Centre for Criminal Justice Studies
School of Law

UNIVERSITY OF LEEDS

The Changing Cyber-threat Landscape and the Challenge of Policing Cybercrimes in the EU

EVIDENCE-BASED POLICING, 2015
CEPOL European Police Research & Science Conference, CEPOL, European Police College, the Escola de Polícia Judiciária, cia Judiciária, Lisbon, Portugal, 5-8th October,

Professor David S. Wall,

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

Abstract

UNIVERSITY OF LEEDS

In this talk I shall, as the title suggests, look at the changing cybersecurity threat Landscape and the challenges that it poses for policing cybercrime and ask the question "when does cybercrime become a problem?" In the first part I shall look at the ways that the threat landscape is changing and how it impacts upon policing. In the second, I shall then look at how we can reconcile practically the definitional issue as to what cybercrimes are before, in the third part, exploring the various avenues by which our knowledge of cybersecurity and cybercrime is formed - how we know actually about cybercrimes and who tells us? Finally, in part four, I shall argue that we need to separate the politics from practice in the cybercrime debate and agree on co-productive systems for collecting information to inform future policing policy in the EU.

0. Outline

UNIVERSITY OF LEEDS

1. Transforming Crime Online
2. The changing the cyber-threat Landscape and impacting upon the police
3. What is cybercrime: how do we understand it?
4. What cybercrimes are actually affecting police?
5. How will technological developments impact on the police over the next 5-10 years?
6. What are the consequences of not responding to these changes?
7. Conclusion: What needs to be done & how?

1. Networked and Digital Technology - Transforming Criminal Behaviour Online

- **What is the (cyber) difference?**
- **Networked technologies are globalised, informational and distributed (Castells).**
- **These qualities increase the *distance, speed & volume* of crime. The 'cyber' lift.**
- **Add, Digital technologies and criminals have control over a complete criminal process.**

"Why commit a €50m robbery when you can commit 50 X €1 robberies?"

2. How is technology changing the cyber-threat Landscape and impacting upon policing?

In three ways:

2.1 How has technology impacted upon the police crime workload during the past 5-10 years

2.2 How is technology impacting upon police public service delivery

2.3 How is technology impacting upon the police ability to administer its organisation?

2.1 How has technology impacted upon the police crime workload during the past 5-10 years?

a) More professional - see stuxnet construction

b) More stealthy - see Rootkits, Zeus, Botnets

c) More automated – Ransomware, Fake AV

d) Much larger – see recent DDOS attacks

e) More complex – social network media, cloud

f) Much different to normal routine activities
- Sexting, and social network originated crimes

Are police involved in too much cybercrime?

2.2 How is technology impacting upon police public service delivery?

UNIVERSITY OF LEEDS

a) Methods of victim reporting

b) Police responding to victims

c) Investigation methods and procedures

d) Engaging the public – cyber-sleuths?

e) Accountability to the public, the police profession and to law

2.3 How is technology impacting upon the police ability to administer its organisation?

a) Increasingly less police station centric models of policing

b) It can reconcile the national with the local - enables local forces to have national connectivity and share common policing norms

c) It can increase accountability to police management and the rules of the organisation

BUT this talk focuses on Cybercrime

3. What is Cybercrime – How do we understand it? - When should police get involved?

Everyone agrees it exists but no one agrees what it is! Here is a way to understand it.

Security is about risks, crime about harms

a) Different Security Debates - Personal, Organisation/ Business, National Security

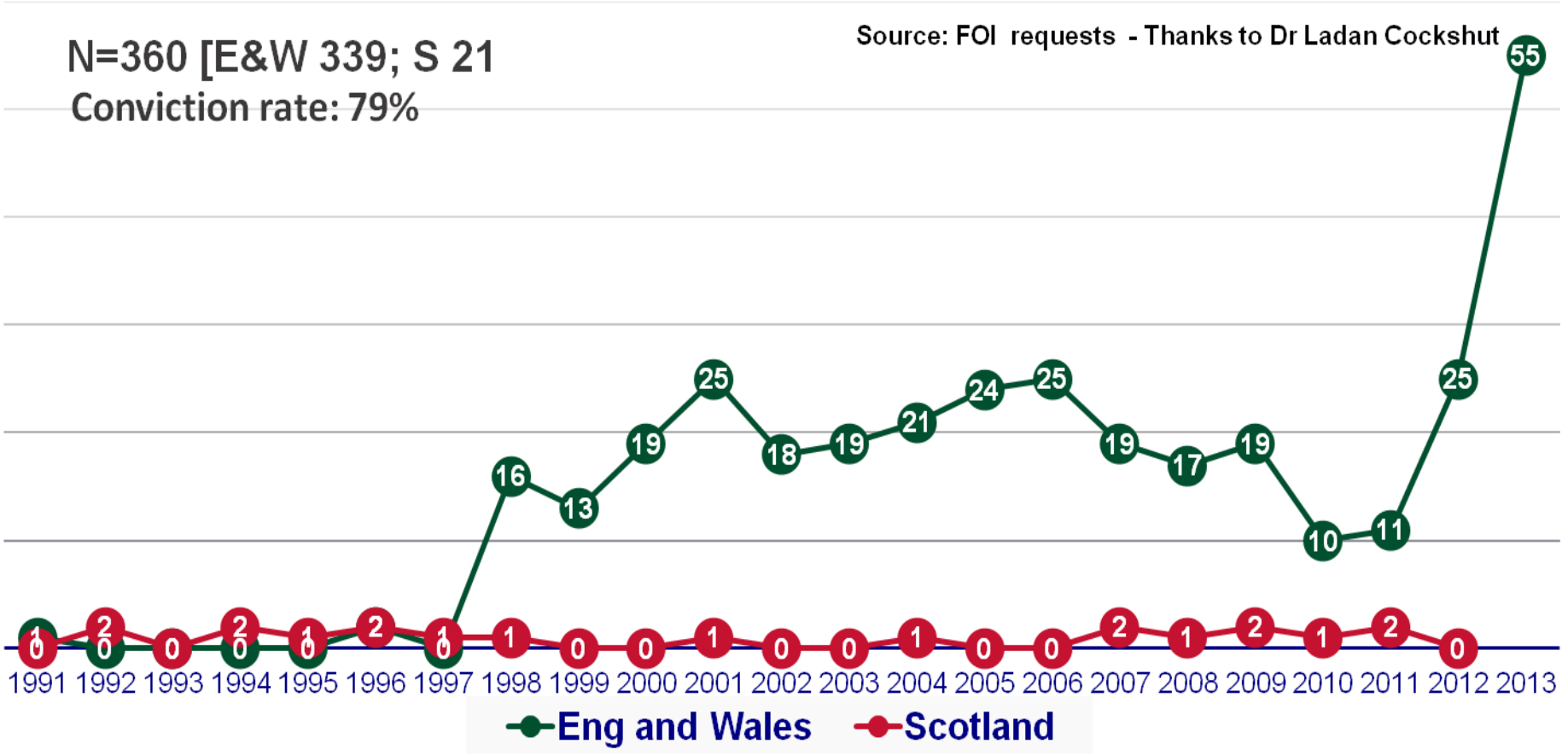
b) Different Technological Impacts on crime – Cyber-assisted, cyber-enabled, cyber-dependent

c) Different Modus Operandi - cybercrimes against systems, using systems, in the systems

WHAT DO THE STATISTICS TELL US??

3.1 Computer Misuse Act 1990

- **Approx 400 prosecutions in 25 yrs, against massive increase of millions of threats.**



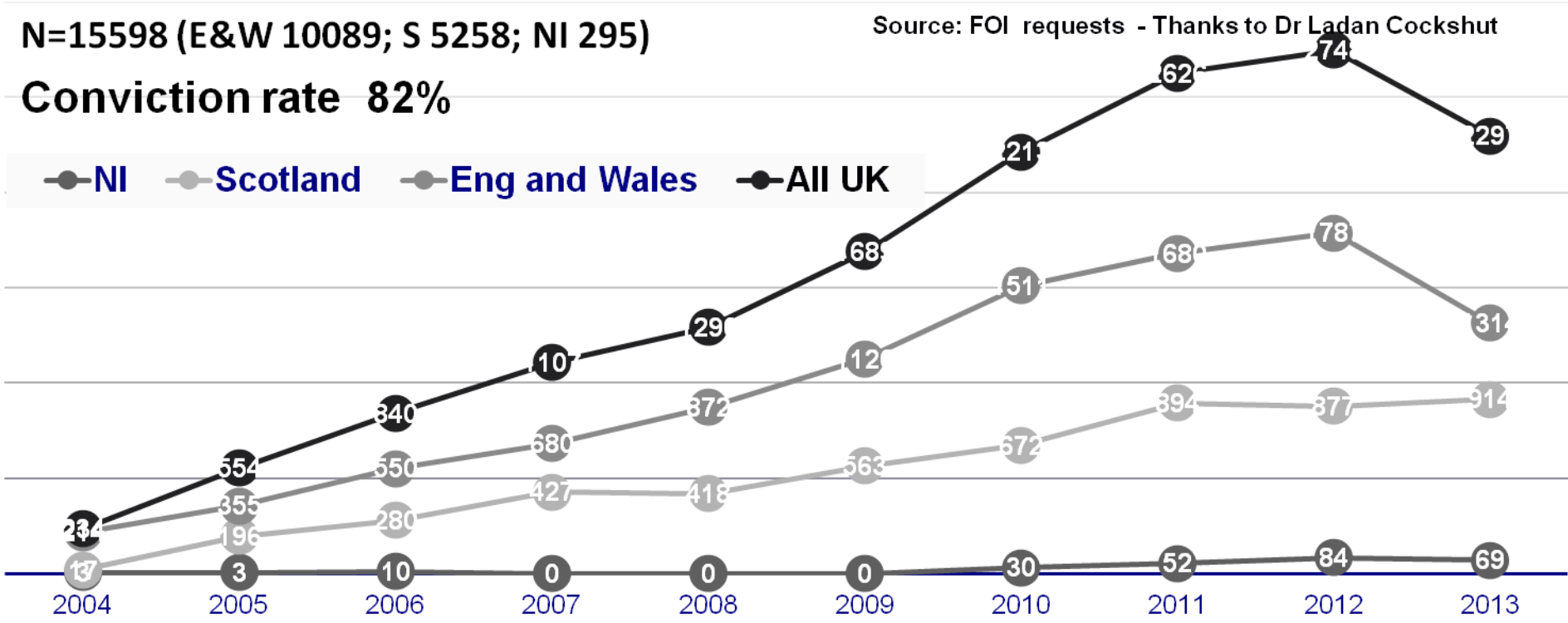
3.2 Why so few prosecutions?

UNIVERSITY OF LEEDS

- **Prosecutions are unreliable indicators of success**
- **There are many different types of cyber-crime**
- **Many different victims, offenders, regulators**
- **Crime is both technical and experiential**
- **Many are prosecuted under other laws – but not all**
- **Under-reporting (despite media over-sensationalisation!)** Individuals – business
- **Police crime profiles differ from local to national**
- **Police are policing the reassurane gap not justice**

3.3 Communications Act 2003, s127

- **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.



3.4 What is affecting local police – from data

a) 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 *Are more localised and demands an individual response from local police forces to meet with parties*

b) social network media aggravated frauds – P2P online relationships which 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. *Dealt with by Action Fraud, Trading Standards or the commercial sector*

c) trolling – trolls takes pleasure in upsetting others online - *are dealt with by both local and national depending upon the profile and severity of the offence.*

National police *- economic and industrial cybercrime*

3.5 What to the statistics tell us? Reassurance Gap Policing

UNIVERSITY OF LEEDS

- **Low Computer misuse prosecution rates**
- **High Computer misbehaviour prosecutions**
- **Culture of fear about cybercrime is creating demands for security that Police and Government cannot deliver – tier 1??**
- **Creates a reassurance gap**
- **Police are policing the reassurance gap rather than justice** – social network media – a) sexting – irate comments - misunderstanding normal behaviour of youth
- **Police need to rethink their engagement with cyber**

4. How will technological developments impact on the police over the next 5-10 years?

a) new regulatory challenges

- Mesh technologies - joining networked devices laterally - reduces the ability to Govern /control
- Self-deleting communications – e.g. Tiger Txt/Snapchat - reduces the Intelligence and evidence gathering potential
- Cryptocurrency – new value exchange – reduces evidence trails

b) new force multipliers and conceptual issues

- The Cloud – increase in computing power and storage
- Advanced Social Network Media technologies – when they come

c) new criminal business models

- New illicit markets - dark web
- New service access - Crime Service delivery crimeware-as-service
- New objects of value (crime drivers) - personal data – IPC

d) Social change – a) Migration b) Young defrauding the Old

5. What are the consequences of not responding to technological changes?

- Police are unable to respond to cyber-criminals
- Increase in online extortion and OCGs
- A growth in the reassurance gap increases between (inflated) public demands for security (culture of fear) 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)

6. Conclusions

UNIVERSITY OF LEEDS

- **Respond to increasingly dynamic situation with more & more variations of crime and complexities**
- **Police need to adopt co-production/ co-creation models of action NOT collaboration?**
- **Work towards developing new systems & standards for understanding changes in crime as they happen & sharing information about it just as quickly.**
- **Work towards developing big data analytic capacities for strategy and policy.**
- **Manage public and business expectations of what levels and types of security police and government can deliver?**
- **Build capacity to help police leaders, officers and staff understand and manage developments in crime**

Relevant Recent References and Essays

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

UNIVERSITY OF LEEDS

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

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

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. (2015) 'Dis-organized Crime: Towards a distributed model of the organization of Cybercrime', *The European Review of Organised Crime 2*(2): 71-90.

Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. (2015) The Implications of Economic Cybercrime for Policing, London: City of London Corporation, October. http://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Pages/The-implications-of-economic-crime-for-policing.aspx

Annex: Policing Research at Leeds

The University Leeds is leading on police research

UNIVERSITY OF LEEDS

1. **N8 Policing Research Partnership** – projects with the College of Policing and others
2. **HEFCE Policing initiative** – leading on various themes
3. **Policing Cybercrime in the Cloud** – new joint interdisciplinary centre (Leeds, Newcastle, Durham)
4. **Leeds Institute for Data Analytics** – Consumer – Health - Crime
5. **Policing Research** – Histories of the Present, Crime Prevention - Organised Crime – Community Support
6. **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