Cybercrime & Cybersecurity

Professor Ian Walden
Institute for Computer and Communications Law
Centre for Commercial Law Studies, Queen Mary, University of London

Introductory Remarks

- Inherently transnational crime
  - e.g. transatlantic bomb plot
- Harmonisation & co-operation
  - Multi-lateral & bi-lateral instruments
    - Budapest Convention (2001)
    - Influence & implementation
  - Preventing ‘data havens’
    - e.g. ‘I love you’ virus
  - Enhance enforcement

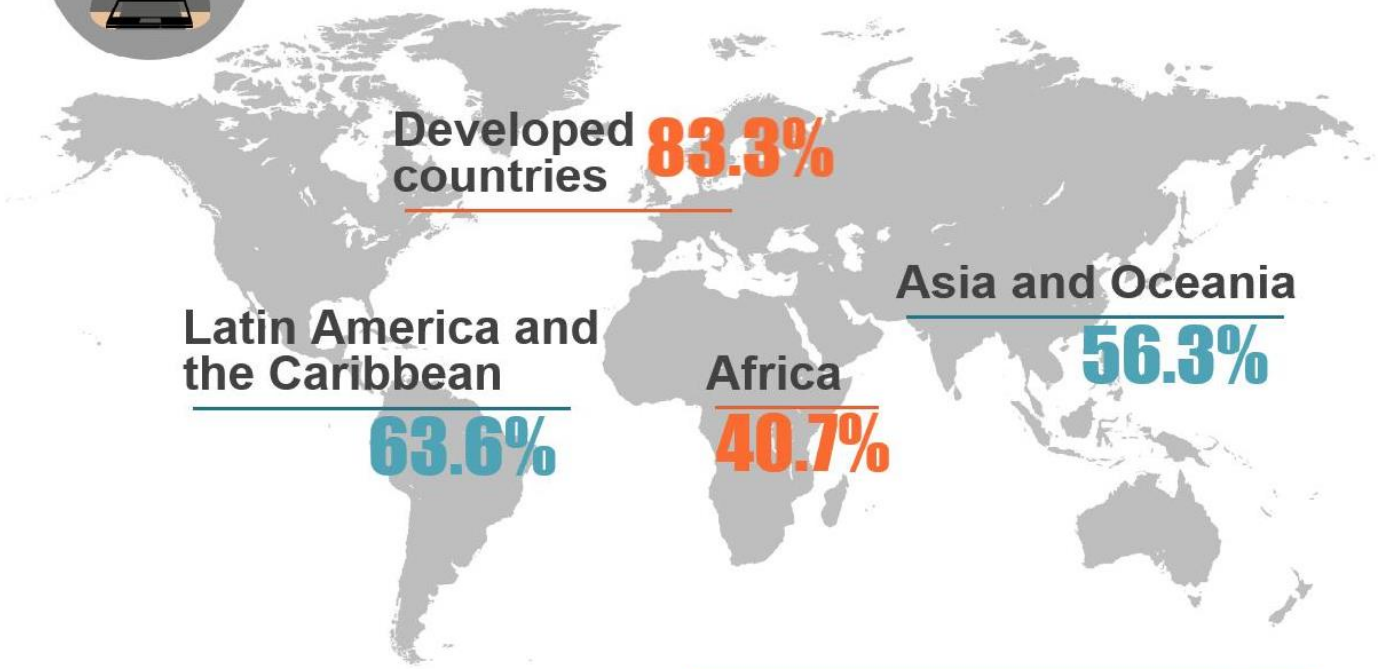
UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

PROSPERITY FOR ALL

Cyberlaws and regulations for enhancing e-commerce around the world 2014

Share of countries with Cybercrime laws



Source UNCTAD, 2015

Information Economy Report #IER2015

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. e.g. Polish airline LOT (21 June 2015)
  - brand & reputational damage
    - as victim (e.g. security breach), as source (‘botnets’)
- Societal harm
  - Critical national infrastructure
    - e.g. Air traffic control systems

Incidence & cost

- Numbers: Always big!
  - Reporting problem
  - Law enforcement experience & resources
  - Statistical recording
- ‘Sex, lies & cybercrime statistics’
  - Losses are concentrated and therefore not representative
  - Unverified and self-reported numbers
  - Outliers can have a huge impact on the result
  - Collected by entities that have an incentive to over report
- Developed & developing country perspectives

Legal response

- Criminalising behaviours
  - Computer-related
  - Computer-integrity
  - Content & contact-related
- Enhancing law enforcement
  - Powers of investigation
    - While safeguarding individual rights
  - Imposing obligations
- Information security
  - Prevention being better than cure.....
    - Obligations to implement

Harmonisation

- ‘Suppression conventions’
  - Homogenization of criminal justice systems
  - Regularization of criminal justice relationships
- Co-operation between states
  - Moving evidence & people
  - Formal & informal
- Jurisdiction
  - Extending material & procedural
    - Concurrency problem
  - Extraterritorial
    - ‘Active nationality’

Law reform

- Convention on Cybercrime (Nº 185, November 2001)
  - 45 (47) Member countries
    - + US, Japan, South Africa, Canada
    - Australia, Dominican Republic, Mauritius and Panama
  - US ratified 1 January 2007; UK ratified 25 May 2011
  - Additional Protocol 'concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems' (Nº 189, January 2003)
    - 35 (47) Member Countries + Canada, South Africa
- Regional initiatives
  - Antigua (2013), Bahamas (2003), Barbados (2005), Costa Rica, Jamaica (2010) and Trinidad (2000)

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

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
- Private law enforcement
  - e.g. Internet Watch Foundation
    - Notice and take-down
    - Controlling access, i.e. filtering

Cybersecurity

- Security services
  - Confidentiality, integrity, availability, authentication & accountability
    - e.g. Digital signatures and certification services
- 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’
    - e.g. FTC enforcement against HTC
- Obligations to notify of security breaches
  - To mitigate losses
- Promoting compliance with standards
  - e.g. IS0/IEC 27002: 2005: ‘Code of practice for information security management’; PCI-DSS....
- Institutional response
  - e.g. Computer Emergency Response Team (CERT)
  - e.g. PKI Certification service & key management

Concluding remarks

- Impact of harmonisation
  - Direct & indirect influence
- Limits of harmonisation
  - Cultural differences
  - Criminal justice system
    - e.g. sentences
- Law enforcement & rights infringement
  - e.g. data retention