTS, ISPs and other stakeholders, initiate cyber security awareness campaigns, support the development of Private Sector CSIRTs, and conduct cyber security audits, assessments and readiness exercises on request.
5. The *Cyber Security Centre* (CSC) is overseen by the State Security Agency (SSA) and is the operational entity of the CRC. The CSC is responsible for coordinating any NCI cyber incident. It has been mandated

[3] https://www.nist.gov/cyberframework

to analyse incidents, trends, vulnerabilities, share information, develop response protocols, to interact with stakeholders, to conduct exercises, and to perform security audits, assessments and readiness. In the event of a cyber incident the CSC will notify stakeholders, analyse information and systems involved in the incident, extract and pool data from various sources, monitor the incident, determine the assistance that is required, request status, reports, etc.

6. The *Cyber Command Centre* of the South African National Defence Force (SANDF) has the responsibility to act when national security is threatened. It has been mandated to facilitate the operational coordination of cyber security incident response activities regarding national defence and to support other activities relating to cyber incidents that involve national defence.
7. The *Point of Contact* centre of the South African Police Service (SAPS). Note that the NCFP refers to a Cybercrime Centre and a 24/7 centre, but as discussed before, the Cybercrimes Act refers to only a Point of Contact centre. This centre's main responsibility is to investigate any cybercrime incident. In addition, it has also been mandated to share information and technologies with law informant agencies, facilitate the analysis of cyber security incidents, and develop and maintain cross-border law enforcement cooperation in respect of cybercrime.

Figure 1 provides an illustration of the structure as described in the NCFP (Jansen van Vuuren J. C., 2016). Note that this figure still shows the two centres which are now replaced by the Point of Contact centre.

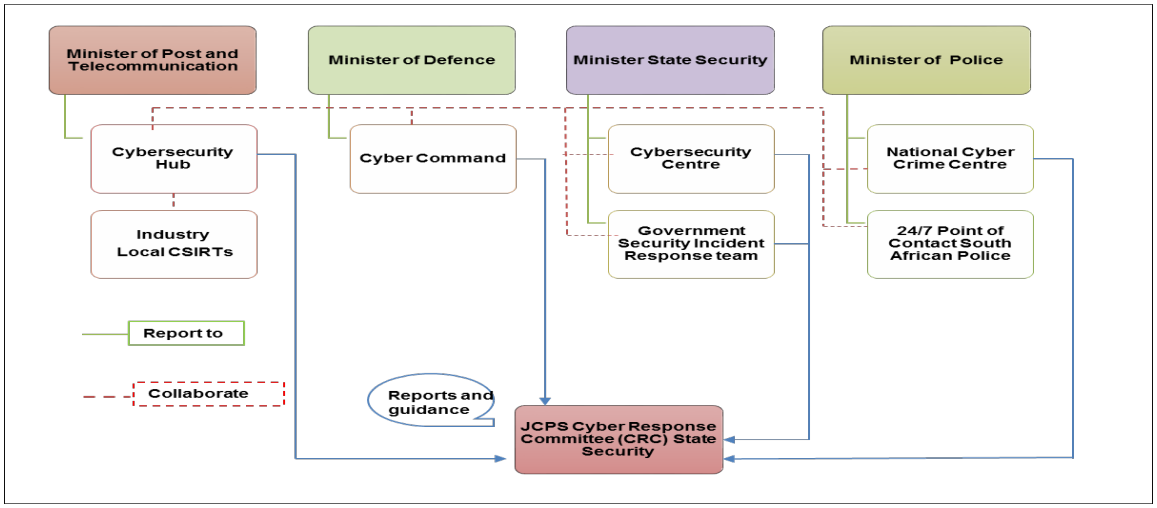


Figure 1: South African cyber structures according to the NCFP (Jansen van Vuuren J. C., 2016)

Our NCI attack scenario considers an attack on the main electricity provider in South Africa, Eskom. Eskom is a public utility and is required to monitor and analyse its systems for anomalies or cyber incidents. Eskom has to determine the severity of any incident, and process and document findings in an attempt to minimise effects and report any incident to the necessary structures. If Eskom finds an incident to be of a serious nature, it will report the attack to the Cyber Security Centre and request assistance from the CSC to co-ordinate the incident. The CSC will notify the Cybersecurity Hub, the Cyber Command Centre, and the National Contact Point centre, and make the first call to request assistance to respond and recover from the attack. Data gathering from various sources will commence under the CRC, and the CSC will announce the incident where necessary, analyse system data and continue to monitor the incident. They will also document the incident. A knowledge base will be created at the SSA (it hosts the CRC and the Cyber Security Centre) Eskom will begin the recovery process by requesting forensic investigation from the Point of Contact Centre for information updates, and then report to CRC. For this high-level scenario, an ontology was developed to map all the role players and relationships (depicting responsibilities and functions) that take place in an event of a cyber-attack incident. Note that the ontology does not aim to present the dynamic flow of events during and after an attack; it is a knowledge base that can be queried to gather information with respect to the various entities that are involved and the complex nature of their roles and responsibilities. The ontology captures the responsibilities of each structure which will assist Cybersecurity Hub in decision making. *Some* of the main concepts (classes) in the model are listed below:

Critical_Infrastructure

1. *WaterProvision*

2. *EmergencyServices*
3. *Energy*
    1. *PowerPlant*
4. *Healthcare*

Incidents

1. *DoS*
2. *Malware*
3. *Ransomware*

RolePlayers

1. *Body*
    1. *ECSP* *(Electronic Communication Service Providers)*
    2. *FIRST* *(The Forum of Incident Response and Security Teams)*
    3. *JCPS* *(Justice, Crime Prevention and Security Cluster)*
        1. *CyberResponseCommittee*
    4. *NCAC* *(National Cyber Security Advisory Council)*
2. *CSIRT*
    1. *CybersecurityHub*
    2. *ElectricitySectorCSIRT* *(Does not yet exist. Inserted for modelling purposes)*
    3. *ECS_CSIRT* *(Government CSIRT)*
    4. *SABRIC* *(Banking Sector CSIRT)*
3. *Private*
    1. *Company*
    2. *SABRIC*
4. *State*
    1. *ArmsofGovernment*
        1. *SANDF* *(South African National Defence Force)*
            1. *CyberCommandCentre*
        2. *SAPS* *(South African Police Service)*
            1. *PointofContact*
    2. *GovernmentAgency*
        1. *CyberCommandCentre*
        2. *CyberResponseCommittee*
        3. *PointofContactCentre*
        4. *SARB* *(South African Reserve Bank)*
        5. *SITA* *(State Information Technology Agency)*
        6. *SSA* *(State Security Agency)*
        7. *CyberSecurityCentre*
    3. *GovernmentDepartment*
        1. *DoJ&CD* *(Justice and Constitutional Development)*
        2. *Finance*
        3. *HomeAffairs*
        4. *Police*
        5. *PS&A* *(Public Service and Administration)*
            1. *SITA*
        6. *Security* *(Ministry of State Security)*
            1. *CyberResponseCommittee*
    4. *PublicEnterprise*
        1. *Telkom* *(Communication company)*
        2. *Eskom* *(Power utility)*

Sector

1. *Communications*

2. *Electricity*
3. *FinancialServices*
4. *GovernmentFacilities*
5. *Military*
6. *Water*
7. *Retail*
8. *Transportation*

The three main activities in a cyber-attack are to Monitor, Analyse and Respond. The Protect activity will not be considered as part of our model because the focus is on the mid-attack or post-attack phase. Each main activity contains sub-activities. A few examples of activities are listed below:

8. Monitoring requires the application of monitoring tools to raise alerts for detected anomalies.
9. Analysis activities entail analyses of the system data.
10. Share data from various sources.
11. Response activities consist of repairing systems and equipment, and minimising the effects of an attack for example the use the use of generators, water tanks or other means to deal with a critical infrastructure outage.
12. Processing and documentation of findings. This includes record keeping of detected threats, issues, and complications, and the preservation of log and system data for future reference or investigation of an incident.

Some of the relationships (object properties) between the main concepts (classes) are:

13. belongsToSector
14. documentFindings
15. hasCNI
16. hostsCNI
17. performsAttack
18. isInRegion
19. reportsTo

For example, the relationship *hasCNI* maps a member of the *Sector* class to a member of the *CriticalInfrastructure* Class.

Figure 2 shows a part of the ontological model for the CNI attack scenario.

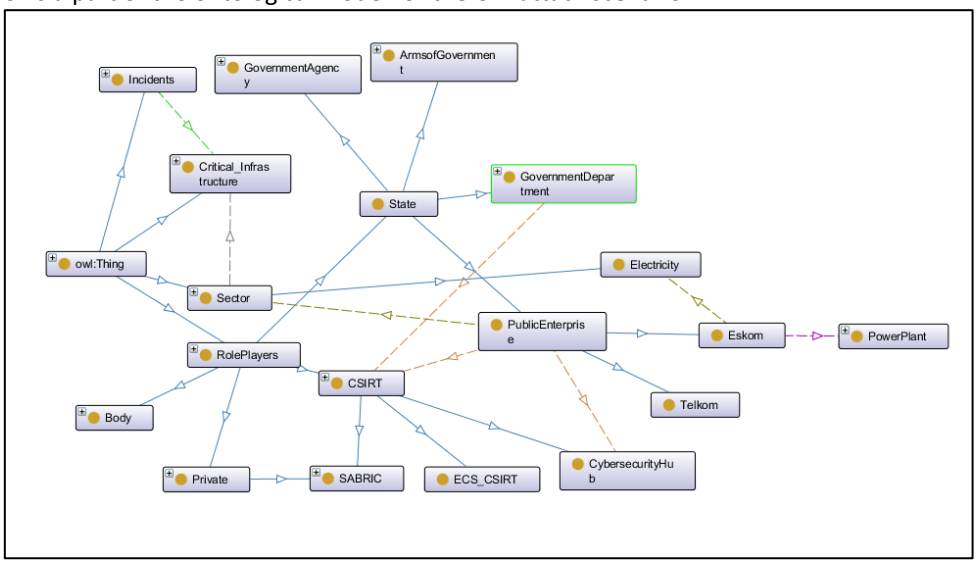
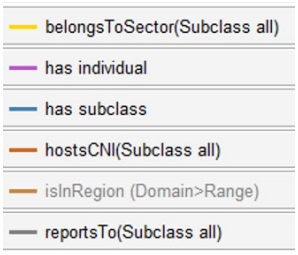


Figure 2: Part of the ontological model for the NCI scenario

The edges in the Figure 2 represents the following relationships:



The solid lines represent subclass relationships, for example, the subclasses of the RolePlayer class are Body, CSIRT, Private and State. The dotted lines represent relationships. For example, the line from Eskom to Electricity indicates that Eskom hosts a CNI which is a powerplant, and the dotted line from Eskom to Electricity shows that Eskom belongs to the Electricity Sector. The dotted line from PublicEnterprise to CybersecurityHub shows that all public enterprises report (incidents) to the Cybersecurity Hub (this thus applies to Eskom because Eskom is a Public Enterprise). Note that the dotted line from PublicEnterprise to CSIRT shows that all public enterprises report incidents to CSIRTs, of which the Hub is just one in particular.

5. Evaluation

The ontological model reflects the first phase of the research project. It is still at a fairly high-level and needs to be expanded with more detail to provide a rich model. More scenarios will be developed in the future. A proper evaluation of the model will be done at a more advanced stage. We show the result of one query to the ontology in Figure 3.

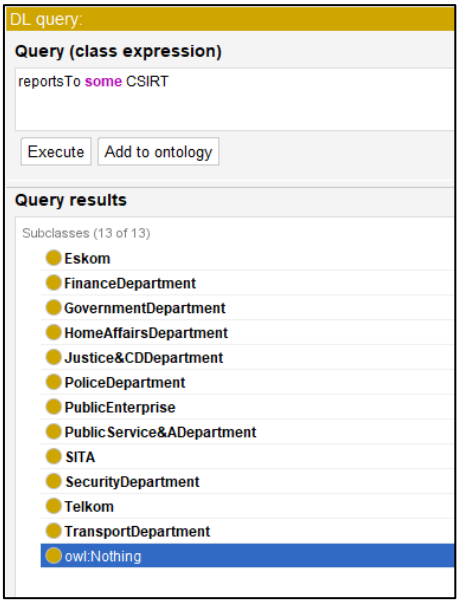


Figure 3: The query "Which entities have to report cyber incidents to a CSIRT?" posed to the ontology

Although this is a simple query, is it used to illustrate that the user can request an explanation for any query result. Figure 4 show the explanation provided for the result “SITA” (SITA is the State Information Technology Agency.) The explanation is that SITA belongs to the Department of Public Service and Administration and this department has to report to at least one CSIRT.

Figure 4: Explanation of the query result "SITA"

6. Conclusion and future work

South Africa has introduced several measures to improve national cybersecurity during the past decade. The core measure has been the approval of a National Cyber Policy Framework (NCFP) in 2012. While the implementation of the Cybercrimes Act and structures such as the Cybersecurity Hub (the national CSIRT) have been developed based on the NCPF, many aspects of the NCPF have yet to be addressed. This paper reflects on research to support the Cybersecurity Hub; a scenario of a cyber-attack on critical infrastructure and the development of an ontological model to map the role players and activities captured in the scenario are described. The next step of this research project is to extend the model and to add more scenarios. The aim of the ontological model is to provide a common and shareable view of the actions required to respond and recover from cyber-attacks. Cyber governance in South Africa is still being developed and this research will support a core national cyber structure.

References

Alison, G., Onkokame, M., & Rademan, B. (2018). *The State of ICT in South Africa.* Cape Town: Research ICT Africa. Retrieved from https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

Cyber Infrastructure & Security Agency. (2019). *A Guide to Critical Infrastructure Security and Resilience*. Retrieved from https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience

ENISA. (2021). *ENISA Threat Landscape 2021: April 2020 to mid-July 2021*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Gavaza, M. (2021, Sep 7). *Cyber threats are costing SA firms millions, Business Day 7 Sep 2021*. Retrieved from Business Day: https://www.businesslive.co.za/bd/companies/telecoms-and-technology/2021-09-07-cyber-threats-are-costing-sa-firms-millions/

Gcaza, N., von Solms, R., & Jansen van Vuuren, J. (2015). An Ontology for a National Cyber-security Culture Environment. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA.*

Greiman, V. (2018). Reflecting on Cyber Governance for a new World Order: An Ontological Approach. Rome, italy: European Conference on Research Methodology for Business and Management.

Gruber, T. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition, 5*, 199-220.

Jansen van Vuuren, J. C. (2016). *Methodology and Model to Establish Cybersecurity for National Security in Africa using South Africa as a Case Study (Doctor of Philosophy (PhD) in Business Management).* Thohoyandou, South Africa: University of Venda.

Jansen van Vuuren, J., Leenen, L., & Zaaiman, J. (2014). Using an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa. (pp. 107-115). 9th International Conference on Cyber Warfare and Security (ICCWS).

Lee, K., & Lim, L. (2016). The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the Korea Hydro & Nuclear Power Co., Ltd. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 10*(2).

Obrst, L., Chase, P., & Markeloff, R. (2021). *Developing an Ontology of the Cyber Security Domain.* McLean, Virginia: The MITRE Corporation,.

Parliamentary Montoring Group (PMG). (n.d.). *Bills*. Retrieved from https://pmg.org.za/bill/684/

Phahlamohlaka, J., & Hefer, J. (2019). The Impact of Cybercrimes and Cybersecurity Bill on South African National Cybersecurity: An Institutional Theory Analytic Perspective. *THREAT2019 Cybersecurity Summit.* Sandton, South Africa,: THREAT2019 Cybersecurity Summit.

RSA Governmemnt. (2016). *Cybercrimes and Cybersecurity Bill*. Retrieved from https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6-2017-21-feb-2017-0000

RSA Government. (n.d.). *Structure & Functions of the South African Government*. Retrieved from https://www.gov.za/node/537988

RSA Government. (2021). *The Cybercrimes Act 19 of 2020*. Retrieved from https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

SABRIC. (2017). *Media and News*. Retrieved from SABRIC: https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/#:~:text=In%202017%2C%2013%20438%20incidents,the%20same%20period%20in%202017.

Samuel, C., & Sharma, M. (2016). *Securing Cyberspace: International and Asian Perspectives.* Pentagon Press.

Shehod, A. (2016). *Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US*. Retrieved from Working Paper CISL# 2016-22: https://web.mit.edu/smadnick/www/wp/2016-22.pdf

State Security Agency. (2015). *The National Cybersecurity Policy Framework (NCPF).* Government Gazette (39475). Retrieved from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

Statistica. (n.d.). *Share of internet users in Africa as of December 2020, by country*. Retrieved from https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/

Sutherland, E. (2017). Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication, 20*, 83-112.

Talib, A., Alomary, F., Alwadi, H., & Albusayli, R. (2018). Ontology-Based Cyber Security Policy Implementation in Saudi Arabia. *Journal of Information Security, 9*, 315-333. Retrieved from https://doi.org/10.4236/jis.2018.94021

Tatar, U., Calik, O., Celik, M., & Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. *In International Conference on Cyber Warfare and Security* (p. 211). 9th International Conference on Cyber Warfare and Security (ICCWS).

Veerasamy, N., Mashiane, T., & Pillay, K. (2019). Towards cyber incident response strategic planning. *THREAT 2019 Cybersecurity Summit.* Sandton, South Africa.

World Economic Forum. (2021). *The Global Risks Report 6th Edition*. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf