Expert Meeting on

CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE: INCLUDING CASE STUDIES AND LESSONS LEARNED

25-27 March 2015

Cyber Security Challenges & Capacity Building

By

Marco Obiso

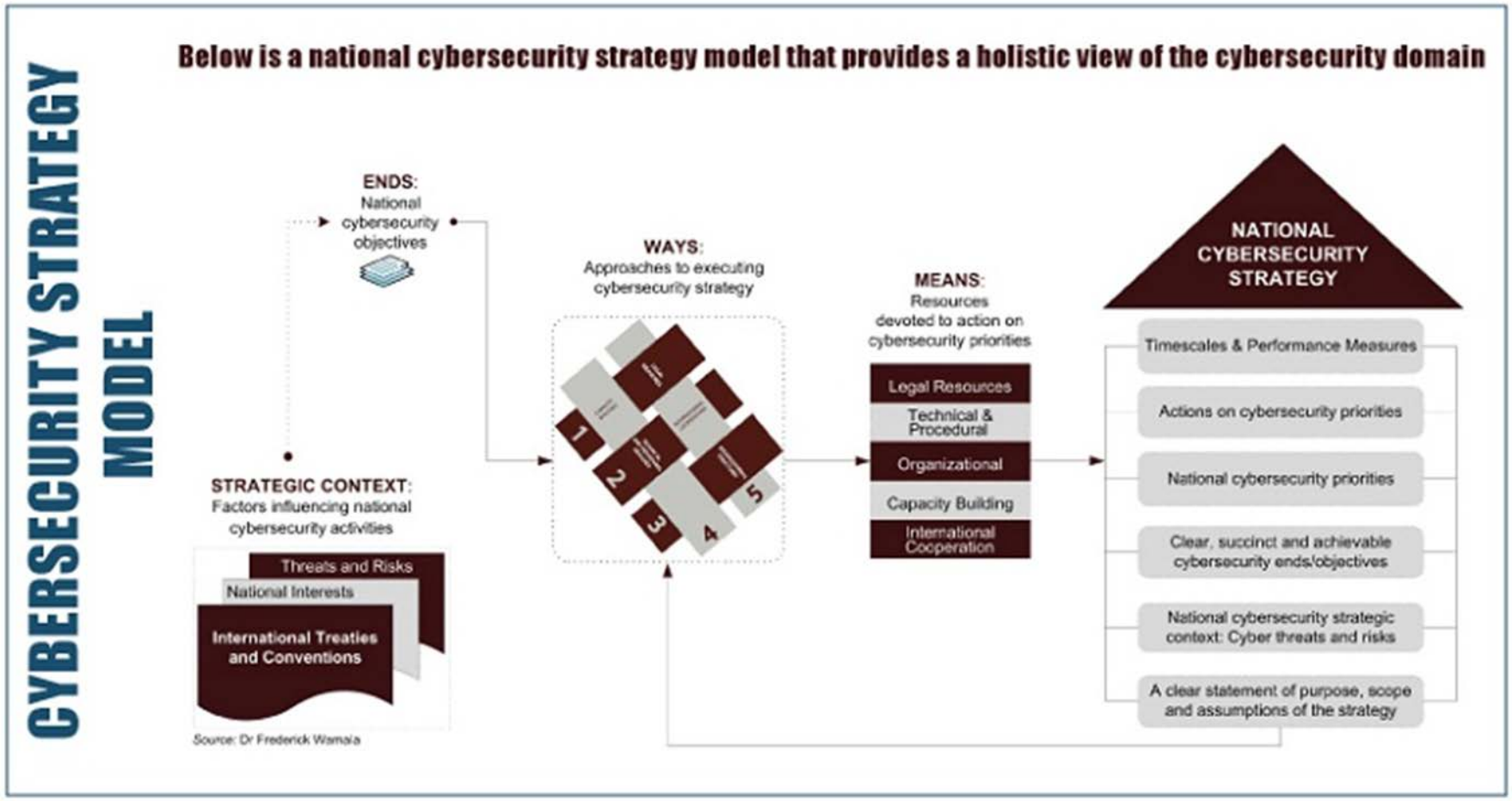
International Telecommunication Union

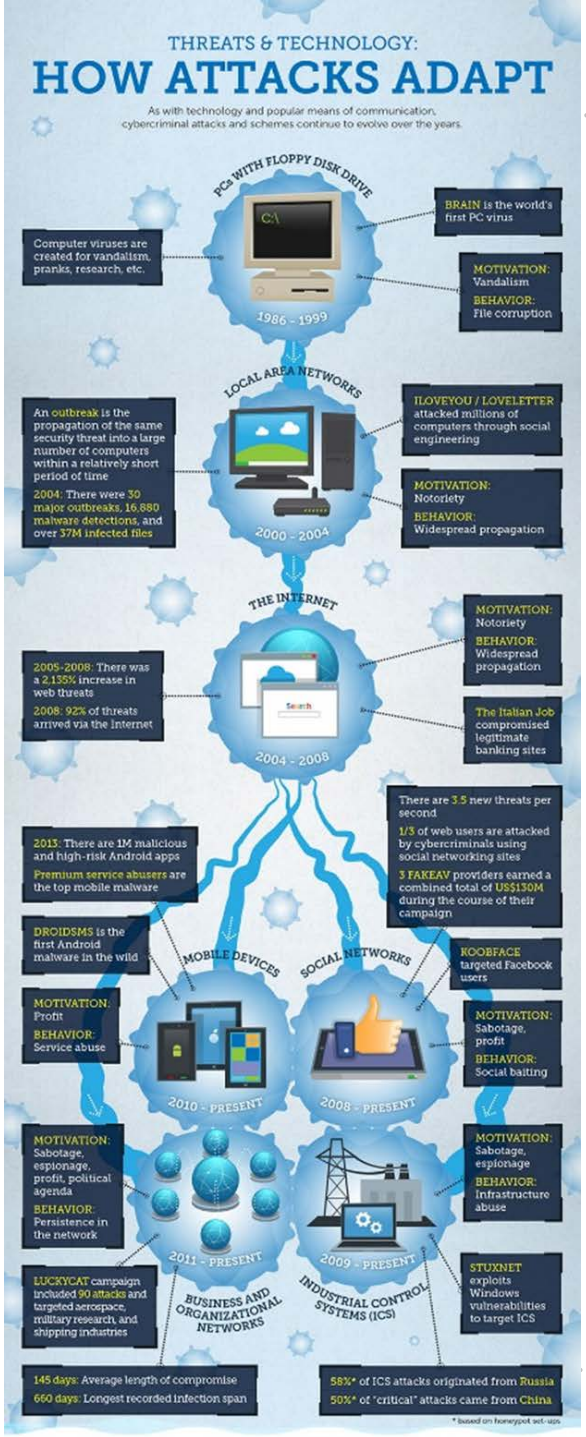
Cybersecurity Challenges & Capacity Building
March 2015

Cybersecurity Challenges

Challenge 1: International Cooperation

Challenge 2: Critical Information Infrastructure Protection (CIIP)

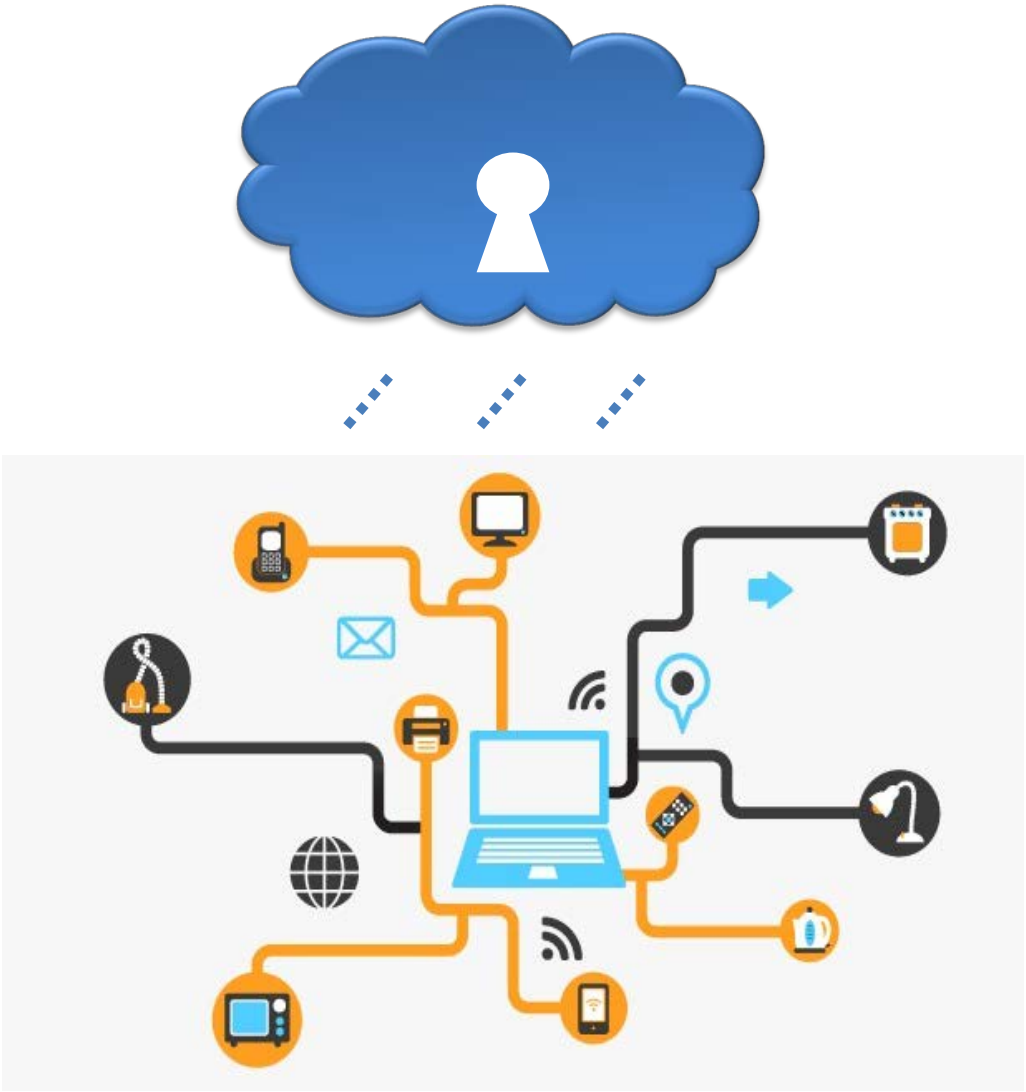




Challenge 3: Attacks are evolving and Malware is becoming increasingly complex

Source: Trend Micro

Challenge 4: M2M technology, IoT and Cloud computing



Challenge 5: Secure digital identification

Challenge 6: Development of common standards

Challenge 7: Child Online Protection (COP)

Challenge 8: Increasing awareness

Recommendations

Strengthen Cooperation

Information and best practice sharing

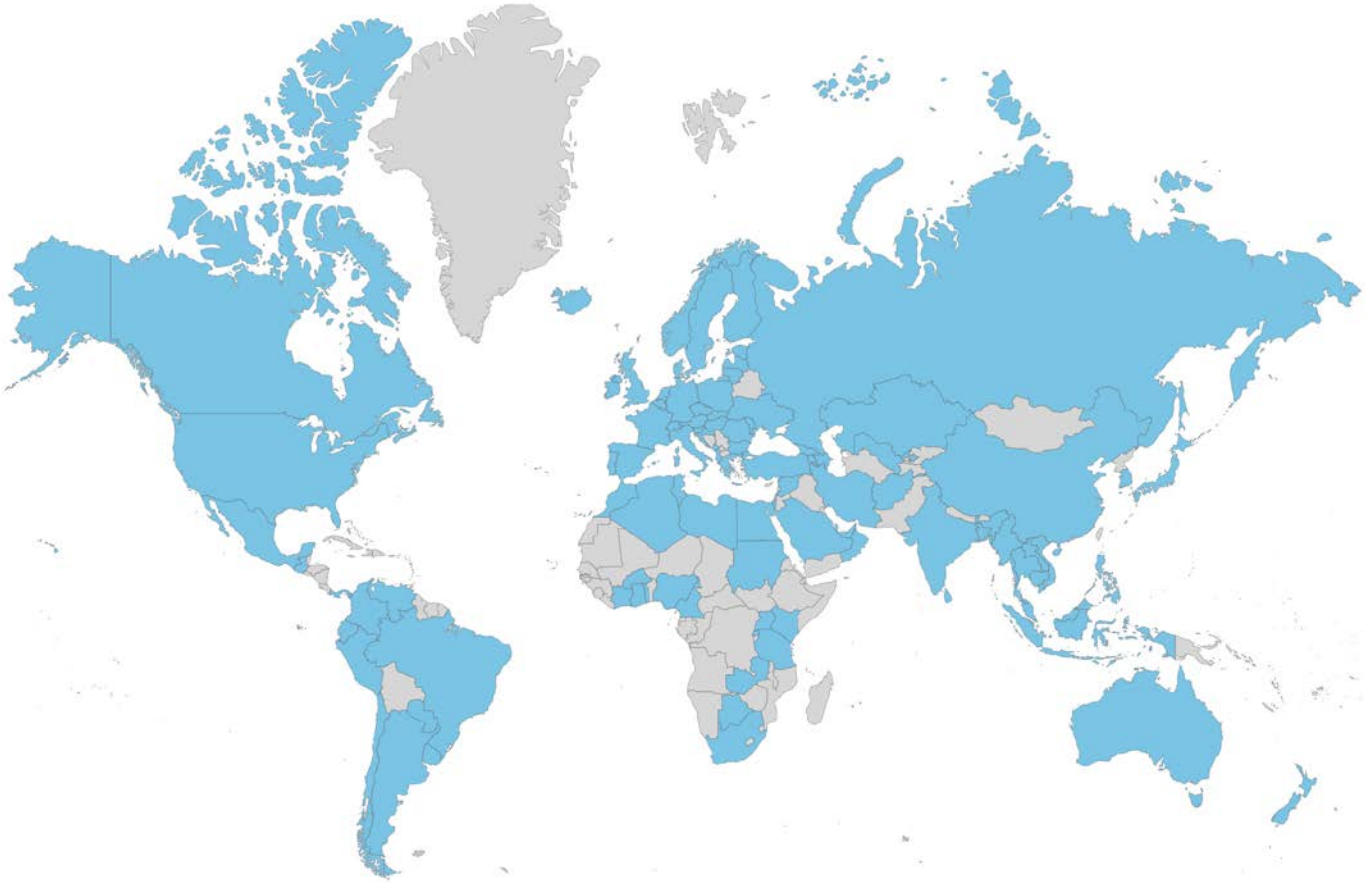
Public-Private Partnerships

Develop National Capabilities

Measuring Cybersecurity

Elaboration of Standards

Protection of vulnerable groups



101 National CIRTs Worldwide

ITU's National CIRT Programme

- Assessments conducted for **61** countries

  25 of them in Africa. In progress in Ethiopia and Republic of Congo

- Implementation completed for **9** countries

  7 of them in Africa

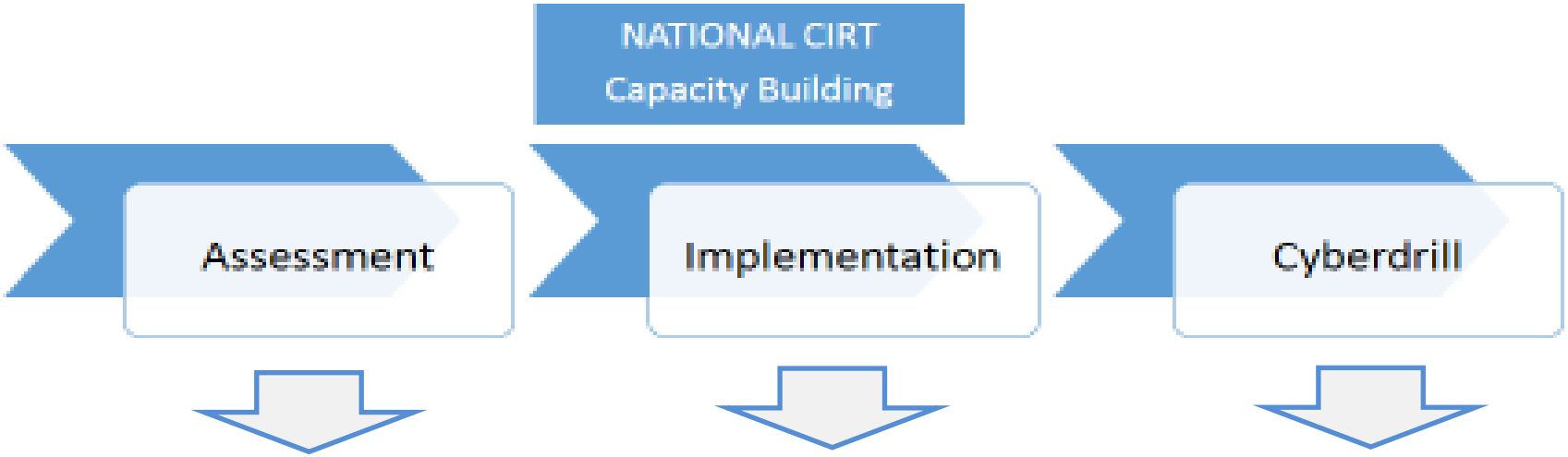
- Implementation in progress for **6** countries

  Burundi and Gambia among others

- **9** cyber drills conducted with participation of over **90** countries

  Last Cyberdrill was for Africa in September 2014, in Livingstone, Zambia

ITU's National CIRT Programme



- 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)

- 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

- 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

National CIRTs - Critical Success Factors

- Government Commitment
- Identify the right constituencies
- Engage the key players
- Be visible and collaborate within the country, regionally and internationally
- Have a strong technical team with right expertise

Objective

The Global Cybersecurity Index (GCI) aims to measure the level of commitment of each nation in cybersecurity in five main areas:

- **Legal Measures**
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation

Goals

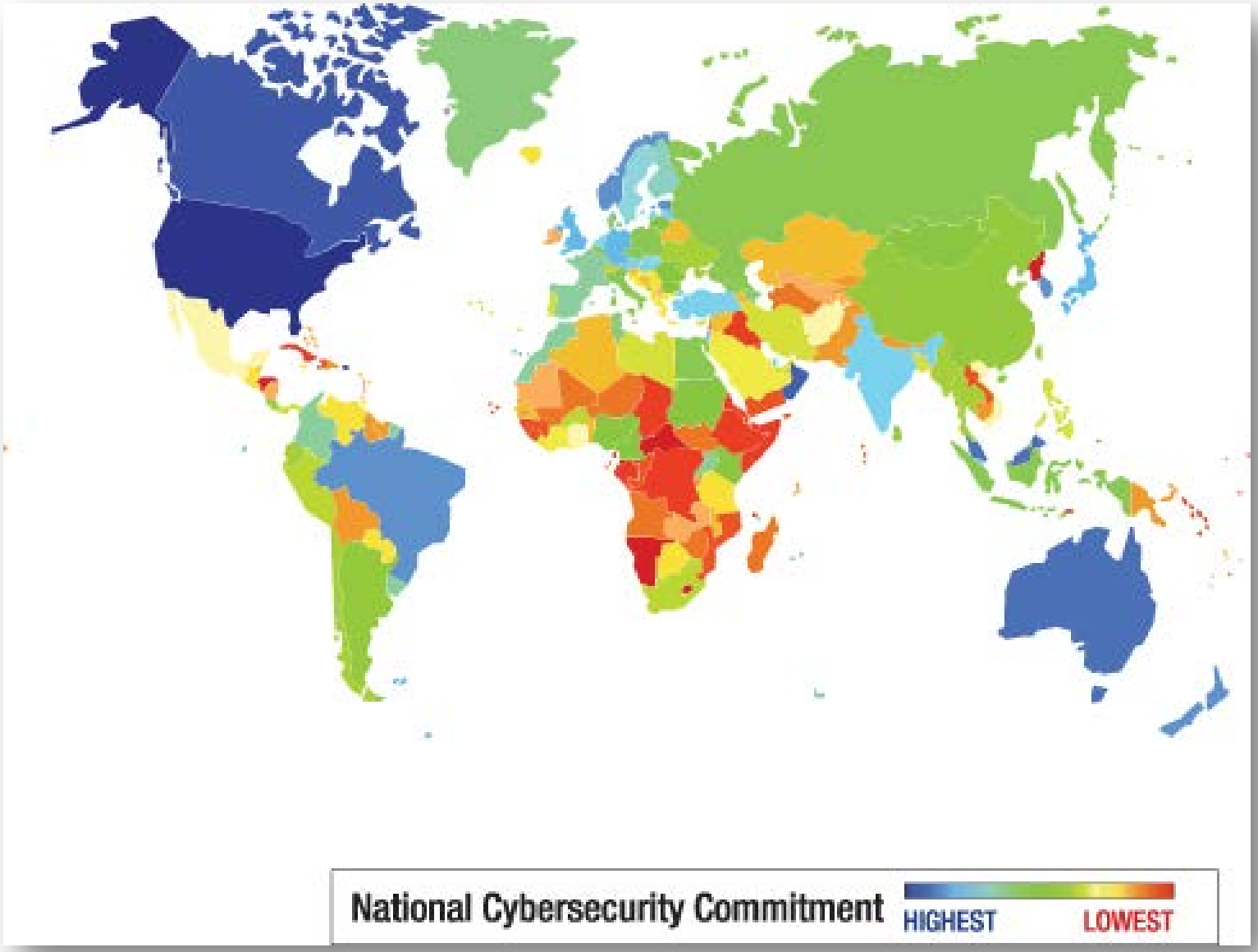
- Promote cybersecurity strategies at a national level
- Drive implementation efforts across industries and sectors
- Integrate security into the core of technological progress
- Foster a global culture of cybersecurity

104 countries have responded

Final Global and Regional Results 2014 are on ITU Website

http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Next iteration in progress


National Cybersecurity Commitment
HIGHEST
LOWEST

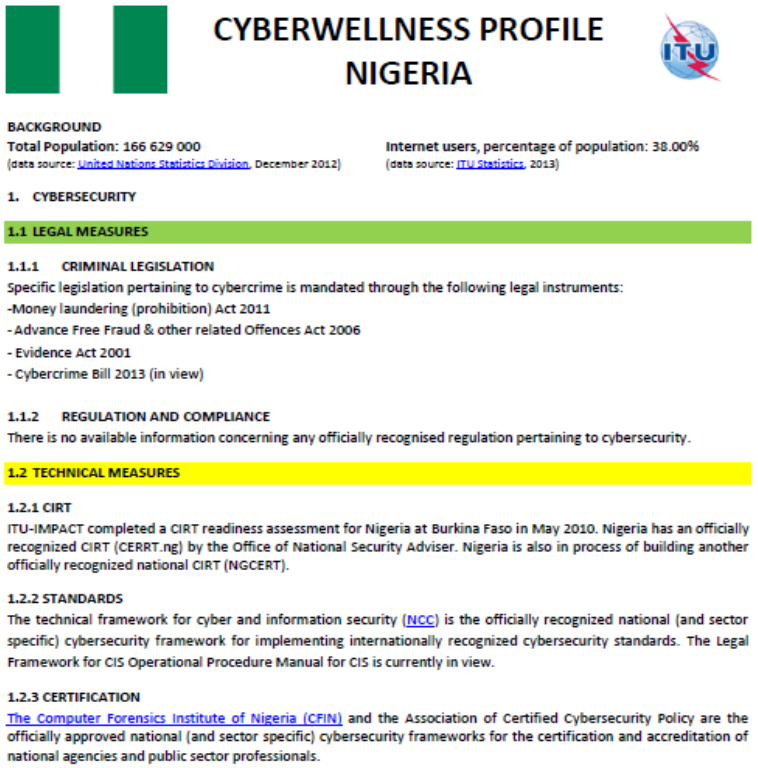
Cyberwellness Country Profiles

Factual information on cybersecurity achievements on each country **based on the GCA pillars**

Over 190 profiles to date

Live documents –
Invite countries to assist us in maintaining updated information
cybersecurity@itu.int

EXAMPLE →



CYBERWELLNESS PROFILE
NIGERIA

BACKGROUND

Total Population: 166 629 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 38.00%
(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation pertaining to cybercrime is mandated through the following legal instruments:
-Money laundering (prohibition) Act 2011
- Advance Free Fraud & other related Offences Act 2006
- Evidence Act 2001
- Cybercrime Bill 2013 (in view)

1.1.2 REGULATION AND COMPLIANCE

There is no available information concerning any officially recognised regulation pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU-IMPACT completed a CIRT readiness assessment for Nigeria at Burkina Faso in May 2010. Nigeria has an officially recognized CIRT (CERRT.ng) by the Office of National Security Adviser. Nigeria is also in process of building another officially recognized national CIRT (NGCERT).

1.2.2 STANDARDS

The technical framework for cyber and information security (NCC) is the officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards. The Legal Framework for CIS Operational Procedure Manual for CIS is currently in view.

1.2.3 CERTIFICATION

The Computer Forensics Institute of Nigeria (CFIN) and the Association of Certified Cybersecurity Policy are the officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

Building a global partnership

Capacity building initiatives, joint consultations and more.

Best practices in cybercrime legislations, joint technical assistance to member states, information sharing

Tap on expertise of globally recognized industry players and accelerate info sharing with ITU member states

Collaboration with ABI Research – **The Global Cybersecurity Index (GCI)**

Collaboration with FIRST – To share best practices on computer incident response, engage in joint events, facilitate affiliation of national CIRTS of member states

Collaboration with Member States – Regional Cybersecurity Centres

Thank You

http://www.itu.int/cybersecurity

cybersecurity@itu.int