Governance of CyberSecurity in South Africa

JC Jansen van Vuuren[1] J Phahlamohlaka [1] L Leenen[1]
[1] Defence Peace Safety and Security: CSIR, Pretoria, South Africa
jjvvuuren@csir.co.za
jphahlamohlaka@csir.co.za
lleenen@csir.co.za

Keywords: Cybersecurity, National Security, Governance, Policy Implementation. Cybersecurity Awareness Toolkit

Abstract: It is each government's responsibility to provide oversight on national security, which includes human security for its citizens. Recent declarations from the UK and USA governments about setting up new cybersecurity organisations and the appointment of cyber czars reflect a global recognition that the Internet is part of the national critical infrastructure that needs to be safeguarded and protected. South Africa still needs a national cybersecurity governance structure in order to effectively control and protect its cyber infrastructure. Structures need to be in place to set the *security controls* and policies and also to govern their implementation. It is important to have a holistic approach to cybersecurity, with partnerships between business, government and civil society put in place to achieve this goal. The aim of this paper is to propose an approach that South Africa could follow in implementing its proposed cybersecurity policy.

This paper investigates different government organisational structures created for the control of national cybersecurity in selected countries of the world. The main contribution is a proposed structure that could be suitable for South Africa, taking into account the challenges of legislation and control of cybersecurity in Africa, and in particular, South Africa.

1 Introduction

Around the world cybersecurity challenges give rise to serious national security alarms. There is an international drive by various governments to either develop and implement, or review existing cybersecurity policies. From the United States of America's (USA) point of view, the policies include strategies and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The USA has created a Cyber Command (CYBERCOM) under the Strategic Command led by the head of the National Security Agency (NSA), who reports directly to the President. The main reason stated was that the current capabilities to operate in cyberspace have outpaced the development of policy, law and precedent to guide and control these operations.

Developing nations such as South Africa focus more on the increase of connectivity and neglect the risks that accompany the connectivity. The over reliance on cyberspace compelled the USA to start all its cybersecurity initiatives. Developing nations will have no option, but to join in the race for cybersecurity policy development and implementation. They need to satisfy themselves, as well as instill the confidence across their nations, that the networks that support their national security and economic wellbeing are safe and resilient. Statistics also has shown that despite a low Internet penetration rate, South Africa ranks third in the world after the USA and United Kingdom (UK) on the number of attacks in a country (Amit, 2011).

In its cybersecurity policy (SA Goverment Gazette, 2010), South Africa has acknowledged that it does not have a coordinated approach in dealing with cyber security. Whilst various structures have been established to deal with cybersecurity issues, they are inadequate to deal with the issues *holistically.* There are some interventions to deal with cybercrime, 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.

As part of the cybersecurity strategy and implementation, we propose a cybersecurity governance structure and an implementation model based on the Cyber Security Awareness Toolkit (CyberSAT) (Phahlamohlaka et al, 2011) that is underpinned by key National Security imperatives as well as by

international approaches. Our proposal draws on several analyses derived from international trends and comparing them with key elements of South Africa's cybersecurity policy.

Section 2 contains an overview of the evolution of cybersecurity structures and policies in a number of countries. In Section 3 we draw on these international approaches to craft a proposal for cybersecurity structures and the implementation of a cybersecurity policy for South Africa. The paper is concluded in Section 4.

2 International Approaches

2.1 Estonian Approach

Estonia is seen as the world's first victim of cyber war, although web traffic was already jammed during the Kosovo war 10 years ago. When Estonia came under cyber attack in 2007, the country realised the necessity of a cyber defence policy. Multiple botnets were used to conduct Distributed Denial of Service (DDoS) attacks against critical national infrastructure, media, telecommunications and the main banks. Websites were also defaced and a significant portion of the economy and government ground to a halt. Although it was suspected that the culprits were Russian nationals, the Russian government did not want to assist in the search for these cyber attackers (Boyd, 2010). These attacks resulted in NATO creating the NATO Cyber Defence Research Centre in Tallinn, a county in Estonia, in 2008, where research and operations take place to counter future activity of this sort. In addition, Estonia adapted its governmental structures due to the realization of the importance of cybersecurity. A National Cyber Security Council was formed as part of its National Security (Tiimaa-Klaar 2010).

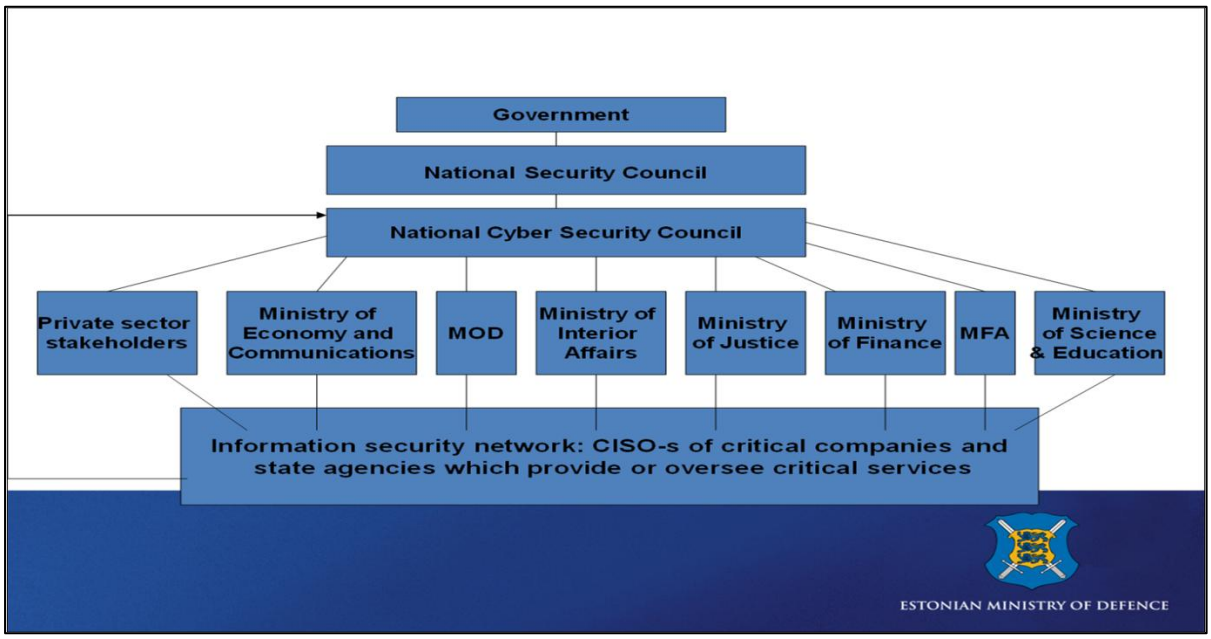

Figure 1: Estonian Cyber Security Structure (Tiimaa-Klaar)

In 2009, the NATO Computer Incident Response Capability was founded in Mons, Belgium, with intrusion detection and prevention capabilities for NATO networks.

2.2 USA Approach

The USA took note of cyber war scenarios and threats they could face from countries with advanced cyber warfare capabilities and thus established the Office of the Assistant Secretary for *Cyber Security and Communications (CS&C)* as part of *Homeland Security* in 2006. This organization is discussed later in this section. In reaction to the cyber attacks worldwide and, in particular, an attack on South Korea (United States. Executive Office of the Presiden,t 2009), the USA embarked on a program to emphasise these cyber issues. President Obama announced that he will make cybersecurity the top priority for the 21st century. He reiterated this vision when he said that cyber-infrastructure is a strategic asset and stressed the need for the appointment of a national cyber adviser to report directly to the president during a summit on national security at Purdue University.

He further stated that the USA needs to coordinate efforts across the federal government, to implement a truly national cybersecurity policy and tighten standards to secure information, from all the networks, federal government and personal networks of civilians (Jansen van Vuuren et al, 2010).

As a result, the USA created the CYBERCOM led by the head of the NSA in October 2009. The cyber units associated with each branch of the military fall under the control of the head of CYBERCOM and the NSA. The CYBERCOM will support the Director of the Defence Information Systems Agency (DISA), which in turn has input into a Joint Operations Centre that will be the core of operations under the command of a Deputy Cyber Commander.

Outside the military, the National Cyber Security Division (NCSD) within the USA Department of Homeland Security (DHS) bears responsibility for overall cybersecurity in the USA. It oversees the US-CERT (Computer Emergency Readiness Team) and coordinates activities between public and commercial security groups as part of their mandate. In addition, the DHS operates the CS&C which is concerned with protecting critical information infrastructure. There also exists a National Cyber Security Centre that is responsible for the central coordination of the many organisations within the USA government that deal with cybersecurity. It is still unclear how these cybersecurity offices will work with the Department of Defense (DOD) CYBERCOM.

During the hearing for the appointment of the first head of CYBERCOM, Senator Carl Levin posted three scenarios from the USA side on the responsibilities of cyber defence in the USA. The scenarios as well as responses to them, can be summarised as follow (Stienon 2010):

- If the legal framework under which the USA military operates is used during a traditional operation against an adversary, the commander will execute an order approved by the President and the Joint Chiefs that would presumably grant the theatre commander full leeway to defend USA military networks and to counter cyber attacks that emanate for the attacking country.
- In the case where cyber attacks emanate from a neutral third country, additional authority would have to be granted.
- In a case of a major attack during peace time against computers that manage critical infrastructure, routing the attack through computers owned by USA citizens and routers inside the USA, it will most probably be the responsibility of the Department of Home Affairs and the Federal Bureau of Investigation, but there is no clear guidance in this regard.

From the discussion of the above scenarios, it is clear that this new CYBERCOM needs some research to determine the assignment of responsibility for setting up policies on how the USA should deal with cyber attacks. The creation of USA Cyber Command resulted in other countries following suit as discussed in the following subsections.

The USA cyber Organisation (Figure 2) makes provision for the separation of control of private networks and that of the security sector and is mostly controlled by the Department of Homeland Security.

The CS&C office consists of three divisions:

- *National Cyber Security Division*: Works collaboratively with public, private, and international entities to secure cyberspace and USA cyber assets.
- *Office of Emergency Communications*: Integrates and coordinates government-wide efforts addressing interoperable emergency communications.
- *National Communications System*: Works with the public and private sectors to ensure continuity and restoration of communications for the Nation in times of domestic emergencies.

The *National Cyber Security and Communications Integration Center (NCCIC)* is a center responsible for the production of a common operating picture for cyber and communications across the state, and local government, intelligence and law enforcement communities and the private sector. The NCCIC is operated within the DHS's CS&C as part of the National Protection & Programs Directorate. Operational elements include the US-CERT, the Industrial Control Systems Cyber Emergency Response Team, (ICS-CERT), National Coordinating Center for Telecommunications (NCC) and DHS Office of Intelligence & Analysis. The NCCIC integrates information from all partners including the Department of Defense, Department of Justice, Federal Bureau of Investigation, Secret Service, and

the NSSA, private sector and non-governmental partners. During a cyber or communications incident, the NCCIC serves as the national response center.

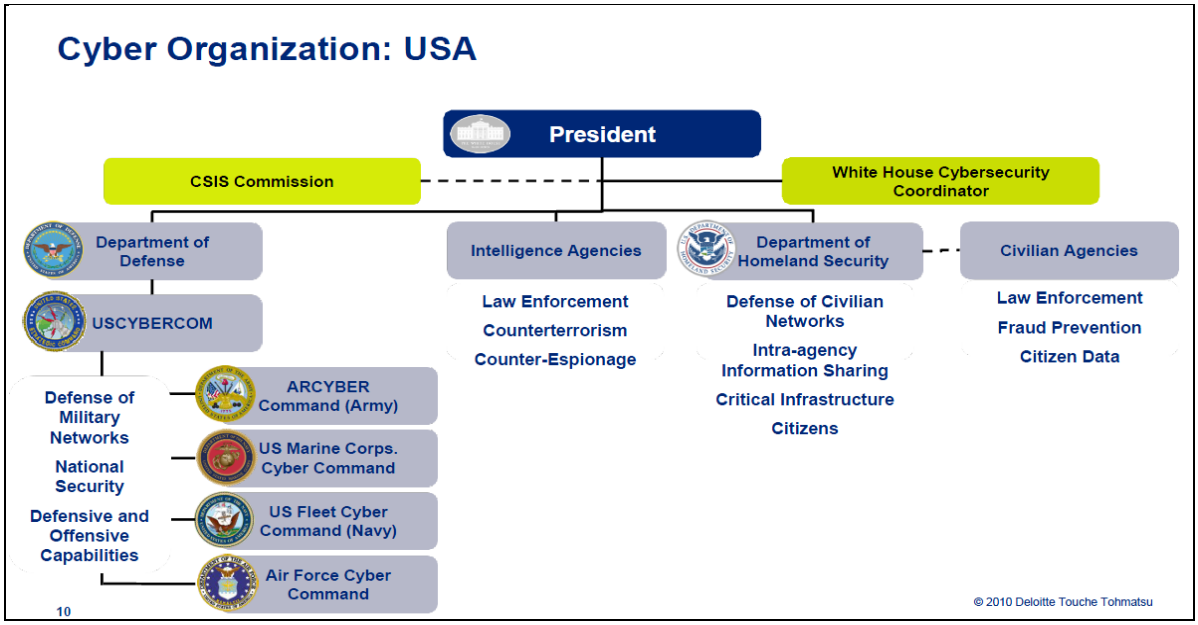

Figure 2: USA Cyber Organisation:(Deloitte & Touch 2010)

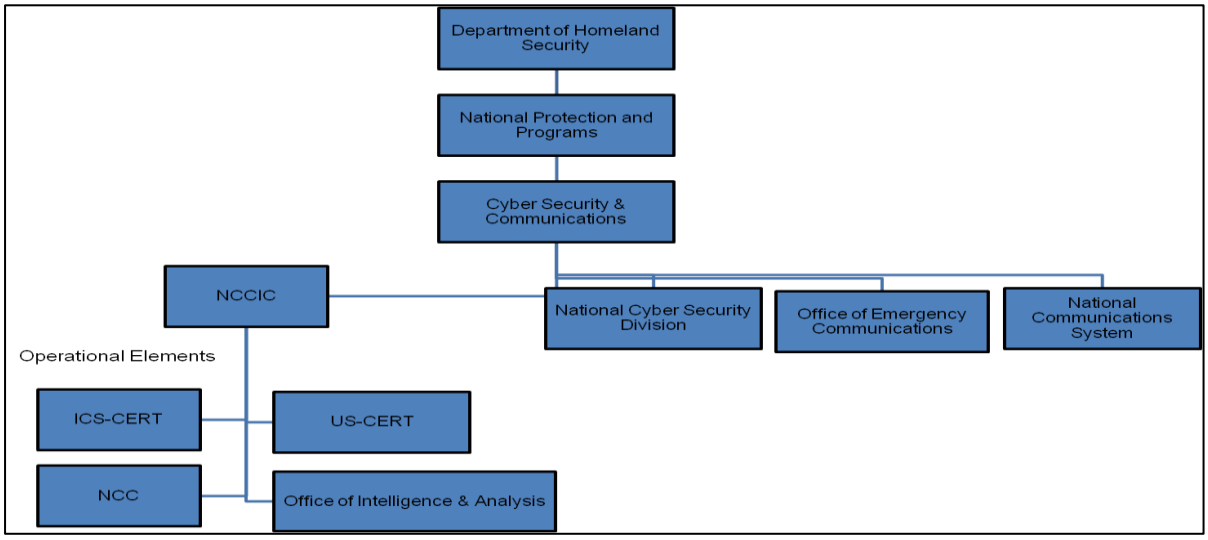

Figure 3: USA Homeland Security Structure

2.3 South Korean Approach

South Korea, a country with advanced IT developments, experienced a DDoS attack in July 2009 and experts indicated that it was politically motivated and revealed weaknesses in the national Internet security. A total of 26 domestic and foreign sites were attacked, included the Korean presidential office, government and defence sites. Thousands of infected personnel computers were turned into zombies spreading malicious codes with connection requests to websites, which in turn, paralysed the websites creating this DDoS attack. In addition, malicious code were spread that overwrote the infected PCs' hard drives which could have resulted in massive loss of data and information (Jansen van Vuuren et al. 2010).

North Korea was blamed for a wave of attacks against USA and South Korean websites, but since botnets were used in the attack the true orchestrator of the attack remains unclear. Trojan-based attacks targeted at South Korean government agencies dating back to 2004 were blamed on Chinese

hackers rumoured to have the support or perhaps even the involvement of the Peoples' Liberation Army. More recently, North Korean hackers were suspected of stealing a secret USA-South Korean war plan from South Korean systems. Some reports suggested that the hack was done by the use of an insecure memory stick. This cyber attack resulted in the Ministry of Defence in South Korea launching a cyber warfare command centre (mimicking the USA defensive steps), designed to fight against possible hacking attacks blamed on North Korea and China (Zorz 2010). The Centre, which along with a cyber police force, is charged with protecting government organisations and economical subjects from hacker attacks. The centre consists of 200 technical staff members, who are tasked to identify and counter the threat of Chinese hackers and others responsible for the reported 95,000 hacking attacks the country's military networks face every day. It is interesting to note that North Korea already started 20 years ago with the training of cybersecurity experts. It is believed that North Korea has more than 1000 skilled cyber hackers (Zorz, 2010); (Leyden, 2010).

The latest attack in March 2011 targeted 40 institutions in South Korea including banks and financial regulators, as well as military facilities and facilities controlled by the USA forces in South Korea, and the presidential office. The on-line trading system was temporarily shut down under the force of the attack but a spokesperson of the South Korean president indicated that no damage was done. The attacks were done by 11000 zombie computers, very similar to the 2009 attacks (Duncan, 2011; Evron, 2008). As mentioned above, South Korea established their Cyber Warfare command in December 2009. The South Korean cyber organization is shown in Figure 4 (Deloitte, 2010).

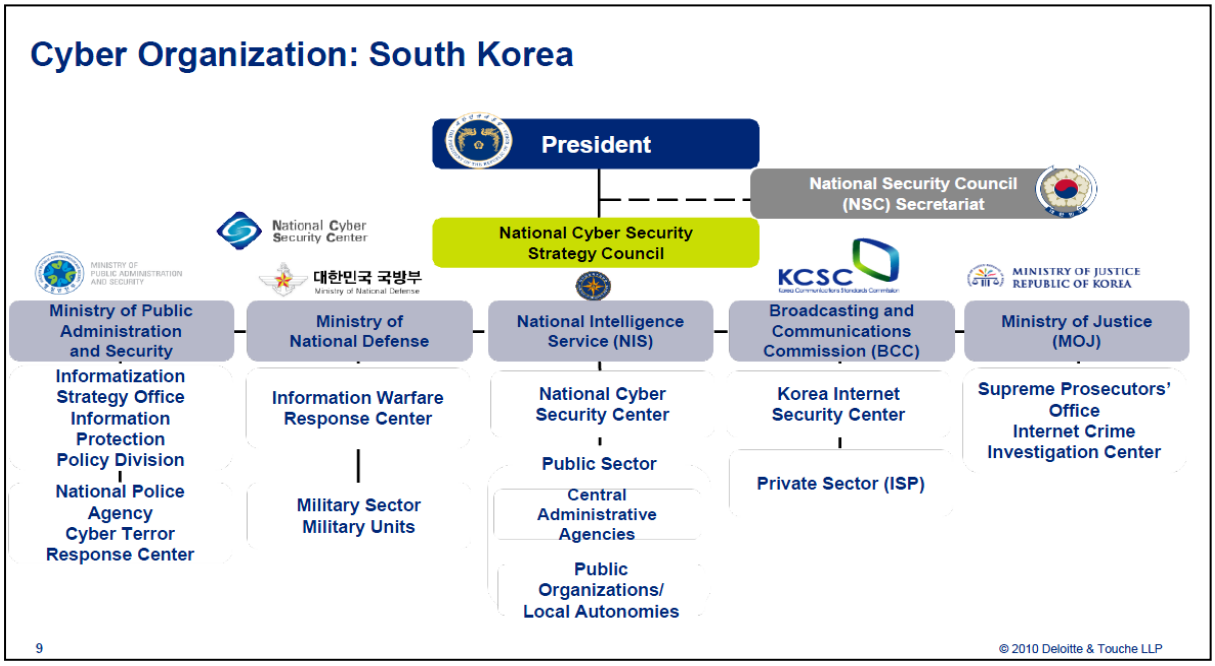

Figure 4: Korea Cyber Security Structure,(Deloitte & Touch 2010)

It is important to note the similarity between the structures of Estonia and the USA with the separation between government, defence and the private sector.

2.4 UK Approach

The UK‘s head of MI5 gave a written warning in 2007 to 300 UK companies that they were likely targets of hacking attempts by the Chinese Government. He confirmed that UK Government systems had also been attacked. This was the first time that such an event had been publicly acknowledged in the UK. Other nations as Germany and Belgium also indicated that they had experienced similar attacks. The UK‘s defence minister stressed the need to build robust cyber defences in November 2010 after a Romanian hacker cracked the Royal Navy’s Website.

The Government Communication Headquarters (GCHQ) is a British Intelligence Agency responsible for providing signals intelligence as well as providing advice and assistance to UK Government departments and the Armed forces on the security of their communications and information technology systems. It operates under the Joint Intelligence committee. The CESG, originally the

Communications-Electronics Security Group, is a branch of the GCHQ that provides the cyber security assistance to armed forces and government departments. They are also responsible for cryptography and to secure critical parts of the UK national infrastructure. In addition, the CESG is the UK national technical authority for information assurance: it primarily advices government and armed forces staff tasked with handling and processing official information, as well as agencies and firms carrying out work for the government.

The increase in expense at a time of economic cutbacks, was justified by stating that future battles will be fought not just on the ground, but in cyberspace. The role of cyber-tactics in offensive actions against enemy states, not just defensive concerns, was also acknowledged (Allan, 2010).

With the publication of the UK Cyber Security Strategy in June 2009 it became clear that the UK's growing dependence on cyberspace, results in the security of cyberspace becoming even more critical to the health of the nation and the protection of national critical infrastructure. Currently, all the approaches to cyber attacks are reactive. The current onslaught of attacks is always one step ahead of the "defender". As a result, Great Britain decided to establish a dedicated team of computer experts that will monitor, analyse and counter hostile computer-based assaults in an attempt to defend the country against cyber attacks (Phahlamohlaka et al, 2011). Lord West, the Security Minister, admitted that the UK already has its own online attack capability. "It would be silly to say that we don't have any capability to do offensive work from Cheltenham and I don't think I should say any more than that." The Cyber Security Operations Centre (CSOC) was set up in conjunction with the Office of Cyber Security, the government computer security agency with its primarily co-coordinating role in the defence of critical IT systems, such as those at utilities or financial institutions. The centre will also have an offensive role to conduct cyber attacks on those posing a threat to the security of the critical infrastructure (Espiner, 2010). Whitehall officials said that the UK and USA will be co-coordinating as there are a close relationship between GCHQ and its USA equivalent.

The UK government also initiated a cyber security hub that will enable the exchange of Cyber security threats by the public and private sectors (Nguyen, 2011).

2.5 Republic of China's Approach

In the 1990s, China realised that it needed to develop an alternative way of fighting wars in order to even the odds of defeating a likely opponent with their outdated technologies. The government's relied heavily on cyber warfare to attack modern targets. China was also the first country to start with the formation of cyber-warfare units. In 2000, a series of high-technology combat exercises by the People's Liberation Army (PLA) was suspended when a computer hacker attacked the military's network (Stokes et al, 2011). It is not clear if they are responsible for both private and public networks. Since 2003, China has worked on developing the capability and acquired new technology, reducing the time to design and build new systems.

China's General Staff Department (GSD) Third Department and its counterparts in the Air Force, Navy and Second Artillery, oversee the vast infrastructure for monitoring and collection of information inside China. GSD Third Department is specifically responsible for network surveillance and intelligence. It controls several operational bureaus responsible for technical reconnaissance. (Stokes et al, 2011). The focus of the GSD Third Department's signals intelligence, historical lack of an offensive role, and its large staff of trained linguists and technicians, make it well suited for oversight of the computer network defence (CND) and computer network exploitation (CNE) missions in the PLA (Krekel, 2009). The Third Department is comparable to the USA National Security Agency (Stokes et al, 2011).

The Fourth Fepartment most probably has the computer network attack responsibilities. Both the Third and Fourth Departments are said to jointly manage a network attack and defence training system (Stokes et al. 2011). The Fourth Department has set up the Blue Army that will be responsible for offensive cyber attacks as well as defensive actions. As early as 2010, China identified a need to establish a National Cyber Command similar to the USA CYBERCOM due to the need for the prevention of cyber attacks by the Ministry of Home Affairs and the Ministry of Defence to prevent cyber attacks (Guardian, 2010).

As a result of the USA CYBERCOM, the PLA has initiated a dedicated department in December 2010, the Information Security Base, to tackle cyber war threats and protect information security (Hsiao, 2010). Its goal is to gather information and to safeguard confidential military information.

However, an officer in the General Staff headquarters told the Global Times: "It is a 'defensive' base for information security, not an offensive headquarters for cyber war." (Guardian, 2010).

In addition, China has a National Computer Network Emergency Response Technical Coordination Center (NCNERTCC) in Beijing. This team released a report claiming that more than 4,600 Chinese government websites had their content modified by hackers in 2010, an increase of 68 percent over the previous year.

3 Cybersecurity Governance Strategies for RSA

In this section we consider requirements for establishing cybersecurity governance structures and give a proposal for such a structure in Section 3.1.

A cyber security implementation plan must be implemented on a national level to improve national security levels regarding ICT risks and misuses. To effectively implement a national strategy for a cyber security policy you need an effective approach and culture (Ghernouti-Helie 2010). This include:

- Political will and national leadership to ensure that the plan receives governmental support. It therefore must be supported by
    - the justice system and policing with a legal frameworks that supports police to combat cyber crime on national and international level;
    - cybersecurity capacity that include organisational structures, human capacity as well as the use of technical and procedural cybersecurity solutions; and
    - cybersecurity culture and awareness training of citizens

The USA policy review team suggested that at a minimum, the following elements must be considered (Phahlamohlaka et al, 2011).

- *Governance* structures for policy development and coordination of operational activities related to the cyber mission across the executive branch. This element will typically include the review of overlapping missions and responsibilities that are the result of authority being vested with various departments and agencies.
- *Architecture* that will include the performance, cost, and security characteristics of existing information and communications systems and infrastructures as well as strategic planning for the optimal system characteristics needed in the future. This element will typically include standards, identity management, authentication and attribution, software assurance, research and development, procurement, and supply chain risk management.
- *Norms of Behaviour* will include those elements of law, regulation, and international treaties and undertakings, as well as consensus-based measures, such as best practices, that collectively circumscribe and define standards of conduct in cyberspace.
- *Capacity Building that will include* the overall scale of resources, activities, and capabilities required to become a more cyber-competent nation. This element will typically include 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 communications infrastructure of the future.

Structures at national level should exist to sustain the 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 in consideration. National as well as international needs must also be considered.

Ghermouti-Helle (2011) also argues that the building of capacity should be based upon the understanding of the role of cybersecurity's 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 public and private sectors linked to cybersecurity organizational structures, dedicated to support operational proactive and reactive activities linked to cybersecurity management at a national level in turn, should exist.

Based on the South Africa's constitution, the key national security imperatives must be aligned with the governing principle, principle 98 of the South African Constitution, which states very clearly that "National Security must reflect the resolve of South Africans as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want, and to seek a better life" (Constitution of the Republic of South Africa, 1996). The human security aspect is therefore central to South Africa's perspective on national security. The modern definition of national security defines national security in terms of the respective elements of the power base of a state (Jablonsky 1997). Jablonsky identifies two such elements, the natural determinants and the social determinants. The natural determinants (geography, resources, and population) are concerned with the number of people in a nation and with their physical environment. Social determinants (economic, political, military, psychological, and informational) on the other hand concern the ways in which the people of a nation organize themselves and the manner in which they alter their environment.

The strategy discussed by Ghermouti-Helle as well as the USA cybersecurity policy strategy argue for a holistic approach in the implementation of the Cybersecurity Policy. Phahlamohlaka et al (2011) also argue that the philosophical position; the fundamental premise on which cybersecurity policies are developed is an absolute necessity. This is because cyberspace is a socially constructed, man-made space and therefore a cross-cutting social dimension of national power. At the core of any cybersecurity awareness initiative must therefore be the realisation that no full proof technological protection is possible in a socially constructed space. We argue that the holistic approach to cybersecurity policy that South Africa is looking for is likely to be enhanced by this philosophical position and understanding (Phahlamohlaka et al. 2011). As a cross-cutting social determinant of national power, a cybersecurity awareness programme developed with national security in mind could be confined to the economic, political, military, psychological and informational dimensions. It is these dimensions that constitute their proposed Cyber Security Awareness Toolkit for national security (CyberSAT).

3.1 Cybersecurity Governance

In this section we present a proposed cybersecurity governance structure for South Africa based on similar structure in other countries.

Estonia established 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 on-line attacks (Stienon, 2010). In addition, they developed and implemented their cyber security strategy. Estonia's cyber security strategy seeks primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole. The strategy is governed by a structure with a National Cyber Security Council reporting to government. All ministries that are responsible for different aspects of cyber security report to this council. They also differentiate between private sector, government and the military.

The USA created the CSIS commission at the highest level with the White House Coordinator representing the president. The USA cyber organisation makes provision for the separation of control of private networks by the DHS and that of the security sector. The security sector is managed by the CYBERCOM under the Strategic Command led by the head of the NSA.

In South Korea, the Ministry of Defence launched a cyber warfare command centre. Along a cyber police force, the centre is charged with protecting government organisations and economical subjects from hacker attacks. Their structure has at the highest level the National Security Strategy Council and a distinction is also made between security networks and private networks.

The UK established the GESQ and CSOC with the motivation that future battles will be fought not just on the ground, but in cyberspace. As a key part of their Cyber Security Strategy, the UK government also initiated a cyber security hub that will enable the exchange of cybersecurity threats by the public and private sectors.

The Chinese approach is mostly done from a military perspective with the establishment of the Information Security Base which that may serve as the PLA's cyber command. The NCNERTCC in Beijing is responsible for monitoring government websites. It is uncertain who is responsible for the private sector.

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 the cybersecurity be controlled on a very high level, as in the case in the USA, Estonia and Korea and other countries.

The proposed RSA structure (Figure 5) provides for a national body (National Cyber Security Council) reporting to the president as done in the USA, Estonia, UK and Korea. There is also a separation of the civilian and the security networks. The difference between our proposed structure and those of the USA and Estonia is that the government networks will also be controlled by the security services. The official structure for the control of cyber security is still debated in South Africa. Pressure is applied for control by State Security and thus the National Intelligence Agency. As seen in the literature with the establishment of the Cyber Command in the USA, the private sector questioned the fact that the military will play such an important role in the process. The same concerns on privacy of data might be in South Africa if State Security controls cybersecurity, and therefore also civilian networks. The concerns raised in the USA where whether the NSA will overshadow the civilian cyber defence efforts and on what assistance for civilian cyber defence there will be. Some concerns were laid to rest with the assurance that the Department of Homeland Security will be responsible for federal civilian networks including the dot-gov, and that CYBERCOM will only assist the Department of Homeland Security in the case of Cyber hostilities as a response to an executive order (Burghardt, 2012).

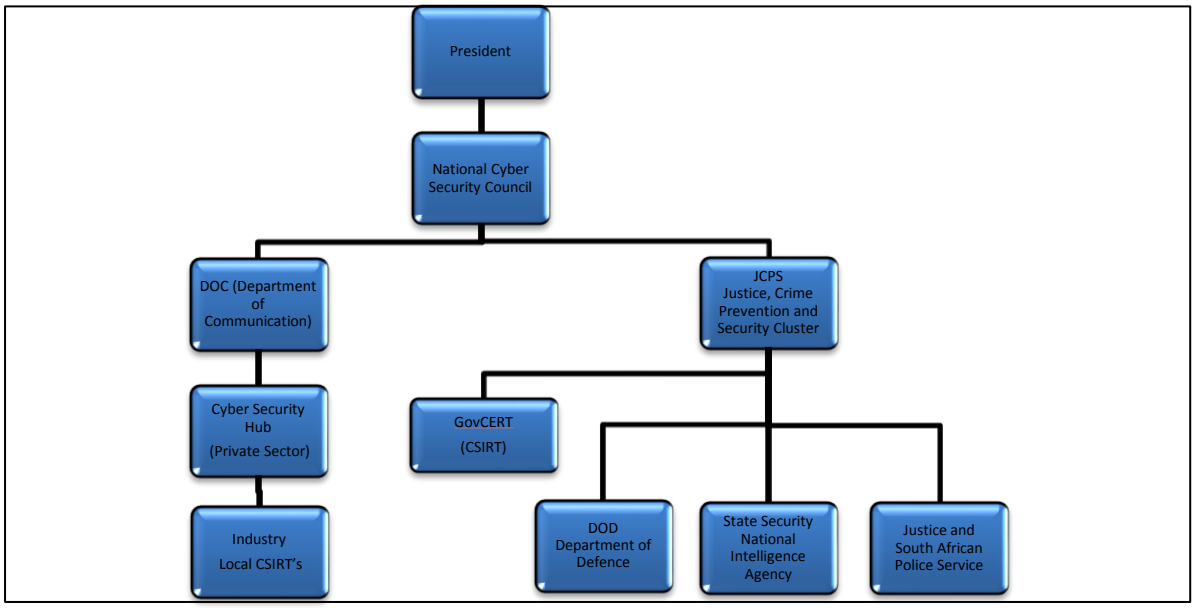

Figure 5: Proposed Cyber Security Structure South Africa

The model proposed by Phahlamohlaka et al (2011) for the implementation of the proposed Cybersecurity Strategy in South Africa is the CyberSAT that makes provision for policy decisions and the determinants of national power. Although the toolkit is based on policy elements from the South African environment, the determinants of national power are generic, and thus the toolkit could be adopted for cybersecurity awareness raising by other countries when national security considerations are pertinent.

4 Conclusion and Future Work

This paper gives an overview and analysis of cybersecurity organisational structures in the USA, UK, Estonia, South Korea, and China. Based on the result, we proposed a cybersecurity organisational structure for South Africa. In addition, a methodology for the implementation of the cybersecurity strategy and policy in South Africa is also considered. An organisational structure for effective governance was proposed as well as the Cyber Security Awareness Toolkit for national security (CyberSAT) as an operational guideline that could be used in the implementation of South Africa's proposed cybersecurity policy. In order to implement a cybersecurity strategy South Africa needs a formal approach to describe the cybersecurity environment.

We are in the process of developing an ontology for the cybersecurity strategic environment which we will use to support the implementation process. An ontology is a technology that allows one to encode a shared understanding and representation of a domain.

5 References

Allan, D. (2010) *Defence Minister to stress need for cyber-defence*. Retrieved 15 February, 2011, [online]
http://www.techwatch.co.uk/2010/11/09/defence-minister-to-stress-need-for-cyber-defence/
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
Boyd, C. (2010) *Why Estonia Is the Poster Child for Cyber-Security*. Retrieved 5 February, 2011, [online]
http://news.discovery.com/tech/why-estonia-is-the-poster-child-for-cyber-security.html
Burghardt, T. (2012) *The Launching of USA Cyber Command (CYBERCOM)*, Offensive Operations in Cyberspace. Retrieved 24 February 2012, [online]
http://www.globalresearch.ca/index.php?context=va&aid=14186
Constitution of the Republic of South Africa. (1996) *Chapter 11, Governing Principle 198*. Retrieved. from Deloitte & Touch. (2010) *National Cybersecurity Strategies*. Paper presented at the GOVCERT.NL symposium
Duncan, G. (2011) *New cyberattacks hit South Kore.a* Retrieved 5 March, 2011, [online]
http://www.digitaltrends.com/computing/new-cyberattacks-hit-south-korea/
Espiner, T. (2010) *UK's cyberdefence centre gets later start date*. Retrieved 21 February, 2011, [online]
http://www.zdnet.co.uk/news/security-threats/2010/03/10/uks-cyberdefence-centre-gets-later-start-date-40082405/
Evron, G. (2008) *Estonian Cyber Security Strategy Document: Translated and Public*. Retrieved 15 February, 2011, [online] http://www.circleid.com/posts/estonian_cyber_security_strategy/
Ghernouti-Helie, S. (2010). *A national strategy for an effective cybersecurity approach and culture*. Paper presented at the 2010 International Conference on Availability, Reliability and Security.
Guardian. (2010) Chinese army to target cyber war threat
(Publication.: http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department)
Hsiao, R. (2010) China's Cyber Command? *China Brief, Volume: 10 Issue: 15*.
Jablonsky, D. (1997) National power. *Parameters, 27*, 34-54.
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.
Krekel, B. (2009) *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*: DTIC Document.
Leyden, J. (2010) *South Korea sets up cyberwarfare unit to repel NORK hackers*. Retrieved 4 March 2011, [online]
http://www.theregister.co.uk/2010/01/12/korea_cyberwarfare_unit/
Nguyen, A. (2011) Government launches cyber security hub pilot [online]
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.
SA Goverment Gazette. (2010) *South African National Cyber Security Policy*.
Stienon, R. (2010) *Seven Cyber Scenarios that should keep you up at night.* [online]
http://threatchaos.com/
Stokes, M. A., Lin, J., & Russell Hsido, L. C. (2011) *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure: Project 2049*.
Tiirmaa-Klaar, H. (2010). *International Cooperation in Cyber Security: Actors, Levels and Challenges*. Proceedings of Cyber Security 2010, Brussels.
United States. Executive Office of the President. (2009) *Cyberspace Policy Review, Assuring a Trusted and Resillient Information*. Retrieved 12 February 2011 [online]
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
Zorz, Z. (2010) South Korea preparing for cyber war. Retrieved 5 February 2011, 2010, [online]
http://www.net-security.org/secworld.php?id=8722