Cybersecurity & Cybercrimes: Overview (of some) of the Issues

Professor Ian Walden

Queen Mary
University of London

Centre for Commercial Law Studies

Introductory remarks

- State response to cybercrime
    - Harmonisation of criminal justice systems
        - Council of Europe Convention on Cybercrime (2001)
            - 57 signatories, including 11 non-members (e.g. Chile & Senegal)
    - Regularization of criminal justice relationships
- Policing cyberspace
    - Evolving policing strategies
        - Prevention & disruption *not* prosecution
    - ‘Third party policing’
        - Service providers, e.g. registries & registrars
- Cybersecurity strategies
    - Prevention being better than cure…
        - Cultural shift, target hardening, standards-making

Evolving environment

- From POTS to the Internet
  - IPv6 & the ‘Internet of Things’
    - e.g. hacking the fridge
- From the desktop to apps & the Cloud
  - Shifting locus of data and applications
    - Data ‘at rest’ or ‘in transmission’
- Shifting threats & harms
  - From ‘script-kiddies to ‘Crime-as-a-Service’ to State-sponsored actors
  - Critical national infrastructures
- Policy concerns
  - Economic development
  - National security
    - Identifying cyberwarfare

Legal & regulatory responses

- Criminalizing conduct
  - Computer-related, computer integrity, content-related & contact crimes
    - Sanctions: ‘Effective, proportionate and dissuasive’?
- Enhancing law enforcement powers
  - Facilitating cross-border access to evidence
  - Data retention & encryption policy
    - Safeguarding rights: privacy, expression & fair trial
- Cybersecurity framework
  - Prevention regimes
    - Privatizing the costs, e.g. product liability
    - Breach notification & vulnerability disclosure obligations
  - Disruption regimes
    - Permitting ‘active defence’
    - Notice & take-down (intermediary liability)