CYBER CRIMES & ONLINE CRIMINAL MARKETS

Gloria Laycock

Professor Emeritus of Crime Science
University College London

UCL Jill Dando Institute of Security and Crime Science

Day 1: Identifying problems

Administrative issues

- Data accuracy and access
- Different agencies have very different cultures – “the US is easier to work with”
- Individual crime problems are diverse, as are the solutions – there is no co-ordination
- Lack of awareness of cyber-crime problems, particularly at corporate board level
- Traditional criminal justice responses are generally ineffective, especially when offenders are operating with impunity overseas – e.g., in Russia
- Cyber-criminals are entrepreneurial and can move fast – those tackling cyber-crimes are rule based and constrained
- High rewards are causing skilled potential actors to choose cybercrime as a career

Day 1 continued:

Specific crime issues

- Cyber-criminals also need secure systems: A vast underground economy caters for large numbers of traditional and cyber criminals with specialised security products and service – *this is a vulnerability*
- To what extent do cyber-crimes/cyber-criminals differ from 'regular' offences/offenders?
  - Their criminal careers appear very different
  - Displacement is far more common in cyber-space
  - Offenders appear to co-operate with each other instead of competing
  - Cyber-criminals appear to be getting more professional and ruthless
- What, specifically, can be done about:
  - Ransomware
  - Human trafficking for sexual exploitation
  - Illegal goods sold on legitimate websites including protected species and plants e.g. eBay only takes down between 2-7% of ivory sales?

DAY 2: Undermining SOC

Administrative issues

- Improve data accuracy and access, use a common language for law enforcement, industry and academe
- Set clear priorities for action with co-ownership of the problems and co-production of solutions
- Invest in legal, organisational and technical harmonisation with international partners (the latter includes shared ontologies, data schemes, tooling, data science models)
- Consider the use of data science as a means of automating and scaling interventions
- Use scenario-based training for corporate leadership
- A paradigm shift in the way in which law enforcement agencies approach cyber-crime is needed, making greater use of data analytics
- Collaboration with industry through public and private sector cooperation

DAY 2: continued:

Specific crime issues

- Determine the vital security infrastructure for specific cyber-crimes and attack it
- Develop leverage to increase the rate at which legitimate platforms take down illegitimate operations
- Reward computer users for identifying websites selling illegal products
- We know a great deal about ‘regular’ crime and criminals but less about the extent to which those lessons transfer to the virtual world
  - fund research to develop this area of knowledge
  - Specifically develop ways of increasing the perceived risk to offenders, increasing the effort needed to successfully commit an offence and reducing rewards

Thank you

UCL Jill Dando Institute of
Security and Crime Science