Pravin HARRAH & Kaleem USMANI, Mauritius

The experience of capacity building

Launching of the Glacy Project 24 March 2014

The Objectives of EARCN are to:

- Promote effective exchange of information
- Facilitate working relationships/collaboration
- Facilitate and promote efficient informal and formal international cooperation
- Exchange information on best practices, technical assistance and capacity building to combat cybercrimes

GPEN
Global Prosecutors E-Crime Network

Judicial Training of Trainers on Cybercrime and Electronic Evidence,19th to 23 of August 2019, IJLS Mauritius, organised by the CoE in collaboration with the Office of DPP/ EARCN/IAP : Re capacity building program which we intend to impart in the region/ among members of the EARCN.

Mauritius acceded to the Budapest Convention on Cybercrime in November 2013

– Country level assessment on the sate of cybercrime

– Series of capacity building programmes organised by the Council of Europe (CoE) in Mauritius to prevent and fight cybercrime for Judiciary, Law Enforcement, CERT and Policy makers.

– Legal Framework Assessment

How GLACY/GLACY+ project helped Mauritius to build capacity

- Alignment of Computer Misuse and Cybercrime Act 2003 with the Budapest Convention on Cybercrime

- Development of the national Cybercrime Strategy 2017-2019

- Development of CIIP Policy

- Conceptualization of National Cyber Incident Response Plan

- Setting up of Centralised Online Incident Reporting System

- Setting up of ITU Centre of Excellence (Regional trainings planned in Sep and Nov 20

- Mauritius facilitated the study tours of Tonga & Philippines for their CERT setup

- Conducted Cyber exercise for the 15 SADC countries in September 2018

- Facilitated study tour of Madagascar for their CERT setup

- Assisted Senegal to build CERT capacity as part of COE mission

1. Incident Resolution

2. Not allowing state territory for internationally wrongful acts

3. Cooperate to exchange information with states

4. Right to Privacy (Data Protection Act)

5. Appropriate measures to protect state critical infrastructure from ICT threats

6. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.

7. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities.

8. States should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age.

9. States should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions.

10. States should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.

11. States should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices;