Cyber Security Awareness Toolkit for National Security: an Approach to South Africa's Cybersecurity Policy Implementation

LJ Phahlamohlaka [1], JC Jansen van Vuuren[1], and AJ Coetzee[2]

[1] Defence Peace Safety and Security

CSIR, Pretoria, South Africa

[2]Directorate Information Warfare, CMIS, Department of Defence, Pretoria, South Africa

jphahlamohlaka@csir.co.za

jjvvuuren@csir.co.za

abrie.coetzee@sita.co.za

Abstract: The aim of this paper is to propose an approach that South Africa could follow in implementing its proposed Cyber security policy. The paper proposes a Cyber Security Awareness Toolkit that is underpinned by key National Security imperatives as well as by international approaches. This is achieved by drawing on several analysis work derived from international trends and comparing them with key elements of the South Africa's draft Cybersecurity policy. The analysis is then synthesised into sets of policy recommendations, with possible implementation mechanisms suggested in conclusion

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

1. Introduction

The cyber security challenges facing nation states and governments around the world elicit from leaders, responses that could be described as raising serious national security alarms. For instance, the United States of America 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.

One of the findings of the "clean-slate" 60-day United States Presidential policies and structures review on cyber security [17] was that the United States nation was at a crossroads. This was so because on the one hand, cyberspace underpins almost every facet of American society, providing critical support for their economy, civil infrastructure, public safety and national security. Yet, on the other hand cyber security risks pose some of the most serious economic and national security challenges of the 21st Century. The study points out that the digital infrastructure's architecture was driven more by considerations of interoperability and efficiency than of security, and consequently, a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems.

There is an international drive by various governments to either develop, or review existing Cybersecurity policies. From the US 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 [op cit].

With developing nations such as South Africa, the crossroads of the nation is of a different kind, the *need for an increased connectivity to the Internet* despite the cyber security risks that accompany the connectivity. So, what has brought the US nation to a crossroads because of over reliance on cyberspace is exactly what developing nations are aspiring for, ironical as it might sound. The bottom line here is that developing nations have no option, but to be part of the cyber citizenry. Developing nations needs to join in the race for cyber security policy development and implementation. They need to satisfy themselves as well as instil the confidence across their nations that the networks that support their national security and economic well being are safe and resilient. An interesting and thought provoking point counter point argumentative analysis from a national security point of view related to issues of access to the technology vs Cybersecurity risks is

presented by Phahlamohlaka et al [14]. Also, there are surprising recent statistics that shows that despite such a low internet penetration rate, South Africa ranks third in the world after the USA and UK on the number of countries being attacked [20].

In its draft Cybersecurity policy, South Africa has acknowledged that it does not have a coordinated approach in dealing with Cybersecurity, pointing out that whilst various structures have been established to deal with Cybersecurity issues, they are inadequate to deal with the issues *holistically.* It notes further that development of interventions to address cybercrime requires a partnership between business, government and civil society and that unless these spheres of society work together, South Africa's efforts to ensure a secured cyberspace could be severely compromised. It then calls for a holistic approach to Cybersecurity policy.

This paper is a response to that call. We propose in this paper an approach that South Africa could follow in implementing its Cybersecurity policy. We propose a Cyber Security Awareness Toolkit that is underpinned by key National Security imperatives as well as by international approaches. This is achieved by drawing on several analyses derived from international trends and comparing them with key elements of South Africa's draft Cybersecurity policy. The analysis is then synthesised into sets of policy recommendation, with possible implementation mechanisms suggested in conclusion.

2. Elements of the approach from international trends

2.1 Estonian experience and approach

In the case of Estonia, multiple botnets were used to conduct Distributed Denial of Service (DDoS) attacks against the Estonian Critical National Infrastructure, media, telecommunications and the main banks. Routers at the main Internet Service Providers (ISPs) were also attacked with ICMP flood attacks. Multiple botnets (up to 6) were involved in the attack, in excess of 400 Million packets per second were aimed at Estonia. Websites were also defaced and much of the economy and governing of the country ground to a halt. Identifications of the culprits could not be made as Russia did not want to assist in the search for these cyber attackers. Although there is no evidence of Russian involvement, many believe that they in all likelihood were behind the attacks. These attacks resulted in NATO creating the NATO Cyber Defence Research Centre in Tallinn in 2008, where research and operations take place to counter future activity of this sort. In 2009 the NATO Computer Incident Response Capability was founded in Mons, Belgium, with Intrusion detection and prevention capabilities for NATO networks

Cyber Attacks are not new. Web traffic was jammed during the Kosco war 10 years ago. But when Estonia came under cyber attack in 2007 the alliance realised the necessity of a cyber defence policy.

Although NATO did not participate, Cyber Europe 2010 comprised 20 EU member countries as well as Norway and Switzerland. The purpose of the exercise was to avoid a simulated total network crash. The exercise's scenario involved attempts to install fake malware on critical online services by around 130 experts and then block it under the hypothetic situation that the Internet-connection between the EU and other European countries has been disrupted. (ENISA, 2010) [5]. Chris Eves explained that the cyber threat is tackled by a number of analysts who are constantly reviewing information, looking for the more serious threats. "We have [about] 100 sensors at the moment deployed at something close to 30 different sites across the NATO countries... one of these sensors could be on the east coast of the United States, one could be in London, one could be in Iraq and a number of them could be in Afghanistan. All that information is simultaneously feeding back to us at the centre here" [9]

2.2 South Korean experience and approach

South Korea, a country with advanced IT developments experienced a distributed denial of service (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 was the Korean presidential office, government and defence sites and the US white house. 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 PC's hard drives that could have resulted in massive loss of data and information [11]. North Korea was blamed for a wave of attacks against US 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 for stealing a secret US-South Korean war plan from South

Korean systems. Some reports suggested that the hack was done by the use of an insecure (malware infected?) memory stick.

This 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 blamed on North Korea and China [16]. The Centre, which along a cyber police force is charged with protecting government organizations and economical subjects from hacker attacks. The centre consists of 200 techies, 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. North Korea already started 20 years ago with the training of cyber security experts It is believed that North Korea has more than 1000 skilled cyber hackers [16, 13]

The latest attack in March 2011, targeted 40 institutions in South Korean including banks and financial regulators, as well as military facilities and facilities controlled by U.S. forces in South Korea, including the presidential office. The online trading system was temporarily shut down under the force of the attack but the spokesperson from the office 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 [4, 7]

2.3 USA experience and Approach

The US took note of cyber war scenarios and threats that could face them from countries with advanced cyber warfare capabilities. In reaction to the current cyber attacks worldwide and in particular the attack on South Korea [17], the US embarked on a program to emphasise these cyber issues. President Obama already announced that he, in his position as president, will make cyber security the top priority that it should be in the 21st century. During a summit on national security at Purdue University, he further said that cyber-infrastructure is a strategic asset, and that it was necessary to appoint a national cyber adviser to report directly to the president. He further stated that the US needs to coordinate efforts across the federal government, to implement a truly national cyber security policy and tighten standards to secure information, from all the networks, federal government and personal networks of civilians [11].

As a result, the US created a Cyber Command (CYBERCOM) under the Strategic Command led by the head of the National Security Agency (NSA). One of the reasons 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. The CYBERCOM was thus created in October 2009 around this mission.

Senator Carl Levin noted on the recent nomination hearing where the operational responsibilities of the CYBERCOM were discussed, that *"…this policy gap is especially worrisome because cyber weapons and cyber attacks potentially can be devastating, approaching weapons of mass destruction in their effects, depending on how they are designed and used. The United States economy and government are the most dependent in the world on the Internet, and are therefore the most vulnerable to attacks, and therefore the Nation must not only invest in the effectiveness of its defence, but must also think carefully about the precedents it sets, and act wisely in ways that we will accept, if others act in the same or similar ways."* [3].

The cyber units associated with each branch of the military will be under the control of the head of the US CYBERCOM and NSA. The cyber units associated with each branch of the military will be under his operational control. These include the Army, Navy, Marine Corp, and Air Force CYBERCOMs, as well as supporting other combat commanders. 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 US Department of Homeland Security (DHS) bears responsibility for overall cyber security in the US. It oversees the US-CERT and coordinates activities between public and commercial security groups as part of their mandate. In addition, the DHS operates the Office of Cyber Security and Communications, 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 US government that deal with cyber security. It is still however unclear how these cyber security offices will work with the DOD CYBERCOM.

During the hearing for the appointment of the first head of CYBERCOM, Senator Carl Levin posted three scenarios from the US side on the responsibilities of cyber defence in the US. The answers and scenarios can be summarised as follows (Stienon, [15]):

- If the legal framework under which the US 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 US 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 US citizens and routers inside the US, it will be most probably the responsibility of the Department of Home Affairs and the Federal Bureau of Investigation, but there is no clear guidance in this regards.

From the discussion of the above scenarios, it is clear that this new CYBERCOM needs some research in their responsibility for setting up policies on how the US must deal with cyber attacks.

2.4 UK experience and Approach

The UK 's head of MI5 wrote in 2007 to 300 UK companies, formally warning them that they were likely targets of hacking attempts by the Chinese Government. He confirmed that HM 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 experienced similar attacks. Most probably most of the NATO nations did experience these attacks and prepared themselves for counter attacks. The UK's defence minister stressed the UK's need to build robust cyber defences in November 2010 after a Romanian hacker cracked the Royal Navy's Website. The increase in expense (while cuts are the order of the day) 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 [1].

With the publication of the UK Cyber Security Strategy in June 2009 it was clear that as the UK's dependence on cyberspace grows, so the security of cyberspace becomes even more critical to the health of the nation and the protection of the 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 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. Lord West, the Security Minister, admitted that Britain 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), based near GCHQ in Cheltenham is part of a new government strategy on cyber security. Whitehall officials said that the UK and USA will be co-ordinating as there are a close relationship between GCHQ and its US equivalent. The official said the strategy was of huge importance because critical national infrastructure is dependent on cyber space in a way it was not five years ago [8].

The CSOC was set up in conjunction with the Office of Cyber Security, the government computer security agency with it's primarily coordination 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 [6].

2.5 China experience and approach

In the 1990s the Chinese realised that they needed to develop an alternative way of fighting wars in order to even the odds of defeating a likely opponent with their outdated technologies. They came up with a doctrine "Unrestricted Warfare, Qiao Liang and Wang Xiangsui, (Beijing: PLA Literature and Arts Publishing House, February 1999)". This relies heavy on cyber warfare to attack modern targets. They were also the first to start with the formation of cyber-warfare units. Since 2003 they have worked on developing the capability and then using it to acquire new technology, reducing the time to design and build new systems.

China has also engaged in large scale industrial espionage in various forms, including the use of the internet to find and copy Intellectual Property and designs for useful items. The information that is most of interest to them includes:

- Intellectual property
- Intelligence data
- Future plans & intentions
- Strategic intent

- Command & signals data

Google has also publicly declared that they have been hacked by the Chinese. These attacks have been happening since at least 2003. The latest publicly declared incident is the loss of over a terabyte of design data for the F35 strike fighter to a Chinese IP address in Shangdong province, the home of their hacking activities. The targets are mainly government, military, suppliers to both and financial sector organisations. In 2007 the US Congress was told that Chinese Espionage represented "*The single greatest risk to the security of US technology*".

2.6 Georgian experience and approach

The first pre mediated cyber attack was launched during the conflict between Georgia and Russia over the Georgian province of South Ossetia in August 2008. Denial-of-Service (DoS) attacks were initiated by Russian civilians and sympathizers in coordination with the Russian military and organized crime were scheduled to be synchronised with the invasion of the Russian military into the former Soviet state. From August 7th to 13th a massive DDoS attack took down government and banking services, a day before the Russian army crossed the border. In the investigation of the analysis of the computer logs from the targets, it showed that probes and enumeration (reconnaissance) of systems were happening already from July 20th onwards. The hackers made use of sophisticated SQL injection attacks, designed to consume processing time and steal data from the Georgian servers. Although attackers and activities showed every sign of being civilian and there was little or no direct government involvement, the general belief was that the attacks could be attributed to the Russian state as the attack were carried out very fast and was timed to coordinate with military activities and demonstrated the knowledge of the military plan [11].

2.7 Iranian experience and approach

The most recent cyber attack is the attack on the Iranian nuclear plant in 2010, by the Stuxnet worm. The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. The computer program also secretly recorded what normal operations at the nuclear plant looked like, and then played those readings back to plant operators, like a pre-recorded security tape in a bank heist. With these recordings everything appeared to be operating normally while the centrifuges were actually tearing themselves apart. The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived. Some experts who have examined the code believe it contains the seeds for yet more versions and assaults and therefore it is clear that the attacks are not over yet. It is suspected that the research was done in early 2008 by the German company Siemens in cooperation with one of the United States' premier national laboratories in Idaho. Siemens said that program was to identify the vulnerabilities of computer controllers that the company sells to operate industrial machinery around the world and this was part of the company's routine efforts to secure its products against cyber attacks. Nonetheless, it gave the Idaho National Laboratory, which is part of the Energy Department responsible for America's nuclear arms, the chance to identify well-hidden holes in the Siemens systems that were exploited the next year by Stuxnet. It is widely believed that the Stuxnet worm has bbeen created and delivered by Israel to delay the Iranian nuclear weapons program.

3. Comparative analysis of Cybersecurity policies

3.1 Key elements identification

RSA key elements

The RSA Cybersecurity policy [19] is made out of six key elements or strategic objectives, to:

- 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

USA key elements

A USA policy review team suggest that any complete national cyber policy must consider, at a minimum, the following elements:

- *Governance:* Encompasses U.S. Government (USG) structures for policy development and coordination of operational activities related to the cyber mission across the Executive Branch. This element includes reviewing overlapping missions and responsibilities that are the result of authority being vested with various departments and agencies.
- *Architecture:* Addresses the performance, cost, and security characteristics of existing information and communications systems and infrastructures as well as strategic planning for the optimal system characteristics that will be needed in the future. This element includes standards, identity management, authentication and attribution, software assurance, research and development, procurement, and supply chain risk management.
- *Norms of Behaviour*: Addresses 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:* Encompasses the overall scale of resources, activities, and capabilities required to become a more cyber-competent nation. These include resource requirements, research and development, public education and awareness, and international partnerships, and all other activities that allow the USG to interface with its citizenry and workforce to build the digital information and communications infrastructure of the future.

Canadian key elements

- *National, cross-sectoral strategies are effective*. They can encourage cooperation across entrenched barriers or silos, and can lead to information sharing and collaboration between wide varieties of stakeholders. Government has a role to play in encouraging these relationships and partnerships, analyzing progress, and monitoring new developments.
- *Roles and responsibilities are in need of clarification, and even codification*. Understanding lines of accountability and appropriate behaviours can lead to trust and confidence in the strategy that emerges.
- *It's the individual, stupid.* Government and business alike have a role to play in encouraging public awareness and "cyber literacy," but it is ultimately "people, not systems" that matter.
- *Leadership matters*. Organizational leaders who are willing to step forward and acknowledge risks and vulnerabilities will ultimately encourage trust and confidence among the "followership."
- *Think globally*. International partnerships and shared global spaces are necessary tools in the fight against transnational crime. This requires cooperation between states and sharing the valuable information developed within national jurisdictions. This can serve to enhance Canada's reputation as a country committed to multilateral initiatives, especially those relating to international peace, security, and justice.

3.2 National Security imperatives and international approaches

3.2.1 The Philosophical National Security imperative on Cybersecurity

South Africa's key national security imperatives derive from its Constitution, where the first governing principle, principle 98 of the South African Constitution state 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" [18]. Human security is therefore central to South Africa's perspective on national security. This is in line with the modern definition of national security, which is an improvement of the traditional one which defined national security in terms of the respective elements of the power base of a state. Jablosnky [12] identifies two such elements, called determinants of national power. They are 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.

It is our argument that a 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 crosscutting 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.

As a crosscutting 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 our proposed Cybersecurity Awareness Toolkit for national security (CyberSAT) which we present in section 4.

3.2.2 A snapshot on the international approaches

From the Estonian experience, the lesson is that the only way we will learn to move forward on Cybersecurity related issue 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 [2,15]

In South Korea, the 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 organizations and economical subjects from hacker attacks. Despite the establishment this Cyber warfare command centre, there have been repeat attacks in March 2011.

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. From China we learn about a focus on Industrial espionage with the goal of stealing IP and designs, command signal data and information of financial and commercial nature.

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. 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 as the basis of 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.

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. Underpinned by a set of philosophical positions that we suggest, these elements are synchronised in the next section with five dimensions of national power resulting in what we propose as the Cybersecurity Awareness Toolkit for national security.

4. The proposed Cybersecurity Awareness Toolkit for National Security

The Cybersecurity Awareness Toolkit (CyberSAT) for national security is presented in Table 1. In the first column are the elements of the policy while the second row contains 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 awareness raising by other countries when national security considerations are pertinent.

The Toolkit

Table 1: *The Cyber Security Awareness Toolkit for National Security (CyberSAT)*

	Philosophical position	**Social Determinants of National Power**				
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	Establish a National security level institutional arrangement on Cybersecurity	Establish Military CSIRT	Build confidence in the response capacity of established institutions	Let the public to trust in the security of communication channels and systems
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
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
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
Capacity building, culture of Cybersecurity	*Focus internally and on the basics.Insider threats are more than external threats*	Focus on public education and awareness	It is the behaviour of individual users that is the single most important part of the Cybersecurity battle	It is the behaviour of individual users that is the single most important part of the Cybersecurity battle	It is the behaviour of individual users that is the single most important part of the Cybersecurity battle	Focus on public education and awareness
Compliance with technical and operational Cybersecurity standards	*Actively Participate in the creation of international standards*	Define standards of conduct in cyberspace.	Articulate coordinated national information and communications infrastructure objectives	Define standards of conduct in cyberspace.	Define standards of conduct in cyberspace.	Articulate coordinated national information and communications infrastructure objectives

4.1 A Short Description of CyberSAT in Table 1

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 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

Capacity building, culture of Cybersecurity: *Focus internally and on the basics.Insider threats are more than external threats*

Promotion of a national program so that the general population across all sectors secure their own parts of cyberspace

Compliance with technical and operational Cybersecurity standards: *Actively Participate in the creation of international standards*

Defining the standard of conduct in cyberspace is critical and active participation in the creation of these standards is therefore a must.

4.2 Recommendations and possible implementation mechanisms

The CyberSAT presented in this paper could be used as a stepping stone to the implementation of South Africa's proposed Cybersecurity policy. Because South Africa does not yet have a consolidated national security policy and strategy, an 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. The reader should note 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. Amongst other possible uses, it could be used to:

- Initiate a national public awareness and education campaign to promote cybersecurity.
- facilitate a national strategy that touches all sectors and encourages widespread buy-in.
- make cybersecurity popular for children and for older students choosing careers.
- develop a framework for research and development strategies that focus on providing the research community access to event data to facilitate development of tools, testing theories, and identification of workable solutions.
- develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in government
- develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
- develop mechanisms for cybersecurity related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial

- engage in constant monitoring and analysis of changes in threats and vulnerabilities.

All these are important because policy implementation in South Africa is in general not a simple matter, let alone on Cybersecurity matters when less than six percent of the population has access to the Internet.

5. Conclusion

We presented in this paper the Cybersecurity Awareness Toolkit for national security (CyberSAT) as an operational guideline that could be used in the implementation of South Africa's proposed Cybersecurity policy, which the country hopes will be approved by parliament before the end of 2011 [10]. The popularity of social networking tools worldwide, especially among young people, indicates that people cannot value security without first understanding how much is at risk. The surprising recent statistics mentioned in the introduction that shows that despite such a low internet penetration rate, South Africa ranks third in the world after the USA and UK on the number of countries being attacked, indicates the scale of potential future cyber attacks. A Cybersecurity awareness campaign is therefore urgently needed in South Africa. The Cybersecurity Awareness Toolkit for national security presented in this paper could contribute towards the design and implementation of such a campaign. Also, an increased investment in research that could help address cybersecurity vulnerabilities while also meeting socio-economic needs and national security requirements is necessary.

References

[1]. Allan, D. (2010). Defence Minister to stress need for cyber-defence. Accessed 15 February, 2011, available online from http://www.techwatch.co.uk/2010/11/09/defence-minister-to-stress-need-for-cyber-defence/

[2]. Boyd, C. (2010). Why Estonia Is the Poster Child for Cyber-Security. Accessed 5 February, 2011, available online from http://news.discovery.com/tech/why-estonia-is-the-poster-child-for-cyber-security.html

[3]. Carl Levin, S. (2010). *Opening Statement of Senator Carl Levin, Senate Armed Services Committee Hearing on Nominations of Vice Admiral James A. Winnefeld and Lieutenant General Keith B. Alexander*. Accessed. available online from http://levin.senate.gov/newsroom/release.cfm?id=323856.

[4]. Duncan, G. (2011). New cyberattacks hit South Korea , accessed 5 March, 2011, available online from http://www.digitaltrends.com/computing/new-cyberattacks-hit-south-korea/

[5]. ENISA. (2010). 'CYBER EUROPE 2010' -the 1st pan-European CIIP exercise. Accessed 5 March, 2011, available online from http://www.enisa.europa.eu/media/news-items/2018cyber-europe-20102019-the-1st-pan-european-ciip-exercise-phase-one

[6]. Espiner, T. (2010). UK's cyberdefence centre gets later start date. Accessed 21 February, 2011, available online from http://www.zdnet.co.uk/news/security-threats/2010/03/10/uks-cyberdefence-centre-gets-later-start-date-40082405/

[7]. Evron, G. (2008). Estonian Cyber Security Strategy Document: Translated and Public. Accessed 15 February, 2011, available online from http://www.circleid.com/posts/estonian_cyber_security_strategy/

[8]. Ford, R. (2009). GCHQ to get cyber defence squad to protect British computers.

[9]. Frank, G. (2009). Nato's cyber defence warriors. Accessed 5 February, 2011, available online from http://news.bbc.co.uk/2/hi/europe/7851292.stm

[10]. 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-this-year&catid=48:Information%20&%20Communication%20Technologies&Itemid=109

[11]. Jansen van Vuuren, J., Phahlamohlaka, J., & Brazzoli, M. (2010). *The impact of the increase in broadband access on South African national security and the average citizen*. Journal of Information Warfare , 9(3) pp 1-13.

[12]. Jablonsky, D. (2001) "National Power", In Cerami, J.R., Holcomb, J.F, Jr. (eds). U.S. Army war college guide to strategy, 2001, also available online at http://www.au.af.mil/au/awc/awcgate/army-usawc/strategy2004/index.htm.

[13]. Leyden, J. (2010). South Korea sets up cyber warfare unit to repel NORK hackers Accessed 4 March 2011, available online from http://www.theregister.co.uk/2010/01/12/korea_cyberwarfare_unit/

[14]. Phahlamohlaka, J., Modise, M., Nengovhela, N. The Digital Divide: A National Security Argumentative Analysis within a South African Context. Workshop on ICT uses in warfare and the safeguarding of peace, SAICSIT Conference, Bela-Bela, October 2010.

[15]. Stienon, R. (2010). Seven Cyber Scenarios that should keep you up at night available online from http://threatchaos.com/

[16]. Zorz, Z. (2010). South Korea preparing for cyber war. Accessed 5 February 2011, 2010, available online from http://www.net-security.org/secworld.php?id=8722

[17]. Cyberspace Policy Review, Assuring a Trusted and Resilient Information, accessed on 12 February 2011 available online from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[18]. Constitution of the Republic of South Africa, Chapter 11, Governing Principle 198, pp 112, 1996.

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

[20]. Information Security Intelligence Report: A Recap of 2010 and Predictions for 2011, accessed on 26 January 2011, available online from www.security-art.com