



Cybercrime: a complex problem requiring a multi-faceted response

26 March 2014

Challenges and Prospects of Frameworks to combat Cybercrime – a critical perspective

Prof Basie Von Solms
Director : Centre for Cyber Security
Academy for Computer Science and Software Engineering
University of Johannesburg
basievs@uj.ac.za



“Cyber crime ‘is a national crisis”

June 20, 2013

**“National crisis’ of cybercrime poses major threat
to SA business’**

Sep 18, 2013

‘Cybercrime 'national crisis' costing SA R1b a year’

Oct 23, 2013



What must we do to decrease Cyber Crime?

My hypothesis

to decrease Cyber Crime



we need

to move towards a more secure Cyber Space



we need

a proper Architecture for a Secure Cyber Space

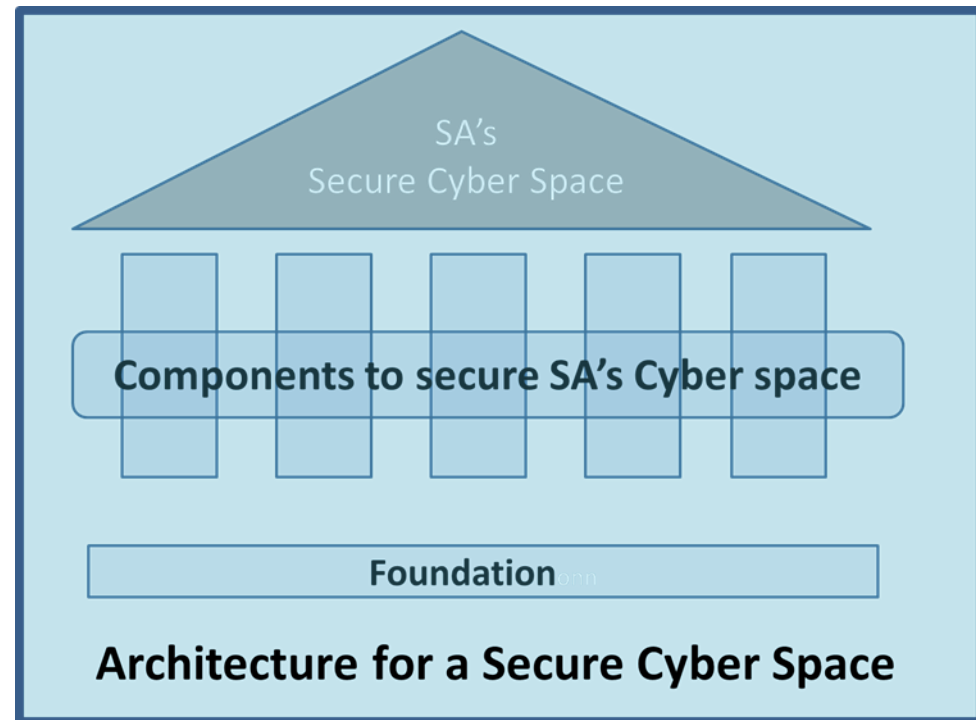
SA's
Secure Cyber Space

The diagram is shaped like a house. The roof is a dark gray triangle containing the text 'SA's Secure Cyber Space'. Below the roof is a light blue rectangular area containing five empty square boxes arranged in a row. A horizontal light blue bar with rounded ends is superimposed over the middle of these boxes, containing the text 'Components to secure SA's Cyber space'. Below the boxes is a light blue rectangular bar containing the text 'Foundation'. At the very bottom of the diagram is the title 'Architecture for a Secure Cyber Space'.

Components to secure SA's Cyber space

Foundation

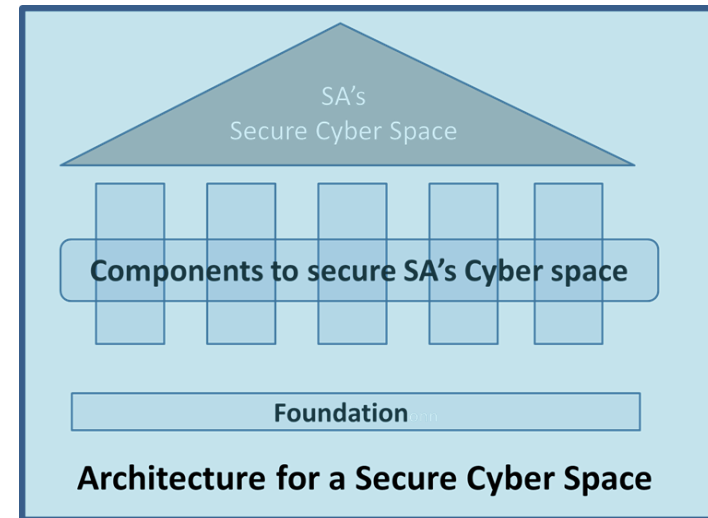
Architecture for a Secure Cyber Space



- **What is this Foundation?**
- **What are these components?**
- **What is the 'gold standard' to protect a country's Cyber Space?**

Determining the ‘gold standard’:

Foundation :



(Government's) primary role is to define the national strategy and provide the policy framework. The policy framework describes the architecture by which the national efforts are built and operated.

Best Practices for National CyberSecurity: Building a National Computer Security Incident Management Capability, Version 2.0, 2011

Each Member State, shall put in place a national cyber security policy ...

Draft African Union Convention on the Confidence and Security in Cyberspace

SA's
Secure Cyber Space

The diagram is set within a light blue rectangular frame with a dark blue border. At the top is a grey triangle representing a roof, containing the text 'SA's Secure Cyber Space'. Below the roof is a horizontal row of five light blue squares. A light blue rounded rectangle with a dark blue border is superimposed over the middle of these squares, containing the text 'Components to secure SA's Cyber space'. Below this row of squares is a light blue horizontal bar with a dark blue border, containing the text 'National strategy and the policy framework'. At the bottom of the frame is the main title 'Architecture for a Secure Cyber Space'.

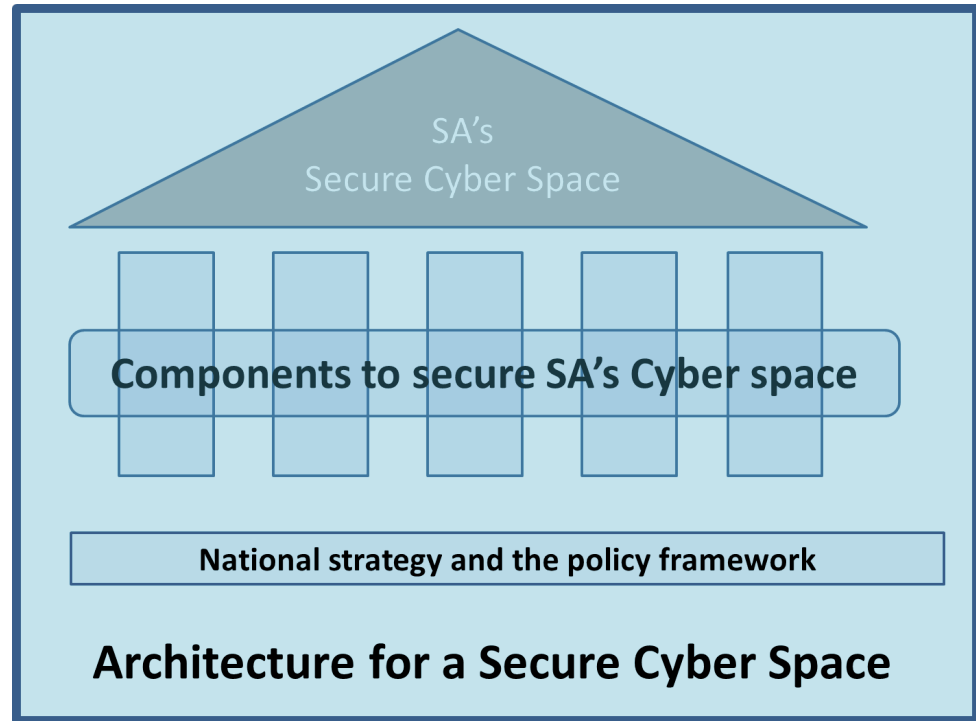
Components to secure SA's Cyber space

National strategy and the policy framework

Architecture for a Secure Cyber Space

Determining the 'gold standard':

Components



Let's investigate some other existing National Strategies to determine *some* common components are

Component 1

A National program for Cyber Security skills/capacity building

- **India's National Cyber Security Policy**

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

- **Draft African Union Convention on the Confidence and Security in Cyberspace**

- Each Member State have to undertake measures to develop capacity building measures

The diagram is set within a light blue rectangular frame with a dark blue border. At the top is a grey triangle representing a roof, containing the text 'SA's Secure Cyber Space'. Below the roof are five vertical rectangular columns. The first column on the left contains the text 'A National program for Cyber Security skills/ capacity building'. The second column contains a single closing parenthesis ')'. The remaining three columns are empty. Below these columns is a horizontal rectangular box containing the text 'National strategy and the policy framework'. At the very bottom of the frame is the main title 'Architecture for a Secure Cyber Space' in a large, bold, black font.

SA's Secure Cyber Space

A National
program
for Cyber
Security
skills/
capacity
building

)

National strategy and the policy framework

Architecture for a Secure Cyber Space

Component 1

A National program for Cyber Security skills/capacity building

- **Shortage of skills in SA**
- **UJ effort**
 - Certificate in Cyber Security
 - Certificate in Digital Forensics

Component 2

A Culture of Cyber Security

- **India's National Cyber Security Policy**

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

- **AU's Draft Convention**

- Each Member State have to undertake measures to take the lead in the development of a cyber security culture within its borders and to this end enhance awareness-building

The diagram is shaped like a classical building. At the top is a triangular pediment containing the text 'SA's Secure Cyber Space'. Below the pediment are five vertical rectangular columns. The first two columns contain text, while the other three are empty. Below the columns is a horizontal rectangular base containing the text 'National strategy and the policy framework'. At the very bottom of the diagram is the main title 'Architecture for a Secure Cyber Space'.

SA's Secure Cyber Space

A National
program
for Cyber
Security
skills/
capacity
building

A National
Cyber
Security
Awarenes
s Program
(Cyber
Security
Cuilture)

National strategy and the policy framework

Architecture for a Secure Cyber Space

Component 2

A Culture of Cyber Security

Isolated initiatives

- **SACSAA**
 - UJ, NMMU, UNISA
- **CSIR**
- **Integrated national initiative needed**

Component 3

A National Critical Information Infrastructure Protection Centre

- **India's National Cyber Security Policy**

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

- **AU's Draft Convention**

- Member States have to undertake necessary measures to encourage the establishment of institutions ...such as Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIR)

The diagram is shaped like a classical building facade. At the top is a triangular pediment containing the text 'SA's Secure Cyber Space'. Below the pediment are five rectangular columns. The first three columns contain text: 'A National program for Cyber Security skills/ capacity building', 'A National Cyber Security Awareness Program (Cyber Security Culture)', and 'A National Critical Information Infrastructure Protection Centre'. The last two columns are empty. Below the columns is a horizontal rectangular base containing the text 'National strategy and the policy framework'. At the very bottom of the diagram is the main title 'Architecture for a Secure Cyber Space'.

SA's Secure Cyber Space

A National
program
for Cyber
Security
skills/
capacity
building

A National
Cyber
Security
Awarenes
s Program
(Cyber
Security
Culture)

A National
Critical
Informatio
n
Infrastruct
ure
Protection
Centre

National strategy and the policy framework

Architecture for a Secure Cyber Space

Component 3

A National Critical Information
Infrastructure Protection Centre

- **National CSIRT**
- **Cyber Threat Intelligence**
- **Cyber Counterintelligence**
 - Centre for Cyber Security at UJ

Component 4

Public-Private Partnerships in the Cyber Space

- **India's National Cyber Security Policy**

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

- **AU's Draft Convention**

- Each Member State have to undertake measures to adopt public-private partnership as a model to engage industry, civil society and the academia ..

The diagram is shaped like a classical building. The roof is a large triangle containing the text 'SA's Secure Cyber Space'. Below the roof are five vertical rectangular pillars. The first four pillars contain text describing national programs and partnerships, while the fifth is empty. Below the pillars is a horizontal rectangular base containing the text 'National strategy and the policy framework'. The entire diagram is enclosed in a blue border.

SA's Secure Cyber Space

A National
program
for Cyber
Security
skills/
capacity
building

A National
Cyber
Security
Awarenes
s Program
(Cyber
Security
Culture)

A National
Critical
Informatio
n
Infrastruct
ure
Protection
Centre

Public-
Private
Partner
Ships

National strategy and the policy framework

Architecture for a Secure Cyber Space

Component 4

Public-Private Partnerships in the Cyber Space

- **Most Critical Infrastructures are in private hands**
- **Government needs the private sector in this matter**

Component 5

Gov support for cyber security in SMMEs

- **India's National Cyber Security Policy**

- 9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

The diagram is shaped like a classical building facade. At the top is a triangular pediment containing the text 'SA's Secure Cyber Space'. Below the pediment are five rectangular columns, each containing a specific program or initiative. At the base of the columns is a wide horizontal rectangular foundation containing the text 'National strategy and the policy framework'. The entire diagram is set against a light blue background with a dark blue border.

SA's Secure Cyber Space

A National
program
for Cyber
Security
skills/
capacity
building

A National
Cyber
Security
Awarenes
s Program
(Cyber
Security
Cuilture)

A National
Critical
Informatio
n
Infrastruct
ure
Protection
Centre

Public-
Private
Partner
Ships

Gov
support
for cyber
sec rity
in
SMMES

National strategy and the policy framework

Architecture for a Secure Cyber Space

Component 5

Gov support for cyber security in SMMEs

SMMEs as growing targets of Cybercrime

- 150 000 SMMEs in SA are dependent on their cyber presence
- > 1,5 million jobs (in SMMEs) exist because of this cyber presence
- SMMEs are a growing target for cyber criminals
- POPI

Component 5

Gov support for cyber security in SMMEs

SMMEs as growing targets of Cybercrime

USA

With small businesses prime targets for cyber attacks, the US Government announced (2011) that it designed a free online resource (tool) to help companies improve their online security

<http://www.secure128.com/u-s--government-helping-small-businesses-combat-cyberattacks.aspx>

Component 5

Gov support for cyber security in SMMEs

- The UK government's Technology Strategy Board has extended its Innovation Vouchers scheme to allow small and medium enterprises (SMEs) to bid for up to £5,000 from a £500,000 pot to improve their cyber security by bringing in outside expertise.

<http://news.techworld.com/security/3443429/uk-government-offers-smes-5000-to-improve-their-cyber-security/>

The diagram is shaped like a house. The roof is a grey triangle containing the text 'SA's Secure Cyber Space'. Below the roof are five light blue rectangular pillars. From left to right, they contain: 'A National program for Cyber Security skills/ capacity building', 'A National Cyber Security Awareness Program (Cyber Security Culture)', 'A National Critical Information Infrastructure Protection Centre', 'Public-Private Partnerships', and 'Gov support for cyber security in SMMEs'. To the right of the fifth pillar are three dots and the word 'More'. Below the pillars is a horizontal light blue bar with the text 'National strategy and the policy framework'. At the very bottom is a large black title 'Architecture for a Secure Cyber Space'.

SA's Secure Cyber Space

A National
program
for Cyber
Security
skills/
capacity
building

A National
Cyber
Security
Awareness
Program
(Cyber
Security
Culture)

A National
Critical
Information
Infrastructure
Protection
Centre

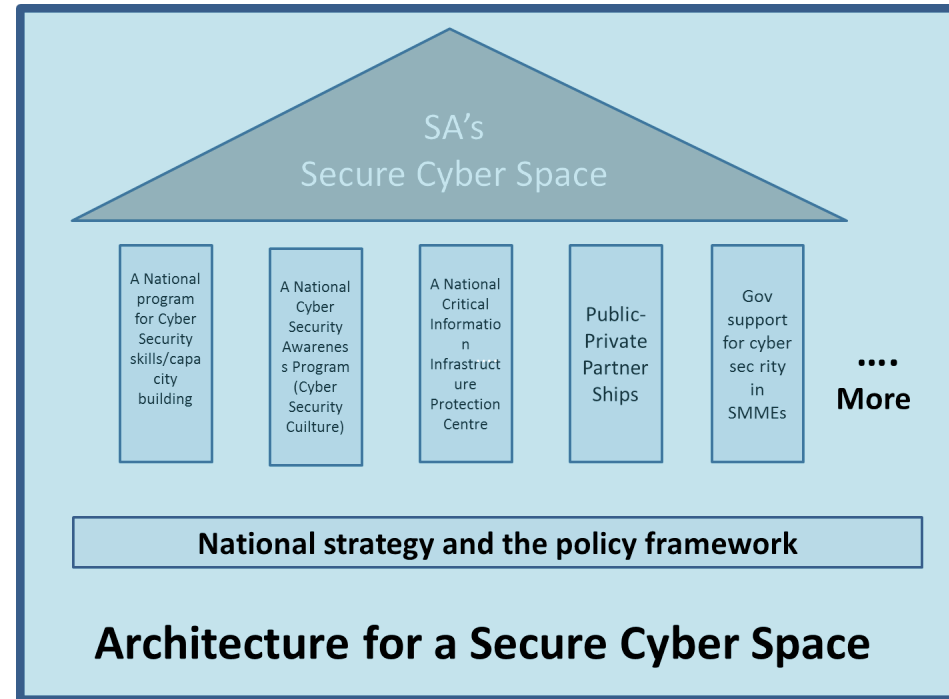
Public-
Private
Partners
Ships

Gov
support
for cyber
security
in
SMMEs

....
More

National strategy and the policy framework

Architecture for a Secure Cyber Space



More components

- International cooperation
- Legal infrastructure

My hypothesis

to decrease Cyber Crime



we need

to move towards a more secure Cyber Space

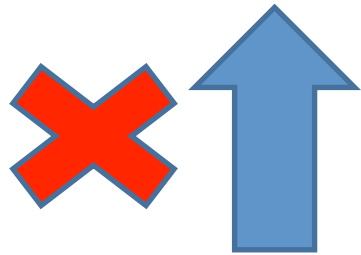


we need

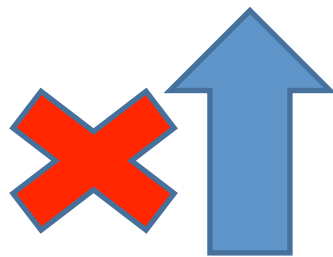
a proper Architecture for a Secure Cyber Space

Conclusion – as matters stand at the moment

Therefore we will not decrease Cyber Crime



Therefore we are not moving to a more secure Cyber Space



We do not have a proper Architecture for a Secure SA Cyber Space

1. Norton Report 2012/3

South Africa have the 3rd highest number of cybercrime victims in the world

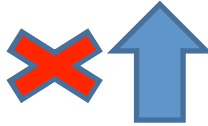
2. FBI : South Africa is a cyber crime hot spot

The FBI listed South Africa as the sixth most active country where cyber crime took place

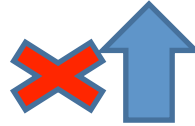
<http://businesstech.co.za/news/international/48142/south-africa-is-a-cyber-crime-hot-spot-fbi/22>

Conclusion

Therefore we will not decrease Cyber Crime



Therefore we are not moving to a more secure Cyber Space



We do not have a proper Architecture for a Secure Cyber Space

A proper integrated Architecture for a Secure Cyber Space for SA is the starting point to start decreasing Cyber Crime and is URGENTLY needed !!!

Conclusion

Therefore we will not decrease Cyber Crime



There fore we are not moving to a more secure Cyber Space



We do not have a proper Architecture for a Secure Cyber Space

- **SA will NOT reduce Cybercrime before we have a proper Architecture for a Secure Cyber Space**
- **This message MUST be conveyed to the highest levels in SA**

Thanks

basievs@uj.ac.za



INSTITUTE FOR SECURITY STUDIES
POLICY BRIEF

RECOMMENDATIONS

African countries should:

- Adopt a universal definition of cybercrime, which must be included in national cybercrime laws.
- Strengthen international and regional collaboration to counter cybercrime.
- Designate a civilian rather than a military government agency to lead governmental response to cybercrime.
- Develop domestic criminal justice capacity to understand cybersecurity and respond appropriately to threats.
- Create cyber emergency response teams with 24/7 capabilities to respond to significant threats and provide technical assistance.

Cybercrime
A complex problem requiring a multi-faceted response

Eric Tamarkin

SUMMARY

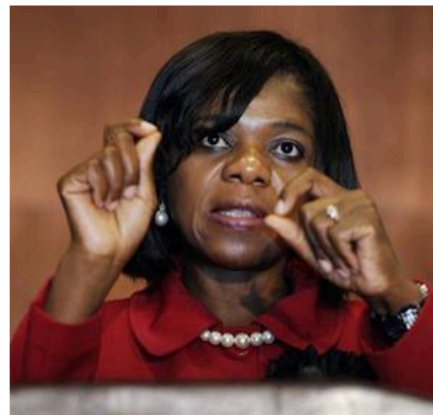
The Internet has revolutionised the way in which businesses, government and the public interact. However, criminal actors have used this to their advantage. Given reports that Africa is becoming a cybercrime safe harbour, this problem could hamper economic growth, foreign investment and security. African policymakers need a cogent response to cybercrime, which is informed by a clear understanding of emerging threats and how other countries have formed strategies in response.

In the absence of a universal definition of cybercrime, the term is often confused with other types of malevolent cyber activity and it is difficult to quantify its financial impact worldwide. A recent study estimated the cost of malicious cyber activity to the global economy to be as high as US\$1 trillion. Recent high-profile cyber attacks and emerging threats such as attacks on mobile technologies demonstrate that cybercrime is an urgent issue for policymakers. In devising a strategy to combat cybercrime, countries on the continent should adopt a multi-layered approach.

Subscribe to ISS email
newsletters
www.issafrica.org

Having trouble viewing this email? [Click here](#) to view in your browser

20 March 2014



Feature: Thuli Madonsela: a triumph for constitutional democracy

The Nkandla report is only one example of why South Africa needs a brave and honest public protector like Madonsela.

Yesterday, all Africans had a reason to be proud of the brave and principled leadership that exists on this continent in the form of South African Public Protector, Thuli Madonsela. In a sober and considered manner, she read out the findings of the long-awaited Nkandla report - her investigations into the 'unconscionable' amount of R246 million of taxpayers' money spent on upgrades to President Jacob Zuma's private residence to no public benefit.

[Read more...](#)