Development of a South African Cybersecurity Policy Implementation Framework

CONFERENCE PAPER · MARCH 2013

DOI: 10.13140/2.1.3659.8727

4 AUTHORS:

J.C. Jansen van Vuuren
Council for Scientific and Industrial Resear…
18 PUBLICATIONS **30** CITATIONS
SEE PROFILE

Louise Leenen
Council for Scientific and Industrial Resear…
24 PUBLICATIONS **37** CITATIONS
SEE PROFILE

Jackie Phahlamohlaka
Council for Scientific and Industrial Resear…
22 PUBLICATIONS **37** CITATIONS
SEE PROFILE

Jannie Zaaiman
University of Venda
6 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Development of a South African Cybersecurity Policy Implementation Framework

JC Jansen van Vuuren[1], L Leenen[1], J Phahlamohlaka [1], JJ Zaaiman[2]
[1] Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[2] University of Venda, South Africa, Limpopo, South Africa
jjvvuuren@csir.co.za
jphahlamohlaka@csir.co.za
lleenen@csir.co.za
jannie.zaaiman@univen.ac.za

Keywords: Cybersecurity, National Security, Cybersecurity Toolkit, Policy Framework, Policy Implementation

Abstract: National governments have the responsibility to provide, regulate and maintain national security, which includes cybersecurity for their citizens. Although South Africa has recently published its first draft cybersecurity policy, the implementation of the policy is still in its very early stages. In this paper, the authors propose and describe a possible cybersecurity implementation framework for South Africa. This implementation framework is based on previous analysis of structures in other countries, a cybersecurity awareness toolkit, guidelines for cybersecurity strategies in the literature, and an implementation framework proposed for Jordan.

1 Introduction

The development, implementation and review of national cybersecurity policies have become tasks of utmost importance for all governments. The urgent need to address national cybersecurity protection is driven by the growing cybersecurity challenges and threats as well as dependence on technology around the globe. Any cybersecurity policy should include strategies and standards to enable and sustain cybersecurity.

The United States of America (USA) approaches this responsibility by employing a broad view; it encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery. Their approach is supported by strong measures: the USA has created a Cyber Command (CYBERCOM) under the Strategic Command led by the head of the National Security Agency (NSA) which reports directly to the President (US Cyber Command Public Affairs, 2011).

In developing nations the focus has been on increasing connectivity whilst largely neglecting the associated security risks. These countries will have to develop and maintain policies, strategies and structures to secure the networks that support their national security and economies. Despite a low Internet penetration rate, South Africa ranks third in the world after the USA and United Kingdom (UK) in terms of the number of cyber-attacks encountered (Amit, 2011). The draft version of the South African Cybersecurity Policy Framework was approved by government in March 2012 (South African Government Information, 2012). Whilst various structures have been established to deal with cybersecurity in South Africa, they are inadequate and implementation of the draft policy is still in the very early stages. Jansen van Vuuren et al. (2012) investigated different government organisational structures created for the control of national cybersecurity in selected countries of the world. The main contribution of this work was a proposed structure for South Africa taking into account the challenges of legislation and control of cybersecurity in developing countries.

In this paper, a cybersecurity implementation framework for South Africa is described. This framework is based on previous work by Jansen van Vuuren et al. (2012), an implementation framework proposed by Otoom & Atoum (2012), guidelines for the implementation of national cybersecurity strategies by Ghernouti-Helie (2010), and a cybersecurity awareness toolkit (Phahlamohlaka et al., 2011).

Section 2 contains an overview of results on which the proposed cybersecurity policy implementation framework is based, and in Section 3 the authors introduce the proposed framework. The paper is concluded in Section 4.

2 Background

An efficient cybersecurity policy relies on a holistic approach; there is a need for a partnership between business, government and civil society (Ghernouli-Helle, 2010; Phahlamohlaka et al., 2011). Phahlamohlaka et al. argue that a cyber security awareness programme should incorporate social dimensions and not just rely on fully technical solutions. This team of researchers proposed a Cyber Security Awareness Toolkit

(CyberSAT) with national security in mind, and included economic, political, military, psychological and informational dimensions. Details of the CyberSAT are given in Section 3. Jansen van Vuuren et al. (2012) proposed a cybersecurity governance structure and an implementation model based on CyberSAT and organisational structures in other countries. Otoom & Atoum (2012) proposed a cybersecurity implementation framework for Jordan. This framework is applied in order to develop a similar framework for South Africa.

Ghernouti-Helie (2010) argues that an effective approach and culture for national cybersecurity strategy includes political will and national leadership to ensure that the plan receives governmental support; a justice system and police service with a legal framework that supports the police to combat cyber-crime on national and international level; a cybersecurity capacity that include organisational structures, human capacity as well as the use of technical and procedural cybersecurity solutions; and a cybersecurity culture and awareness training for citizens.

The National Cybersecurity Policy Implementation Framework (NCPIF) of Otoom & Atoum (2012) uses a strategic planning process consisting of the Strategic formulation, Strategic Implementation and Strategic Evaluation (Figure 1). The elements are:

- A detailed analysis of the policy strategy in manageable, understandable parts. This analysis must be done by different people than those who write the policy. Different stakeholders are to be identified and a reconciled analysis to be done of the necessary implementation needs.
- A management structure responsible for the implementation of the strategy. The responsibilities include the breaking down of long terms objectives into annual objectives and development of organisational structures to fulfil the strategy. Resource allocation should be done and change management plans developed.
- Strategic moves designed to achieve the different strategic goals. It should consist of a set of coherent implementation programmes identifying exactly what has to be done and direct actions to achieve their objectives.
- A set of applicable strategic controls should be deployed. Strategic controls will allow decision makers mechanisms to ensure that innovation, efficiency, and quality are achieved. These controls should be adaptable to the culture and they should evolve.

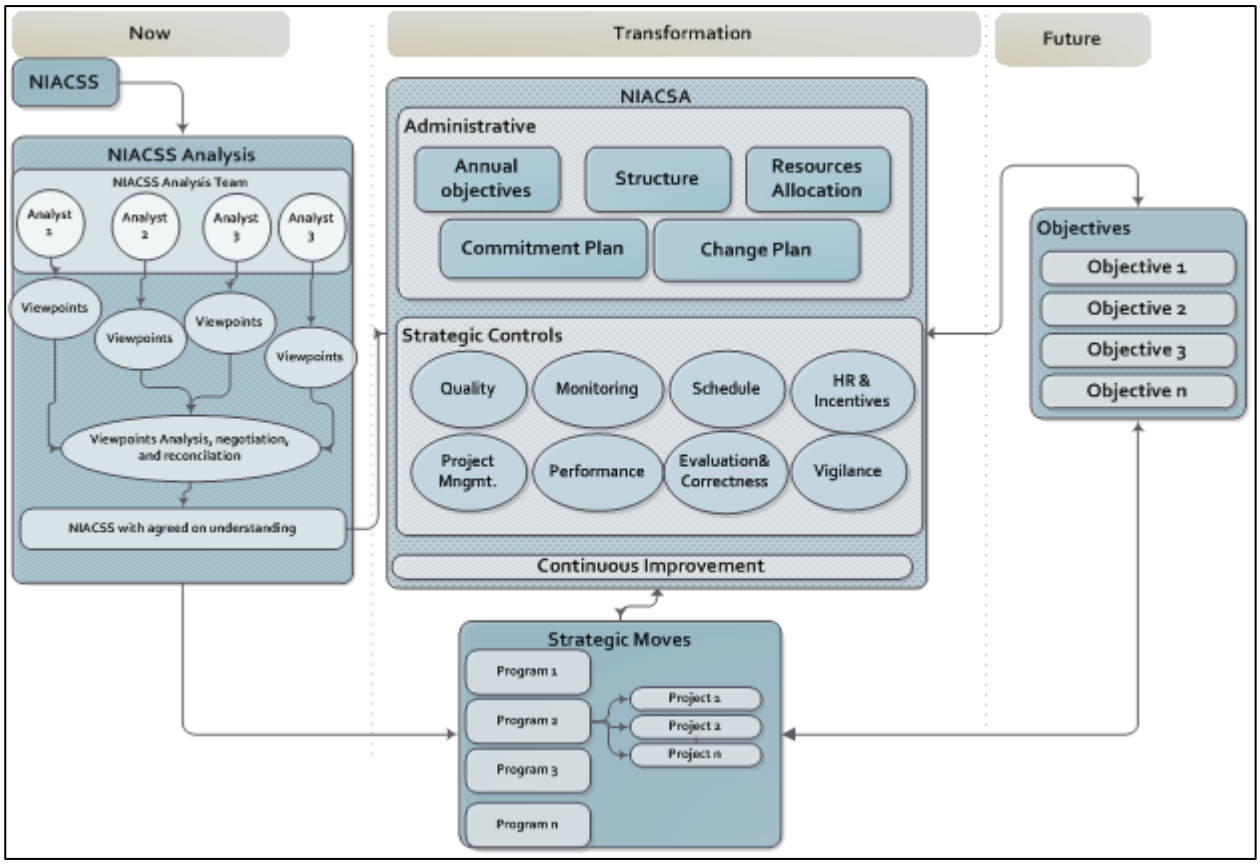

Figure 1: Proposed Implementation Framework (Otoom & Atoum, 2012)

3 Proposed Implementation Framework

The major goal of the NCPIF of Otoom & Atoum (2012) is to facilitate the implementation of a national cybersecurity policy framework (NCPF). The NCPIF proposes a methodology to analyse the NCPF and break it down into four well-defined components: an analysis, a management structure, strategic moves and strategic controls. Each of these components is applied to the South African Cybersecurity environment in the subsections that follow below. The analysis results will be used to guide the design of governance structures for cybersecurity in South Africa and to determine the strategic moves that are necessary to achieve the national objectives.

3.1 Analysis

The analysis of the national cybersecurity policy framework of South Africa was done using the description of Jablonsky (1997) for national security. Jablonsky defines national security in terms of natural and social determinants of national power. The Cybersecurity toolkit, CyberSAT, (Phahlamohlaka et al., 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 is adapted to the Extended Cyber Security Toolkit (XCYBERST) to include stakeholders. In addition, we adjusted the toolkit by the splitting the *Capacity building, culture of Cybersecurity* into two separate policy elements**;** *Research and capacity building* and *Culture promotion*, and made some minor changes inside the table. In the authors' opinion, research and capacity building address other aspects than the creation of a cybersecurity culture.

The XCyberST for national security is presented in Table 1. 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. While 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. The major stakeholders are presented in the last column: 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), South African Banking Risk Information Centre (SABRIC), and Internet Service Providers (ISP). The table consists of:

- ***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.

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 Military CSIRT	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 ongoing 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
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
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
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 communica-tions infrastructure objectives	Protection of citizen & enhance-ment of ethical behaviour is an important part of the cyber-security 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 and operational cybersecurity standards	*Effectual legal system and active participation in creation of international standards*	Define standards of conduct in cyberspace.	Articulate coordinated national information and communications infrastructure objectives, standards and legal framework	Protection of citizens with effectual legal framework adherence and defining of standards of conduct in cyberspace	Legal adherence of citizens to cyber policy guidelines and standards of conduct in cyberspace.	Articulate coordinated national information & communica-tions infrastructure objectives	SABS DOJ DOC SAPS

It should be noted that the toolkit is a possible operational guideline that could be used and is not meant to be exhaustive. Its entries could be varied, expanded on and applied at different government levels and institutional arrangements.

Further analysis of the stakeholders, their relationships and responsibilities is currently being done by the authors. Workshops are planned with some of the major stakeholders mentioned in Table 1. During the workshops general morphological analysis (GMA) will be used to extract information and views from these stakeholders regarding the main variables and relationships that need to be addressed in the implementation of the policy. GMA is a method for identifying and investigating the total set of possible relationships or "configurations" contained in a given problem complex. This is accomplished by going through a number of iterative phases which represent cycles of analysis and synthesis (Ritchie, 1997).

3.2 Management Structures for Implementation

3.2.1 Objectives

The key elements or objectives that must be covered in a cybersecurity policy differ between countries. The USA policy review team suggest that any complete national cyber policy must at least consider relevant government structures, a supporting architecture, norms of behaviour, and capacity building (Phahlamohlaka et al., 2011).

Governmental structures for policy development and the coordination of cyber operations should address the responsibilities and specifically the likely overlap of responsibilities of various stakeholders in the cyber security domain. A supporting architecture refers to the communications systems and infrastructures that are required for cyber security operations and includes aspects such as performance, cost, security characteristics, strategic planning, research and development, and risk management. Norms of behaviour include legislation, regulations, and international treaties required to circumscribe and define standards of behaviour in cyber-space. Capacity building refers to the provision of resources, activities, and capabilities required to become a more cyber-competent nation. It typically includes resource requirements, research and development, public education and awareness, and international partnerships, and all other activities that allow the government to interface with its citizenry and workforce to build the digital information and communication infrastructure of the future.

The Canadian policy emphasises strategies, responsibilities, the importance of individuals, leadership and a global approach (Phahlamohlaka et al., 2011). Effective national strategies should encourage cooperation and information sharing across different agencies. The roles and responsibilities of different agencies should be clarified such that there exist accountability and appropriate behaviour which lead to trust. Although the government and businesses have a strong role to play in advancing cyber awareness and literacy, the role of the individual should not be underestimated. Organisational leadership and international partnerships are considered to be vital aspects of the Canadian cybersecurity policy.

It is clear that nations and governments are responding to the cybersecurity challenges by setting up institutional coordination, control and response mechanisms. Linked to the institutional arrangements are also research, development and innovation plans. The elements of South Africa's draft cybersecurity policy compares favourably with those of the broader international community. The key strategic objectives of the NCPF of South Africa (as identified in the analysis in Table 1) are

- Facilitate the establishment of relevant structures in support of cybersecurity;
- Ensure the reduction of cybersecurity threats and vulnerabilities;
- Foster cooperation and coordination between government and private sector;
- Promote and strengthen international cooperation on cybersecurity;
- Build capacity and promoting a culture of cybersecurity; and
- Promote compliance with appropriate technical and operational cybersecurity standards.

Policy implementation in South Africa will be particularly difficult due to the number of stakeholders, the recent significant increase in the broadband roll-out and fact that the population is ill prepared for this situation.

3.2.2 Organisational Structures

Considerations setting up structures

Structures should exit at the national level to sustain an effective cybersecurity solution for all. These structures include adequate organisational structures which should take local cultures, particular economic contexts, country size, ICT infrastructure development, and users into consideration. National as well as international needs must also be considered.

A snapshot of the international approaches

From the Estonian experience, the lesson is that the only way we will learn to move forward on cybersecurity related issues, is by going through a painful growing process of suffering from, and dealing with, online attacks. Estonia's approach was to establish the Cooperative Cyber Defence Centre of Excellence (CCD COE), a NATO-approved think-tank whose mission is essentially to formulate new strategies for understanding, and preventing, online attacks (Czosseck et al., 2011; Tiirmma-Klaar 2010).

In South Korea, a cyber-attack resulted in the Ministry of Defence in South Korea launching a Cyber Warfare Command Centre (mimicking the US defensive steps), designed to fight against possible hacking attacks. Along a cyber-police force, the centre is charged with protecting government organisations and economical subjects from hacker attacks. Despite the establishment of this Cyber Warfare Command Centre, there have been repeat attacks in March 2011. (Jansen van Vuuren et al., 2010; Deloitte & Touche, 2010)

The lesson from Iran is that the Stuxnet type attacks are not over yet, while the key message from Georgia is that attacks could be disguised as civilian while they are military, with some hostile government's knowledge. In China there is a focus on Industrial espionage with the goal of stealing IP and designs, command signal data and information of financial and commercial nature. (Phahlamohlaka et al., 2011).

The UK approach was the establishment of the Cybersecurity Operations Centre, with the motivation that future battles will be fought not just on the ground, but in cyberspace (Espiner, 2010).

The USA created a Cyber Command (CYBERCOM) under the Strategic Command led by the head of the National Security Agency (NSA). One of the reasons stated for its creation was that the current capabilities to operate in cyberspace have outpaced the development of policy, law and precedent to guide and control these operations. The CYBERCOM was thus created in October 2009 around this mission. (Deloitte & Touche, 2010)

The Australian government initially followed a hands-off approach to cybersecurity and regarded it largely as a private sector responsibility. However, due to security challenges, the government changed it approach in 2009 and created a number of bodies with new capabilities and responsibilities. Their approach is still problematic because of the large number of separate agencies that are involved (Warren & Leitch, 2012).

The Dutch government follows a joint approach with the establishment of a National Cyber Security Centre which includes state institutions, the business community and knowledge and research institutions. The existing GOVCERT also forms part of this centre (Enisa, 2011). As of 1 January 2012, GOVCERT.NL evolved into the National Cyber Security Centre (Ministerie van Veiligheid en Justitie, 2012).

It is clear that nations and governments are responding to the cybersecurity challenges by setting up institutional coordination, control and response mechanisms. Linked to the institutional arrangements are also research, development and innovation plans. These national structures responsible for cybersecurity must also lead the capability building processes that will ensure collaboration on international level to achieve the goals identified by global cyber security policies. As seen from the literature, it is important that cybersecurity be controlled on a very high level, as in the case in the USA, Estonia and Korea and other countries.

Proposed Structures for South Africa

The South African Cybersecurity Policy Framework (SACFP) was approved by government in March 2012. The policy framework identifies specific areas of responsibility by a number of government departments, and the State Security Agency is the custodian for the development and implementation of cybersecurity measures (South African Government Information, 2012).

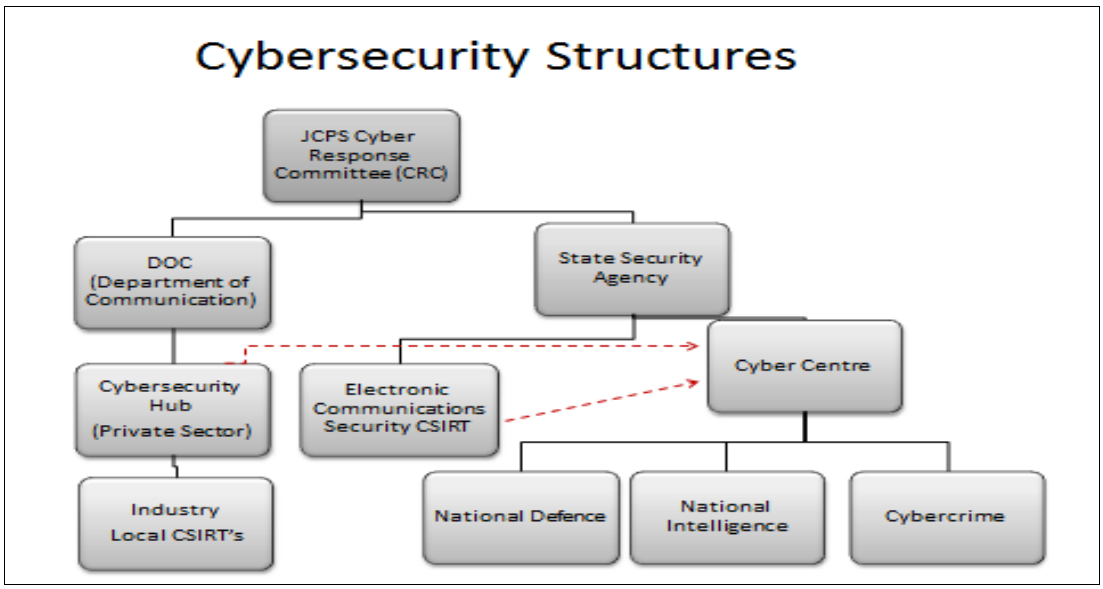

Figure 2: South African Cybersecurity Structure

The South African structure (Figure 2) as described in the SACFP provides for a national body (Cybersecurity Response Committee) reporting to the Department of State Security. The Cybersecurity Hub will be responsible for the private sector and civil society. The Electronic Communications Security (ECS-CSIRT) will be the Government CSIRT. There is also a separation between the civilian and the governmental networks which include state and military security networks (Dlomo, 2012).

A notable difference between this structure and those of the USA and Estonia, is that both government and military networks will be controlled by the State Security Agency in South Africa. The State Security Agency is the department of the South African government with overall responsibility for civilian intelligence operations. It was created in 2009 to incorporate the formerly separate National Intelligence Agency, South African Secret Service, South African National Academy of Intelligence, National Communications Centre and COMSEC (South Africa). Political responsibility for the agency lies with the Minister of State Security. Government and civilian systems in the USA and Estonia are not controlled by Intelligence Agencies (Klimburg & Tirmaa-Klaar, 2011). It should be noted that the JCPS Cyber Response Committee of South Africa reports to the Minister of State Security. During the establishment of the Cyber Command in the USA, the private sector questioned the fact that the military would play such an important role in the process. The concerns raised in the USA were whether the NSA will overshadow the civilian cyber defence efforts and on what assistance for civilian cyber defence there will be. Some concerns in the US were laid to rest with the assurance that the Department of Homeland Security (DHS) will be responsible for federal civilian networks including the dot-gov, and that CYBERCOM will only assist the DHS in the case of cyber hostilities as a response to an executive order (Burghardt, 2012). Similar concerns on the privacy of data may still be raised in South Africa due to State Security controlling the Cyber Centre, and therefore also indirectly, the civilian networks. There will be close collaboration between the Cyber Centre, the Cybersecurity Hub and the ECS-CSIRT. The Cyber Centre will be responsible for operational coordination of cybersecurity incidence response activities regarding national intelligence, national defence and cybercrime (Dlomo, 2012).

3.2.3 Resources

Ghermouti-Helle (2010) argues that the building of capacity should be based upon the understanding of the role of cybersecurity actors including their motivation, their correlation, their tools, mode of action, and the generic relevant security functions of any security actions. These considerations will be the underlying principles to be applied for organisational structures to be effective and to determine the kind of tools, knowledge, and procedures necessary to contribute to solving cybersecurity problems. Efficient partnerships between the public and private sectors, linked to cybersecurity organisational structures which are dedicated to support operational proactive and reactive activities should exist. The objectives of the Cybersecurity Hub make provision to achieve these objectives. These organisational structures should also be linked to cybersecurity management at a national level. This will be achieved by the Cybersecurity Response Committee.

3.3 Strategic Moves

The five elements identified as part of a successful development of a national cyber security strategy (Ghernouti-Hélie, 2010) can be used to identify the strategic moves.

3.3.1 Political will

National leadership is imperative as both an individual and an organisational role to ensure effective cybersecurity policies. Although the South African national cyber security policy framework has been approved by the cabinet, partial implementation has only started in May 2012 (Dlomo, 2012). The policy aims to ensure that government organisations and the private sector cooperate to secure South African networks (Guy, 2011), and it does address some levels of compatibility at an international level.

3.3.2 Adapted organisational structures

A proposal for a South African Cybersecurity structure has been presented in Figure 2. Organisational structures should exist to sustain effective cyber security solutions deployment for individuals, organisations and governmental agencies. A national CSIRT can be considered the most prominent organisational structure in joining communication networks and information systems with economic and social development structures. Previous research has identified nine steps to ensure the successful adaptation of a CSIRT as organisational structure. Of these steps, clarifying the mandate and policy related issues are the first and most crucial step (Grobler & Bryk, 2010).

3.3.3 Identifying accurate proactive and reactive measures

Both individuals and groups are largely dependent on data. This dependence relates not only to the physical data, but also to the relation of this data to specific infrastructures. Ghernouti-Hélie (2010) proposed that cybersecurity actors can be classified into specific roles: the protector, the protected, or the criminal. With the strong digital component of everyday actions, the multiplicity and automation of cybersecurity is becoming more prominent to maximise outputs and minimise human error. Accordingly, it is important that these roles can take on proactive or reactive measures.

3.3.4 Reducing criminal opportunities

Due to the international scope of the Internet and wide reach of technological usage, cybersecurity intersects largely with the application and implementation of international legislation. Regardless, the foundation for an adequate security strategy is twofold: raise the level of risks taken by the criminal, and raise the level of difficulties faced by the criminal. In all instances, legislative and regulatory measures should assist to raise the level of risk perceived by a criminal and decrease the favourable context to perpetrate an illegal action (Ghernouti-Hélie, 2010).

3.3.5 Education and awareness

Organisational structures should encourage, lead or coordinate continuing education for professionals in the legal, economic and political fields. In addition, the realisation of a global cybersecurity awareness culture will contribute to help achieving part of the goals of a national cybersecurity strategy (Ghernouti-Hélie, 2010). In South Africa, there is a number of cyber security awareness programmes aimed at educating different user groups in different geographical parts of South Africa (Grobler et al., 2011).

3.4 Strategic Controls

Otoom & Atoum (2012) stress that applicable controls are essential to the success of an implementation framework: they will enable decision makers to make necessary adjustments and improvements during the implementation process. Atoum (2012) elaborates on the strategic controls that are required: holistic performance control, quality controls, risk control, human resource incentives, evaluation and correctness, vigilance, and global schedule monitoring. This is one aspect of our implementation framework that requires thought and research and will be addressed in future work.

4 Conclusions

This paper describes a cybersecurity policy implementation framework for South Africa which is based on previous work of the authors as well as guidelines and other frameworks in the literature. An Extended

Cybersecurity Toolkit (XCyberST) and an organisational structure are presented with the intention that it could be used as a stepping stone for the implementation of South Africa's proposed cybersecurity policy. Because South Africa does not yet have a consolidated national security policy and strategy, a cybersecurity awareness raising campaign designed in accordance with the proposed toolkit could go a long way in preparing the country to respond to the cybersecurity challenges it is currently facing.

5 References

Amit, I. I. (2011). Information Security Intelligence Report: A Recap of 2010 and Prediction for 2011. Retrieved 5 February 2011 from www.Security-Art.com

Atoum, I.A.F. (2012). A Holistic Cyber security Strategy Implementation Framework. Master Thesis, Published by the University of Philadelphia, Philadelphia, USA.

Burghardt, T. (2012). The Launching of USA Cyber Command (CYBERCOM), Offensive Operations in Cyberspace. Retrieved 24 February 2012 from http://www.globalresearch.ca/index.php?context=va&aid=14186

Czosseck, C., Ottis, R., & Talihärm, A-M. (2011). Estonia after the 2007 Cyber Attacks : Legal, Strategic, and Organisational Changes in Cyber security. International Journal of Cyber Warfare and Terrorism, Volume 1, Number 1, pp. 24-34.

Deloitte & Touche. (2010). Constitution of the Republic of South Africa. (1996). Chapter 11 Principle 198. National Cybersecurity Strategies. Paper presented at the GOVCERT.NL symposium.

Dlomo, D.T. (2012). Cyber Sceurity Policy Discussions and ICT Security Approach in the Republic. Presentation at the Stakeholders Worskhop on 2 November 2012 at the CSIR International Convention Centre, Pretoria, South Africa. Organised by the Department of Communications.

ENISA, (2011). European Network and Information Security Agency (ENISA): Dutch Cyber Security Strategy. Retrieved on 2 December 2012 from http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented

Espiner, T. (2010). UK's Cyberdefence Centre Gets Later Start Date. Retrieved 21 February 2011 from http://www.zdnet.co.uk/news/security-threats/2010/03/10/uks-cyberdefence-centre-gets-later-start-date-40082405/

Ghernouti-Helie, S. (2010). A National Strategy for an Effective Cybersecurity Approach and Culture. The 2010 International Conference on Availability, Reliability and Security.

Grobler, M. & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT. Presented at the ISSA conference 2010. Sandton, South Africa.

Grobler, M., Flowerday, S., von Solms, R. & Venter, H. (2011). Cyber Awareness Initiatives in South Africa: A National Perspective. Proceedings of the First IFIP TC9 / TC11 Southern African Cyber Security Awareness Workshop (SACSAW). Gaborone, Botswana.

Guy. (2011). Cyber security policy will go before cabinet for approval this year. Accessed 5 March 2011, available online from http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13783:cyber-security-policy-will-go-before-cabinet-for-approval-thisyear&catid=48:Information%20&%20Communication%20Technologies&Itemid=109

Jablonsky, D. (1997). National Power. Parameters, Volume 27, pp. 34-54.Otoom, A., & Atoum, I.A.F. (2012). An Implementation Framework (IF) For the. National Information Assurance and Cyber. Security Strategy (NIACSS) of Jordan [Electronic Version]. IAJIT. Retrieved 15 November 2012 from www.ccis2k.org/iajit/PDF/vol.10,no.4/4842-10.pdf.

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.

Jansen van Vuuren, J. Phahlamohlaka, J., Leenen,L. (2012). Governance of Cybersecurity in South Africa. Proceedings of the 11th European Conference on Information Warfare and Security. Laval, France.

Klimburg, A. & Tirmaa-Klaar, H. (2011). Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU. Reference number EP/EXPO/B/SEDE/FWC/2009-01/Lot6/09. Published by the Directorate-General for External Policies, European Parliament.

Ministerie van Veiligheid en Justitie. (2012). Dutch National Cyber Security Centre. Retrieved 15 November 2012 from http://www.govcert.nl/english/service-provision/knowledge-and-publications/national-cyber-security-centre/ncsc.html

Otoom, A., & Atoum, I. (2012). An Implementation Framework (IF) For the. National Information Assurance and Cyber. Security Strategy (NIACSS) of Jordan [Electronic Version]. IAJIT. Retrieved 15 November from www.ccis2k.org/iajit/PDF/vol.10,no.4/4842-10.pdf.

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. Proceedings of the First IFIP TC9 / TC11 Southern African Cyber Security Awareness Workshop (SACSAW). Gaborone, Botswana.

Ritchie, T. (1997). Scenario Development and Risk Management using Morphological Field Analysis. Proceedings of the 5th European Conference on Information Systems. Cork publishing Company, Vol 3, pp. 1053-1059.

SA government gazette, 2010. South African National Cybersecurity Policy. Retrieved on 02 March 2011 from http://www.pmg.org.za/files/docs/100219cybersecurity.pdf

South Africa Government Information. (2012). Statement on the Approval by Cabinet of the Cybersecurity Policy Framework for South Africa. Retrieved on 21 October 2012 from http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794

Tiirmaa-Klaar, H. (2010). International Cooperation in Cyber Security: Actors, Levels and Challenges. Proceedings of Cyber Security 2010, Brussels.

US Cyber Command Public Affairs. (2011). US Cyber Command. Retrieved on 4 January 2013 from http://www.stratcom.mil/factsheets/Cyber_Command/

Warren, M. J., & Leitch, S. (2011). Protection of Australia in the Cyber Age. International Journal of Cyber Warfare and Terrorism, Vol. 1, No. 1, pp. 35-40.