Cybercrime & Cybersecurity

Briefing Session for Commonwealth Parliamentarians on Electronic Commerce and Cyberlaws

24 April 2013

Threats

- Hacking & cracking
  - Unauthorised access to....
- Viruses, spyware or 'malware'
  - Unauthorised modifications to systems and data
  - 'malicious marketplace'
- Denial of Service attacks
  - 'zombie' computers & 'botnets'
- Illegal content
  - e.g. race hate, child abuse images…
- Fraud
  - Theft of proprietary information ('industrial espionage')
  - Financial and communications fraud

Harms

- Physical harm
  - Hate speech, child abuse, harassment
- Economic harm
  - loss of business/information assets
    - e.g. music industry & P2P
  - loss & disruption of business activity
    - e.g. 'denial of service' (DoS, DDoS), SPAM
  - brand & reputational damage
    - as victim (e.g. security breach), as source ('botnets')
- Societal harm
  - Critical national infrastructure
    - e.g. Air traffic control systems

Law reform

- Law N° 2010/012 relating to Cybersecurity and Cybercriminality in Cameroon
  - Criminalising conduct (Criminal Code)
    - Computer-related, e.g. fraud
    - Computer-integrity, e.g. viruses
    - Content-related, e.g. indecent images
    - Contact-related, e.g. unsolicited emails & harassment
  - Enhancing law enforcement (Criminal Procedure)
    - Powers of investigation
    - Service provider obligations
  - Information security
    - Prevention being better than cure.....

Reform concerns

- Over criminalisation
- Infringement of individual rights
- Imposing excessive burdens on service providers and other intermediaries

Policing cyberspace

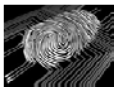
- Public law enforcement
  - Industrial scale
    - e.g. Operation Ore
  - Specialised training & resources
    - Police, prosecutors and judiciary
  - International co-operation
    - Tools, e.g. Interpol African Working Party on IT Crime
    - 24/7 policing, e.g. www.virtualglobaltaskforce.com
  - Interaction with private sector
    - Role of telecoms operators and ISPs

Policing cyberspace

- Assistance to law enforcement
  - Interception
    - Building an intercept capability
  - Communications data
    - Data preservation *v* data retention?
  - Protected data
    - Cryptographic technologies, e.g. Blackberry, Apple's FaceTime
- Private law enforcement
  - e.g. Internet Watch Foundation
    - Notice and take-down
    - Controlling access, i.e. filtering
  - e.g. Rights-holders

Information security

- Security services
  - Confidentiality, integrity, availability, authentication & accountability
    - e.g. Digital signatures, certification services & 'Certification Authorities'
- Provision of services
  - e.g. Electronic payments
- Protection of rights
  - Privacy & intellectual property rights
    - e.g. Digital watermarking



Legal response

- Obligations to implement
  - 'appropriate technical and organisational measures'
- Obligations to notify of security breaches
  - To mitigate losses
- Promoting compliance with standards
  - e.g. ISO/IEC 27002: 2005: 'Code of practice for information security management'; PCI-DSS....
- Institutional response
  - e.g. Computer Emergency Response Teams (CERT)
  - e.g. PKI Certification service & key management

Questions & discussion