Workshop on Cyber Security & Cyber Crime Policies

Policies for African Diplomats

ROLE OF INTERPOL IN FIGHTING CYBERCRIME IN AFRICA

SRIAU Office

Augusto de CARVALHO

12-13 APRIL 2018 ADDIS ABABA
OVERVIEW

- Vision and Mission
- Global Presence
- Global Programmes: Crime priority areas
- Types of Cybercrime in Africa
- Cyber Incident Response Plans
- Regional Responses
- INTERPOL’s global cybercrime strategy
- The Role of SRIAU
Vision: Connecting police for a safer world

Mission: Preventing and fighting crime through enhanced international police cooperation

This is done by:

• Facilitating international police cooperation
• Ensuring secure communication
• Providing operational support to member countries
• Training to enhance capabilities of law enforcement agencies to combat organised crime.
INTERPOL’s GLOBAL PROGRAMMES

Crime Priority Areas

COUNTER-TERRORISM
- Terrorist Networks
- Maritime Security
- CBRNE

ORGANIZED & EMERGING CRIME
- Illicit Goods & Counterfeit Pharmaceuticals.
- Drug Trafficking
- THB – People Smuggling
- Environmental crimes.

CYBERCRIME
- Borderless crime
- Make cyberspace safer.
- Identify cyber attacks & perpetrators
Types of Cybercrime in Africa

- Hacking
- Denial of service attack
- Virus Dissemination
- Computer Vandalism
- Cyber Terrorism
- Software Piracy
Threats of Cybercrime in Africa

- Internet Security
- Computer Security
- Mobile security (Online Business Services)
- Network security
Cyber Incident Response Plans in Africa

- Develop national Cybercrimes and Cybersecurity legislations in line with relevant international conventions & model laws.

- Mitigate & manage potential cyber security breaches (organizations/clients/customers).

- Gather threat intelligence on a regular basis to avoid any gaps in protection, IT to be improved as necessary.
Cyber Incident Response Plans in Africa (cont..)

- Conduct an IT risk assessment by data & network mapping to determine data, assets & devices the business holds & value.
- Engage government authorities to develop cyber security protocols & necessary funding for implementation.
- Set up a regional response team (with back-ups) with members of business functions, IT legal, etc.
- Publish companies policies on cyber security & response to all staff.
- Updated training of personnel on a regular basis
Regional Responses

- Develop a common regional policy framework rooted in the broader cybercrime strategy;
- Enhance operational information & expertise between public & private sectors to combat cybercrime;
- Establish a regional real-time information sharing & analytical platform for enabling INTERPOL & LEA users worldwide to conduct research & analysis on cybercrime;
- Develop a comprehensive analytical intelligence reports on cybercrime in Africa;
- Adherence on Annual African Working Group Meeting on Cybercrime for Heads of cybercrime.
INTERPOL’s Global Cybercrime Strategy

Five Action Streams

- Threat Assessment & Analysis
- Trends Monitoring.
- Access to & Exploitation of Raw Data
- E-Evidence Management Process
- Correlation of Cyber & Physical Information.
- Harmonization & Interoperability
Information Sharing & Analysis

Global Coordination in Cybercrime Investigations

Digital Forensics

Cyber Training
Identify active cybercriminal groups & their membership.

Collect, exchange, analyse & store information about cyber criminals & their activities.

Assist member countries to build national digital forensic capacity & multi-stakeholder expertise.

Provide analytical support on complex cyber crime investigations to member countries.
CONCLUSION

- Young population that is quickly using new technologies, Africa is on the verge of an Internet boom.

- Africa needs to urgently address efforts to combat cybercrime & improve its cyber security attitude.

- INTERPOL will continue its efforts to facilitate and effectively coordinate joint operations against cybercrime.

- To produce and distribute actionable intelligence to mitigate risks posed by cybercrime, while drawing on private-sector experience, using INTERPOL Cyber Fusion Centre.

- Member countries in Africa should increase their understanding of Internet governance to actively voice the regional needs.
I thank you for your attention
Je vous remercie pour votre attention
Gracias por su atención
نشكركم جزيل الشكر على انتباهكم