GLACY

Global Action on Cybercrime

Action globale sur la cybercriminalité

GLACY Launching Conference

Dakar

Senegal

24th to 27th March 2014

Today's Agenda

- Country Reports and Conclusions
- Recommendations
- Country Work Plans
- Coffee
- **Round Table**
- Your comments on the Country Reports
- Identify your 5 top priorities for COE support

GLACY – Expected Results

Result 1 - Engagement of decision-makers: Decision-makers of project countries are aware of cybercrime threats and rule of law/human rights implications and have identified strategic priorities regarding cybercrime

Result 2 - Harmonisation of legislation: Amendments are drafted to bring domestic legislation fully in line with the BCC and to improve legislation and regulations on data protection and child online protection

Result 3 - Judicial training: Enhanced skills for judges and prosecutors regarding cases on cybercrime and electronic evidence

Result 4 - Law enforcement capacities: Enhanced specialised skills and institutions for investigations on cybercrime and electronic evidence

Result 5 - International cooperation: Enhanced international law enforcement and judicial cooperation against cybercrime

Result 6 - Information sharing: Increased public/private and interagency information sharing in line with data protection standards

Study Visits

Philippines

Senegal

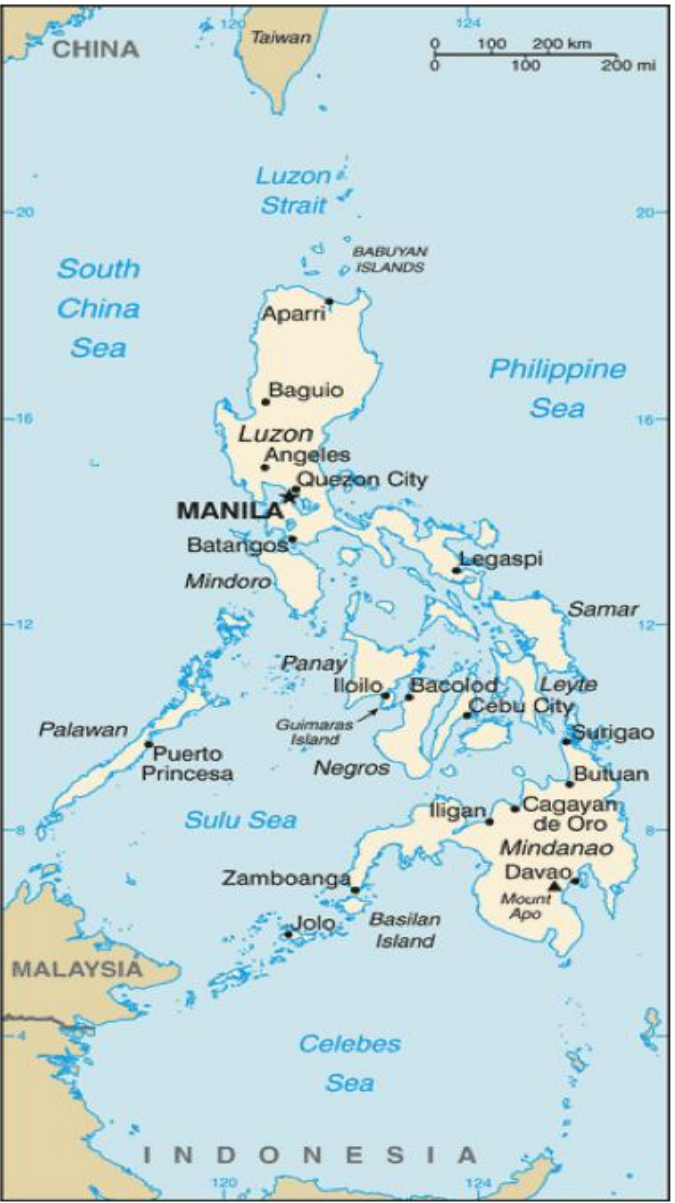
Mauritius

Morocco

South Africa

The purpose of the study visits is to build on the initial assessments of criminal justice capacities regarding cybercrime and electronic evidence, provided by each country. The teams will work with countries to identify areas in each country, requiring support through the GLACY project and to identify benchmarks against which to determine progress made in the course of the project.

Philippines



Study Visit

27th to 31st January 2014

Visiting Team

Nigel Jones – UK

Giorgi Jokhadze – Georgia

Angel (Lito) Averia - Philippines

Cybercrime Situation

- Over 1/3 of the population has Internet
- Over 100% of the population has a cell phone
- About 1,000 “cybercrimes” reported for each of 3 previous years.
- NBI and PNP investigate
- Different recording systems in place.
- Under cybercrime law ICTO is to create a CERT.

Cybercrime Situation

- Challenges
  - Insufficiency of legislation and policies that deter cybercrimes;
  - Concurrence of roles of government agencies without delineation of their respective tasks and coordinated actions;
  - Technical constraints in investigating and prosecuting cybercrimes;
  - Insufficiency of government support in enhancing the capabilities of law enforcement agencies, prosecution and the judiciary;
  - Absence of mechanisms that require telco's and ISP's to assist law enforcement authorities in investigating and prosecuting cybercrime.

Legislation

- Various laws currently cover cybercrime
- Cybercrime Prevention Act 2012 was declared unconstitutional
- Ruling made on 24th February 2014
- Electronic Evidence often held inadmissible in criminal proceedings.
- Data Privacy Act 2012 in place

Institutional Framework

- Department of Justice (Office of Cybercrime)
- National Bureau of Investigation (NBI)
    - 8 Agents/5 Special Investigators/regional operatives
    - Digital Forensic Capability
- Philippines National Police (PNP)
    - 110 Special Investigators
    - Digital Forensic Capability 569 cases in 2013
- National Prosecution Service
    - No specialist prosecutors
    - No involvement in investigation

International Cooperation

- Mechanisms
  - Mutual Legal Assistance Treaties (MLATs)
  - 24/7 Point of Contact (POC) Network of the Interpol and G8

The CPA provides:

- "SEC 23. *Department of Justice (DOJ*— There is hereby created an Office of Cybercrime within the DOJ designated as the central authority in all matters related to international mutual assistance and extradition."

Training

- PNP has developed its own training
- Ready made cybercrime training room
  - Identification and Seizure of Digital Evidence Course
  - Introduction to Cybercrime Investigations Course
  - Introduction to Digital Forensics Course
  - Proactive Internet Investigation Course
  - A handout guide for officers entitled “Guide for Identification, Seizure and Handling of Electronic Evidence”.
  - PNP-ACG Digital and Electronic Evidence Laboratories Manual
- Ad Hoc but no formal training for Judges and Prosecutors.

Conclusions

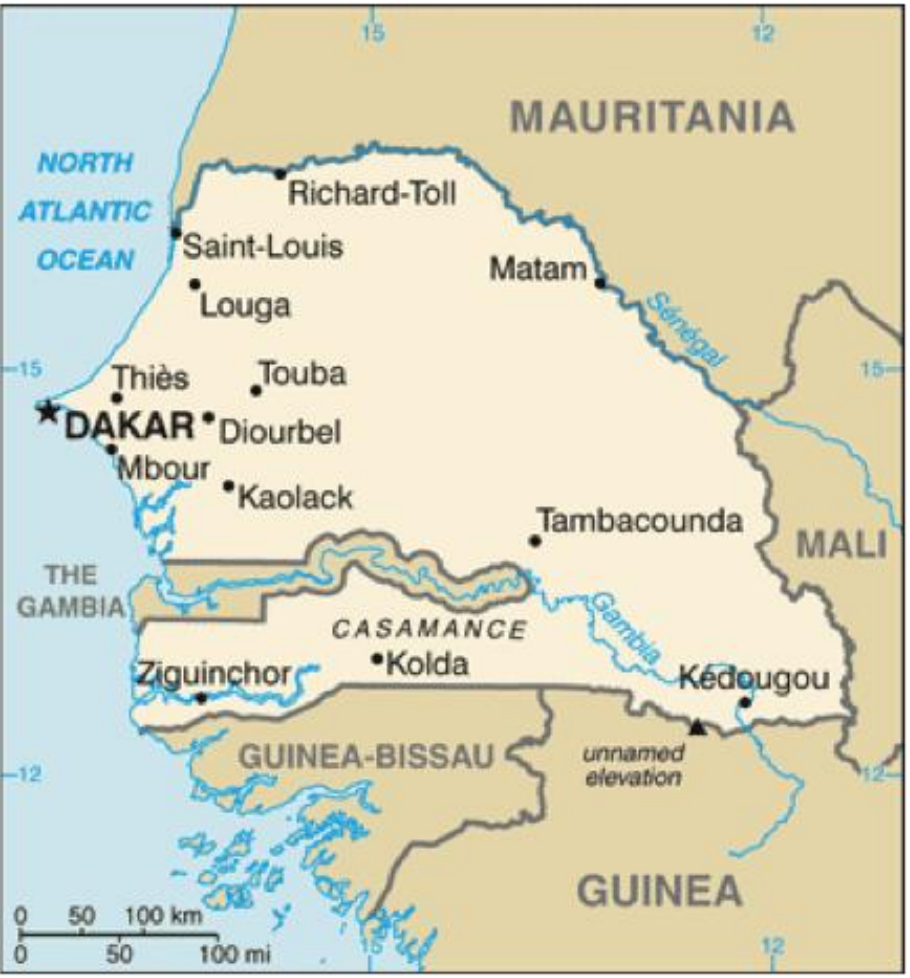
- CPA to be implemented
- Electronic Evidence Clarification
- Delineation of responsibility for NBI and PNP
- Role of the Prosecutor
- Digital Forensics Laboratory to be considered
- LE/Industry cooperation needed
- PNP Training Programme
- National Work Plan being developed

Proposals

- All statistical information on cybercrime offences committed in the Philippines should be integrated into a unified location.
- National Privacy Commission be created in line with the provisions of the Data Privacy Act (RA10173).
- Consider the potential for the availability of legal advice during cybercrime investigations.
- Consider incorporating electronic evidence and introductory cybercrime training within the curriculum for all new LE recruits.

QUESTIONS?

Senegal



Study Visit

10th to 14th February 2014

Visiting Team

Jean-Christophe Le Toquin - France

Jonathan Bourguigon - France

Laurent Baille - France

Marie Agha-Wevelsiep - COE

Situation de la cybercriminalité

- Pénétration de la **téléphonie mobile : 93,60%** (source ARTP 2013)
- Pénétration des utilisateurs d'**Internet : 19,2%** (Source UIT 2012)
- **Statistiques pénales** : le parquet de Dakar dispose d'un système de gestion informatique des affaires, qui doit être étendu au niveau national
- **Infractions les plus courantes** sont relatives aux personnes : diffamation, e-reputation, escroqueries en ligne et par téléphone mobile, atteinte aux mineurs

Législation

- **2008 :** Mise en place arsenal législatif (dont loi 2008-11 sur la cybercriminalité)
- **2013** : Groupe de travail interdisciplinaire installé par Mme le Ministre de la Justice, actuelle Premier Ministre : Justice, Intérieur, Commission Données Personnelles,
- **2014 :**
  - Installation de la Commission des Données Personnelles
  - Réforme Code Pénal et Code de Procédure Pénale
  - Projet de décret portant création d'un Centre national de cybersécurité

Législation : réforme en cours

- Injonction du juge d'instruction aux fournisseurs de services Internet de fournir des données de trafic
- Extension du régime des interceptions de télécommunications à toutes les infractions, dans le cadre d'une information judiciaire
- Renforcement du rôle du Procureur de la République sur l'Officier de police judiciaire (ex: interception de contenu)

Cadre institutionnel

- **Police nationale** : Brigade spéciale de lutte contre la cybercriminalité (BSLC)
- **Gendarmerie** : Cellule cybercriminalité au sein de la Section de recherches (SR) de Dakar
- **Services de poursuite et juridictions** : pas de magistrats spécialisés
- **CERT** : en projet
- **Coopération public-privé** : intérêt des opérateurs de télécommunications

Coopération internationale

- Point de contact 24/7 du Conseil de l'Europe dans le futur Centre national de Cybersécurité
- Projet en cours de connecter la Brigade spécalisée au point au réseau INTERPOL I-24/7
- Conventions de la CEDEAO sur l'entraide judiciaire en matière pénale (signée à Dakar le 29 juillet 1992) et sur l'extradition (signée à Dakar le 06 août 1994).

Formation

- **Préoccupation majeure**
- **Montée en capacité récente** : formations depuis 2012, notamment auprès de la Brigade Spécialisée, avec aide des USA
- Centre de formation judiciaire (CFJ) rayonne au plan régional (Guinée, Tchad, Commorres…)
- Besoins importants en formation initiale et en formation continue, pour les autorités répressives et les magistrats
- **Stratégie nationale à développer**

Conclusions

- **Volonté et vision politique** sur la cybercriminalité fortement réaffirmées et à haut niveau depuis 2013
- Importance de l'**interdisciplinarité** est comprise et intégrée par les praticiens
- Opportunité réelle de démarrer la **coopération avec les opérateurs** de télécommunications, sur des sujets opérationnels

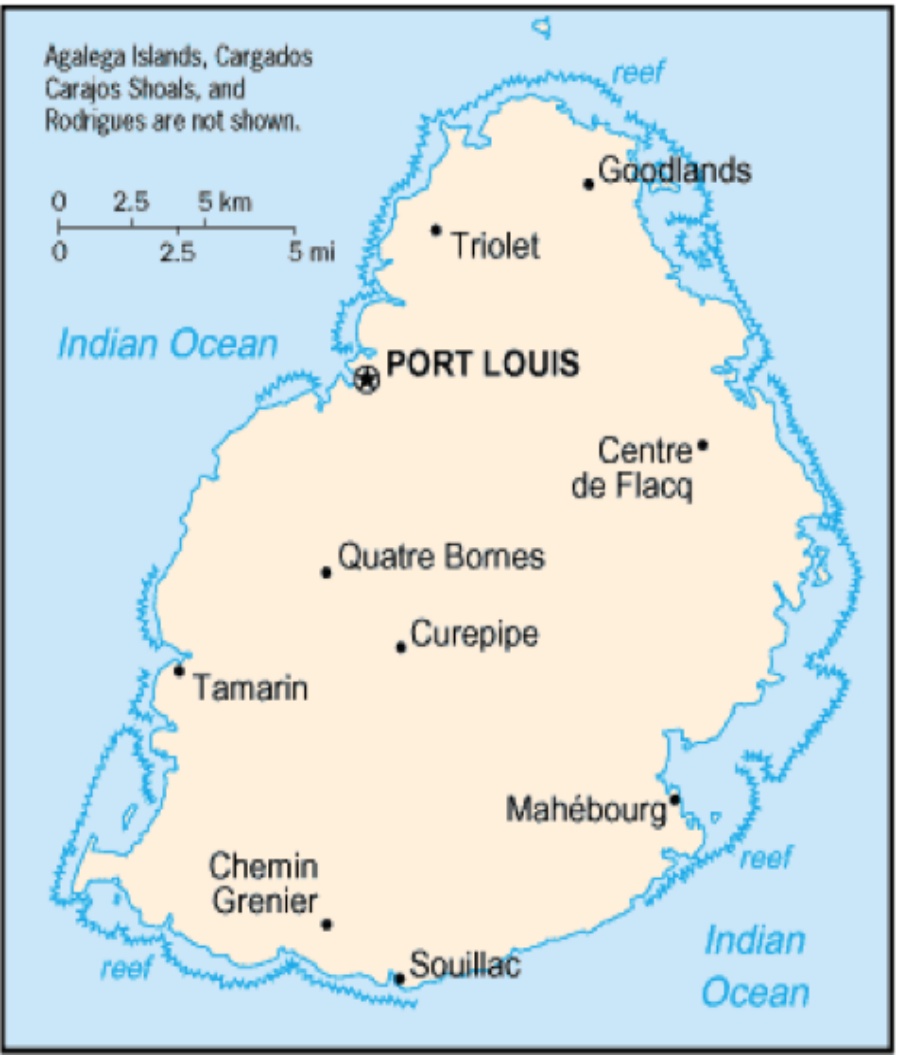
Recommandations

Soutenir et accompagner :

- la création du Centre national de Cybersécurité
- l'adoption de la réforme du code pénal et du code de procédure pénale (interceptions)
- la construction d'un système statistique à partir de la « chaîne pénale »
- création d'un plateforme de signalement cybercrime pour le public
- le développement d'une stratégie nationale de formation autorités répressives et magistrats

QUESTIONS?

Mauritius



Study Visit

10th to 14th February 2014

Visiting Team

Nigel Jones – UK

Pedro Verdhelo – Portugal

Victor Voelzow - Germany

Cybercrime Situation

- 35% of the population has Internet
- The population has 1.2 cell phones each
- About 1,300 “cybercrimes” reported for each of 3 previous years.
- Mainly Offensive/Threatening Material

Cybercrime Situation

- Challenges
  - Dealing with large amount of data (personal, financial etc…),
  - Jurisdiction problems (cross border) with countries like China, Ukraine, Russia etc,
  - No data retention law for ISPs,
  - Minor offences occurring at financial institutions are not reported at the initial stage and only reported when reaching a larger scale thus requiring a complicated investigation.

Legislation

- Computer Misuse and Cybercrime Act 2003
- Various other relevant acts
- Data Protection Act 2004
- Culture of the digital evidence is not yet readily assumed

Institutional Framework

- Mauritius Police Force
- Central Criminal Investigative Department IT Unit provides all digital forensics services
- Investigative Cybercrime Unit
  - 14 staff
- Police Prosecution Service
- Independent Commission Against Corruption
  - Embryonic Forensic Laboratory – 3 persons
- CERT-MU in place
- Different Standards for handling electronic evidence across agencies.

International Cooperation

- The IT unit provide the G8 24/7 point of contact, which is the officer in charge of the unit, with provisions for when that person is absent. G8 point of contact has not been used so far.
- The Interpol 24/7 point of contact is located at the National Central Bureau of Interpol within the CCID and is used as channel for request to other countries.
- There is a 24/7 judge for preservation orders and search warrants.
- No statistics were provided with regard to the requests in cybercrime and electronic evidence cases.
- The Central Authority for MLA's is the Attorney General

Training

- No standardised training for LE
- Some training fro 1st responders
- IT Unit has had some forensics training
- Cybercrime Unit does not have good training
- Institute for Judicial and Legal Studies (IJLS) recognised need for training and asked France
- IJLS has remit to train all lawyers

Conclusions

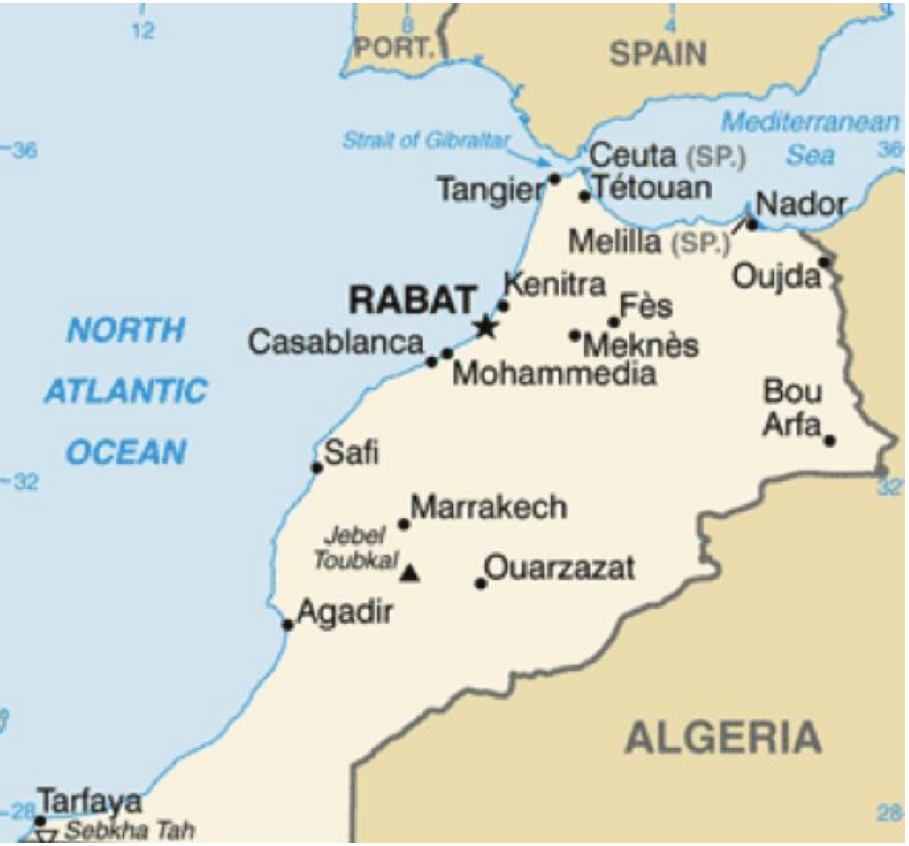
- Different mechanisms for reporting cybercrime
- Procedures for handling electronic evidence should be across agencies
- Lawful Interception only covered in Dangerous Drugs Act
- Different 24/7 POC's
- Training needed for LE and CJS players

Proposals

- All statistical information on cybercrime offences committed in Mauritius should be integrated into a unified location.
- Develop standard operating procedures for the digital forensic laboratory hosted by the Information Technology Unit and those planned by ICAC and DPO
- Deliver a train-the-trainer course on electronic evidence and introductory cybercrime training to trainers from police training school.
- Deliver a train-the-trainer course on electronic evidence and introductory cybercrime training to trainers from the Institute for Judicial and Legal Studies.

QUESTIONS?

Maroc



Visite d'étude

17 – 21 février 2014

Equipe d'étude

Jean-Christophe Le Toquin– France

Delphine Gay – France

Jonathan Bourguignon – France

Alexander Seger - COE

Situation de la cybercriminalité

- Pénétration de la **téléphonie mobile : 120%** (source InternetWorldStats 2012)
- Pénétration des utilisateurs d'**Internet : 51%** (Source 2012)
- **Facebook** : 5 millions d'utilisateurs
- **Statistiques pénales** : 44 affaires en 2008, 19 en 2011, 13 en 2012
- **Infractions les plus courantes** : diffamation, chantage (« sextorsion ») sur internet et réseaux sociaux, attaques des systèmes de traitement de données (affaire Zotob, 2005), fraudes bancaires en ligne.

Législation

- La législation marocaine apparaît en grande partie conforme à la Convention de Budapest, sous réserve d'étude plus approfondie.
- Etablir des mesures procédurales spécifiques en matière de preuves informatiques (article 16 à 21 de la Convention)
- Adopter décret d'application sur la loi n°09-08 sur la conservation des données de connexion
- Etablir obligation légale des fournisseurs de services internet de fournir données de connexion lors d'enquête judiciaire

Cadre institutionnel

- **Direction Générale de la Sureté Nationale** (DGSN a deux unités à compétence nationale :
  - Service de lutte contre la Criminalité liée aux nouvelles technologies
  - Service de lutte contre la Cybercriminalité (SLC)
- Gendarmerie dispose également d'un laboratoire technique
- **Importance particulière d'autres acteurs :**
  - **Ministère des Affaires Etrangères** est un relais avec le CoE
  - **Ministère de l'Industrie** a rôle dans la stratégie numérique nationale
  - **Commission Nationale des Données Personnelles**

Coopération internationale

- Coopération judiciaire se fait sur la base de l'article 714 Code de procédure pénale, par conventions bilatérales, ou sur la base de la courtoisie internationale
- Toute coopération internationale requiert de la DGSN l'aval des autorités judiciaires, y compris pour le gel de données
- Le Maroc n'est pas membre des réseaux 24/7 du G8 et INTERPOL

Formation

- **Préoccupation majeure**
- Institut Royal de Police a formé 2876 stagiaires et formé 892 fonctionnaires en 2012 sur différentes spécialités dont police scientifique, et 30 en 2013 en cybercrimalit.
- Formation de base pour les 28 Officiers de police judiciaires par la DGSN
- Institut Supérieur de la Magistrature : module cybercriminalité de 3 heures en formation initiale

Conclusions

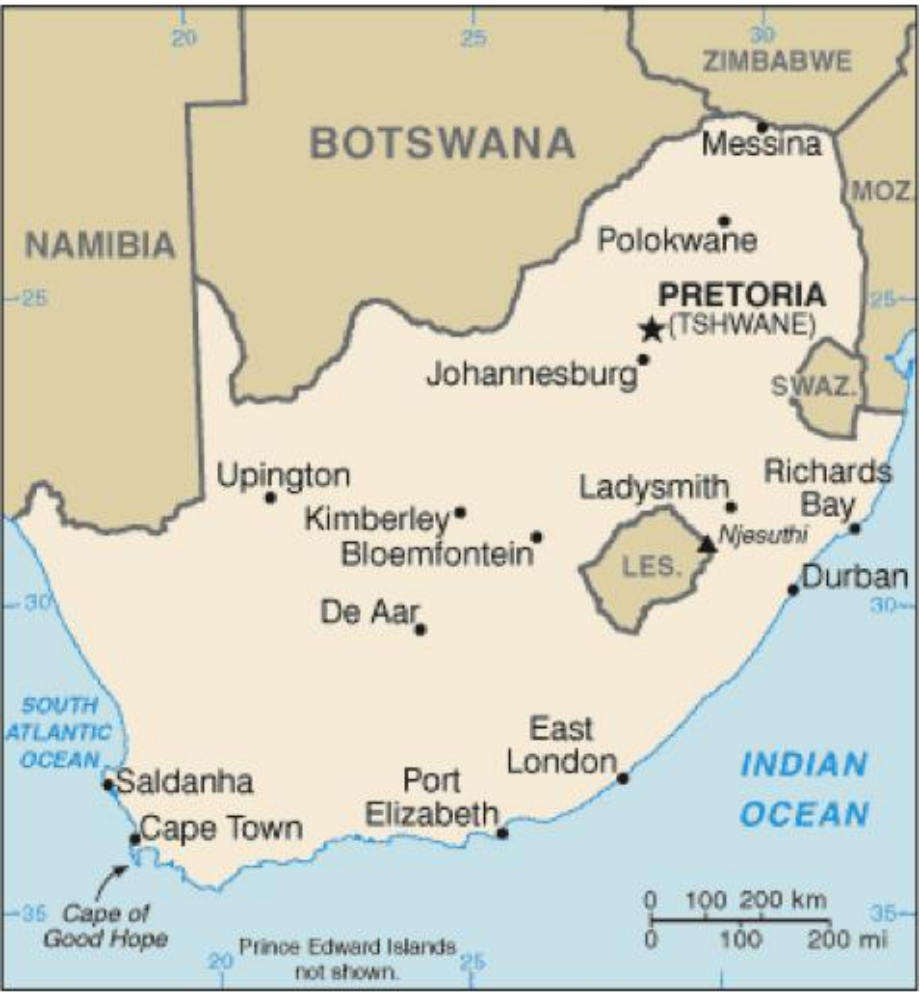
- Intense activité législative, ratification de différentes conventions du CoE, le tout dans le cadre de l'importante réforme constitutionnelle de 2011
- Deux projets nouveaux se dégagent :
  - Création d'un **centre d'excellence de formation** contre le cybercrime, réunissant autorités, industriels et monde académique, potentiellement animé et hébergé par l'Institut Royal de Police
  - Mise en place d'une **plateforme nationale de recueil et d'échanges d'informations** sur les cybermenaces, pluridisciplinaire, réunissant acteurs publics et privés.

Recommandations

- Soutenir les projets de Centre d'excellence (formation) et de plateforme d'échanges d'information (évaluation de la menace), pour développer coopération et échange avec le secteur privé et les différentes prenantes (autorités et ministères)
- Coopération internationale : créer un point de contact 24/7, faciliter les procédures y compris avec les acteurs globaux (Facebook…), établir des statistiques

QUESTIONS?

South Africa



Study Visit

24th to 28th February 2014

Visiting Team

Nigel Jones – UK

Zahid Jamil– Pakistan

Victor Voelzow - Germany

Cybercrime Situation

- 1 in 5 of the population has Internet
- The population has 1.3 cell phones each
- No cybercrime statistics available
- Serious Economic Crime cases encountered
- Also botnets, hacking, web defacements etc
- The National Cybersecurity Policy Framework (NCPF), is being developed (presentation yesterday)

Cybercrime Situation

- Challenges
  - Gathering evidence where social media platforms are involved.
  - International acquisition of evidence.
  - Insufficient legislative measures to provide for international cooperation in obtaining evidence and preservation of evidence.
  - Electronic evidence gather is dealt with in terms of out-dated legislation, which does not cater for the perplexities of cybercrime.
  - Law reform is absolutely necessary to set specific standards for the admissibility of electronic evidence.

Legislation

- Mixture of a singular generally applicable legislation, the Electronic Communications and Transactions Act, 2002 (“ECTA”) and a number of sector/issue specific legislations that criminalise a patchwork of cybercrimes limited to their specific scope and mandate.
- Major review into cybercrime legislation is under way.

Institutional Framework

- National Cybersecurity Policy Framework (NCPF)
  - Main activity dealing with:
    - National Critical Infrastructure Protection
    - Cybersecurity Policy
    - Cybercrime Strategy
    - Coordination and collaboration between departments
- Cybercrime
  - South African National Police (SAPS)
    - Division for Priority Crime Investigation (DPCI)
      - Organised and economic crime
    - Crime Intelligence Unit (CIU)
      - Digital forensics.

International Cooperation

- Currently the Interpol 24/7 mechanism is vested in the police and the G8 24/7 in a named prosecutor in the National Prosecution Authority (NPA).
- Currently no legal mandate exists to enable LEAs to request cross border assistance from foreign LEAs or respond to cross border foreign LEA requests

Training

- Ad Hoc training for LE available
- No sustainable programme.
- Pilot course ran in 2009 but not again
- Plans for a new courses
- Forensic Training for Intelligence Unit
- Justice College has 5 day external course
- South African Judicial Education Institute (SAJEI) has no known training

Conclusions

- Legal framework is somewhat fragmented but work is ongoing to improve the situation
- The NCPF is an interesting initiative and should be monitored
- Large gap in SAPS capability to deal with cybercrime and electronic evidence.
- Different 24/7 POC's
- Training needed for LE and CJS players

Proposals

- Consider the integration into a unified location of all statistical information on cybercrime offences committed in South Africa.
- Consider the report legal proposals in the context of the work on new cybercrime laws
- Consider amalgamation or at least coordination of 24/7 point of contact regimes in cybercrime and electronic evidence.
- Consider joint training programmes between the agencies responsible for different aspects of cybercrime investigations (e.g. SAPS Crime Intelligence Unit, DPCI, Division: Human Resource Development (DHRD)).

QUESTIONS?

Common areas

- Crime reporting and recording
- Legal updates
- SOP’s for electronic evidence and digital forensics
- Inter agency cooperation mechanisms
- Harmonising international cooperation mechanisms
- Training, training training !!!!!

QUESTIONS?