N8 Policing Research Partnership: Innovation Forum on Cybercrime

Market Place Discussions

7. International Challenges and Enforcement

- PhD project proposal – looking for a supervisor
- Jurisdiction needs boundaries (should there be cyber specific treaties to avoid law free zones?)
- Cyber space has no boundaries
- Principles of jurisdication (Cottim)
    - Territoriality
    - Nationality of criminal
    - Nationality of victim
    - Protective theory – which state is jeopardised
    - Universality – international character of the fence
    - (Read more "The cybercrime and cyberspace investigators handbook"
- What is the digital equivalent of investigative assumptions eg a crime scene?
- Contact Fraser Sampson, OPCC West Yorkshire

Rapporteur Notes:

Fraser Sampson

- I wrote a chapter on this subject in the 'Cybercrime and Cyber Terrorism Investigators' Handbook' Ed. Baback Aghar.
- The challenge of dealing with cybercrime is jurisdiction – without which you cannot enforce.
- There are five existing theories of jurisdiction: 1. Territoriality (where the crime was committed) 2. Nationality (the active personality – what is the national of the offender? This is difficult in many cases. For example the US will claim jurisdiction anywhere if there is a US citizen involved) 3. Passive nationality (the nationality of the victim – again this is difficult to find out) 4. Protective theory (which state's interests are jeopardised?) 5. Universiality (international character of the offence – it feels right so we ought to e.g. piracy and trafficking offences. This is difficult to defend and define).
- Artificial approaches to jurisdiction are difficult because you will be drawn to the jurisdiction attached e.g. to the offender or victim however this might not be relevant to the case.
- The only source of legitimacy will come from jurisdiction – cyber hasn't addressed this.
- There is an assumption that there is a crime scene, an offender etc.
- Cannot claim jurisdiction therefore this cannot be legitimate.
- Various uncertainties with cybercrime.
- The US can switch off the internet if they wish to but this doesn't mean they have jurisdiction!

- Research is needed! At the moment we police the entrances, users and exits but we can't have people in the system all the time dealing with offenders.
- International laws also an issue – if you commit a crime in our country we have jurisdiction but how can we do this with cybercrime?
- Needs to be considered properly in terms of international law – should there be international treaties on cybercrime? An assumption that all countries will be on board? Problem with different justice systems, methods, ideas about cybercrime etc.
- Legal systems need to catch up! The older a law is the more reliable it is – the more cyber related a law is the more unreliable/untested – we simply don't know what works.
- Is it impossible? Unpoliceable? Do you just focus on the people? But how can you find them? What if it is a state rather than a person?
- Need boundaries (there aren't any in cyberspace) but to police cybercrime we need boundaries!
- We need to explore this – without international treaties/agreements on how to deal with it.

Outcomes

- Develop a PhD project? Proposal for a study of these issues.
- Intelligence sharing – MLAT perspective trying to gauge the amount of offences, types etc.
- Must act with jurisdiction – required (COTTIM principles).
- Need a defendant to claim jurisdiction – how can we find the offenders?
- Research questions – should there be cyber specific treaties to a void the law free zone?
- Relate to the plane shot down in Russia – if you were to cause substantial economic loss (as opposed to human loss) to a company there is no crime scene, offender etc. Hence we need to change investigative assumptions - what is the digital equivalent of a 'crime scene' or an 'offender'?
- Everything you know as a detective is wrong! Bring in new concepts (those who are not from a conventional detective background).
- Legislative preconceptions also an issue. Which sentencing principles should be used?
- Case example – R v Shephard – case of extreme right wing material, extradited and charged in the UK (UK based sat on a US website).
- Cannot be certain of where it is in cyberspace – cyber trail can be misleading.
- Software that changes your mac address is readily available – almost anyone can commit a cybercrime! Further difficulties.