# Cyber Crime and Cyber Warfare with International Cyber Collaboration for RSA – Preparing Communities

**Dr Marthie Grobler, Joey Jansen van Vuuren', Dr Jannie Zaaiman[2]**

**Council for Scientific and Industrial Research, Pretoria, South Africa[1]**
**University of Venda[2]**

## ABSTRACT

The international scope of the Internet and wide reach of technological usage requires the South African legislative system to intersect largely with the application and implementation of international legislation. One of the problems associated with the technological revolution is that cyberspace is full of complex and dynamic technological innovations that are not well suited to any legal system. A further complication is the lack of comprehensive treaties facilitating international cooperation with regard to cyber defense. The result is that many developing countries is particular, are either not properly aware, not well prepared, nor adequately protected by both knowledge and legislation, in the event of a cyber-attack on a national level. This article will address this problem by looking at the impact of technological revolution on warfare in a developing country. The article will evaluate the South African legal system with regard to international cyber defense collaboration. The article addresses cyber security and cyber warfare acts occurring on a significant scale, and briefly touches on proposed Cyber security policies for South Africa.

South Africa does not have a coordinated approach in dealing with Cyber security, and the various structures that have been established to deal with Cyber security issues are inadequate to deal with the issues *holistically.* It is further noted that 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 Cyber Warfare in an attempt to assist governments from developing countries to prevent their countries to be used as targets for either Cyber Crime or Cyber Warfare.

## 1. INTRODUCTION

The international scope of the Internet and global reach of technological usage requires all legislative systems to address issues related to the application and implementation of international legislation. The complexities of cyberspace and the dynamic nature of technological innovations require a cyber-defense framework that is not well suited to any current legal system. This article will address the problem posed by the disjoint relationship between modern cyber space, cyber warfare and traditional legislation. As a starting point, cyber warfare is defined for the purpose of this article 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. (Williams & Arreymbi 2007).

This article will look at some international technological revolutions, evaluate the South African legal system, address international cyber warfare and the influence of cyber defense on the international position of the South African Government and 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

## 2. THE EVOLUTION OF WARFARE INTO CYBER WARFARE

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.

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. *"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 but, 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.

## 3. THE NEED FOR CYBER DEFENSE COLLABORATION

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. 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. It is necessary for organizations and for nations to collaborate in cyber defense activities. The key to these collaboration efforts is open communication and a willingness to give and accepts inputs from others.

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).

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. It is suspected that the increased bandwidth will also lead to an increase in cyber attacks on the civil networks in the country. The South African DoD is well aware of this threat. (Roodt, Oosthuizen & Jansen van Vuuren 2010). It is necessary to evaluate the possibilities of the South African legal system with regard to cyber defense collaboration.

## 4. THE SOUTH AFRICAN POSITION ON INTERNATIONAL CYBER DEFENSE COLLABORATION

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. Cyber terrorists have the capability to shut down South Africa's power, disrupt financial transactions, and commit crimes to finance their physical operations. Therefore, South Africa needs a national cyber defense system to which everybody must obey.

## 5. LEGAL ASPECTS

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, (PAIA Act 2000). 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. (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. (Giles 2010).
- *Information Bill* that is meant to replace an existing piece of legislation, the Protection of Information Act of 1982. (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. In combination with this treaty, all the

South African bills and acts play an important role in the collaboration of South Africa with other nations on cyber defense.

## 6. CURRENT COLLABORATION EFFORTS

Cyber crime damages economies and State credibility. It has become crucial for nations to collaborate in order to protect themselves from cyber warfare. 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. Over the last five years, South Africa focused on modernizing and expanding its information technology sector and structures.

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

The signers of the report identified a number of concerns, such as:

- lack of collaboration between industry and the defense environment;
- capacity of the legal fraternity to comprehend the complexity of the cyber environment;
- collaboration between countries and the agreements on protocols;
- lack of collaboration between State Departments on cyber warfare;
- lack of collaboration between municipalities and provinces; and
- lack of collaboration between urban and tribal authorities.

Another successful intervention, the Cybersecurity 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 CSAP program focus on educating beginner internet and technology users in basic computer security, and safe and secure online habits. 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.

The CSAP modules are divided into four main topics:

- Physical security – It addresses the importance of securing the physical computer to protect the computer user from potential cyber security dangers.
- Malware and malware counter measures – This session touches on the different types of malware that can be encountered in cyberspace, and advice on how to protect computers or mobile phones from these malware types.
- Safe surfing – This session addresses guidelines that internet users should practice to ensure that time spend online are productive and secure.
- Social aspects of cyber security – This session addresses the safest way to use social networking as well as the associated dangers.

This collaborative effort has made a significant impact to address the shortage of cyber security awareness in the South African rural areas. 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. Significant progress has been made in South Africa.

## 7. INFLUENCE OF CYBER DEFENSE ON THE INTERNATIONAL POSITION OF GOVERNMENTS

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. With the cyber domain, 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.

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. 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.

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. (FIRST 2009).

## 8. WORKING TOWARDS INTERNATIONAL CYBER DEFENSE COLLABORATION

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). Another crucial issue would be to establish the standards for releasing a State from any international responsibility for not providing due diligence. (Kulesza 2010).

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. (Geers ND).

## 9. WORKING TOWARDS NATIONAL CYBER DEFENSE COLLABORATION

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.

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. (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)
- Military/Security: The Department of Communications (DOC) will present the National Cyber Security Policy Framework for South Africa to Cabinet in March 2012. (ITWeb 2012)
- Citizens: 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. (Da Silva 2011)

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.

## 10. 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)

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).

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 Page?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).

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).

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).