Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa – Has the CIIP and Cyber Security Rubicon Been Crossed?

Basie von Solms[1] and Elmarie Kritzinger[2]

[1] Academy for Computer Science and Software
Universtity of Johannesburg
Johannesburg, South Africa
basievs@uj.ac.za
[2] School of Computing
University of South Africa
kritze@unisa.ac.za

Abstract. This paper reviews some very negative views, made over the last few years, about Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa. The paper addresses the expressed negative views that Africa can become the vehicle or platform from where cyber-attacks could be launched against the rest of the world. The paper evaluates the reasons for such negative views and then suggests some steps which should be taken in Africa to counter such negative impressions and to protect itself cyber wise.

Keywords: Critical Information Infrastructure Protection, Cyber Security, Africa.

1 Introduction

Over the last few years, several negative comments about Africa's lack of preparedness to combat cybercrime and protect its own CIIP have been made. This creates the impression that Africa has no control over such cyber protection matters and that the continent therefore becomes a risk and a danger to the rest of the world.

Three such comments will be reviewed.

In [1] it is stated:

Africa: The Future Home of the World's Largest Botnet? IT experts estimate an 80% infection rate on all PCs continent — wide (in Africa), including government computers. It is the cyber equivalent of a pandemic. Few can afford to pay for anti-virus software, and for those who can, the download time on a dial-up connection makes the updates out of date by the download is complete. Now, with the arrival of broadband services delivered via undersea cables, …there will be a massive, target-rich environment of almost 100 million computers available for botnet herders to add infected hosts to their computer armies.'‘

R. Popescu-Zeletin et al. (Eds.) AFRICOMM 2011, LNICST 92, pp. 116–124, 2012.

This statement was made in 2008, and is therefore about 3 years old. Whether it was a valid statement at that time, can be debated, but have impressions changed over the next few years? Not if the second comment on this matter is reviewed!

In [2] it is seems even worse!

'Think that Russia and China pose the biggest hacking threats of our time? The virus-plagued computers in Africa could take the entire world economy offline. Imagine a network of virus-driven computers so infectious that it could bring down the world's top 10 leading economies with just a few strokes. It would require about 100 million computers working together as one, a "botnet" -- the cyber security world's version of a WMD. But unlike its conventional weapons equivalent, this threat is the subject of no geopolitical row or diplomatic initiative. That's because no one sees it coming -- straight out of Africa. Broadband Internet access will allow Africa's virus and malware problems to go global. With more users able to access the Internet (and faster), larger amounts of data can be transferred both out and inward. More spam messages in your inbox from Africa's email fraudsters will be only the beginning.'

This statement above was made in March 2010, a little more than a year ago, and it continues as follows!

'Unfortunately, in cyberspace, the whole is only as strong as its weakest link -- and the majority of African countries are downright frail. That fact won't be lost on skillful cybercriminals operating out of an unregulated Internet café in the slums of Addis Ababa, Lagos, or Maputo. The biggest botnet the world has ever known could be lurking there.'

Microsoft states:

'As Internet penetration increases across the continent, so does the risk of sophisticated cyber-attacks, threatening African nations' security, infrastructure, economic growth and citizen services. Microsoft detected over 126 million samples of malware worldwide in the second half of 2009 alone, an increase of 8.9% over the first half of the year. Worse still is the association of cybercrime with Africa, where such countries as Nigeria have become synonymous with advance fee fraud or "419" scams. The cybercriminals who pose as government "officials" requesting assistance in exchange for advance payments undermine the trust as well as the freedom of a healthy Internet economy'. [3]

For Africa, it is important to evaluate these comments, and investigate whether such situations do exist or whether they will exist in future, and if so, what should be done about it from an African level.

In the next paragraph these comments will be briefly commented on, and in paragraph 3 possible reasons for such pessimism will be investigated. Paragraph 4 will discuss some solutions, while paragraph 5 will elaborate on one specific proposal. Paragraph 6 provides a brief summary.

2 Evaluating the Comments above

An immediate knee-jerk reaction is probably to reject these comments as wrong and unscientific. However, the author of this paper, coming from Africa, would hesitate to do so! Surely the comments are 'overstated' and maybe a little too much 'over the top', but they do contain aspects which should be evaluated. They do contain certain truths which may indicate that Africa has not yet crossed the CIIP and Cyber Security Rubicon.

These truths will be investigated in the next paragraph.

3 Why Is Africa at Risk Cyber Security-Wise?

Developing countries, such as those in Africa, are particularly vulnerable to cyber-attacks due to a combination of factors, including increasing Internet penetration rates, high levels of computer illiteracy, and ineffective legislation. These factors all introduce a higher level of cyber security risks and expose the critical infrastructures in such countries to higher levels of risk.

Some factors driving such increased risks, as discussed in [4], are briefly discussed below.

3.1 Increasing Bandwidth

Traditionally bandwidth available to Africa has been limited. However, this is no longer the situation. In recent years, Sub- Saharan Africa has experienced a growth in the number of fiber-optic cables that have made landfall. This has had a dramatic effect on how governments, companies, and individuals interact with Internet-based technologies.

With the increasing bandwidth, there is a drive for governments and businesses to adopt and implement e-services and citizen e-participation. Governments are specifically moving towards e-Government and e-Governance environments.

[5] States :

'E-governance and e-participation are therefore crucial phases in the development of government processes. However, despite the opportunities they offer, they also introduce new challenges, particularly for the countries targeted by this study and, more broadly, West African countries: limited and unequal access to ICTs, lack of infrastructure, electronic fraud, and the absence of or inadequate legal frameworks. The initiatives studied illustrate that citizen participation through the use of ICTs is developing effectively in Africa. Governments have demonstrated a real willingness to transform relationships between government services and their users, particularly by strengthening the use of ICTs and by offering information services online.'

All such systems use the Internet. This has the promise of allowing these bodies to interact with their customers in a more efficient manner. Along with adopting Internet-based technologies for the provision of services, there is also a drive to utilize

these technologies to provide interconnection for a number of critical systems. The development of these interconnecting systems allows developing nations to compete more effectively in an increasing interconnected world.

In [6] the following is stated

"With a new decade beginning, the continent of Africa which was regarded as "backwards" has been able to get a leap into the world of ICT. This leap has not come without a heavy price. The rapid rate of diffusion of cybercrime in Africa has been a call for concern. This concern even gets more sickening when literature indicate that, out of the top ten countries in the world with a high level of cybercrime prevalence, Sub Sahara Africa is host to four of these countries (Nigeria, Cameroon, Ghana and South Africa)."

However, this wider access to the Internet creates new risks to Critical Information Infrastructure systems.

3.2 Increasing Use of Wireless Technologies and Infrastructure

Developing nations have long experienced problems in providing services to far-flung regions within their borders. The prospect of providing a physical link to a remote region is not feasible in many cases. However, the growing use of wireless technologies allows vast areas to be connected by investing in a number of wireless transmitters. Cellular networks, wireless mesh networks, and similar technologies are connecting communities at a much greater pace than what would have been possible using traditional means. Wireless technologies often present an attractive alternative for developing countries.

Statistics of mobile telephone users support these observations. As outlined in a report published by Cisco Systems, of the 4 billion cellular telephone users worldwide, 75 percent of those are in developing countries. The use of these new technologies creates a wider user base; however, these new users often do not have the computer security skills that in turn increase the overall risk in developing countries.

Again, such infrastructures essentially use the Internet, and provide access to the Internet, again creating cyber risks. This cyber risks are not only related to PCs n Africa but also to new and intrusive technologies for example smartphones.

"In the rapidly evolving mobile landscape in Africa, the growth has been fuelled in large part by the liberalization effort resulting in the formation of independent regulatory bodies and increased competition in the market. The total African mobile subscriber base is roughly 280.7 million people (30% of the total). With at least 15 mobile operators already announced plans of introducing 3G and data services (including Tanzania, Kenya and Nigeria)". [7]

The realization of above mentioned is that smartphones and Africa is not as impossible combination as one imagined. [8]

Result of increase in Smartphone use [9]:

"In a major shift in cybercrime trends, scammers are now moving their focus from Microsoft's Windows-based computers to other operating systems and platforms including smart phones, tablet computers and mobile platforms."

It is therefore vital that cyber risks connected to smartphones must be realized and taken into account within the Critical Information Infrastructure. It is also vital that independent regulatory bodies as mentioned above are involved within improving and protecting the Critical Information Infrastructure (see section 3.5).

3.3 Lack of Cyber Security Awareness

Developing nations are often seen has having poor literacy rates. Consequently, there is a severe lack of computer literacy and computer security awareness. In order to access eServices, new users must utilise the Internet without being equipped with the necessary skills to identify well-known threats (such as phishing). Attackers are now able to reuse old techniques, as users in developing nations have not experienced this type of attack before.

It is well known that banks in Africa are 'aggressively' rolling out internet-based banking services. Many such new users have maybe never used a desk top computer, and are not cyber security aware.

The situation in Africa is summarized in the quote from [10]:

'Millions of Africans are using mobile phones to pay bills, move cash and buy basic everyday items. It has been estimated that there are a billion people around the world who lack a bank account but own a mobile. Africa has the fastest-growing mobile phone market in the world and most of the operators are local firms. In countries like South Africa, for example, mobile phones outnumber fixed lines by eight to one. In Kenya there were just 15,000 handsets in use a decade ago. Now that number tops 15 million'.

In [11] some consequences of this growth are highlighted.

.'as more individuals worldwide gain Internet access through mobile phones, Cyber criminals will have millions of inexperienced users to dupe with unsophisticated or well-worn scamming techniques that more savvy users grew wise to (or fell victim to) ages ago.'

This surely increases the cyber security risks in Africa.

3.4 Ineffective Legislation and Policies

Legislation and policy in developing countries often do not adequately address Internet-based technologies. This often prevents cyber security measures and CIIP structure from having the required legal backing to operate effectively. The development of effective legislation and policies is essential to create effective cyber security and CIIP infrastructures.

Many African countries, including leaders like South Africa, do not yet have a proper national Cyber Security Policy or a national Computer Security Incident Response Team (CSIRT).

Without proper legislation and policies, very often well intended cyber security measures are not effective.

3.5 Technical Cyber Security Measures

The whole world is struggling with attacks using malicious software, and often the best and up to date anti-virus protection measures do not prevent infections. This problem is even more acute in Africa, as the cost to just keep up to date on anti-virus software updates, and patches for operating systems may be financially not reachable.

To approach this problem, Africa needs some new models for technical cyber security protection. One such example, placing more responsibilities in Internet Service Providers (ISPs) is described in [12] and [13].

3.6 Summary

Taking all the aspects discussed above, and some others not even mentioned, into account, it seems clear that Africa is still on the wrong side of the Cyber Security Rubicon! (The idiom "Crossing the Rubicon" means to pass a point of no return, and refers to Julius Caesar's crossing of the river in 49 BC).

4 What Must Africa Do to Cross the CIIP and Cyber Security Rubicon?

Surely there are a multitude of actions which can and should be taken to make Africa more Cyber secure. Maybe that is the reason why progress is slow and the cyber risks remain worryingly high.

However, international experiences and best practices in this area highlight one core issue, and that is **collaboration.** Before African states do not really start cooperating on CIIP and Cyber Security, progress will remain disjointed and incomplete.

It is well known that expertise in CIIP and Cyber Security is at a premium internationally, and so much more so in Africa.

Internationally there are regional bodies in the area of CIIP and cyber Security which are very active. In Europe ENISA is such an example, while CLARA plays a similar role in Latin America.

ENISA is the EU's response to these cyber security issues of the European Union. As such, it is the 'pace-setter' for Information Security in Europe, and a centre of expertise. [14]

The development of cooperation among CERTs in the region of South America and the Caribbean took a path similar to that in European. CLARA (Cooperation of Advanced Networks in Latin America) has established a working group to address security issues The group is focusing on two main areas:

- The protection of the critical infrastructure of REDClara – the network connecting Latin America National Research and Education Networked (NRENs) with each other and Europe
- The creation of security working groups in the NRENs [15].

At an ITU conference in 2008 it was stated:

'Africa is in dire need of such a regional facility which will really deliver value. Very often initiatives are taken in Africa, but never really implemented. In Africa, he said, the ICT revolution might fail to bring the desired and much needed results if countries do not adopt a sound regional approach to establishing national cyber security policies and legislation. In this respect he noted that constant developments in ICT make up an ever-changing environment which is too complicated for any one country to understand and handle alone. Therefore, countries in the region need external expertise to effectively meet the challenges posed by ICTs. Over time, the region as a whole must develop collective expertise and establish public-private partnerships to help each other in their respective approaches in building cyber security capacity.' [16]

The first, and most important step for Africa to cross the CIIP and Cyber Security Rubicon, is to build a bridge over this Rubicon river. The form of this bridge will be a Regional (or continental) CIIP and Cyber Security Alliance between African States. This Alliance establishes and fund a Centre to address CIIP and Cyber Security in Africa.

For discussion purposes, let this Alliance be called the African Cyber Security Agency (ACSA), and the Centre the African Cyber Security Centre (ACSC).

5 ACSA – The Bridge over Africa's Cyber Security Rubicon

ACSA will have African countries as members, and one of its main priorities will be to establish and fund the African Cyber Security Centre (ACSC).

ACSC could perform a wide range of services, of which the most obvious are briefly discussed below.

5.1 Cyber Security Awareness

A comprehensive set of Cyber Security Awareness material should be made available to all member countries of ACSA. Cyber Security Awareness courses are very much standardized internationally, and it is unnecessary for everyone to develop new material. Internationally the ITU has material which can be adapted and used. The National Cyber Security Alliance in the US also has a wide range of material available.

The challenge is not to create such material, but rather to consolidate and 'package' it for Africa – That is what ENISA and Clara do.

ACSC must be the central place in Africa where all member countries can get their material.

5.2 Provide Capacity Development and Skills Development

There is a dire need for such courses in Africa. In May 2011 the author chaired a session during a recent ITU event in Genève – The Fourth Parliamentary Forum on

Shaping the Information Society: The Triple Challenge of Cyber-Security, Information, Citizens and Infrastructure. The Forum was attended by a number of Parliamentarians form Africa, and all of them desired to attend some course to bring them up to date on their oversight role as far as CIIP and Cyber Security in their countries are concerned. Hap hazard ad hoc courses do not work – it must be centralized in one body – ACSC.

Such course for a wide range of other industrial and specifically Government officials are sorely needed.

ACSC must be the central place in Africa where all member countries van be exposed to such courses.

5.3 Legislative and Policy Aspects

Many countries in Africa are struggling to create national policies and relevant regulations. Again, redeveloping the wheels in such cases only delays or completely stalls the issue. ACSC could provide help and support in drafting such documents and even present short courses on how to create such policies and related problems.

ACSC must be the central place in Africa where all member countries could get advice on these aspects – even draft policy templates.

5.4 National Computer Security Incident Response Teams (CSIRTs)

CSIRTs are essential for CIIP and proper Cyber Security, but few countries in Africa already have such institutions. Only two countries in Africa belong to FIRST, the international Forum of Incident Response and Security Teams [17]. The single most benefit of a CSIRT is its international connections.

ACSC could play a central role in providing expertize to member countries to create CSIRTs and to cooperate and coordinate between them. It should be a contact body for CSIRTs in Africa and for CSIRTs from outside Africa.

ACSC must be the central place in Africa where all member countries could get expertize to create CSIRTs and to cooperate and coordinate between them.

5.5 Research in Cyber Security and CIIP

ACSA should also have a research and development facility of which all member states can make use of.

5.6 Many Other Functions

ACSC must be the central place and contact point in Africa where all aspects related to CIIP and Cyber Security are coordinated and where expertize and skills in these areas are available.

It should be the starting point in any search or problems related to CIIP and Cyber Security.

5.7 The Structure of ACSC

Although it seems the best way to start ACSC as a geographically centralized facility, it seems logical that in time it should have distributed facilities in member countries to make it easier for stakeholders to use the facilities provided by ACSC.

6 Summary

Surely Africa has not yet crossed the CIIP and Cyber Security Rubicon, but with political will, and starting platforms like ACSA and ACSC, it will do so. It will be Africa's best interest to do so very soon.

References

1. Carr, J.: Inside Cyber Warfare. O'Reilly (2009)
2. http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd
3. http://blogs.technet.com/b/microsoft_on_the_issues_africa/archive/2010/07/01/laying-the-foundation-for-cybersecurity-in-africa.aspx
4. Ellefsen, D., von Solms, S.H.: A Community-Oriented Approach to CIIP in Developing Countries, CIP Report, Center for Infrastructure Protection and Homeland Security, vol. 9(12). George Mason University, USA (2011)
5. http://ictdegov.org/e-gov/WA-epart.html
6. Akuta, E.A.M., Ong'oa, I.M., Jones, C.R.: Combating cyber crime in Sub-Sahara Africa; A Discourse on Law, Policy and Pricatice. Journal of Peace, Gender and Development Studies 1(4), 129–137
7. http://news.bbc.co.uk/2/hi/business/8194241.stm
8. http://allafrica.com/stories/201102150340.html
9. http://www.mikekujawski.ca/2009/03/16/latest-mobile-phone-statistics-from-africa-and-what-this-means/
10. http://internationaldigitalmarketing.com/2010/10/29/mobile-marketing-trends-smartphones-conquering-africa/
11. http://www.cisco.com/en/US/.../annual_security_report.html
12. Kritzinger, E., von Solms, S.H.: A New Role for Information Service Providers (ISPs) as Part of Critical Information Infrastructure Protection in Africa, CIP Report, Center for Infrastructure Protection and Homeland Security, USA, vol. 9(12) (2011)
13. Kritzinger, E., von Solms, S.H.: Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security 29, 840–847 (2010)
14. http://www.enisa.europa.eu/about-enisa
15. http://www.enisa.europa.eu/
16. http://www.itu.int/ITU-D/cyb/events/2009/tunis/index.htm
17. http://www.first.org/members