The impact of the increase in broadband access on South African national security and the average citizen.

JC Jansen van Vuuren[1], J Phahlamohlaka [1] and M Brazzoli[2]

[1] Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[2]Government Information Technology Officer in the Defence Secretariat, Department of Defence, Pretoria, South Africa
jjvvuuren@csir.co.za
jphahlamohlaka@csir.co.za
gito@mil.za

Keywords: Cyber Warfare, National Security, Broadband access, Rural areas, Home Battlefield, Security Threat Analysis.

Abstract: South Africa is the entry point to the African continent and with the impending increase in broadband access from 120 Gbps to 12 Tbps over the next 2 years, it could in future be used as a hub for launching cyber warfare type attacks on the rest of the world. In addition, there are arguments that RSA's strong ties with China could place it at high risk of cyber war attacks. Presently because of very low broadband penetration in South Africa and in Africa, chances of it being used to launch attacks to other countries are limited. However, the fact that it will be hosting the 2010 FIFA World Cup increases the vulnerabilities as was experienced with previous soccer world cups in other countries. In either case there are national security implications associated with an increase in broadband access. In addition the compromised PC's of citizens could in future be used as a hub for launching cyber warfare type attacks on the rest of the world. This in turn will pose a national security threat not only to South Africa but also to the rest of the world. The central argument in this paper is that the exponential increase in internet broadband will result in an increase in security threats that will also take the battlefield to the home of the average citizen in rural South Africa. The paper adopts an argumentative analytical approach with the intention to sensitise all nations on issues of national security. We draw on the South African case to demonstrate the potential impact on South Africa that could follow the planned increase in broadband access in Africa as well as on the average RSA citizen. A national security generic framework is used to analyse these threats and the impact on the average citizen. In conclusion the paper proposes the ways of addressing the threats flowing from the security threat analysis.

1. Introduction

South Africa is the entry point to the African continent and with the impending increase in broadband access from 120 Gbps to 12 Tbps over the next 2 years, it could in future be used as a hub for launching cyber warfare type attacks on the rest of the world. In addition, there are arguments that RSA's strong ties with China could place it at high risk of cyber war attacks (Stiennon 2009). Daved, CISSP of Naval Warfare Command indicates that all these developments moved the battlefield to the average citizen's home as it was observed that attackers can take over a brand new computer in 30 seconds after connecting to the internet (Armistead 2007).

Presently because of very low broadband penetration in South Africa and in Africa, chances of it being used to launch attacks to other countries are limited. However, the fact that it will be hosting the 2010 FIFA World Cup increases the vulnerabilities as was experienced with previous soccer world cups in other countries.(Symantec 2009). In either case there are national security implications associated with an increase in broadband access.

This paper adopts an argumentative analytical approach with the intention to sensitise all nations on issues of national security. We draw on the South African case to demonstrate the potential impact on South Africa that could follow the planned increase in broadband access in Africa as well as on the average RSA citizen.

With the above as the background, the key question that this paper addresses is the following:
In what way will the increase in internet broadband impact on cyber warfare in RSA rural areas and what are the associated security threats to national security and the average citizen?

In addressing the above central question, the paper first presents a background on broadband access in South Africa and the anticipated exponential increase in threats due to the access. A national security generic framework is then used to analyse these threats. Using this framework the negative impact envisaged to be associated with the rollout of this broadband to South African rural areas as well as the influence on the average RSA citizen is addressed; as indications from the literature are that this broadband rollout could result in the battlefield moving to the home. In conclusion the paper proposes ways of addressing the security threats flowing from the above analysis.

2. Broadband access in South Africa; a brief literature survey

South Africa regards access to ICT and its benefits as a universal right for all its citizens. Access to broadband within the South Africa context is understood to form part of this right. According to the Draft Broadband Policy for South Africa (September 2009) ICT have to form part of the basic need priorities in order to increase uptake and usage and needs to be promoted at house hold level to form part of socialisation within the family structure. In order to reach a knowledge economy, which drives the development and usage of ICT, households and business should continuously be exposed to the use and benefits of ICT. The policy further identifies access to broadband by needy persons as essential to social development in the same manner as access to job opportunities (Department of Communications 2009). From a South African persprective, It could be argued that the majority of the needy persons live in rural areas (Aliber 2003).

While the intention of the broadband policy is well meaning - it is important to recognise that the same technologies that provide access to information and services through the broadband, would also allow potential criminals to electronically enter an average citizen's home via the personal computer. With this commitment reflected through the broadband policy, the government recognise its role as the provider of cyber security as part of national security.

South Africans will have access to an increased broadband within the next 18 months. The current as well as the anticipated increase in capacity of the undersea cables around the African continent shown in Figure 1 will enable the increase in broadband access. Currently there are submarine cable SAT-3/WASC and South Atlantic 3/West Africa Submarine Cable bandwidth capacity linking South Africa with Spain and Portugal and several West African states. The current SAT3-SAFE system is 120 Gbps (MyBroadband 2009). The SAFE cable is also part of the same system and provides the link between South Africa and Asia with a capacity of 130 Gbit/s. This total capacity of 2.5 Gbit/s wavelengths will soon be increased to 10 Gbit/s . By 2011 a total of 12.28 Gbit/s bandwidth will be available.

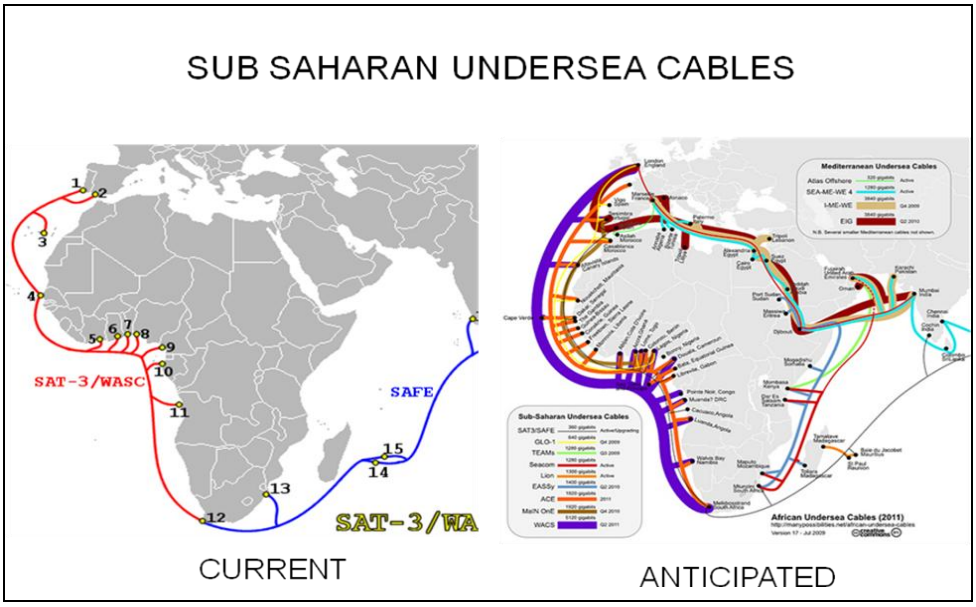

Figure 1: Increase in Sub-Saharan undersea cables

Although the increase in broadband holds many positive socio-economic promises, Brett Myroff of Sophos SA indicated that more connections will result in higher cyber crime due to the more opportunities for computers to be exploited (Doyle 2009). Costin uses the example of South Korea who was hit the worst by the Slammer worm in 2003, because they already had high speed internet links at home. It was not that common to have these type of connections in other countries at that stage (Doyle 2009; IT News Africa 2009a). “In addition, there seems to be a link between the Internet speed and software piracy rate.

Symantec’s annual Internet Security Threat Reports have shown that countries introducing pervasive broadband services experience an immediate increase in threats, as cybercriminals take advantage of breaches and vulnerabilities arising from inadequate security. This has been witnessed in countries such as Brazil, Turkey and Poland. South Africa is likely to follow this trend once new undersea cables have been successfully installed (IT News Africa 2009a).

3. Classification of cyber threats

For purposes of this paper, we adopt a classification of cyber crimes published by McConnel in a 2000 report titled ‘*Cyber crime and punishment? Archaic laws threaten global information*’ (Aitoro 2008). In the report, they classify the crimes into four categories: data crimes, network crimes, access crimes and related crimes. In a high speed broadband enabled cyber space and global contexts, these crimes become threats to national security. A brief description of each of the threats is presented next, followed by an analysis of the South African situation using these categories within a national security context.

Data threats

- Data Interception: Interception of data in transmission.
- Data Modification: Alteration, destruction, or erasing of data.
- Data Theft: Taking or copying data, regardless of whether it is protected by other laws, e.g., copyright, privacy, etc.

Network threats

- Network Interference: Impeding or preventing access for others. The most common example of this action is instigating a distributed denial of service (DDOS) attack, flooding Web sites or Internet Service Providers. DDOS attacks are often launched from numerous computers that have been hacked to obey commands of the perpetrator.

- Network Sabotage: Modification or destruction of a network or system.

Access threats
- Unauthorized Access: Hacking or cracking to gain access to a system or data.
- Virus Dissemination: Introduction of software damaging to systems or data.
- Aiding and Abetting: Enabling the commission of a cyber crime.

Related threats
- Computer-Related Forgery: Alteration of data with intent to represent as authentic.
- Computer-Related Fraud: Alteration of data with intent to derive economic benefit from its misrepresentation.

4. National security analysis framework.

The analysis of the impact of the increase in broadband access on South African national security and the average citizen using the threat categories presented in the last section necessitate a brief introduction to the concept of national security**.**

David Jablonsky (2001) defines national security as that part of government policy whose objective is to create national and international political conditions that are favourable to the protection or the extension of vital national values against existing or potential adversaries. Jablosnky defines national security in terms of the respective elements of the power base of the state and the priorities that are seen as of vital and/or national interest. He categorises the elements of national power into natural determinants and 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. Jablonky's description of the concept of national security in terms of the elements of national power could be regarded as a major contribution to national security theory, eventhough the literature indicates that there are as many definitions of the concept as there are scholars of national security. For this reason, we also adopt in this paper the definition of national security as formulated by Phahlamohlaka (2008), who defines national security as: *The provision of security to the state and of human security to its citizens as well as the protection of national and human interests together with state borders through the projection of national power*.

To understand national security, one must understand the elements of national power and how they interrelate. Jablonsky (op cit.) presented a formula to develop a rough estimate of "perceived" national power - focused primarily on a state's capacity to wage war:

Pp = (C + E + M) x (S + W) in which:
Pp = Perceived power
C = Critical mass: population and territory
E = Economic capability
M = Military capability
S = Strategic purpose
W = Will to pursue national strategy

One of the lessons from this formula is that the more tangible elements (C, E, M) that can be quantified objectively also involve varying degrees of subjective qualifications. The formula demonstrates that national power is a product, not a sum of its components. It thus serves as a reminder of the importance of relational and contextual aspects. In demonstrating the usefulness of this formula, reference is made to how the United States discovered in Vietnam that no matter how large the sum of the more tangible economic and military capabilities in relation to an adversary, their utility is determined by the intangibles of strategic purpose (S) and national will (W).

5. Analysis of the cyber security threats

In the following section the elements of national power described above are used to analyse the cyber security threats associated with the broadband access as cited in the literature. In this way, the main research question raised in the introduction is systematically addressed within a national security framework.

5.1 Natural determinant analysis

5.1.1 Geography and resources

Africa has approximately 100 million PC's, of which 80% are infected with some kind of malware - compared to 30% in the UK. The shipment of outdated PC's to Africa pose a security threat to the continent as old and outdated software is very vulnerable to attacks because security updates are not available anymore (Michael 2009).

According to the Microsoft's Technical teams report of the first semester 2009, computers in Africa have in average less infections per 1000 executions of the Malicious Software Removal Tool than China and South America. Figure 2 below gives a presentation of the latest Infection rates of differing regions based on the number of infected computers discovered per 1000 executions of the Malicious Software Removal Tool (MSRT) of Microsoft . E.g. A region with lighter colour will have less infected computers (7-10). From this report it can be seen that high infections are already visible in some countries in Africa (Microsoft 2009).

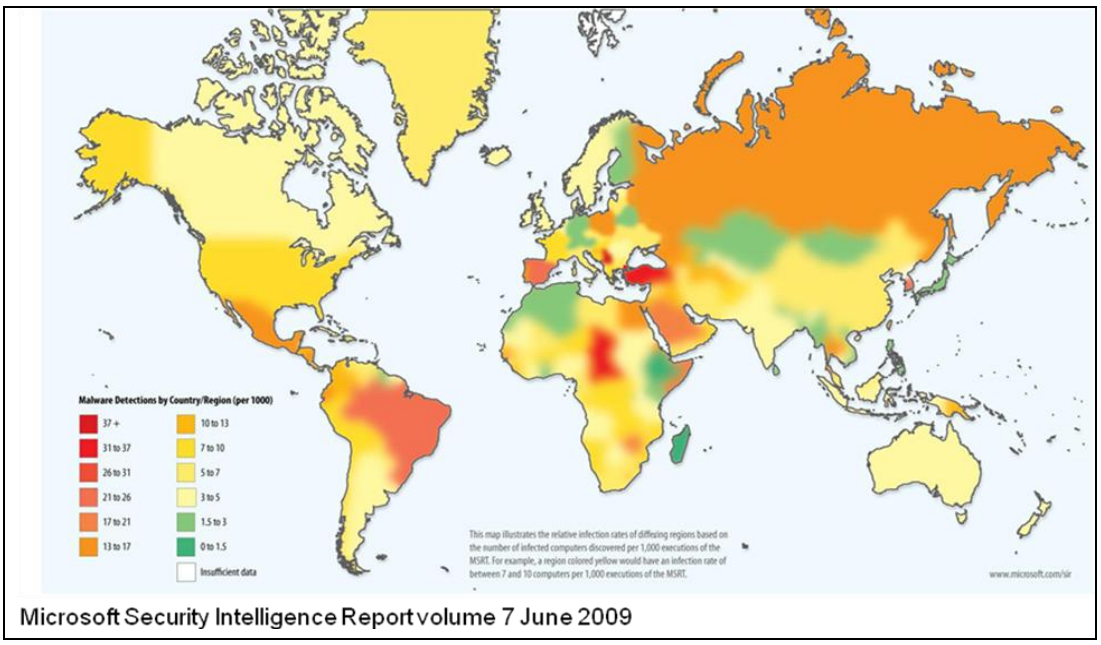

Figure 2: Worldwide Infections of computers

The current low broad band penetration in Africa resulted in low malware distribution rates as shown in figure 3 below.

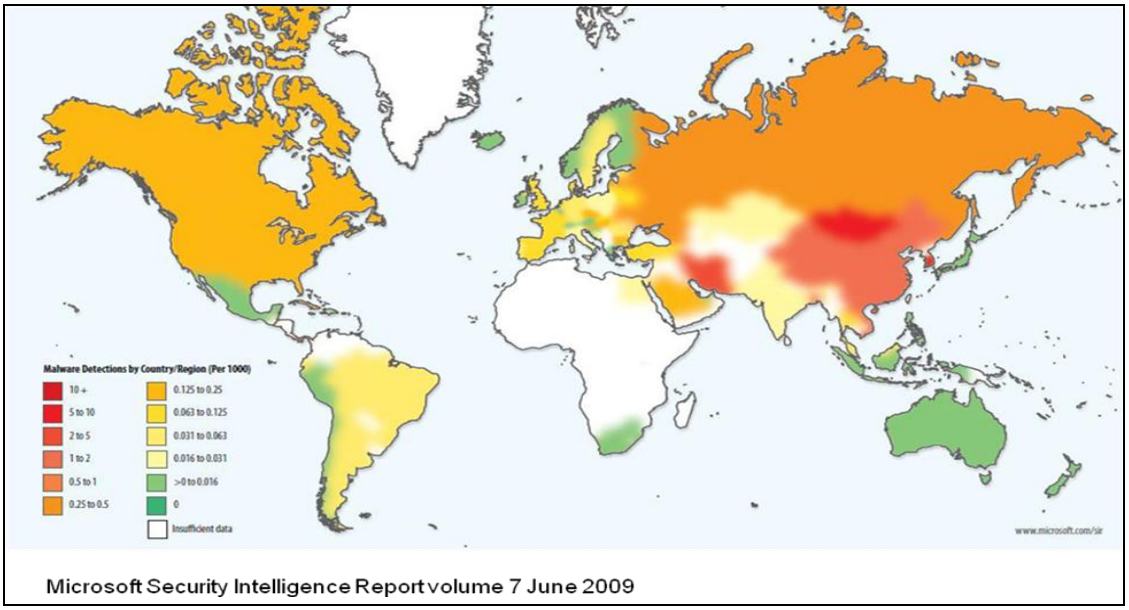

Figure3: Malware distribution sites per 1,000 Internet hosts for locations around the world in 2009

Due to the general poverty situation throughout the continent, people cannot afford to buy antivirus software. As a result pirated software is used, making regular software updates impossible (WATCH 2009). Ultimately computers become highly vulnerable to infections. Wuest of Semantic Labs (2009) predicted that the increased access to broadband will result in internet users being attacked up to a thousand times a day, while larger websites can experience up to one million attacks per day (Symantec 2009).

5.1.2 Population

In the past year, the Internet user base in South Africa has seen its highest rate of growth since 2001, increasing by 12.5% to 4,5-million. There are currently 67 million internet users in Africa. That is 6.8% of the total population. Worldwide the internet users are 29% of total population. Compared to the world, Africa currently only has 3.9% of the total internet users in the world. The new broadband access could see millions of new users connecting to the Internet via unprotected devices. (Internet_World_Stats 2009)

Wuest states that “Because broadband penetration has been so low thus far, the introduction of improved broadband access this year is likely to bring a major increase in threats to Internet users,” said Wüest. “And you can expect to be attacked perhaps a thousand times a day. Larger websites might see up to a million attacks daily. (Symantec 2009).

Botnets are weapons in the hands of bad operators. A botnet's originator can control a group of compromised networked computers remotely, usually for wicked purposes. Naxal watch state that if PC’s can be related to people and if every infected PC were a person this can be the worst pandemic in the history of the word. (WATCH 2009).” We can have armies of networked but compromised computers in the homes of average citizen, posing serious threats to a country’s national security

5.2 Social determinants

5.2.1 Economical

Although access to broadband is still very low in South Africa it did not prevent hackers to con the public in South Africa to reveal their vital personnel information. The Public is warned on a regular

basis of fraudulent emails send to gain these information (SAPA 2009). In an example a large number of citizens lost money due to phishing attacks where a “spoofed” email was send from a forged email address indicating the South African Revenue Services (SARS) banking details has changed and payments must be made in the another address. A link in the email directed citizens to a fake website where their personnel details such as username, password and credit card details are requested. Warnings on this scam were sent to the public and were also published on the official website of SARS.

South Africa would become more vulnerable in 2010 to these cyber threats as history has shown that the country hosting the soccer world cup is attacked more than other countries. In 1998 a World Cup-themed malware wiped out hard drives and with the next world cup in South Korea and Japan was attacked by the VBSChick-F virus. South Africa already experienced the first attacks in June 2009 with an email worm Sixem-A that disables anti-virus products, attempts to download more malware, and also forwards itself to e-mail addresses saved on the victim's computer (McMillan 2009).

The first of the scamming attacks already started with the email advertisement where SAA the South African airline offers 200 people a free opportunity and all expenses paid trip to watch the first two games of the FIFA 2010 soccer in South Africa. The only request to the bidder was to send their personnel information to a certain email address (Dirro 2009).

Bank serve (the company responsible for all bank clearances in South Africa) which experienced a network problem in October 2009 and 120 000 transactions failed in one day, gave an indication of what a catastrophe it would be if a DOS could attack it. The problem resulted in payments debited against customer’s accounts not transferred to vendors. Bank serve handles 2.5bn transactions worth R8tm per year (Carte 2009). If an attack were to happen, business to business transactions would be impossible, nobody will be able to use ATM and in addition no salaries will be paid, except by resorting to manual system.

5.2.2 Political

There have been increases in reports received of cyber attacks and network infiltrations that appear to be linked to national states and political goals. Politically-motivated cyber assaults have surged in the US, France, Russia, Israel and China, according to findings of the latest McAfee's report. (DeWalt 2009). In addition the report discussed illustrations of politically-motivated assaults and reveal how this crossfire among different nations will affect the private sector.

Cyber attacks with political connotation were seen in Estonia, Georgia and South Korea in the last few years. 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 (Hankyoreh 2009)

Advanced free fraud is often used in scams where political figures names are used in requests to advance money to accounts with a promise that they would be handsomely rewarded. Recently the names of former president Nelson Mandela, former ANC Chief Whip Tony Yengeni and Archbishop Emeritus Desmond Tutu have all surfaced in 419 email scams originated in Nigeria. Last year, fraudsters used the Nelson Mandela Foundation (NMF) name to get donations via the internet. (Nkuna 2009).

Cyber attacks are also used to discredit political parties through rumours that will indicate instability in the country. The Congress of South African Trade Unions (COSATU), the African National Congress (ANC) alliance partner, had been victims of such an attempt when a scam email was send with the information that they will soon embark on a nationwide strike. This followed a recent attack on the

ANC's website where the party was embarrassed when pornographic advertisements appeared on their website (IT News Africa 2009b).

5.2.3 Military

"Fast increasing broadband penetration such as we are seeing locally can be dangerous, as many South African companies are not security-savvy enough to be able to thwart attacks successfully," says Gordon Love, regional director for Africa at Symantec. He added that "Newly-connected computers that are unprotected will be rapidly compromised and used to launch attacks on other computer systems across the globe" (Doyle 2009)

Several countries across the world are busy preparing themselves for cyber wars (DeWalt 2009). SA could also face cyber war. The founder of Threat Chaos and IT-Harvest, Richard Stiennon. Indicated that SA's strong ties with China places it at high risk of cyber war attacks. He further explained that, despite the low penetration of Internet connectivity, SA has a high risk of becoming a victim in global cyber warfare.

Ans seen in 2009 during the conflict between Georgia and Russia over the Georgian province of South Ossetia, the Military also consider using cyber attacks on their enemies. 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. Although attackers and activities showed every sign of being civilian and there was little or no direct government involvement, the attack were carried out very fast and was timed to coordinate with military activities and demonstrated knowledge of the military plan (Jackson 2009).

These cyber opportunities and threats will result in moving the war to the civilians' households using their personal PC's. Compromised armies of machines could be used to launch attacks on the enemies' infrastructure with or without the knowledge of government or the military.

5.2.4 Psychological

The Georgian attack done by supporters and civilians can be seen as a relatively decent example of cyber warfare combining PSYOPs (psychological operations) and self-mobilization of the local Internet users by spreading "For our motherland, brothers!" or "Your country is calling you!" hacktivist messages across web forums. The attackers defaced the presidential website, and while keeping up the DDoS attack, played an integrated slide show portraying President Saakashvili next to Hitler, with identical images of both Saakashvili and Hitler's public appearances. This act can be seen as a real PSYOPs attack as a normal script kiddy or attacker will not even understand the PSYOPs effect of coming up with identical gestures of both parties and integrating them within the defaced sites. Information like these must have been distributed by knowledgeable sources. These sources only forgot a simple rule of engagement in such a conflict – they forwarding the risk responsibility of the attack to each and every Russian or Russian supporter that ever attacked Georgian sites using publicly obtainable DDoS attack tools in a coordinated fashion (Danchev & Naraine 2008).

5.2.5 Informational

Dan Kuehl (2007, p1) is spot on in his analysis when he says "where we need the greatest improvement is in the development of information 'strategists', those who are able to coordinate and exploit the contribution of the information component of power and the synergies it offers to the other elements of national power". It is increasingly difficult for states to attain their desired levels of information superiority in cyber space.

South Africa identified the need for ICT access to all its citizens as indicated in the Draft Broadband Policy of September 2009. This must be promoted on all levels of the community and everybody must be exposed to the use and benefits of ICT. Along with increased broadband access and connectivity by all its citizens goes the possibilities of malicious code that could overwrite the infected PC's hard drive which could result in massive loss of data and information (Kebbs 2009). Attacks with similar malware, used in the cyber attack on the US and Korean government and commercial Web sites in 2009, can have serious impact on service delivery and information required by the citizens. If these malicious codes include instructions that will overwrite the PC's infected hard drives, it will spell out disaster for many tens of thousands of PCs. Citizens, communities and businesses would be severely affected in this process.

6. Conclusion.

The central question that this paper addressed was the following:

In what way will the increase in internet broadband impact on cyber warfare in RSA rural areas and what are the associated security threats to national security and the average citizen?

We answered this question by framing our analysis in accordance with the elements of national power argued for by David Jealousy. Drawing from international and national sources as well as from historical and recent examples, ways in which an increase in internet broadband would impact on cyber warfare in South Africa were described. Emerging from the analysis were also the associated security threats to national security as well as the security of the average RSA citizen.

Table 1 below gives a matrix of threats that will have an influence on national security. The reader will notice from the analysis in section 5 that the table is not exhaustive. Evidence on all the categories reflected in the matrix is not discussed in this paper.

Table 1: Summary of threats in national security analysis framework

		Data threats	**Network threats**	**Access threats**	**Related threats**
Physical determinants	**Geography**	Regulation of internet LAW Rural awareness phishing	Regulation of internet LAW	Regulation of internet LAW Rural poverty no antivirus	Regulation of internet LAW Urban commission cyber crime more
	Resources	Technological advancement Broadband Access	Technological advancement Broadband Access	Technological advancement Broadband Access	More or less resources equal impact, need capability
	Population	Size give potential access to broadband	Size	Size More computer= higher distribution of viruses	Immaterial of size need capability
Social determinants	**Economic**	Confidential financial information used for theft Modification bank accounts SARS modification wrong account rebates	Transaction failures, Web sites down Economic catastrophe	Passwords, Access to Confidential financial information used for theft SARS returns Disable servers of companies. No service to citizens	Access to Confidential financial information used for theft SARS returns Electronic signatures Home affairs? Access to Confidential financial information used for theft SARS returns
	Military	Espionage Confuse and conduct PsyOps	Disable command and control		
	Political	Discredit party by untruths	Discredit party by lack of service		

	Psychological		Influence citizens with messages placed on defaced websites		
	Informational			Destroy citizens valuable data	

South Africa needs a dedicated strategy to be prepared for this cyber war. The USA already embarked on a program to emphasise these Cyber issues. President Obama already announced that he 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, who will report directly to the president. He further stated that the USA needs "Well coordinate efforts across the federal government, to implement a truly national cyber security policy and tighten standards to secure information, from the networks that power the federal government to the networks that you use in your personal lives." (Aitoro 2008).

There is no short cut to mitigating the threats highlighted above. For this reason, we propose a long term research, development and innovation approach linked to broadband rollout in South Africa. Some of the threats identified above can be addressed by determining the most important security risks of the current broad band wireless networks implemented in rural communities. Research indicates that in future, mobile phones will be the most important tools for connectivity in the rural areas as there are no fixed telecommunication lines. Security instructions can have an effect on all the participants in the wireless network. These will include the government sector as well as schools and community centres. These security risks can be determined by monitoring the wireless networks in a pilot area (e.g. set up a botnet to determine what intrusions and the number of each appearing on the mobile wireless network). The most important security risks will be determined by monitoring a pilot area for security intrusions in one of the rural communities. This research will then be expanded by identifying the most important security risks using mobile phones for connections to the internet.

This research information could be used:

- as input for cell phone manufacturers (e.g.) Nokia to include better security in cell phone operating systems to try and prevent these intrusions.
- to set up an awareness program to educate the rural communities of the dangers of outside intruders intruding their network and what they can do to ensure that their data and information is not compromised.
- to raise awareness and cooperation in cyber security. Cooperation can be acquired by setting up a Computer Security Incident Response Team (CSIRT) for South Africa. This could include a National CSIRT supported by industry specific CSIRTs.

In line with what President Obama suggest for the US, a national security advisor could be appointed for South Africa who will report to the president of the RSA. The president of the consulting firm McConnell International indicated that such an advisor must be hard-wired into the decision structure (Aitoro 2008).

6. References

Aitoro, J. (2008). *Security analysts praise Obama's pledge for a cyber chief* [online]. NextGov, http://news.google.co.za/nwshp?sourceid=navclient&ie=UTF-8.

Aliber, M. (2003). "Chronic poverty in South Africa: incidence, causes and policies", *World Development,* Vol. 31, No. 3, pp. 473-490.

Armistead, L. (ed.) (2007). *Information warfare: separating hype from reality*, Potomac Books Inc,

Carte, D. (2009). *Glitch at Bankserv* [online]. Moneyweb, http://moneyweb.co.za/mw/view/mw/en/page292516?oid=330282&sn=2009%20Detail&pid=292681.
Danchev, D. & Naraine, R. (2008). *Coordinated Russia vs Georgia cyber attack in progress* [online]. BNET Business Network, http://blogs.zdnet.com/security/?p=1670.
Department of Communications (2009). "DRAFT BROADBAND POLICY FOR SOUTH AFRICA", *Government Gazette,* Vol*.* 531, No. 32578.
DeWalt, D. 2009. *Virtual Criminology Report 2009*.
Dirro, T. (2009). *FIFA World Cup Scams Start Early* [online]. McaAfee avert labs blog, http://www.avertlabs.com/research/blog/index.php/2009/09/08/fifa-world-cup-scams-starting-early/.
Doyle, K. (2009). *South Africa could be the next country to lead the cyber crime rankings.* [online]. ITWeb http://www.itweb.co.za/index.php?option=com_content&view=article&id=27948:could-sa-lead-cyber-crime-rankings
Hankyoreh (2009). *DDOS attack strikes S. Korea* [online]. The Hankyoreh Media Company, http://www.hani.co.kr/arti/english_edition/e_national/364832.html.
Internet_World_Stats (2009). *Internet Usage Statistics for Africa* [online]. Internet Coaching Library, http://www.internetworldstats.com/stats1.htm.
IT News Africa (2009a). *Cyber attacks may increase leading up to the 2010 Soccer World Cup* [online]. ITNewsAfrica.com, http://www.itnewsafrica.com/?p=2635.
IT News Africa (2009b). *Hackers pounce on ANC alliance partner* [online]. ITNewsAfrica.com http://www.itnewsafrica.com/?p=2935.
Jackson, W. (2009). *Russian Military, Organized Crime Involved in Georgia Cyberattacks* [online]. Redmondmag.com, http://redmondmag.com/articles/2009/08/17/russian-military-organized-crime-georgia-cyberattacks.aspx.
Kebbs, B. (2009). *PCs Used in Korean DDoS Attacks May Self Destruct* [online]. washingtonpost.com http://voices.washingtonpost.com/securityfix/2009/07/pcs_used_in_korean_ddos_attack.html.
McMillan, R. (2009). *World Cup used as lure for malware* [online]. IDG News Service, http://news.techworld.com/security/6267/world-cup-used-as-lure-for-malware/.
Michael, C. (2009). *Computer viruses slow African expansion* [online]. guardian.co.uk, http://www.guardian.co.uk/technology/2009/aug/12/ethiopia-computer-virus.
Microsoft 2009. *Microsoft Security Intelligence Report*
MyBroadband (2009). *SAT-3/SAFE bandwidth capacity tripled* [online]. MyBroadband.co.za, http://mybroadband.co.za/news/Telecoms/8879.html
Nkuna, B. (2009). *SA icons used as bait in fake email scams* [online]. Western Cape News, http://westcapenews.com/?p=299.
SAPA (2009). *Free porn on ANC website* [online]. News24.com, http://www.news24.com/Content/SouthAfrica/Politics/1057/d9c91bbe9aa44a81bed4104489bd0c86/19-07-2009%2006-07/ANC_website_offers_free_porn.
Stiennon, R. (2009). *SA could face cyber war* [online]. ITWeb Security Summit 2009, http://ww2.itweb.co.za/sections/internet/2009/0905291159.asp?A=COV&S=Cover&T=Section&O=C.
Symantec (2009). *Symantec warns of increasing cyber attacks leading up to the 2010 Soccer World Cup* [online]. http://www.symantec.com/about/news/release/article.jsp?prid=20090512_01.
WATCH, N. (2009). *Africa - home of the world's largest cyber pandemic* [online]. INTELLIBRIEFS, http://intellibriefs.blogspot.com/2009/10/africa-home-of-worlds-largest-cyber.html.