BDT CIRT PROGRAM

Serge Valery Zongo
International Telecommunication Union

Agenda

1. Coordinated Response
2. BDT cybersecurity program
3. Why a CIRT
3. CIRT SERVICES
4. NATIONAL CIRT PROGRAM
5. STUDY GROUPS
6. PUBLICATIONS

Coordinated Response

Need for a multi-level response to the cybersecurity challenges

BDT Cybersecurity program

7 Service areas – 16 Services

Engagement and awareness

- Global Cybersecurity Index
- Global, Regional and National events
- Information dissemination

Computer Incident Response Team (CIRT) Program

- CIRT design
- CIRT implementation
- CIRT enhancement

Cyber Drills

- Regional drills
- National drills

National Cybersecurity Strategy (NCS)

- National Cybersecurity assessment
- NCS development support

In-Country Technical Assistance

- Technical Support (e.g. vulnerability assessments)
- Risk Management Support

Information sharing

- Best Practices Sharing
- Information Exchange Tools and Techniques

Human Capacity Building

- Curricula and Training Programs
- Bespoke Training

Developing National CIRTs

Resolution 58 – Encourage the creation of national computer incident response teams, particularly for developing countries

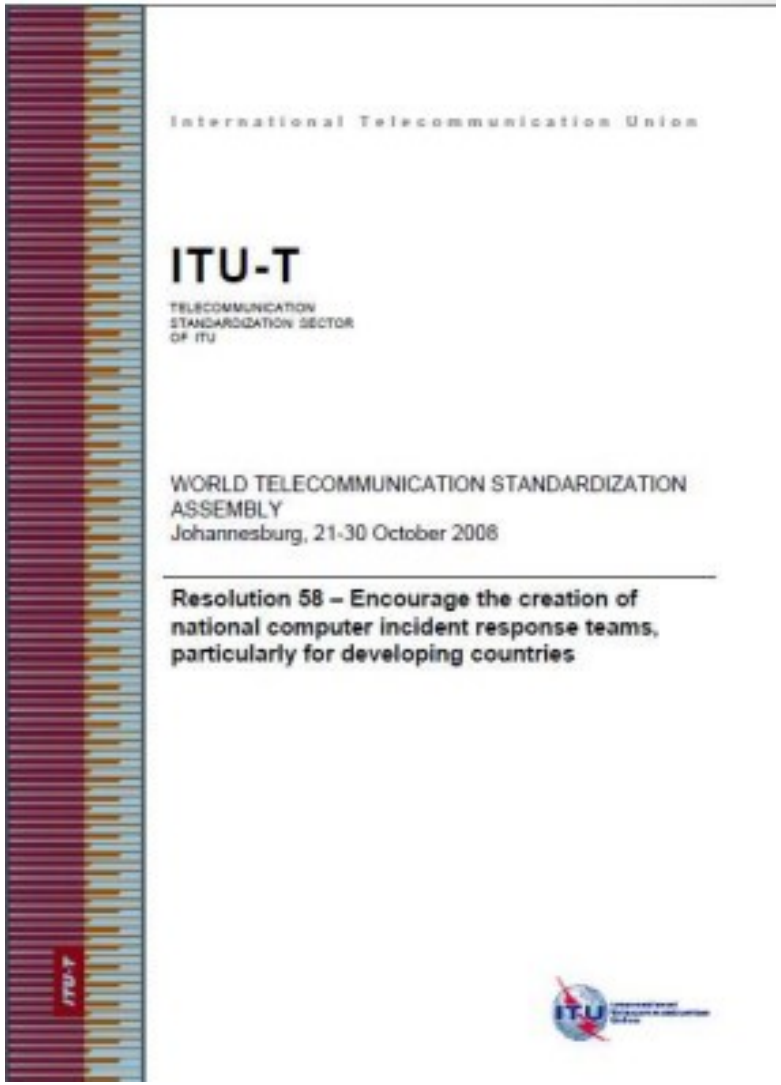
there is still a low level of computer emergency preparedness within many countries particularly developing countries

- the high level of interconnectivity of ICT networks could be affected by the launch of an attack from networks of the less-prepared nations, which are mostly the developing countries

- the importance of having an appropriate level of computer emergency preparedness in all countries

- the need for establishment of computer incident response teams (CIRTs) on a national basis

- importance of coordination within and among the regions,



WHY A NATIONAL CIRT

CIRT

- Serve as a trusted focal point
- Develop a capability to support incident reporting.
- Develop an infrastructure for coordinating response.
- Conduct incident, vulnerability & Artifact analysis.
- Participate in cyber watch functions.
- Help organizations develop their own incident management capabilities.
- Provide awareness, education & trainings
- Make security best practices & guidance available.

ITU's National CIRT Program

National CIRT
Capacity building

Assessment

- Assess existing capability of/need for national cybersecurity mechanisms
- On-site assessment through meetings, training, interview sessions and site visits
- Form recommendations for plan of action (institutional, organizational and technical requirements)

Implementation

- Implement based on the identified needs and organizational structures of the country
- Assist with planning, implementation, and operation of the CIRT.
- Continued collaboration with the newly established CIRT for additional support
- Capacity Building and trainings on the operational and technical details

Cyberdrill

- Exercises organized at both regional and international levels
- Help enhance the communication and response capabilities of the participating CIRTs
- Improve overall cybersecurity readiness in the region
- Provide opportunities for public-private cooperation

CIRT SERVICES

Phase1- Reactive Services

- CIRT portal
- Incident management system
- CIRT mailing list
- Incident response framework

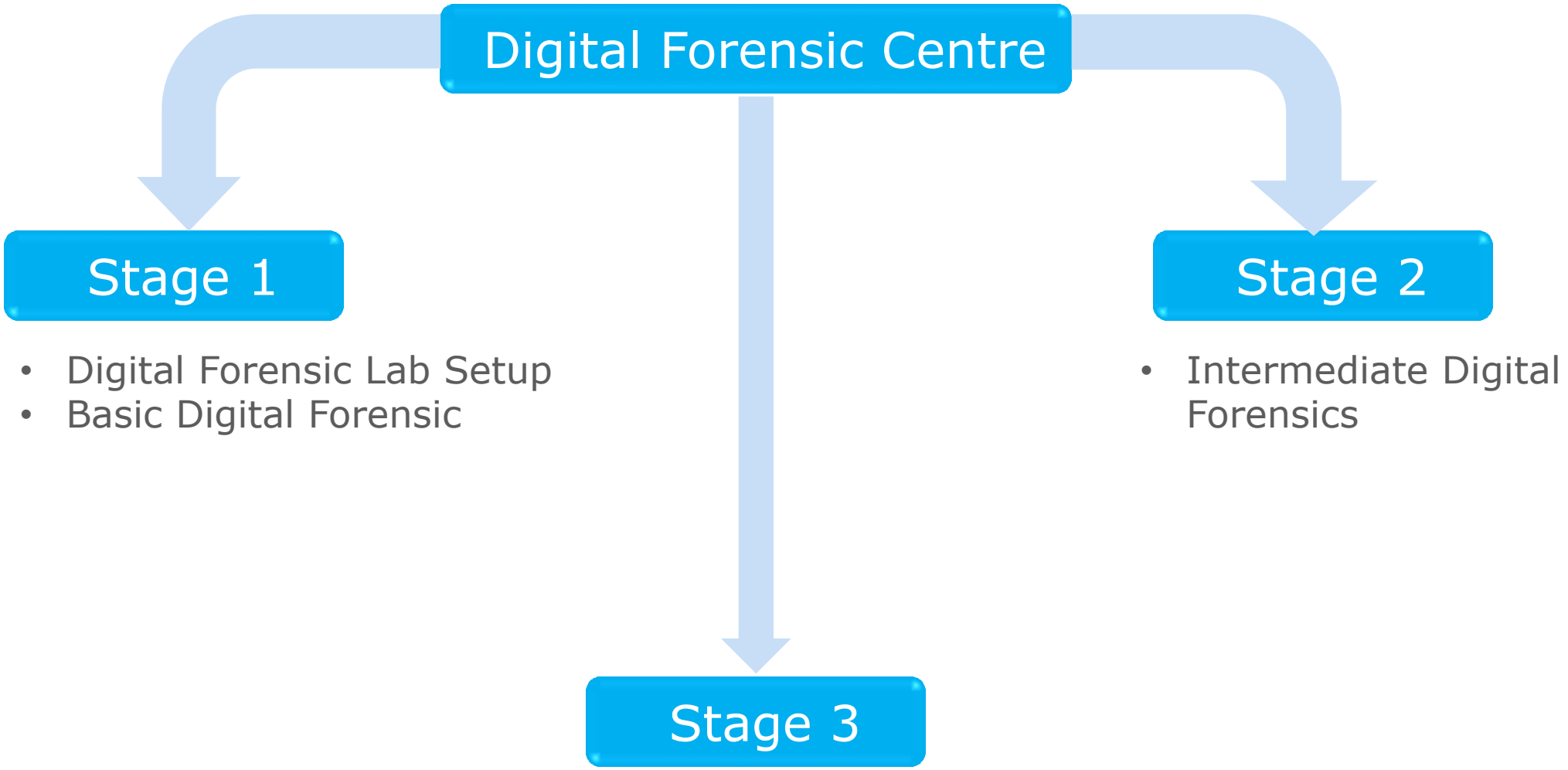
Phase 2: Proactive Services

- AWARE
- HORNET
- Security assessment framework

Phase3 : Forensics services

- Digital forensic services
- Risk analysis and compliance
- Security consulting

Phase3 : Forensics services



CIRT SERVICES

Reactive Services	Proactive Services	Artifact Handling
Alerts & Warnings	Announcements	Artifact Analysis
Incident Handling	Technology Watch	Artifact response
Incident Analysis	Security Audits	Artifact response coordination
Incident response support	Security Assessments	**Security Quality Management**
Incident response coordination	Configuration & Maintenance of Security	Risk Analysis
Incident response on site	Development of Security Tools	BC and Disaster Management
Vulnerability Handling	Intrusion detection services	Security Consulting
Vulnerability Analysis	Security related information dissemination	Awareness Building
Vulnerability Response		Education/Training
Vulnerability Response Coordination		Project Evacuation or Certification

National CIRTs for enhancing global resilience

ALGERIA, BURKINA FASO, CAMEROON, COTE D'IVOIRE, EGYPT, ETHIOPIA, GHANA, KENYA, NIGERIA, RWANDA, SOUTH AFRICA, SUDAN, TANZANIA, TUNISIA, UGANDA, ZAMBIA

16 countries with National CIRTs in Africa

103 countries with National CIRT worldwide

National CIRT Program in Africa

- Assessments conducted for **30** African countries: Angola, Botswana, Burkina Faso, Burundi, Cameroon, Chad, Congo (Dem Rep), Congo (Republic), Comoros, Côte d'Ivoire, Gabonese Republic, Djibouti, Gambia, Ghana, Kenya, Lesotho, Liberia, Mauritania ,Niger , Nigeria, Rwanda, Senegal, Sierra Leone, Sudan, Swaziland, Tanzania , Togolese Republic, Uganda , Zambia, Zimbabwe.
- Implementation completed for **7** African countries :Burkina Faso, Côte d'Ivoire, Ghana, Kenya, Tanzania, Uganda, Zambia.
- Implementation in progress for **2** African countries Burundi and **Gambia**
- CIRT Enhancement in progress in **1** country: Kenya

Cyberdrill

Objectives

- Improve incident response skills
- Promote CIRT-to-CIRT cooperation
- Human capacity building for CIRT staff
- Awareness raising for decision and policy makers

Status

- 15 Regional exercises undertaken at regional level in 4 years with the participation of 100 countries
- For Africa Region – 2015, Rwanda, 21 countries – 2014, Zambia, 18 countries.
- 2016 Drills in Mauritius (4- 8 April) for Africa Region, 16 countries, Tunisia (24-27 May) for Arab Region, Ecuador (27 June- 1rst July) for America Region

ITU Study Groups

A platform for information exchange between ITU Member States and Sector Members (industry, academia etc.)

- ITU-D Study Group 2
  - Question 3/2: Securing information and Communication networks: Best practices for developing a culture of Cybersecurity
- ITU-T Study Group 17 : Security
  - Standardization work on cybersecurity

Sub-Regional Forum on Cybersecurity for Central African States

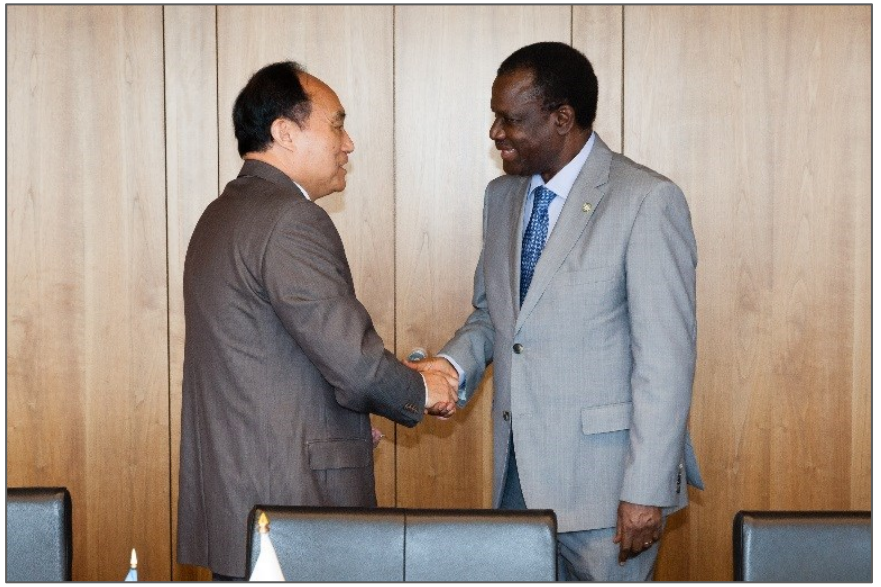
- 24-27 February 2015, Yaounde, Cameroon
- 300 participants, 15 countries
- Economic Community of Central African States (ECCAs) Ministers' meeting on the 27 February
  - A set of recommendations approved to enhance cybersecurity readiness through actions at ECCAS and at the country level

Cooperation with ECOWAS

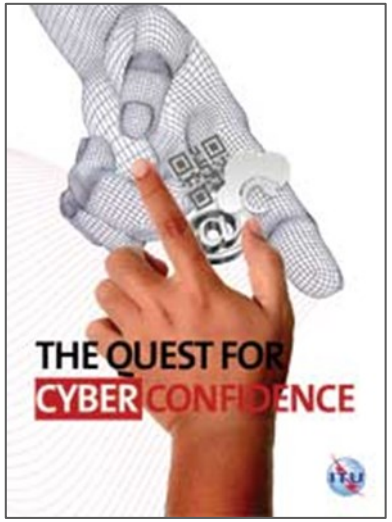
MoU signed with ITU on 8 June 2015

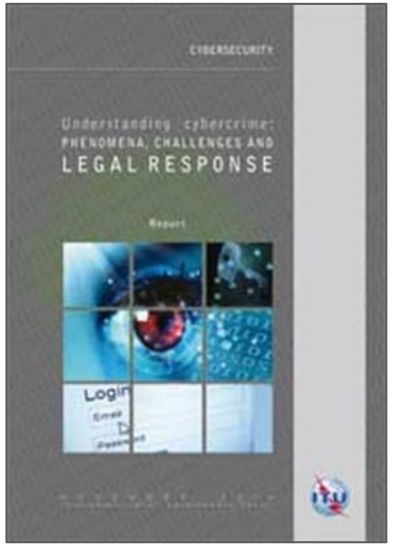
To enhance the Cybersecurity posture of ECOWAS member countries through country specific initiatives as well as regional initiatives including

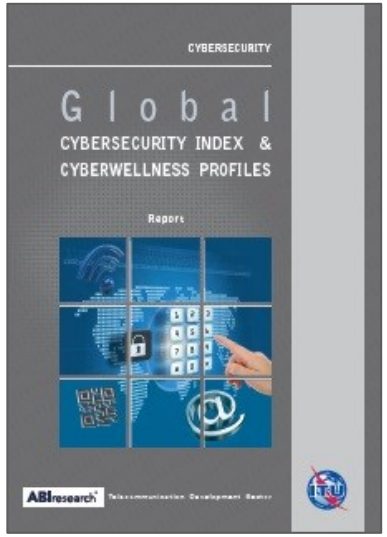
- National CIRT/CERT program
- customized capacity building initiative
- elaboration of a sustainable Cybersecurity roadmap
- the Global Cybersecurity Index
- the Child Online Protection initiative
- the harmonization and enhancement of legislations
- the elaboration of national Cybersecurity strategies



Publications







Free download from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx

Merci
Thank you

Cybersecurity@itu.int