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

Summary & Conclusions

Opening and Keynote Speeches

- **Meriem Slimani,** The Standardization and Development Coordinator of the African Telecommunication Union, ATU
- **Mohamed Elhaj,** SG17-RG-AFR Vice-Chairman
- **Ebrahim Alhaddad,** Regional Director, ITU Arab Regional Office
- **Tahani Abdalla Attia**, Minister of Information and Communication Technology, Sudan

The objective of the workshop is to build capacity and to share experiences and best practices in countries and to provide information regarding the status of implementations of existing cyber security strategies; to identify any gaps; and to yield a way forward.

Session 1

National Cybersecurity Strategies development (what is needed, and the way toward elaboration)

- **Moderators: Kiru Pillay**, South Africa
  Abusofian Dafalla, COMESA

- Objectives:
  Discuss the best way to initiate the work toward the development of a National Cybersecurity Strategy.

  What are the initial requirements, who should be involved?

  A further objective of this session is to understand the development process toward a solid National Cybersecurity Strategy, what are the main components or propriety areas.

Session 1 – Presentation 1

Towards a Multi-stakeholder Initiative to Develop and Improve National Cybersecurity Strategies

Serge V. Zongo, BDT

- *‘**What**’ is a National Cybersecurity Strategy and ‘**Why**’ is one required*
- *The ‘**How’** of developing a National cybersecurity Strategy was also identified with the following being main points:*
  - Have a champion who can ensure a move into implementation phase
  - Set up a dedicated local team with relevant expertise
  - Use existing models, tools and resources
- The Cybersecurity Toolkit helps nations develop or improve their National Cybersecurity strategies was introduced, which has an ultimate aim of:
  - Facilitate the elaboration, review and evaluation of National Cybersecurity Strategies
  - Harmonise and optimise the development effort of tools, guidelines, etc.
- Information sharing mechanism.

Session 1 – Presentation 2

A Maturity Model for National Cyber Security Strategy

Almerindo Graziano, Silensec

- *The presentation identified the Strategic Areas of a National Cybersecurity Strategy and introduced a Security Quadrant Model*
- *The adoption of the above maturity model was discussed*
- *Other issues highlighted included the need for the following*
  - *Creating a Governance Structure*
  - *Citizens Awareness and Competence*
  - *National Risk Assessment approach.*

Session 1 (continued) – Presentation 3

Etat de lieux de la stratégie de la cyber sécurité au Cameroun

Bertrand Kisito Nga, République du Cameroun

- *Mr Nga made a presentation on cyber security strategy in Cameroun.*
- *He highlighted the five pillars: infrastructure, policy and regulations, technology, capacity building.*
- *Cameroun has legislation and received support from ITU and South Korea.*
- *They conducted awareness.*

Session 1 (continued) – Presentation 4

Stratégie relative à la Cyber Sécurité dans les Pays Africains
Jean Pierre Pongo Konga, République Démocratique du Congo

- *Mr. Pongo presented the status of ICT and cyber security in D R Congo.*
- *The country faced the challenge of changing the policy makers frequently.*
- *D R Congo is ready to develop the cyber security and the necessary instruments.*
- *It has been discussed that the countries have to request the assistant from the regional and international organization.*
  It is emphasized to work with the regional and international frameworks to ensure harmonization and cooperation since cybercrime is a border less.

Session 1 – Discussion

- *The presentations highlighted the need for toolkits, model and specifically maturity models that could help countries 'kick-start' their National Cybersecurity Strategy initiatives.*
- *It was noted that no country starts from a zero-base and no country has a completed national strategy i.e. it is a constantly evolving process.*
- *The precedent for the use and adoption of Maturity Models within the ICT sector (the CMMI) was highlighted*
- *The discussion also focused on practical ways in which the Toolkit could be used.*
- *The current version Cyber Security Capability Maturity Model (CMM) – V1.2 would be piloted in late 2016.*

Session 2
Implementation of the National Cybersecurity Strategy (NCS)

- **Moderator: Meriem Slimani,** ATU

- Objectives:
  Understand pros and cons in having a national strategy implemented and at what cost.

  What are the financial implications, the lessons learnt?

Session 2 – Presentation 1

Implementation Strategy for Cybersecurity

Joey Jansen Van Vuuren, Council for Scientific and Industrial Research (CSIR)

- Although all countries are vulnerable to cybercrime, African countries are particularly vulnerable to cybercrimes due to the exponential growth in broadband access, the use of wireless technologies and infrastructure, high levels of computer illiteracy and ineffectual or insufficient legislation to deal with cyberattacks and threats .

- The presentation explained a cybersecurity policy implementation framework that will support the process of the implementation of cybersecurity in African countries for effective control and protection the countries' cyber infrastructure and citizens. The presentation included proposed implementation strategies, structures and sustainment measures for cybersecurity in an African country so that national cybersecurity is regarded as an integral part of national security.

Session 2 – Presentation 1

- It highlighted that national governments have the responsibility to provide, regulate and maintain national security and that cybersecurity is an important aspect of national security and the safekeeping of a nation's constituency and resources, which includes both cybersecurity and human security for their citizens and an efficient cybersecurity policy relies on a holistic approach;

- There is a need for a partnership between business, government and civil society.
  Governance structures were used in the development of the implementation framework for Africa with national security in mind.

Session 2 – Presentation 2

A Practical Overview Zain-SD Experience
Abdelgadir Alsayed, ZAIN Sudan Telecom

- The presentation provides an overview on implementation of cyber strategy in private telecommunications companies and the speaker highlighted the importance for the company to comply to international cyber security standards and best practices such as **Strategies, Policies and Compliance Antivirus-Firewall and Threat Management.**

- The challenge for the future is clearly a standardization issue.

- How to establish standards that make ICT devices and equipment secure and not need to look for added applications such as antivirus and others.

Session 2 – Presentation 3

On the Role of the Civil Society in the Implementation on Cybersecurity Programs in Africa

Cisse Kane, African Civil Society On the Information Society (ACSIS)

- The presentation explained how the civil society could play a key role in the process of the implementation of cyber security strategy.

- Indeed, the civil society role among others is to link between connected and unconnected people; reach grassroots populations at a local level;

- Promote the local languages for awareness campaign and could provide as well expertise for advocacy, training, research, sensitization and also lead implementation of projects on ICT development at regional and national levels.

Session 3
Integration of a National Cybersecurity Strategy (NCS) in the overall national ICT strategy

- **Moderators: Cisse Kane,** ACSIS

- Objectives:
  Analyse how the National Cybersecurity Strategy is an integral part of a national and regional framework, the interdependencies and the constraints with the other ICT cybersecurity related plans.

Session 3 – Presentations

- *Enhancing Cybersecurity in Africa: New Challenges for Regional Organizations?*
  Meriem Slimani, ATU

- Cyber *Security - Lessons From World Bank Projects*
  Anat Lewin, World Bank (remote)

- *Cloud Computing in Arab States: Legal Aspects, Facts and Horizons*
  Rouda Alamir Ali, BDT

Session 3 – Main issues discussed

- Cybercrime leads to very big losses for African countries economies and for the community
- Investing in prevention and cybersecurity is very important and could help preventing these losses
- Trust is very important in setting up cooperation between different stakeholders
- Cyber education and sensitization on Internet and ethics is needed
- Needs to allow means for R&D
- Africa is vulnerable 80% of pirated software, Cyberespionage
- Enormous losses
- Africa is a land of potential growth for the ICT sector
- Africa is running late in terms of Cybersecurity
- Africa is not benefitting enough from international opportunities.

Session 3 – Main recommendations (1/2)

- A lot to do for legal framework at a national and regional level
- There are very interesting initiatives Africa could learn from (e.g. WorldBank)
- Ratification of the African Union Convention on Cybersecurity to be accelerated
- E-commerce and m-commerce is a tremendous opportunity for African countries. Measures to protect e-commerce and m-commerce sector and to accompany its growth in a way that Africa could better benefit from it.
- There is a need of strong commitments at a very high level of decision in terms of cybersecurity
- Awareness and training at all levels is the key response

Session 3 – Main recommendations (2/2)

- Put a regional approach that strengthens legal, administrative, technical, executive and practical issues that rise from these services in order to ensure personal and critical data protection and privacy

- Need for regional coordination and cooperation

- Need for to harmonize legislation

- Develop safe harbour agreement for cloud computing in Arab countries.

Session 4
Critical Infrastructure Protection (CIP) as example of a multi-stakeholder approach

- **Moderator: Esam Abulkhirat,** OIC CERT

- Objectives:
  CIP is paying a bigger role than in the past on the management of critical services that most of the time are managed by the private sector. CIP must be an integral part of the National Cybersecurity Strategy and as such the engagement of the private sector and the other critical sectors in the country.

Session 4 – Presentation 1

National Cybersecurity Policy Framework (NCPF)
Kiru Pillay, Department of Telecommunications and Postal Services, South Africa

- This presentation was about the "National Cybersecurity Policy Framework (NCPF) in South Africa and how the banking PPP trans-national initiatives succeeded and gave a model that can duplicated.

- The presentation also outlined the general principles of the NCPF and challenges encountered.

Session 4 – Presentation 2

Critical Infrastructure Protection (CIP) as Example of a Multi-Stakeholder Approach
Christopher Ganizani Banda, Malawi

- This presentation demonstrated the best practices of the topic from a relevant model as well as how to identify prioritize and define roles plus risk and emergency plans.

Session 4 – Presentation 3

Cybersecurity Strategy
Ali Murkid, Group Chief Information Security Officer, ECOBANK

- Provided a different prospective by showing some threats outlook and risks globally and continentally and articulated same key drivers for the cybersecurity strategy.

Session 4 – Presentation 4

Enhancing the security of CIIPs in Europe - ENISA’s Approach

Serge Zongo, BDT

- Displayed the results and key findings of a study conducted by ENISA on CIIP of its member states.

Session 4 – Summary of the key recommendations

- The PPP is very crucial and it should be coupled with clear identification of roles and responsibilities.

- Encourage practical prioritization of what is classified as CI at the national level.

- Promote continues communication with executives and decision making bodies in order build trusted relationship and keep them alerted.

Session 5
National versus regional versus international

- **Moderator: Bertrand Kisito NGA,** Cameroon

- Objectives:
  A roundtable panel will be organized to understand what the impact is of a national strategy in the regional and international context? Is there a need to develop also an international strategy for a country?

Session 5 – Presentations

- *ITU-T CYBEX Standards for Cybersecurity Information Dissemination and Exchange*
  Martin Euchner, TSB
- Stratégie nationale de cybersécurité: impacts et défis régionaux et internationaux
  Emmanuel Adjovi, L'Organisation internationale de la Francophonie (OIF)
- *African Union Perspectives on Cybersecurity and Cybercrime*
  Souhila Amazouz, African Union
- *Overview, Projects & Activities*
  Esam Abulkhirat, *Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT)*
- *COMESA Cybersecurity Program*
  Abu Sufian E Dafalla, COMESA

Session 5 – Presentation 1

ITU-T CYBEX Standards for Cybersecurity Information Dissemination and Exchange

Martin Euchner, TSB

- He has recognized that ITU-T Study Group 17 developed international standards on security and on cybersecurity all the country must integrate in their national strategy:
- The ITU-T X.1500-series of Recommendations on cybersecurity information exchange (CYBEX) provide critical instruments to deal with rapidly changing and diversifying cybersecurity phenomena, directly contributing to data protection;
- Enumeration standards provide effective means of communication across businesses, government agencies as well as communities;
- Cyber-risks are highly volatile and manifest through unexpected combination of components, that require careful examination of technical risks through knowledge-base standards.

Session 5 – Presentation 2

Stratégie nationale de cybersécurité: impacts et défis régionaux et internationaux

Emmanuel Adjovi, L'Organisation internationale de la Francophonie (OIF)

Due to the transboundary nature of cyberspace, it was recognized that:

- his adoption and implementation impact the regional and international contexts;
- the formal convergence strategies / national policies conceal fundamental differences based on the fact that States bear the strategies do not always share the same values do not always pursue the same objectives and do not often defend the same interests.

To mitigate the dynamic tensions and relationships and ensure the effectiveness of digital security, it is recommended:

- to integrate with the national strategy an international component that takes into account international standards and facilitates cooperation with other countries, the region and internationally.

Session 5 – Presentation 3

African Union Perspectives on Cybersecurity and Cybercrime

Souhila Amazouz, African Union

- It was witnessed during the last decade remarkable achievements have been made in developing ICT infrastructures and services and therefore issues relating to cybercrime are emerging in Africa

It is recommended :

- to ensure that citizens, governments and business are protected.
- to implement concrete measures in the area of cyber-security, notably related to data protection, e-transactions and cybercrime;
- to elaborate further national cyber-security frameworks, harmonized at regional level and in line with existing international standards and practices so that trust and confidence in the use of ICTs is facilitated at all levels;
- to get a common approach at continental level on the security of the cyberspace and set up minimum standards and procedures to define a credible digital environment for developing the electronic communications and guarantee the respect of the privacy online.

Session 5 – Presentations 5 and 6

Overview, Projects & Activities

Esam Abulkhirat, *Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT)*

- In order to reduce the vulnerability of cyberspace, the following cybersecurity program has been recommended to:
- establish a multilevel system of security measures;
- expand expertise in and awareness of information security;
- adopt an appropriate regulatory framework to support the secure and extensive use of information systems;
- consolidate the position as one of the leading countries in international co-operative efforts to ensure cyber security.

COMESA Cybersecurity Program

Abu Sufian E Dafalla, COMESA

Session 5 – Discussion & Results

- Importance to have a regional approach to accelerate the cybersecurity approach

- Need to exchange information among African countries

- Cooperation at the regional level

- African countries to ratify the AU convention on cybersecurity and data protection, and transpose its provisions into national laws

Session 6
CIRT: Requirements and implementation

- **Moderator: Abdelgadir Alsayed,** Zain Sudan

- Objectives:
  Understand what the typical requirements are for building a Computer Incident Response Team (CIRT)?

  Which cybersecurity strategies are necessary for setting-up a CIRT?

  How can a CIRT be implemented in a country?

Session 6 – Presentations (1/3)

BDT CIRT Programme

Serge V. Zongo, BDT

- Mr. Zongo, (Phd) delivered his presentation challenging a Multi Level Response covering international, regional and national CIRT.
  He stated seven major points for a successful CIRT which should start with awareness.
  ITU services are available and also the on-demand services are also possible.

Brief about National Computer Security and Incident Response Center (Rw-CSIRT)

Charles Mugisha, Rwanda CSIRT

- Mr. Charles Mugisha remotely presented a country experience from Rwanda. He reported a successful story about Rwanda Cert where they build up a cybersecurity strategy, response coordination and a monitoring mechanism.

Session 6 – Presentations (2/3)

The Importance of Cyber Threat Intelligence for CERTs
Almerindo Graziano, Silensec

- Mr. Graziano (PHD, CEO and founder) presented what is called defence in depth from a practical points of view.

- He introduced an advanced model for tackling Cybersecurity problems for CIRTs and he encouraged all CIRT to think about CTI (Cyber Threat Intelligence) which will level up the CIRT to be a real active CIRT.

- Also he spoke about the big picture of Info Sec and how it is possible to predict cyber attacks in the future.

Session 6 – Presentations (3/3)

- *CIRT: Requirements and implementation*
  Muataz Elsadig, Sudan CERT

- Mr. Elsadig from CERT Sudan explained the strategy behind CERT and how we can benefit from it in national dimension as well as in the private sector – with detailed description for the process and procedures of the CERT and its relation with other similar entities.

Session 6 – Discussion

- A fruitful discussion with comments

- The main discussion point is from Mr Alsayed when he asked Silensec for what is called attack prediction.
  Others asked about getting deep help from ITU in organizing and helping with the CIRT.

- The overall discussion was commenting and thoughts from the audience where it almost looked like what has been said from the speakers.

- The need of more efforts was discussed to emphasize to work with regional and international entities to ensure harmonization and cooperation since cybercrime is border less.

Session 7
CIRT: Experiences and best practices

- **Moderator: Almerindo Graziano,** Silensec
- Objectives:
  Learn from experiences made in establishing and operating a Computer Incident Response Team (CIRT).

  Are there best practices which can be shared?

  How can CIRTs cooperate across country borders?

Session 7 – Presentation 1

- *NISSA in a Nutshell*, **Esam Abulkhirat**
  National Information Security & Safety Authority Libya,

- The presentation covered the following key points:
  - The set up of NISSA and its remit
  - The experience of developing the Libyan CERT and specifically the

- Challenges related to security culture, resources and political stability
  - How a CERT can seek alternative funding through a service exchange

- Mechanism such as the provision of vulnerability assessment and incident investigation services.

Session 7 – Presentation 2

Tunisian experience in the National Cyberspace Security
Nadhir Loghmari, Agence Nationale de la Sécurité Informatique, Tunisie

- The presentation covered the following key points:
  - The experience of the Tunisa-CERT and the range of capabilities developed since its establishment in 2004
  - Emphasis on the use of open source technologies at the core of all the CERT services
  - The role of the CERT is certifying auditors responsible for carrying out security audits within the country
  - The international collaboration and support towards other African CERTs of Nigeria.

Session 7 – Presentation 3

Eg-CERT Lessons Learned

Ahmed Mashaly, NTRA, Egypt

- The presentation covered the following key points:
  - The services offered by Egypt CERT and the development of the CERT over the years
  - The experience of the Egypt-CERT with regards to the challenges competence both in terms of acquisition and retention
  - The international collaboration and support towards other African CERTs of Uganda and in a minor role Tanzania.

Session 7 – Discussion

- The presentations highlighted the need and benefit of international cooperation between national CERTs.

- Discussion and questions were raised regarding the challenges of hiring the right staff and how to ensure staff retention.
  It was noted that loosing staff to private companies is often inevitable but that could also be an enabler for establishing stronger collaborations with those very same companies.

- It was also highlighted how political stability is a key requirement for the establishment and development of the CERT as it naturally affects the resource allocation and the required commitment from the nation.