African Telecommunications Union

Enhancing Cyber Security in Africa:

New challenges for regional Organizations ?

Meriem SLIMANI
Standardization and Development Coordinator
Email: m.slimani@atu-uat.org
Website: www.atu-uat.org

ITU-ATU Workshop on Cybersecurity Strategy in African Countries
Khartoum, Republic of Sudan, 24-26 July 2016

Introduction

According to a recent Norton Cyber-Crime Report, every second, 18 adults are victims of cyber crime, resulting in more than 1.5 million victims globally per day.

A survey of 21 countries in Africa conducted by ECA found that while many countries had proposed legislation, the level of deployment of security systems in both the private and the public sectors to combat cyber-crime was low.

Presentation Summary

Introduction

1. Africa Internet penetration key indicators
2. Cyber threats in Africa and their impact
3. Cyber Security priorities for Africa
4. African legal instruments on Cyber Security
5. ATU Contribution for Cyber Security in Africa
6. Proposals for Strengthening Cyber Security amongst African states

Conclusion

1. Internet penetration in Africa : key Indicators

Africa currently

•More than 650 million unique mobile subscribers,
•More than 30% of the African population, are now using the Internet and more than 7% population are Facebook user.
•More than 80% of Facebook's users in Africa are visiting the site via mobile devices;
•The global share of e-commerce for the Middle East and Africa was expected to rise from 1.6% in 2011 to 2.3% by 2016.

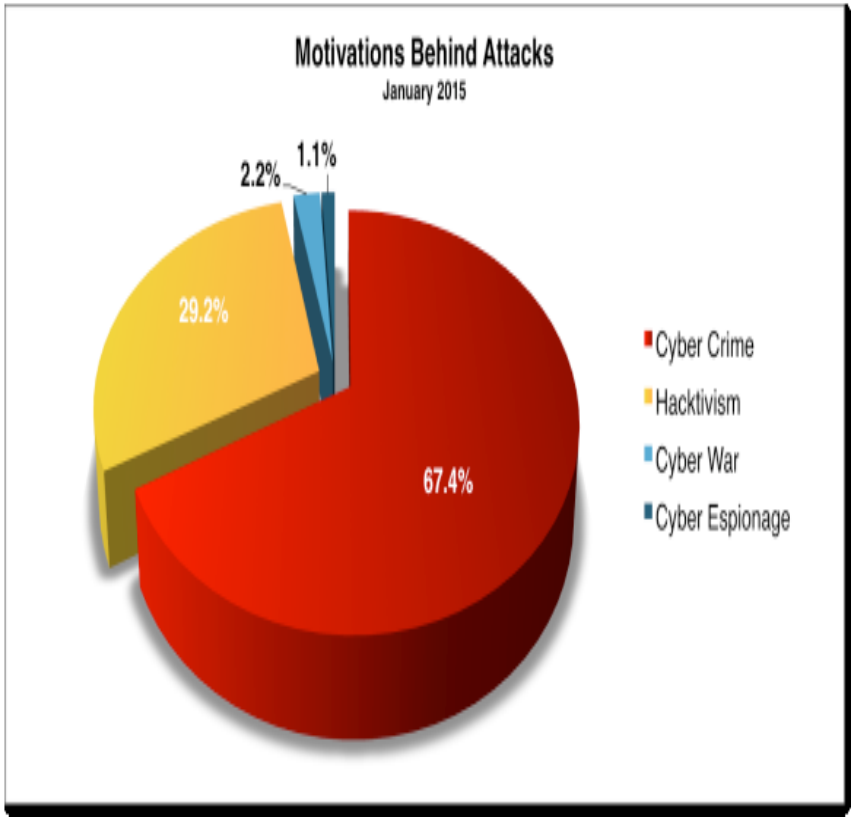
Consequences

New challenges arise alongside growth, and increasing technological exposure poses its own vulnerabilities and risks. One such risk that derives from increased technological exposures and requires urgent policy attention and action is cyber crime.

2. Cyber threats in Africa and their impact

Africa is very prone to cyber-related threats due to the high number of domains coupled with very weak network and information security.

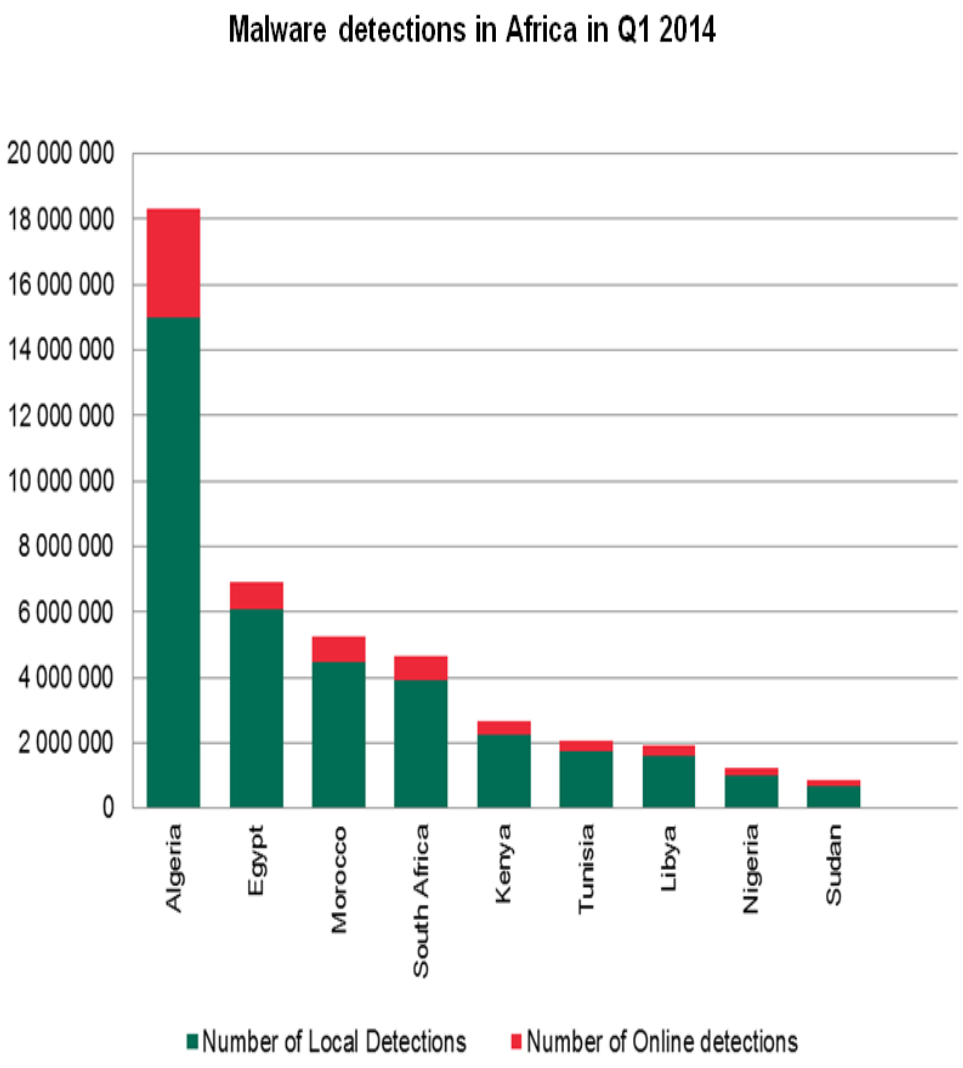
According to a report by Symantec Corporation on Cyber crime, issued in 2013, Cybercrime is increasing at a more rapid rate in Africa than in any other continent in the world. In 2012, the number of targeted *cyber attacks in Africa increased by 42%* and 31% of these attacks, categorized as cyber espionage, have hit both large and small businesses.



2. Cyber threats in Africa and their impact

According to a 2011 study, the average rate of software piracy in Africa is about 73%, with little change in recent years. In addition to the financial loss (of USD 1.785 billion) the high level of use of unauthorized software is likely to aggravate virus and malware woes in Africa.

Cyber security experts estimate that 80% of personal computers on the African continent are infected with viruses and other malicious software.



2. Cyber threats in Africa and their impact

South Africa
- With 80% has the 3rd highest number of cybercrime victims in the world, after Russia (92%) and China (84%);
- Finding of a study by the International Data Group Connect estimates that annually, cyber crimes cost the South African economy USD 573 million;

Kenya
Annually, cyber crimes cost the Kenyan economy USD 36 million.

Zambia
Several commercial banks in Zambia were robbed of more than USD 4 million in the first half of 2013 as a result of sophisticated cyber crime collaborations between Zambians and foreigners.

Nigeria
is the largest target and source of malicious Internet activities;
Annually, cyber crimes cost the Nigerian economy USD 200 million.

A 2011 Deloitte Touche survey found that *financial institutions* in **Kenya, Rwanda, Uganda, the United Republic of Tanzania and Zambia** had registered losses of up to USD *245 million due to cyber fraud*.

3. Cyber Security : Priorities for Africa

PREVENTION	ORGANIZATION
-Awareness campaign; -Promote training for those are responsible of education and Internet facilitation access -Oblige national administration and companies to install cyber security solution.	-Establishment a process to support cyber victims; -Define obligations and responsibilities of Internet professionals vis-à-vis cybercrime; -Provide systems to control and block malicious websites and domain names
COOPERATION AND PARTNERSHIP	**MEANS TO FIGHT AGAINST CYBER CRIME**
- Work to develop international policy instruments; -Foster public-private partnerships in cyber security; -Develop regional and international agreements to unify exchange of information and pooling resources against cyber crimes.	-Create dedicated national as well as regional infrastructure with efficient management and equipped with adequate human and material resources; -Training for key actors such as judges, investigative agents but also technical skills able to manage and develop security solutions.

4. African legal instruments on cyber security

Background on Africa

Africa comprises of 55 sovereign states and it is classified as the world's second largest and second most populous continent after Asia, with a terrestrial mass of 30, 2044, 049 square kilometers and a human population of over one billion people.

The continent has five geographical sub-regions, comprising of: Southern Africa, Central Africa, East Africa, North Africa, and West Africa.

The African Union (AU) is the most prominent regional intergovernmental organization that unites African States and it comprises of 54 sovereign States with Morocco being the only sovereign African State that is not a member of the union.

Some notable intergovernmental organizations that operate within Africa's sub-regions include:
The COMESA which comprises of 19 Member States,
The ECOWAS which comprises of 15 Member States,
The SADC which comprises of 15 Member States.

Sub regional legal instruments for cybersecurity

1- ECOWAS	2- COMESA	3- SADC
In August 2011, the ECOWAS Council of Ministers adopted the *Directive C/DIR.1/08/11 on Fighting Cybercrime* at its Sixty Sixth Ordinary session at Abuja. The Directive imposes obligations on Member States to criminalize cyber crime and also establishes a framework to facilitate international cooperation on cyber security.	In October 2011, the COMESA established a *Model Cybercrime Bill* to provide a uniform framework that would serve as a guide for the development of general framework to facilitate international cooperation, extradition, and mutual assistance and provides for the establishment of national 24/7 points of contact. However, it does not establish any binding obligations on Member States to criminalize cyber crimes.	In March 2012, the SADC adopted the *Model Law on Computer Crime and Cybercrime* to serve as a guide for the development of cyber security laws in SADC Member States. However, it does not impose any obligations on Members to establish cyber crime laws. It does not also establish any provisions to guide the development of international cooperation regimes in Member States and neither does it establish any international cooperation obligations on Member States.

Africa legal instrument

AU Convention on Cybersecurity and personnal data protection

In 27th June 2014, the AU Heads of State and Government adopted a revised version of the draft Convention during the 23rd Ordinary Session of the AU Assembly in Malabo. The Convention which is known as the *AU Convention on Cyber Security and Personal Data Protection* aims to harmonize the laws of African States on electronic commerce, data protection, cyber security promotion and cyber crime control.

The Convention recognizes that cyber crime “constitutes a real threat to the security of computer networks and the development of the Information Society in Africa”.

To a great extent, the Convention adopts a holistic approach to cyber security governance by imposing obligations on Member States to establish national legal, policy and institutional governance mechanisms on cyber security.

For it to be implemented, 15 of the 54 AU member states will need to ratify the text. As yet, only few countries as well as Senegal has done so, though there is optimism it will happen in the next 3-to-5 years.

African Telecommunications Union (ATU)

ITS CONTRIBUTION FOR STRENGHING REGIONAL CYBER SECURITY

ATU is a specialized Telecommunications / ICT agency of the AU and has actively participated in consultations that led to the elaboration of AU Convention on cyber security and personal data protection.

Today as part of its mission, ATU could intervene on some aspects of cyber security, namely:

-Harmonization of regulatory policies regarding cybersecurity aspects as well as data protection and privacy and digital identification;

-Assistance MSs in raising awareness on cybersecurity issues;

-Capacity building and technical assistance on cybersecurity

-Promotion of cooperation and exchanges at regional and international levels;

- Promotion of partnership with others stakeholders within the region.

STRENGTHENING COOPERATION ON CYBER SECURITY AMONGST AFRICAN STATES

Some proposals from African experts

1- Improve the existing framework for adequate and efficient international cooperation and mutual assistance amongst African States;

2- While it is agreed that cyber threats that affect African States may also emanate from outside the continent, which also underscores the need for wide international cooperation amongst all States.

3- Create a regional Computer Emergency Response Team (CERT) to facilitate cyber security efforts and coordinate responses to cyber security incidents at the regional level and also facilitate cyber security cooperation between national CERTs.

STRENGTHENING COOPERATION ON CYBER SECURITY AMONGST AFRICAN STATES

Some proposals from African experts

4- Enhance private sector participation in African cyber security.

5- Promoting the adoption and implementation of measures to strengthen cyber security in electronic services and combating cyber crime and human rights violations in cyberspace;

6- Advising African governments on measures to promote cyber security and combat cyber crime;

7- Analyzing the criminal behaviors of cyberspace users within Africa and transmitting such information to competent national;

8- Create a regional network agency which is similar to the European Information Security Agency (ENISA).

CONCLUSION

The adoption of the AU Cyber Security Convention marks a significant milestone in African cyber security governance and underscores Africa's efforts to promote the development of a secure information society.

However, cybercrime cannot be defeated by any law or convention alone. In fact, it has become increasingly clear that collaboration of all stakeholders in the any governance and operation of the Internet is required to preserve the security and privacy of the internet users.

THANK YOU

FOR YOUR ATTENTION

m.slimani@atu-uat.org

www.atu-uat.org