ISS INSTITUTE FOR SECURITY STUDIES

Cybercrime: a complex problem requiring a multi-faceted response

26 March 2014

Responding Effectively to the Growing Threat of Cybercrime

Eric Tamarkin

Consultant, Institute for Security Studies

Former Senior Counsel to the U.S. Senate Homeland Security & Governmental Affairs Committee

Overview

1. Growth of Internet and Mobile
2. Current Threat
3. Complex Problem - Multilayered Approach
4. Scorecard for South Africa
5. Cybersecurity Standards

Growth of the Internet and Mobile Devices: Global

- Internet users
  - Global: 2.7 billion as of 2013
  - Africa: 167 million as of 30 June 2012
- Mobile devices
- Mobile subscriptions

Growth of the Internet and Mobile Devices: South Africa

- 14 million Internet users in SA (2013)
- 100 per cent broadband by 2020?
- Free Wi-Fi in Pretoria by 2016?
- 32.3 million mobile Internet subscribers by 2017
- Africa’s largest smartphone market

Current Threat: Global

- Cyber espionage, Cyberwar, Cyber terrorism, Hacktivism, Cybercrime
  - Attack intent and attribution?
- All entities and sectors are at risk
  - Softer targets
  - U.S. Retailers - Target, Neiman Marcus
- Massive global economic ramifications
- Increasing impact on poor/uneducated

Current Threat: South Africa Cybercrime Hub

- 3rd highest number of cybercrime victims (Norton)
- 6th most active cybercrime country (FBI)
- Reported costs of R1 billion per year
- Dexter malware, Postbank case
- Threats to mobile devices

Complex Problem - Multilayered Approach

- Policy framework roles and responsibilities
- Define cybercrime and gather statistics
- Legislation
- Computer Emergency Response Teams (CERTS)
- Coordination hubs - information sharing
- Train law enforcement, judges and government officials
- Attract and build workforce

Multilayered Approach (continued)

- Education/Cyber Centres of Excellence
- Public awareness campaigns
- International coordination and cooperation
- Promote R&D
- **Cybersecurity standards**

South Africa’ s Scorecard

US Scale A-F; SA Scale 7-1

Policy framework	C (4)
Define cybercrime	C (4)
Gather statistics	F (1)
Legislation	B (5)
CERTS	C (4)
Coordination hubs - info sharing	F (1)
Train law enforcement, judges, etc.	F (1)
Attract and build workforce	F (1)

South Africa’ s Scorecard

US Scale A-F; SA Scale 7-1

Education/Cyber Centres of Excellence	B (5)
Public awareness campaigns	C (4)
International coordination and cooperation	B (5)
Promote R&D	TBD
Cybersecurity standards	F (1)

U.S. Cyber Standards

Released on 12 February 2014

- Pursuant to Executive Order 13636
- National Institute of Standards and Technology (NIST) process
- Critical infrastructure, but not industry specific
- Voluntary, but could be baseline for what is commercially reasonable
- Incentives for adoption?

U.S. Cyber Standards
continued

- Technology neutral
- Protection of privacy and civil liberties
- Blueprint for global adoption
- Evolving document - Version 1.0

Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Contact

Eric Tamarkin

etamarkin@outlook.com

ISS | INSTITUTE FOR SECURITY STUDIES

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

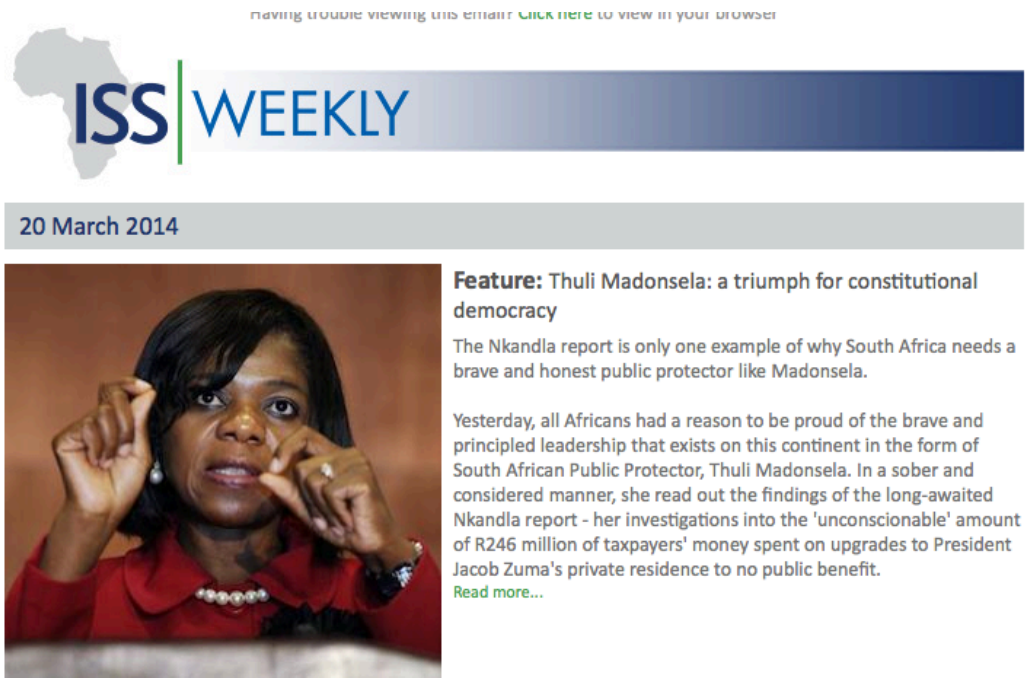
SUMMARY

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

ISS | WEEKLY

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...