# Preparing South Africa for Cyber Crime and Cyber Defense

**Prof Marthie Grobler**
**Council for Scientific and Industrial Research**
**PO Box 395**
**Pretoria, 0001**
**South Africa**

**Joey Jansen van Vuuren**
**Council for Scientific and Industrial Research**
**PO Box 395**
**Pretoria, 0001**
**South Africa**

**Dr Jannie Zaaiman**
**University of Venda**
**Thohoyandou**
**0950**
**South Africa**

**Abstract:** The international scope of the Internet, the fast technological advances, the wide reach of technological usage and the increase in cyber-attacks require the South African administrative and legislative system to both intersect largely with the application and implementation of international legislation, take timeous precautionary measures and stay updated on trends and developments. One of the problems associated with the technological revolution is that the cyberspace is full of complex and dynamic technological innovations that are not well suited to any lagging administrative and legal system. A further complication is the lack of comprehensive and enforceable treaties facilitating international cooperation with regard to cyber defense. The result is that many developing countries in particular, are either not properly aware, not well prepared, or adequately protected by both knowledge and legislation, in the event of a cyber-attack on a national level. Even if these countries realize the threats, the time to react is of such a long nature due to consultation and legislative processes, that the legal systems provide little support to ensure timeous and necessary counter-measures. This article will address this problem by looking at the impact of technological revolution on cybercrime and cyber defense in a developing country and will evaluate the relevant South African legislation. It will also look at the influence of cyber defense on the international position of the South African Government.

South Africa at present does not have a coordinated approach in dealing with Cybercrime and does not have a comprehensive Cyber defense strategy in place. The structures that have been established to deal with Cyber security issues are inadequate to *holistically* deal with these issues. The development of interventions to address cybercrime requires a partnership between business, government and civil society. This article will provide an approach to deal with making the civil community aware of Cyber Crime and provide a defense mechanism to assist governments from developing countries to prevent their countries to be used as targets or intermediary for either Cyber Crime or Cyber Warfare.

**Keywords:** Collaboration, cyber defense, cyber crime, cyber awareness, legislation, government responsibility

**Keywords:** Collaboration, cyber defense, legislation, government responsibility

## 1. Introduction

The international scope of the Internet the fast technological advances, the global reach of technological usage requires all administrative and legislative systems to address issues related to the application and implementation of relevant national and international legislation. The complexities of cyberspace and the dynamic nature of technological innovations require a holistic cyber-defense framework that is unfortunately not well suited to the current legal system due to its fast changing nature and impact. To complicate this further, the lack of comprehensive and effective international cyber defense cooperation treaties resulted in many countries that are not adequately prepared for or protected by legislation and administrative operational systems, in the event of a cyber-attack on a national level. This is also the case for South Africa. One of the major issues to be addressed is turf protection especially from State Departments and the fact that it is sometimes difficult to see the larger picture.

This article will address the problem posed by the disjoint relationship between modern cyber space, cyber warfare

and traditional legislation and a lack of cyber defense mechanisms. As a starting point, cyber warfare for the purpose of this article is defined as the use of exploits in cyber space as a way to intentionally cause harm to people, assets or economies (Owen 2008). It can further be defined as the use and management of information in pursuit of a competitive advantage over an opponent, involving *"the collection of tactical information, assurance that one's own information is valid, spreading of propaganda or disinformation among the enemy, undermining the quality of opposing force information and denial of service or of information collection opportunities to opposing forces"* (Williams & Arreymbi 2007).

The main focus of this article will be on the benefits that South Africa can gain from working together both internally and externally with other nations in the field of cyber warfare. This article will look at some technological revolutions that had an impact on the local and international legal scope and briefly evaluate the South African legal system with regard to national threats and international cyber defense collaboration. The article will also address international cyber warfare and the influence of cyber defense on the international position of the South African Government and nationally on the various South African communities such as defense, business, public sectors and ordinary citizens. The article will conclude with recommendations on working towards preparing the South African Cyber environment to be sensitive to signals of cyber-attacks in all spheres of daily activities and pro-actively identify and put defense mechanism in place.

Dhlamini (2012) is of the opinion that security and protection of individuals and organisation against the fast growing dangers of the cybercrime remain one of the major challenges facing cyber security experts, scholars and politicians. Cybercrime is on the rise in South Africa (SAPS, 2011). The increase is the result of the increased bandwidth and the proliferation of smart phones which has widened access to Internet to the majority of South Africans (RSA, 2011).

Sixteen percent of the cybercrime victims were affected through their phones compared to only 10 percent globally. Malware and computer viruses made up the biggest portion of cybercrime in South Africa. Scams and phishing fraud made up the rest. The total net cost of cybercrime in South Africa is estimated at R10.9 billion (Ferrier Int., 2011), making up one percent of the global net cost of R2.9 trillion. Cyber security awareness is the first line of defense against cyber-attacks.

In South Africa, cyber security awareness initiatives are delivered through a variety of independent uncoordinated mechanisms. Various entities are engage on cyber security awareness training each with their specific objectives and focus areas.

Cyber security is complex and multi-dimensional. An effective approach is that which accommodates and integrates all the dimensions. Therefore, the effectiveness of the current initiatives to the delivery of cyber security awareness initiatives that are relevant needs to be evaluated. The study outlines, evaluates and assesses the relevance of current cyber security initiatives in addressing cyber security challenges facing South Africa. (Dhlamini, 2012).

## 2. The evolution of the cybercrime threat and cyberwarfare phenomenon (nationally and internationally)

Modern society created both a direct and indirect dependence on information technology, with a strong reliance on immediacy, access and connections (Williams & Arreymbi 2007). As a result, a compromise of the confidentiality, availability or integrity of the technological systems could have dramatic consequences regardless of whether it is the temporary interruption of connectivity, or a longer-term disruption caused by a cyber-attack (Warren 2008).

On many levels, cyber warfare brings the battle closer to home since more people can potentially be affected. In many cases the enemy is omnipresent, since any piece of equipment that uses technology is a potential battle field or medium that can be used by enemy forces.

Although each sector is unique and has different aspects that can contribute to National Security, all these sectors are vulnerable to attack by enemy forces. Since the computerization of many of these systems has been automated, many of these sectors are now also vulnerable to attack in the cyber domain. Accordingly, the traditional understanding of battlespace, as implied by military use and warfare, is becoming increasingly difficult to define. Not only does the security of a nation depend on the defense mechanisms in place at the physical battlefield, but now it also depends on the nation's capability to defend in the unchartered, often changing environment of cyber space and computerized systems.

*"Today, cyber-attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity. The nature of a national security threat has not changed, but the Internet has provided a new*

*delivery mechanism that can increase the speed, diffusion, and power of an attack."* (Geers ND).

The internet has changed every aspect of human life. Every political, business, military and many citizenship conflicts now has a cyber-dimensions. (Mele, 2010)

It is important to emphasize that the act of cyber warfare will not physically destruct any of the Critical National Infrastructure (CNI) sectors. However, a number of technological exploits can be employed as part of a cyber-warfare attack aimed at financial loss by disabling or disrupting a CNI sector. For example, if the energy CNI is under attack, the enemy forces may launch a destructive virus within the national energy regulator's mainframe that leads to a root compromise. This will disrupt the computer systems that relay electricity to the different municipal wards, and put the affected nation in darkness. Since the electricity is not working, the communications system will also be affected – company switchboards and computer systems that do not run on battery power will be offline (Niblett 2010).

Those companies that have generators or uninterrupted power supplies available might be able to continue work for a couple of hours, but as soon as the fuel runs out or the batteries run down, these companies will also be offline. Security systems might run on battery power for a while, but these batteries will also run down eventually, leaving physical structures vulnerable to thievery and mutiny. Therefore, as a result of a simple virus, enemy forces enabled a far greater threat than dropping a bomb on an unsuspecting community a disabled CNI leading to probable mass hysteria in an attempt for self-preservation.

**3. The need for cyber defense collaboration (nationally and internationally)**

Governments no longer own and control significant portions of their country's CNI. This varies by country, but is common practice due to consolidation and globalization. In addition, critical infrastructure now crosses borders and may be under foreign control in some cases. Companies that were once owned by the government may now be privatized, while companies that may never have been under government control in the past have become critical to a nation's infrastructure (Niblett 2010).

The need for cyber defense collaboration is imminent. In order to prevent, or at least minimize the type of scenario sketched in the previous section. It is necessary for organizations, or on a larger scale, for nations to collaborate in cyber defense activities. The key to these collaboration efforts is open communication and a willingness to give and accepts input from others.

Governmental structures for policy development and the coordination of cyber operations should also address the responsibilities and specifically the likely overlap of responsibilities of various stakeholders in the cyber security domain.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.

For example, if online government and banking services were under attack by a globally controlled denial of service botnet, it would take international coordinated effort to identify and mitigate the threat. Not only will finance, government and communication industries be involved in these rescue endeavors, but partners from many different countries will have to work together in order to stop the online attacks.

By sharing information about the risks facing CNI, both the government and industry partners can benefit. If each party can learn from the experiences, mistakes and successes of others, they can in turn improve their own level of cyber defense (Niblett 2010). Further, successful collaboration efforts demands respect between partners and a win-win situation for all parties involved (Crow 2002).

Several countries have invested large amounts of money for the implementation of Cyber policies and defense mechanisms. Closer to home, South Africa is a rapidly developing economy. Many of the current initiatives run by government relate to the rollout of Internet connectivity to the nation. This includes access to a new data link on the east coast of Africa to increase bandwidth availability. In return, it is suspected that the increased bandwidth will also lead to an increase in cyber attacks on the civil networks in the country.

As in other countries, the South African DOD is well aware of this threat, and aware of the role of the cyber domain in modern defense missions (Roodt, Oosthuizen & Jansen van Vuuren 2010). To ensure that South Africa can be a partner in such an international collaboration, it is necessary to evaluate the possibilities of the South African legal system with regard to cyber defense collaboration.

**4. The South African effort in combatting cyber attacks**

From recent activity, it is clear that both the South African Government, the defense environment and industry are becoming increasingly aware of the threats posed by and

implications of using the cyber environment. It is also clear that the threats are becoming more sophisticated and advanced when used as an element of cyber warfare and cyber crime, especially since cyber defense often need to address an unseen threat.

Cyber terrorists have the capability to shut down South Africa's power, disrupt financial transactions, and commit crimes to finance their physical operations. Organized crime is also increasingly making use of the Internet as a means of communication and financial gain. Therefore, South Africa needs a national cyber defense system to which everybody must obey.

On 23 March 2012 it was announced that Cabinet has approved a National c\Cyber Security Policy Framework for South Africa, said Collins Chabane, Minister in the Presidency. (Paganini 2012). Chabane went on to say, "the framework was aimed at addressing national security threats in cyber space and it would combat cyber warfare, cybercrime and cyber ills, as well as build confidence and trust in the secure use of information and communication technologies." This policy framework was a collaborated effort between the Departments of State security and the Department of Communications (DOC). Unfortunately a year after this policy framework was announced, the document I still not published. This may hamper the implementation of the framework.

**4. The South African effort in combatting cyber attacks**

Since the mid-1990s, South Africa has taken the first steps to protect its information. It has passed legislation such as the *South African Constitution of 1996* to protect privacy. In 2000, the *PAIA (Promotion of Access to Information Act) No 2 as amended*, was passed to give effect to Section 32 of the Constitution, subject to justifiable limitations (PAIA Act 2000). These limitations are aimed at the reasonable protection of privacy, commercial confidentiality and good governance in a manner that balances the right of access to information with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution (SA Constitution 1996). Linked to this Act is the PAIA Reg 187 Regulations regarding the promotion of information of access to information (Government Gazette 2003).

The *ECT (Electronic Communications and Transactions) Act of 2002* is put in place to facilitate and regulate electronic communications and transactions (ECT 2002). Also in 2002, the *RIC (Regulation of Interception of Communications and Provision of Communication-related information) Act* was passed to regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information. This Act also regulates the making of applications for, and the issuing of, directions authorizing the interception of communications and the provision of communication-related information under certain circumstances (RIC Act 2002).

Towards the end of 2009, the South African Government passed two bills, namely the:

- *PPI (Protection of Personal Information) Bill* that introduces brand new legislation to ensure that the personal information of individuals is protected, regardless of whether it is processed by public or private bodies (Giles 2010).
- *Information Bill* that is meant to replace an existing piece of legislation, the Protection of Information Act of 1982. It deals with the protection of State information and empowers the government to classify certain information in order to protect the national interest from suspected espionage and other hostile activities (Republic of South Africa 2010).

In addition, South Africa has also adopted the Council of Europe Cyber Crime Treaty in Budapest in 2001 but has not ratified it yet. The treaty contains important provisions to assist law enforcement in their fight against trans-border cybercrime. Therefore, it is imperative that South Africa ratifies the cyber crime treaty to avoid becoming an easy target for international cyber crime. The ratification will hopefully be done soon, although the South African government seems to be presently focused on basic service delivery and more traditional crimes given the current local crime situation. In combination with this treaty, all the South African bills and acts play an important role in the potential future collaboration of South Africa with other nations in the domain of cyber defense.

**5 Current collaboration efforts**

In general, governments are struggling to address cyber crime adequately. In many countries, it is a reality that Cybercrime damages economies and State credibility. It has become crucial for nations to collaborate in order to protect themselves from cyber warfare. Up to date, South Africa has made initial efforts to collaborate on an international level.

In February 2010, South Africa published a draft Cyber security policy that would set a framework for the creation of relevant structures, boost international cooperation, build national capacity and promote compliance with appropriate cyber crime standards. Over the last five years, South Africa focused on modernizing and expanding information

technology equipment, applications, and centralized hosting capabilities and network infrastructure.

This was done as part of its strategy to fully modernize and integrate the national criminal justice system to the maximum benefit of society and at minimum cost to crime prevention agencies. This policy has not been adopted, but provides a first step from South Africa towards international cyber defense collaboration.

South Africa participated in the 12th United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil during April 2010. During this congress, Delegates considered the best possible responses to cyber crime as the Congress Committee took up the dark side of advances in Information Technology.

While advances in information and communications technology hold many benefits for society, it also has the potential for sinister motives: computer-based fraud and forgery, illegal interception of private communications, interference with data and misuse of electronic devices. These criminal potentials require States to develop an organized, international response.

Although this conclusion was raised at the United Nations Congress, the attendees remained undecided about the nature of the required response. Some suggestions included an expansion of the treaty, and others suggested new multilateral negotiations (UN Information Officer 2010).

According to Markoff (2010), a group of cyber security specialists and diplomats, representing 15 countries (including South Africa) has agreed on a set of recommendations to the United Nations' Secretary General for negotiations on an international computer security treaty. In recent years, an explosion in cyber-crime has been accompanied by an arms race in cyber weapons, as dozens of nations have begun to view computer networks as arenas for espionage and warfare. The recommendations to the United Nations from the specialists and diplomats reflect an effort to find ways to address the dangers of the anonymous nature of the Internet, as in the case of the object of a cyber-attack misconstruing the identity of the attacker. Among the troubling issues is the existence of proxies. The report also suggests that *"the same laws that apply to the use of kinetic weapons should apply to state behavior in cyber space."* (Markoff 2010).

The signers of the report are major cyber powers and of other nations: the United States, Belarus, Brazil, Britain, China, Estonia, France, Germany, India, Israel, Italy, Qatar, Russia, South Africa and South Korea. From a legal perspective, a number of concerns can be identified, such as:

- lack of collaboration between industry and the defense environment;
- capacity of the legal fraternity to comprehend the complexity of the cyber environment and to deliver a verdict based on a thorough understanding of the facts;
- collaboration between countries and the agreements on protocols;
- lack of collaboration between State Departments on cyber warfare and cyber crime;
- lack of collaboration between municipalities, districts, regions and provinces; and
- lack of collaboration between urban and tribal authorities.

Another very successful intervention, Cyber security Awareness Program (CSAP), was the national collaboration effort between the Council for Scientific and Industrial Research (CSIR) and the University of Venda to empower remote rural communities who were not empowered to deal with these threats.

The current increase in broadband access throughout Africa may potentially increase the cyber related vulnerabilities drastically. As a result, a compromise of the integrity, confidentiality, authenticity or availability of the technological systems could have dramatic consequences regardless of whether it is the temporary interruption of connectivity, or a longer-term disruption caused by a cyber-attack (Warren, 2008).

To prevent innocent internet users from becoming victims of cyber-attacks, the CSAP were initiated to educate novice internet and technology users with regard to basic security in the Limpopo Province of South Africa. It is very clear that, cyber-crime is a reality that unfortunately often targets the individuals that do not know how to identify cyber frauds or how to keep their computers protected.

The CSAP program focus on educating beginner internet and technology users in basic computer security, and safe and secure online habits. The objective of this program was to prepare civilians for use of broadband applications and new applications for cyberspace. It aims to increase awareness and understanding of the dangers of the internet, whilst providing individuals with the necessary knowledge to make the right decisions in internet-related situations. This program is not a computer literacy course, but can be better defined as a self-defense course for internet users.

The target audience is computer users with working computer literacy and awareness and prior exposure to the internet. These individuals should not have any formal

computer related training, with the exception of computer literacy courses. For the time being, four user groups are identified:

- primary schools pupils.
- secondary school pupils.
- teachers or educators
- further education training (FET) college students,\
- company support staff, technical or non-technical; university students not studying towards a technical or information technology degree, and
- community members using the computer facilities of community centres.

The CSAP modules are divided into four main topics:

- Physical security – This training session addresses the importance of securing the physical computer in order to protect the computer user from potential cyber security dangers. This session addresses the physical protection of computers, laptops and mobile phones, as well as the importance of password protection.
- Malware and malware countermeasures – This training session touches on some of the different types of malware that can be encountered in cyberspace, and provide guidelines on how to protect a computer or mobile phone from these malware types.
- Safe surfing – This session addresses the guidelines that internet users should practice to ensure that the time they spend online are productive and secure. This session addresses internet surfing, email security, file sharing, copyright, downloads and storing in more detail.
- Social aspects of cyber security – This session addresses the safest way to use social networking, as well as the dangers that are associated with social media on the internet and cyberspace. This session also introduces social engineering, identity theft, cookies and cyber bullies.

This collaborative effort has made a significant impact to address the shortage of cyber security awareness in the South African rural areas and has made a definite contribution to the national security of South Africa.

Networked computers now control everything, including bank accounts, stock exchanges, power grids, the defense, the justice system and government. Networked computers also control all health records and crucial personal data. From a single computer an entire nation can be brought down. The authors are of the opinion that a series of regional conferences with all stakeholders involved and sponsored by private sector should be conducted. Significant progress has been made in South Africa, but commitments are required to draft a comprehensive Charter for South Africa and its unique situation.

## 6. Influence of cyber defense on the international position of Governments

The opinion of international defense departments officials is that cyber space is a domain available for warfare, similar to air, space, land, and sea (Wilson 2007). As a result, any Cyber-attacks can have either a direct or an indirect influence on the military. Accordingly, the defense departments need to consider the potential effects of an emerging military-technological revolution that may have profound effects on the way wars are fought. Growing evidence exists that over the next several decades, the military systems and operations may be superseded by new means and methods of warfare by new or greatly modified military organizations (Krepinevich 2003).

Technology and the Internet provide the ability to disseminate persuasive information rapidly in order to directly influence the decision making of diverse audiences. In addition, information can be regarded as both a weapon and a target in warfare. By incorporating the cyber domain in the cyber defense structure, a number of new aspects come into play that may have an influence on the manner in which the military reacts to cyber attacks (Wilson 2007):

- new national security policy issues;
- consideration of psychological operations used to affect friendly nations or domestic audiences; and
- possible accusations against the State of war crimes if offensive military computer operations or electronic warfare tools severely disrupt critical civilian computer systems, or the systems of non-combatant nations.

An example of the last bullet point: if wrongful acts are committed inside a country, the State can be held responsible for these acts, since the State is obliged to fulfill the interest of the entire international community. If a representative of a State organ or a private person acting on the State's behalf committed an act, the act may be attributed to the State (Article 3 ILC Draft Articles). The physical location of a computer or hardware used in a cyber-attack does not (and should not) allow for attributing that cyber-attack to a particular State. Such an assumption would be greatly unjustified, since a State does not carry the responsibility for actions of its residents operating hardware located within its territory.

The State, however, can be held responsible in the light of existing international law doctrine, for a breach of an international obligation. This obligation relates not to actions but to omissions, i.e. for not preventing that attack to take place. This interpretation is derived from the wording of Article 14(3) of the International Law

Commission (ILC) Draft Articles, which provides that a State may be held responsible for the conduct of organs of an insurrectional movement, if such an attribution is legitimate under international law. The State has therefore an obligation to show best efforts, and to take all *"reasonable and necessary"* measures in order to prevent a given incident to happen. The occurrence of this obligation was best reflected in the International Court of Justice (ICJ) case concerning the United States diplomatic and consular staff in Teheran. In its decision, the ICJ found that the overriding of the United States embassy in Teheran does not free Iran from the responsibility for that incident, although it also cannot be attributed to Iran (Kulesza 2010).

The State is also responsible for providing sufficient international protection from cyber attacks conducted by its residents from its territory. It is the duty of any State from whose territory an internationally wrongful act is conducted to cooperate with the victim's State and to prevent future similar harmful deeds. If the State itself is not capable of protecting the interests of another sovereign, it may also not allow for private persons acting from within its territory to inflict damage or create danger to that the other State while they are protected by its immunity. Under such an interpretation, Russia's denial to persecute the perpetrators of the attack against Estonia would constitute an internationally wrongful act, while Israeli involvement and punishment of the actors behind the Solar Sunrise attack on United States Airforce databases using the Texas Internet provider exonerates them from any international responsibility (Kulesza 2010).

In this light, it is therefore the obligation of the South African government to launch and support awareness projects to prevent these attacks from inside its borders. This also includes the establishment of a Computer Security Incident Response Team (CSIRT), as proposed in the draft South African Cyber security policy. Currently, South Africa is one of only a handful of countries that does not have a running CSIRT, putting South Africa in a disadvantaged position with regard to cyber-attack and defense (FIRST 2009).

## 7. The collaborative international cyber defense effort

Cyber warfare is an emerging form of warfare not explicitly addressed by existing international law. While most agree that legal restrictions should apply to cyber warfare, the international community has yet to reach consensus on how International Humanitarian Law (IHL) applies to this new form of conflict (Kelsey 2008). In particular, there is a need for an international consensus on the due diligence criteria which have to be fulfilled by a State in order to avoid international responsibility for failing to protecting other sovereigns from cyber-attacks conducted from its territory.

Another crucial issue would be to establish the standards for releasing a State from any international responsibility for not providing due diligence: would the adoption of specific provisions in national criminal laws be sufficient or would State authorities need to initiate a criminal investigation effectively. It should also be clarified whether a due diligence standard can be set *post factum* – after an attack had already taken place (Kulesza 2010). In South Africa, this is not possible.

A suggested approach to create Nation State responsibility in building a credible cyber system involves the following steps (Tiirmaa-Klaar 2010):

- developing a national strategy and making sure all agencies and major stakeholders follow it,
- establishing a national endorsement body for cyber security,
- national coordination mechanism,
- inclusion of all professional communities and private sector, and others in national cyber security effort, and
- providing necessary resources and institutional changes.

If all the States internationally can implement their own credible cyber system, cooperation on an international cyber defense level will be easier to realize. As an initial attempt to enable a more uniform cyber defense system, the European Commission is planning to impose harsher penalties for cybercrimes. Large-scale attacks in Estonia and Lithuania in recent years have highlighted the need for a stronger stance on cybercrime. Estonia, Lithuania, France and the United Kingdom also have longer sentences for such crime, and the European Commission is looking to harmonize practice across the member states. United States president Barack Obama has declared cybercrime to be a priority. In addition to stronger laws, the European Union is looking to set up a system through which member states can contact each other quickly to notify one another of attacks. That would help to build a picture of the scope of cybercrime (Geers ND).

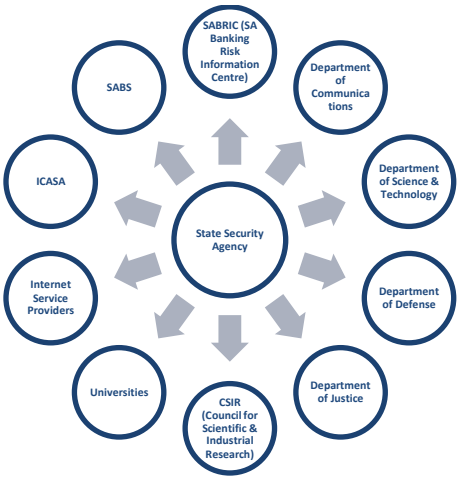
## 8. The collaborative national cyber defense effort

It is of immense importance that while the international collaborations and treaties are being considered, negotiated and agreed upon, governments must take the lead to implement holistic national stakeholder and community collaboration and awareness and then monitor progress on implementation. In developing countries to take-off is

unfortunately slow but if the following model can be implemented in South Africa, it will go a long way to ensure a safer cyber security environment for the country, the economic and defense sectors and its citizens.

The focus should be on four major categories:

- Public Sector: The security of all State Departments and their systems and sensitive information must be protected. The relevant South African institutions here are the state departments of State Security, Defense, Communication, Science and Technology, Police Services and Justice. The relevant State Agencies are ICASA (The Independent Communications Authority of South Africa), SABS (South African Bureau of Standards), and the State Security Agency. The New Year day heist of R42 million from the South Africa Postbank shows the serious flaws in the cyber security systems that still exist. (Mitchell 2012);
- Private Sector: Cybercrime has emerged as a significant contributor to economic crime losses in South Africa and is considered the fourth most common economic crime after the misappropriation of assets, bribery and corruption, and financial statement fraud. (Venter 2011). Relevant authorities here are the Internet Service Providers (including companies' internal security measures) and SABRIC **(**South African Banking Risk Information Centre).
- Military/National Security: The relevant authorities here would be the Department of state Security Department of Defense, the South African Police Services and CSIR **(**Council for Scientific and Industrial Research).
- Citizens: Education of citizens against cybercrime and capacitating them against cyber fraud are Universities who can take the responsibility to empower schools and FET colleges through awareness programmes. Over one million people become victims of cybercrime every day, while 14 adults suffer from cybercrime every second, according to the 2011 Norton Cyber Crime Report. Particular attention should be paid to vulnerable groups including youth, women, children, people with disabilities and the elderly to ensure the internet will be safe and secure for everyone. South Africa is ranked seventh by the Federal Bureau of Investigations Internet Complaints Centre (Da Silva 2011).
- The following is a graphical illustration of a possible South African model based on the aforesaid.




Only an effective strategy and action plans which stay abreast of technological advances will safeguard South Africa from becoming a victim of more cyber-crime and later cyber-warfare. This, however, will only be possible if one body is empowered to collect information from various sectors and advise and assist the various sectors in securing the cyber risks to South Africa.

**9. Conclusion**

The Internet has changed almost all aspects of human life, also including the nature of warfare. Every political and military conflict, every public sector entity, business in its broadest sense and now the general public has a cyber-dimension, whose size and impact are difficult to predict. *"The ubiquitous nature and amplifying power of the Internet mean that future victories in cyber space could translate into victories on the ground. National critical infrastructures, as they are increasingly connected to the Internet, will be natural targets during times of war. Therefore, nation-states will likely feel compelled to invest in cyber warfare as a means of defending their homeland and as a way to project national power"* (Geers ND).

The international scope of the Internet and wide reach of technological usage has a tremendous impact on the nature of war and crimes globally. This article gave an indication of the impact of technological revolutions on warfare, the South African legislative system affecting warfare and cyber war, all relevant communities and the two-fold need for international cyber defense collaboration and urgent national awareness campaigns and collaboration.

**References**


Crow, K. (2002). *Collaboration.* Available from: http://www.npd-solutions.com/ collaboration.html (Accessed 23 May 2011).

Da Silva, I. S. (2011). *Cybercrime increase worries, vulnerable groups targeted.* Available from: http://m.bizcommunity.com/Article/196/19/64855.html (Accessed 1 February 2012)

Dhlamini IZ. C*yber Security Awareness Initiatives in South Africa: A Synergy Approach.* Avalable from http://researchspace.csir.co.za/dspace/bitstream/10204/5941/1/Dlamini_2012.pdf (Accessed 12 June 2013)

ECT Act (*Electronic Communications and Transactions Act No 25 of 2002*). (2002). Available from: http://www.acts.co.za/ect_act/ (Accessed 10 October 2010).

Ferrier International, (2011). "Business Against Crime South Africa on the Latest Crime Statistics", [online], http://ferrierinternational.com/business-against-crime-south-africa-on-the-latest-crime-statistics/, (accessed on 05 /03/2011).

FIRST. (2009). *FIRST: Teams around the world.* Available from: http://www.first.org/ members/map/ (Accessed 14 October 2010).

Gardner, F. (2009). *Nato's cyber defence warriors.* BBC News. Available from: http://news.bbc.co.uk/ 2/hi/europe/7851292.stm (Accessed 22 September 2010).

Geers, K. (ND). *Cyber Defence.* Available from: http://www.vm.ee/?q=en/taxonomy/term/214 (Accessed 22 September 2010).

Giles, J. (2010). *How will the PPI Bill affect you?* Available from: http://www.michalsonsattorneys.com/how-will-the-ppi-bill-affect-you/2586?gclid=COXtlKz6y KQCFcbD7QodHzHJDg (Accessed 10 October 2010).

Government Gazette. (2003). Vol. 451 Cape Town 15 January 2003 No. 24250. *No. 54 of 2002: Promotion of Access to Information Amendment Act, 2002*.

Grobler, MM; Dhlamini IZ. National Security Impact Cyber Security Awareness – SAFIPA Support. July 2011

ITWeb, (2012) *The Department of Communications (DOC) will present the National Cyber Security Policy Framework for South Africa to Cabinet in March.* .Available from: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=23020:sa-to-announce-cyber-security-policy-in-march&catid=48:Information%20&%20 Communication %20 Technologies&Itemid=109 (Accessed 1 February 2012)

Kelsey, JTG. (2008). *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.* P1427. Available from: http://heinonline.org/HOL/Landing collection=journals&handle=hein. journals/mlr106&div= 64&id=&page= (Accessed 22 September 2010).

Krepinevich, AF. (2003). *Keeping pace with the military-technological revolution.* Available from: http://www.issues.org/19.4/updated/krepinevich.pdf (Accessed 22 September 2010).

Kulesza, J. (2010). *State responsibility for acts of cyber-terrorism.* 5th GigaNet symposium Vilnius, Lithuania.

Markoff, J. (2010)**.** *Step Taken to End Impasse Over Cybersecurity Talks.* Available from: http://www. nytimes.com/2010/07/17/world/17cyber.html?_r=1 (Accessed 8 October 2010).

Merriam-Webster. (2011). *Collaborate.* Available from: http://m-w.info/dictionary/collaboration (Accessed 23 May 2011).

Mitchell, N. (2011) *R42m Postbank theft indicative suggests poor controls* Available from: http://www.politicsweb.co.za/politicsweb/view/politicsweb. Accessed February 1, 2012

NATO. (ND). *Defending against cyber attacks.* Available from: http://www.nato.int/ cps/en/natolive/ topics_49193.htm (Accessed 22 September 2010).

Niblett, G. (2010). *Why the Private Sector is Key to Cyber Defence.* Available from: http://www.slideshare.net/INFOSEC_Maven/why-the-private-sector-is-key-to-cyber-defence (Accessed 23 May 2011).

Owen, RS. (2008). *Infrastructures of Cyber Warfare.* Chapter V. In: Janczewski, L. & Colarik, AM. *Cyber warfare and cyber terrorism.* Information Science Reference: London.

*PAIA Act (Promotion of Access to Information Act No 2 of 2000 as amended)*. (2000). Available from: http://www.dfa.gov.za/department/accessinfo_act.pdf (Accessed 10 October 2010).

Paganini P. (2012) *Cyber Security Policy Framework for South Africa.* http://www.cybersafety.co.za/?p=566 (Accessed 16 June 2013)

Republic of South Africa. (2010). *Protection of Personal Information Bill.* Available from: http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf (Accessed 10 October 2010).

*RIC Act (Regulation of Interception of Communications and Provision of Communication-related information Act.* (2002). Available from: http://www.acts.co.za/ric_act/whnjs.htm. (Accessed 10 October 2010).

Roodt, JHS, Oosthuizen, R. & Jansen van Vuuren, JC. (2010). *Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces: Analysis and Synthesis from a Through-Life Capability Management Perspective.* Available from: http://researchspace.csir.co.za/dspace/bitstream/10204/4848/1/Van%20Vuuren1_2010.pdf (Accessed 23 May 2011).

*SA Constitution*. (1996). Available from:

http://www.info.gov.za/documents/constitution/index.htm (Accessed 10 October 2010).
RSA, (2011). "Cyber Security Awareness Month Fails to Deter Phishers", [online], http://www.rsa.com/solutions/consumer_authentication/intelreport/11541_Online_Fraud_report_1011.pdf, (accessed on 22/04/2011).
South African Police Service, (2011). *"Crime Report 2010/2011: South African Police Service (SAPS)"*, [online],http://www.saps.gov.za/statistics/reports/crimestats/2011/crime_situation_sa.pdf, (accessed on 19/08/2011).
Tiirmaa-Klaar, H. (2010). *International Cooperation in Cyber Security: Actors, Levels and Challenges.* Cyber security 2010, Brussels, 22 September 2010 (Conference).
UN Information Officer. (2010). *Delegates Consider Best Response to Cybercrime as Congress Committee - Takes Up Dark Side of Advances in Information Technology.* Available from: http://www.un.org/News/Press/docs/2010/soccp349.doc.htm (Accessed 10 October 2010).
Venter, K (2011). *Cybercrime forces Companies to their Knees.* Available from: http://www.observer.co.za/stories/cyber-crime-forces-companies-their-knees (Accessed 1 February 2012)
Warren, MJ. (2008). *Terrorism and the internet.* Chapter VI. In: Janczewski, L. & Colarik, AM. *Cyber warfare and cyber terrorism.* Information Science Reference: London.
Warren, M., 2008. *Cyber warfare and cyber terrorism*. In: A. COLARIK and L. JANCZEWSKI, eds, *Terrorism and the internet.* London: Information Science Reference
Williams, G. & Arreymbi, J. (2007). *Is cyber tribalism winning online information warfare?* ISSE/ SECURE 2007 Securing Electronic Business Processes (2007): 65-72, January 01, 2007.
Wilson, C. (2007). *Information Operations, Electronic Warfare and Cyberwar: Capabilities and related policy issues.* CRS report for congress. Available from: www.fas.org/sgp/crs/natsec/ RL31787.pdf (Accessed 17 September 2010).