Cybercrime Research Unit,
Centre for Criminal Justice Studies
School of Law

UNIVERSITY OF LEEDS

Researching The Demands on Policing in a Digital and Networked Age

(EPSRC CeRes)

Cambridge Cloud Cybercrime Centre Cybercrime Conference, Law Faculty, Cambridge University, 14 July, 2016

Professor David S. Wall

<d.s.wall@leeds.ac.uk>

https://beijingolympicsblog.files.wordpress.com/2008/07/chinese-armed-police.jpg

0. Objectives and Outline

UNIVERSITY OF LEEDS

1. The current state of affairs
2. Progress so far
3. Legacy Problems
4. The Reassurance gap in cybercrime
5. Closing the reassurance gap via Collaborations
6. Methodological issues
7. Early research findings
8. In an ideal world ...
9. Conclusions and take away points

1. The current state of affairs

UNIVERSITY OF LEEDS

- **Policing cybercrime is currently in a confused state, but is improving.**
- **The UK, USA & other researchers seem to be the leading the field, with others on the heels – *cue for an anti-brexit rant* – we may lose this edge!**
- **I think that we (research community) now have a better picture of the ughknowns (Rumsfeldian unknown-unknowns).**
- **We are working on new ways of understanding the knowns and unknowns.**
- **Today, our cup should be half full, not half empty!**

2. Progress so far: cup half full

UNIVERSITY OF LEEDS

- **We are a lot better now at separating out the risks, threats, harms crimes, & the prosecutions**
- **And appreciating the different contributions**
- **Starts to challenge the claims of the cybersecurity industry (aided by an unquestioning media) that conflated these issues**
- **The reign of the weather reports from umbrella manufacturers is over.**
- **Their current analyses and predictions are not only more responsibly reported, but good and have some credibility – but they are threat reports**

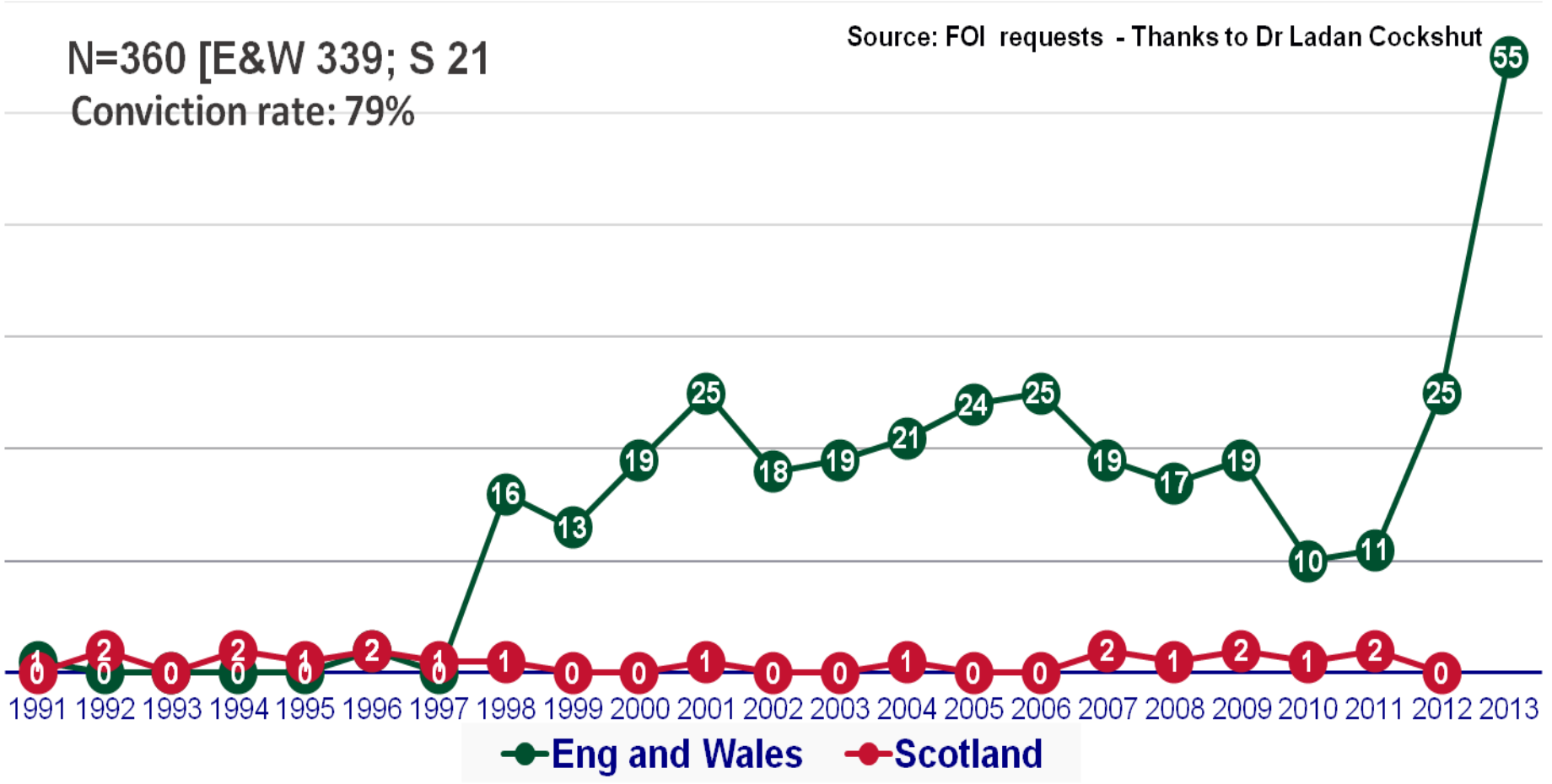
3. Legacy Problems

UNIVERSITY OF LEEDS

- **The overall lack of applied knowledge**
- **Combined with the culture of fear about cybercrime**
- **Has created exaggerated demands for security with regard to cybercrime and cybersecurity that police and government cannot deliver.**
- **This has created a reassurance gap**
- **COMPARE THE FOLLOWING PROSECUTION STATS**

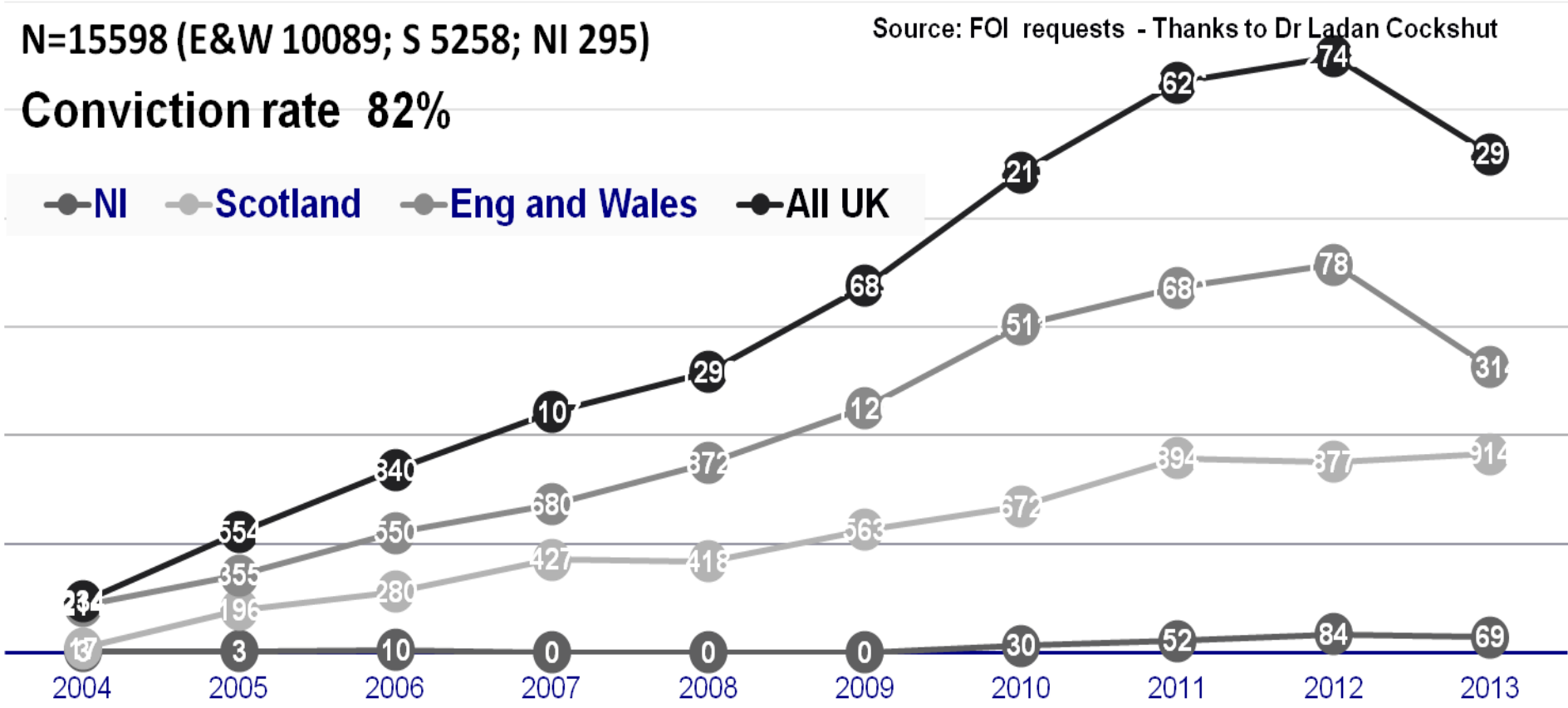
3.1 Computer Misuse Act 1990

•Approx 400 prosecutions in 25 yrs, against millions of active threats circulating at any one time!



3.2 Communications Act 2003 (s.127)

•(online conduct) 15,598 prosecutions 2004 and 2013! (12,777, 82%). **The CA 2003 issue is related to Social Networks** and increasing demands for police to resolve online communications issues.



4. The Reassurance gap

UNIVERSITY OF LEEDS

- The ‘reassurance gap’ shifts police attention from policing for justice in to policing the gap.
- The louder voices tend to get responded to, high profile police operations with arrests.
- The prosecution statistics support this view and suggest that there is more of a focus on internet bad behaviour at the possible expense of computer misuse.
- “You can’t own a problem in cyber in the way that you could” Mike Hulett, NCA
- To close the knowledge gap, collaborations between the Academy, Police & stakeholders are required.
- They are easy to start, but extremely hard to develop and maintain, but are possible and are worthwhile. I will focus upon policing agencies here:

5. Closing the reassurance gap - Police /Academy Collaborations

UNIVERSITY OF LEEDS

Problems related to 45 different UK forces with different systems.

- **vetting**
- **lack of trust within and across forces and across sector**
- **different expectations from i) Senior & ii) middle management and the iii) officers on the coal face, and iv) the analysts and v) information officers**
- **staff turnover (promotion or rotation), usually once a specialist skill has developed**
- **incompatible local police data systems**
- **inconsistent (even erratic) recording practices**
- **varying local & personal interpretations of the rules (counting, investigations, prosecution). A complicated issue.**

6. Methodological issues

UNIVERSITY OF LEEDS

From the different expectations of various parties

- interdisciplinary (within Social Sciences)
- cross-disciplinary across science and social sciences
- cross sector, e.g. i) cybersecurity focus upon risks and threats and police focus upon operational issues
- ii) police data. how to turn tactical operational data collected into data for strategic purposes.
- Governmental Policy expectations-e.g. HO focus on enabled /dependent cyber-crime – which shapes agenda.
- Political expectations – politicians want stats, costings, evidence to support policy.
- Corporate expectations are based private interests and not public good - reluctant to share information.

7. Early findings

UNIVERSITY OF LEEDS

- **What our research is beginning to reveal are supports the ‘reassurance gap’ hypothesis.**
- **The different sources of data (national and local) are revealing very different types of cyber-crime profiles at national and local levels.**

- **At a national level are, as expected, the cyber-enabled and cyber-dependent, but at a local level it is more likely to be cyber-assisted.**

7.1 What is affecting the public – police data

National police *- mostly economic and industrial cybercrime*

Local police *– many social network related crimes 2 types in addition to known cybercrimes:*

- **Social Network Media aggravated crime -**

Person A insults Person B and Person B then physically assaults Person A. Is when Online goes offline and is problematic. Also includes trolling - taking pleasure in upsetting others online*. A big issue at the moment is the breach of exclusion orders by online trolling* (usually former partners).

- **Social Network Media aggravated fraud – Social Network Media brokering offline engagement. P2P online relationships lead to frauds i) advance fee frauds - 419 scams - dating scams - ii) auction frauds - buying goods that don't exist or are not as advertised.**
- *These two crime types appear to be adding significant workload to local police forces and little is known about their dynamics*

SEE THE FOLLOWING THREE TYPES OF CRIME

7.2 CASE STUDY 1: **INTERNET THREATS**

- Jenny (15yr) posted a picture of herself on Facebook wearing a bikini whilst on holiday.
- Jason, her 15 year old boyfriend's friend developed a flirty banter
- Jealous, her boyfriend Kyle, told his friend to 'back off' and began a bad tempered exchange.
- He told his (now former) friend that he would hunt him down and kill him - paraphrasing Liam Neeson in *Taken*
- Jason's parents saw the exchange, concerned they mentioned it to his teacher
- The teacher referred it to the head of year ... and it worked its way up the school's management hierarchy to the headmaster, who also did not know what to do.
- He asked the local police liaison officer, who asked the Crown Prosecution Service for advice. They saw the words 'I will kill you' and deemed it of a menacing character
- The police decided to arrest Kyle, now a potential killer, from his house
- Upon explanation, the case then started to unravel and fall apart
- Kyle was clearly not a killer, and the case was eventually dropped when he would not accept a caution.
- Youth interaction is often ironical and words take on different legal meaning when typed

7.3. CASE STUDY 2: **SEXTING**

UNIVERSITY OF LEEDS

•A 14 year old boy sent a naked photograph of himself via Snapchat to a 15year old girl at school he liked.

•She saved the picture within 10 seconds and sent on to friends at school.

•The picture was brought to the attention of the school police liaison officer

•No charges were brought, but it was officially recorded as a crime - details of both sender and recipient placed on a police sex offender intelligence database.

•They could be stored for up to 10 years and disclosed in a criminal records check.

•If the sender had been aged over 18 he would have been the victim of so-called "revenge porn" and the girl who distributed the image prosecuted.

•The boy’s mother said her son was "humiliated" for being "naive" and being "a teenager".

•Many children at the school now take part in so-called "sexting" as a form of "flirting". It is normalised behaviour!

7.4. CASE STUDY 3: **DATA THEFT**

UNIVERSITY OF LEEDS

- TalkTalk was hacked into via a DDoS attack and SQL injection with data stolen
- The hacker contacted TalkTalk and asked for a ransom to return the data
- The company's CEO claimed TalkTalk was the innocent victim (2 prev attacks).
- Media frenzy arose & speculation over terrorism, vast financial loss & impending cybercrime wave + warnings from business leaders and a Government enquiry announced.
- Reports of customers losing money and the culture of fear around cybercrime went through the roof. Pressure mounted on the police to find the culprit.
- The Met Police arrested the hackers, a 15 yr old + two 16 year olds & 20 yr old from different parts of UK. All were subsequently bailed.
- The media frenzy shifted after the arrest to raise a number of critical questions
- Could the culprits receive a fair trial and proportionality normally found in courts
- The 15 year old is now bringing legal action against various media sources for revealing his personal details. Crimes masterminded from bedrooms!

7.5. QUESTIONS RAISED BY THE CASES
threats - sexting – data theft

UNIVERSITY OF LEEDS

- **Each case raises questions about the role of the police & authority in dealing with disputes and issues arising from social network media.**
- **None of the 3 are unusual and each present the Police with a whole new ball game that falls outside their normal routine activities.**
- **The threats and sexting cases question whether the police should have been involved so directly + question the responsibilities of the other parties. Did the parents over react? Were the teachers over cautious or under-informed? Did the lawyers consider the full context of the cases in their assessment of criminal responsibility? Did the police over-react because of pressure from parents or teachers?**
- **In the data theft case, almost the opposite questions arise, were the parents under-cautious, should they or teachers have picked up signs and involved police earlier? and so on.**
- **All three also question whether any of the authorities involved fully understood the nature of modern youth's apparently normalised behaviour around mobile networked devices?**

8. In an ideal world ...

UNIVERSITY OF LEEDS

- More accurate production of knowledge informs good policing policy
- a) improved call centre responses
- b) improved police capability
- c) increased capacity
- d) more justice being achieved for victims
- f) a wider acknowledgement that the police only play a small part in the overall policing process and they have to work more closely with the other key stakeholders at a number of different levels - which the 4Ps helps identify.

8.1. What are the consequences of not responding to technological change?

- **Inability to respond to cyber-criminals – get away!**
- **Increase in online extortion and OCGs**
- **A widening of the reassurance gap between (inflated) public demands for security and what police and government can (or can not) deliver.**
- **More insecurity discourages investment in the internet and services and citizen participation**
- **A rise in vigilante groups online and offline**
- **Growth of Virtual/ Networked societies growing away from the Westphalian state model (e.g. ISIS)**

9. Conclusions – take away points

UNIVERSITY OF LEEDS

- Collectively we are improving CC knowledge
- Collaborations are not easy, but worth it
- There is also a legacy issue to reverse
- Our statistical sources and their application are imperfect, but can be improved – we're learning
- Early findings are that different forces have quite different cybercrime profiles
- There is a need to widen the lens and understand what is the new 'normal' and accepted behaviour amongst youth and onliners.
- The consequences not responding are quite dire

Relevant Recent References and Essays

http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=376504

UNIVERSITY OF LEEDS

• Wall, D.S. (2016) 'Policing Cybercrime in the EU: Shall I Stay Or Shall I Go?', *British Society of Criminology Newsletter*, 78 (Summer), <http://www.britsoccrim.org/wp-content/uploads/2016/04/Wall_bscn78.pdf>

•Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. (2015) The Implications of Economic Cybercrime for Policing, London: City of London, October.

•Wall, D.S. (2015) 'Dis-organized Crime: Towards a distributed model of the organization of Cybercrime', *The European Rev of Org'n'd Crime* 2(2): 71-90.

•Wall, D.S. (2015) 'The TalkTalk hack story shows UK cybersecurity in disarray', *The Conversation*, 28 October, http://theconversation.com/profiles/david-s-wall-98233/articles

•Wall, D.S. (2014) 'High risk' cyber-crime is really a mixed bag of threats, *The Conversation*, 17 November, https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091

•Wall, D.S. (2013) 'Policing Identity Crimes', *Policing and Society: An International Journal of Research and Policy*, 23 (4): 437-460

•Wall, D.S. (2007) *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity.

Annex: Policing Research at Leeds

The University Leeds is leading on Policing Research

UNIVERSITY OF LEEDS

- **Policing Cybercrime** a) CeRes b) CRITiCal (Cloud) – new joint interdisciplinary centre (Durham, Leeds, Newcastle) c) Bitcoin d) OCGs online e) Ransomware f) EU Policy g) CEPOL
- **N8 Policing Research Partnership** – projects with the College of Policing and others
- **HEFCE Policing initiative** – leading on police educ'n themes
- **Leeds Institute for Data Analytics** – Consumer – Health - Crime
- **Policing Research** – Histories of the Present, Crime Prevention - Organised Crime – Community Support
- **Criminal Justice Research** – a) *Institutional research* – Police, Pre-trial, Courts, Prisons, Victim Support, Youth Justice, Mental Illness b) *Thematic Research* – sex offending - terrorism – police histories – crime prevention - intellectual property crime – crime and technology

Thank You – d.s.wall@leeds.ac.uk

UNIVERSITY OF LEEDS