Law Reform & Cybercrime

Professor Ian Walden
Centre for Commercial Law Studies, Queen Mary University of London
Substantive offences

• Stand-alone statute
  – Legislative efficiency & publicity
    • Relationship to existing offences

• Piece-meal reform
  – Amending the penal code & criminal procedure

• Computer integrity offences
  – ‘protected computers’

• Content & contact-crimes
  – Criminal defamation & intermediary liability

• Sanctions & remedies
  – Legal persons
Criminal procedure

• Powers
  – For whom?
    • ‘Law enforcement’
  – By whom?
    • Authorisation: Judicial, administrative or executive
    • Standards: ‘probable cause’ & ‘necessary and proportionate’
  – Encryption: security & ‘back-doors’
    • Procedural offences

• Safeguarding rights
  – Non-citizens/residents
  – Transparency & notification (pre, post)
  – Oversight
International co-operation

• Inter-state
  – Mutual legal assistance
    • modernization
  – Direct access to forensics
    • Open source
    • Service providers

• Networks
  – Building relationships

• Not too high, nor too low, but just right!
  – International co-operation
    • e.g. Nigeria (death penalty) & US (consecutive sentences)
    • e.g. ‘double criminality’: Minimum 12 months imprisonment
Reform process

- Multi-stakeholder involvement
  - e.g. Kenya ‘Interagency Technical Committee on the Development of a Comprehensive Cybercrime Law’
- Civil society
  - ‘Article 19’
- Technical community
  - e.g. universities
- Law enforcement
  - Police & national security agencies
- External expert input
- ‘Next steps’ capacity building
  - Law enforcement, prosecutors, judiciary