
REPUBLIC OF TRINIDAD AND TOBAGO

# Eighth Meeting of the REMJA Working Group on Cyber-Crime (Washington D.C. - Feb 27 & 28, 2014)

**Presented by**

**Ministry of National Security**

# PRESENTATION OVERVIEW

- The ICT and Cyber Security Landscape
- The Work of the Cabinet-Appointed IMC
  - The National Cyber Security Strategy
  - The Cybercrime Policy and Bill
- The Action Plan
- Lessons Learnt

# ICT Landscape

- There were approximately 224.1 thousand fixed Internet subscriptions in Trinidad and Tobago, as at December 2012. (Source: TATT,2013)
- With 1.88 million mobile voice subscriptions in 2012, it is estimated that 22.4 per cent of the mobile population used mobile Internet services via their phones. As at December 2012, approximately 422.5 thousand mobile voice subscriptions were using mobile Internet services. (Source: TATT, 2013)
- Readiness to leverage ICT for increasing competitiveness and development jumped upwards from 79 out of 133 countries in 2010 to 60 out of 142 countries in 2012 (Source: WEF Global Information Technology Report 2013) and compared regionally among Caribbean countries, Trinidad and Tobago ranked fifth in terms of fixed broadband Internet penetration (Source: BMI and TATT)

# ICT Landscape Cont'd

- Ministry of Science and Technology responsible for national ICT policy and management of the government ICT backbone.
- Ministry of National Security has the oversight for the development of the policy and governance framework for cyber security.
- Government programmes to increase ICT access and reduce the digital divide.
- Movement towards a shared services framework resulting in an increased requirement for security, stability and resilience.
- Government's vision : **"a secure and resilient cyber environment, based on collaboration among all key stakeholders, which allows for the exploitation of ICT for the benefit and prosperity of all"**

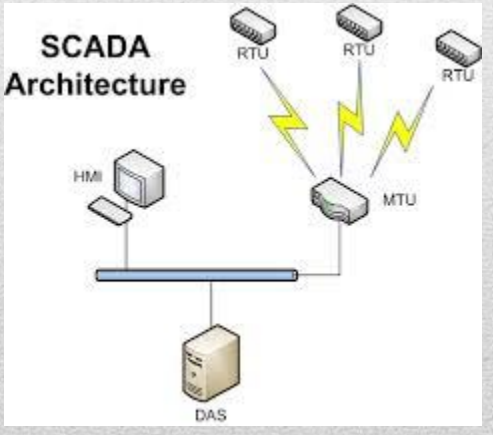
# Cyber Security Landscape

- Isolated incidents are treated on an ad-hoc basis by the ISPs, financial sector or computer related departments in the government.
- Reliance on ISPs and financial sector to provide support and knowledge sharing on best practices and security awareness.
- High need for training of officials in cyber security
- Recent incidents include:
  - Cyber bullying
  - Unauthorised access: Government websites defaced / hacked
  - Data Leaks
  - Skimming
  - Spam, Phishing Scams, Malware

# Cyber Crime Unit (CCU)

- Established in 2008 in the Trinidad and Tobago Police Service
- Investigates all incidents of cyber crime
- Proactive internet investigations including computer crime and Smart Phone related crimes
- Staffed with highly skilled and trained professionals
- Undertakes public awareness through lectures and presentations to schools and any interested persons

# Areas Susceptible to Compromise


TTBizLink

Petrotrin

Energy Based, People Powered

# The Inter-Ministerial Committee

- Established by Cabinet in March 2010 to develop a coordinated cyber security strategy
- Began operations in April 2011
- Given a period of twenty four (24) months to complete its mandate
- Inter-Ministerial in nature inclusive of Regulator and National ICT Company

# MANDATE OF THE IMC

I. To develop a coordinated **National Cyber Security Strategy and Action Plan**

II. To facilitate, guide and ensure the enactment of a **national Cybercrime Act**

III. To facilitate, guide and ensure the implementation of a National Computer Security Incident Response Team **(CSIRT)**

IV. To establish an **implementation mechanism** that would have legislative authority **to develop and enforce cyber security regulations**

V. To create a **mechanism/framework** that ensures the regular conduct of **risk/vulnerability assessments**

# STRATEGIC APPROACH

# Achievements

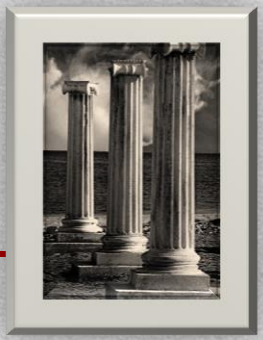
- **Developed and obtained approval for National Cyber Security Strategy (December 2012)**
- **Developed and obtained approval for a National Cybercrime Policy (February 2013)**
- **Coordinated the work of a HIPCAR Consultant which resulted in the development of a Draft Cybercrime Bill**
- **Accessed capacity building and training for government stakeholders (OAS/CICTE, HIPCAR and CCI)**

# STRATEGY: OBJECTIVES

- To create a **secure digital environment**;
- To provide a **governance framework for all cyber security matters**;
- To protect the physical, virtual and intellectual assets of citizens, organizations and the State;
- To ensure the safety of all citizens by **promoting awareness and mitigation** of cyber risks;
- To protect critical infrastructure and secure information networks;
- To **minimize damage and recovery times ;** and
- To create the appropriate **legal and regulatory framework**

# STRATEGIC PILLARS

- **Governance**: establishment of a Trinidad and Tobago Cyber Security Agency (TTCSA).
- **Incident management**: Establishment of Computer Security Incident Response Team (TT CSIRT)
- **Collaboration**: The establishment of public-private/civil society partnership and enhanced external coordination
- **Culture**: Awareness raising, training and education in cyber security throughout the country.
- **Legislation**: The drafting and enactment of amended updated cybercrime legislation.



# DEVELOPMENT OF THE CYBERCRIME BILL

1. **Existing Legislation:**

   Children Act, 2012, Computer Misuse Act, 2000 (draft Cybercrime Bill, 2014), Anti-Terrorism Act (as amended), 2005, Dangerous Drugs Act, Chap 11:25, Electronic Transfer of Funds Crime Act, 2000, Evidence Act (Section 14B), Extradition (Commonwealth and Foreign Territories)Act, 1985, Financial Intelligence Unit of Trinidad and Tobago Act, 2009, Interception of Communications Act, 2010 , Mutual Assistance in Criminal Matters Act (as amended), Offences Against the Persons Act, Chap 11:08 (Section 30A), Proceeds of Crime Act, Chapter 11:27, Trafficking in Persons Act, 2011, Telecommunications Act (as amended), Chap 47:31

# DEVELOPMENT OF CYBERCRIME BILL

**2. Policy Formulation :**

**PURPOSE**

- Ensure a coherent strategy in the prevention, investigation, prosecution and sentencing of computer crime and cybercrime in Trinidad and Tobago
- Enable Trinidad and Tobago to participate in the international endeavour to fight against transnational computer crime and cybercrime.
- Inform the preparation of a legislative framework for the deterrence and prosecution of cybercrime

**OBJECTIVES**

- Prevention and Awareness Raising
- Criminalization of offences related to computer crime and cybercrime
- Institution of investigation mechanisms
- Use of electronic evidence in prosecution
- Creation of an environment that defines the obligations and restricts the liability of ISPs
- Repeal of the Computer Misuse Act (2000) and replace with the Cybercrime Act

# DEVELOPMENT OF THE CYBERCRIME BILL

**3. Comparative Study conducted in conjunction with HIPCAR Consultant**

- Commonwealth Model Law
- Budapest Convention
- HIPCAR Cybercrime Model Policy Guidelines and Legislative Text
- Legislation from other Countries: US, Philippines, Dominican Republic, Jamaica, Belgium
- Scholastic Articles
- Case Law

**4. Stakeholder Consultations**:

Economic/Financial/Banking, Telecoms, Academia, IT Security, Civil Society, Government etc.

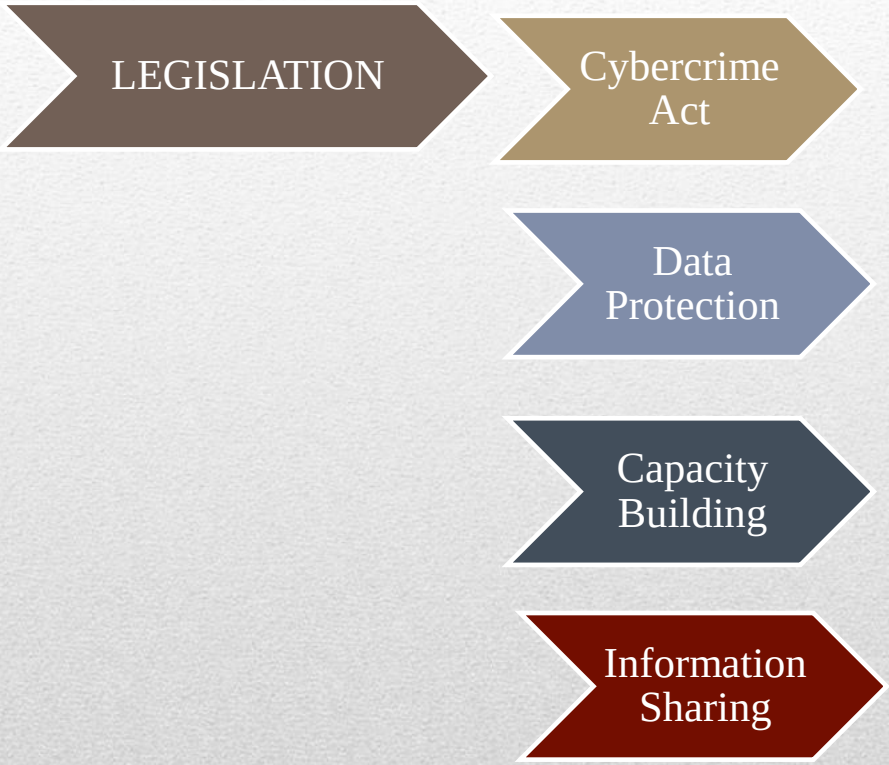
# THE CYBERCRIME BILL

- Illegal access to a computer system ("hacking", circumventing password protection, exploiting software loopholes etc.)
- Illegal interception (violating privacy of data communication)
- Illegal Data interference (malicious codes, viruses, trojan horses etc.)
- Illegal acquisition of data
- Illegal system interference
- System interference (hindering the lawful use of computer systems)
- Misuse of devices and illegal devices (tools to commit cyber-offences)
- Offences affecting critical infrastructure
- Illegal devices
- Unauthorised receiving or granting access to computer data
- Computer-related forgery (similar to forgery of tangible documents)
- Computer-related fraud (similar to real life fraud)
- Identity related offences
- Child pornography
- Luring
- Violation of Privacy
- Multiple electronic mail messages
- Harassment using an electronic means

# Areas covered in the draft Bill

- Jurisdiction of the court is established
- Liability of body corporates is also addressed.
- New tools introduced including search and seizure, order for removal or disablement of data, requirement to assist the police, production orders and expedited preservation orders ( application by police to Magistrate), offence to disclose content of order, disclosure of traffic data (distinguished from interception of communication legislation).
- Order for payment of additional fine (where there is monetary gain) and compensation (where damage is caused because of the commission of the offence)
- Forfeiture order
- Order for seizure and restraint (property, vessels etc. where the accused seeks to dispose of it)

# PLAN OF ACTION



# LESSONS LEARNT

- Assessment:
  - Structure of your Government
  - Legislation (persons with skill set who can articulate terms and relevance of provisions)
  - Local skill set-Law Enforcement ( was not a substantial focus of the legal subcommittee but capacity building)
  - Infrastructure
- Collaboration:
  - Pre-strategy (e.g. Judiciary)
  - Post Strategy (e.g. omitted TTDF, Academia, etc.)
- Continuity:
  - IMC ended-TTCSA
  - Budget
  - Building Confidence (not only in infrastructure but in follow through)

# THANK YOU AND QUESTIONS