N8 Policing Research Partnership

Policing Cybercrime: Evidence Review

Theme Leads: Professor David Wall (Durham University) and Professor Corinne May-Chahal (Lancaster University)

Researcher: Dr Yulia Chistyakova (Durham University)

Background

In an era of ubiquitous computing the boundaries between what is and is not cyber crime are increasingly blurred and agreement about what constitutes cybercrime is elusive. As a consequence, there is much uncertainty as to how to police cybercrime. Should, for example, the Police be centrally involved in policing cybercrime or should other groups, such as internet service providers, be required to take on more responsibility. When should the police take a case and when should they pass it on? Should this be the responsibility of local, regional or national police? Such questions are emerging during a time when the culture of fear about cybercrime is creating demands for levels of cybersecurity that police and government are finding difficult to meet. Whilst recent developments such as the National Crime Agency and its National Cybercrime Unit, plus the overhaul of reporting mechanisms are taking place for the better, there still remains some confusion about the nature of the relationships between local, regional and national police forces and other sectors involved in regulating cybercrime.

Key Findings

- Cybercrime disrupts the boundaries of traditional policing in terms of geography, organisation and expertise. Victims, perpetrators and responsibilities for investigation are diffused across regions and continents, economic and social institutions. This leads to several questions:
    - Can the public expectations of the police be made to match what the police can deliver?
    - Should local Police be centrally involved in policing cybercrime OR should other groups be required to take on more responsibility?
    - What should be the relationship between local, regional and national police forces and other sectors that are regulating cybercrime?
    - When should the police take a case and when should they pass it on? Should they only respond to some types of cybercrime?
    - Would an overhaul of existing reporting mechanisms yield better strategic and tactical intelligence?
    - Are current laws sufficient for effective protection of citizens from cybercrime, or do we need to rethink policing in this area?
- The impact of technology upon crime and policing requires a better understanding. On the one hand, new technology also creates new crimes and enhances existing crimes in different ways, but on the other hand it also creates new, more powerful means of control and regulation. Yet, it also creates a tension between investigative and surveillance powers and human rights and the forensic expertise to respond to cybercrime required puts a strain on existing resources and priorities presents a challenge.
- Traditional partners to policing may not be keeping abreast of a rapidly changing environment, expecting the police to lead the way but without traditional support mechanisms. Examples of good practice involving communities and neighbourhoods should be shared more freely between forces and strategic partners.

1. Introduction

There remain gaps in knowledge about the best practices of policing cyberspace and the optimal relationship between local, regional and national police forces and other sectors involved in regulating cybercrime. This rapid review of the literature provides an overview of the current published research on the policing of cybercrime in the UK and more broadly, identifies what is known and where major gaps remain. It starts with the methodology, describes six areas of research then makes some recommendations for application to operational practice. It ends with some research questions arising from the Cybercrime workshop.

2. Methodology

Several databases were used to conduct searches for this research: IngentaConnect, Google scholar, JSTOR, Swetswise, and Academic Search Complete. The search terms included the following: (a) cybercrimes (cybercrime, cyber-crime, cyber crime, digital crime, e crime, virtual crime, cybersecurity, cyber threat, Internet and crime, computer and crime) and (b) policing (police, policing, law enforcement, law, control, regulation). Most of the sources related to the UK, although relevant evidence related to other countries was included as well. The review also includes questions and ideas for future research that were identified at the Cybercrime workshop held in February 2014. The review is subdivided into the following sections: the unique challenges of policing cyberspace, the role for the public police, the role of technology, social and community control, emergent crimes, networks and partnerships.

3. The Unique Challenges of Policing Cyberspace

There remains some confusion as to what cybercrimes are, even though it is agreed they exist (Wall, 2007a: 399). This is explained by the unique nature of cybercrimes which are borderless, ephemeral and fluid, distant and anonymous, non-routine activities that fall outside the traditional police mandate and are not given the same priority in each jurisdiction (Wall, 1997, 2004, 2007a, 2007b; Urbas, 2006; Grabosky, 2007, 2013; Yar, 2005). In addition, differences between jurisdictions in defining cybercrimes make the offenders often difficult or impossible to prosecute (Wall and Williams, 2013; Williams and Wall, 2013; Wall, 2007b; Schneider, 2003; Grabosky, 2007; Jewkes and Andrews, 2005). The characteristics of cybercrimes can often make traditional policing methods seem inadequate. The nature of digital evidence requires a different set of skills, while existing knowledge, skill-sets and experience are increasingly insufficient to meet the new challenges (Wall, 2004; Jewkes and Andrews, 2005; HMIC, 2014). This also means that the traditional police occupational culture is at odds with the requirements of regulating cyberspace (Wall, 1997: 224; Wall, 2008; Wall, 2007b), and that its organizational structures may need to be changed in order to respond to cyber threats more effectively (Jewkes and Andrews, 2005). Furthermore, there are operational, organisational and legal obstacles to the allocation of police resources for investigation and prosecution of cybercrimes (Wall, 2004: 318; Williams and Wall, 2013). Police forces may also lack cyber-specific investigative powers: powers for search and seizure, power to 'enter' electronic networks to search for evidence, as well power to ensure preservation of data (UNODC, 2013; see also Hunton, 2012: 227). In addition to real demands, there are a range of demands (often felt) for more investigatory powers in cyberspace which raises questions about the privacy of users' data, and the circumstances under which privacy may legitimately be infringed (Sommer, 2004; UNODC, 2013: 134, 141). There is also the challenge to police officers' 'digital identity' that 'requires greater consideration about the appropriate balance between personal privacy and transparency (accountability)' (Goldsmith, 2013: 17). Another challenge for the police is the gap between the Cybersecurity Strategy rhetoric and the reality of policing on the ground, and gaps and barriers in cooperation between different cybersecurity nodes (Wall, 2008; Levi and Williams, 2013: 439). Finally, the under-reporting by the victims impedes effective responses to cybercrimes (Wall, 2007a; 2007b; 2013).

4. The Role of the Public Police

Scholars agree that while it is unrealistic for the public police to hold a monopoly on the policing of the internet, they will have a role to play (Wall, 1997; Wall and Williams, 2013; Bossler and Holt, 2012). One of the reasons for this is that even though cybercrimes occur globally, they are reported locally, which means that there is a role for local police to play (UNODC, 2013: 118). Wall and Williams (2013) argue that the police are likely to intervene where strong public concerns or economic issues motivate them to do so. However, where costs are likely to outweigh benefits, online community members will be more appropriate regulators

(Wall and Williams, 2013: 409). In many situations, serious offending behaviour in virtual worlds online communities is best left to police themselves without outside assistance (Lastowka and Hunter, 2003). However, the public police also have an important symbolic role to play. Police remain the source of legal authority 'which justifies and legitimises action, provides some transparency and also allows recourse in cases where injustice occurs' (Wall, 2004: 332). Similarly, police access to a range of investigative powers must be firmly grounded in legal authority (UNODC, 2013: 121).

5. The Role of Technology

Technology changes policing and law and order landscape in several ways. First, it provides law enforcement agencies with investigative tools, but can present problems for security and law enforcement: for example, strong encryption or other increasingly sophisticated perpetrator techniques for hiding or deletion of computer data (Berkowitz and Hahn, 2003; McQuade, 2006: 61; UNODC, 2013: 142-3). Secondly, technology creates new, more powerful means of control and regulation: it can disrupt human action, is easily shaped by actors, imposes constraints on how people can behave, is more readily and rapidly adaptive than laws, and changes to system architecture incorporate a preventative approach (Wall and Williams, 2013: 401-2). Thirdly, new technological tools produce a tension between investigative and surveillance powers and human rights: some technological tools such as, for example, interception of communications and electronic surveillance have the potential to infringe upon privacy-based rights (UNODC, 2013: 121). Reliance on keyword searches to mine data and identify suspects proved to be controversial, as they often rely on stereotypical assumptions about how a 'criminal' or 'terrorist' looks or behaves and they also unnecessarily subject many innocent people to routine monitoring (Haggerty and Gazso, 2005). Therefore 'any successful interventions will have to be set within acceptable moral, ethical, social, economic and technological frameworks' (Williams and Wall, 2013: 258).

6. Social and Community Control

The best strategy to deal with cybercrime, according to some scholars, is to increase the care taken by citizens online and improve the legal system to protect them (Bossler and Holt, 2012). It is argued that civilian policing by a range of organisations is a valuable component of cybersecurity networks; citizens use their computer skills and knowledge to collect information on suspected offenders and pass it on to criminal justice agencies (Huey, Nhan and Broll, 2012). Online communities (Internet users and user groups) can maintain online behaviour through the application of censure or withdrawal of access rights (Wall, 2008: 57). While the use of shaming is popular among members of online communities, there are questions over the successful application of shame in this context (Wall and Williams, 2007: 406). Disintegrative shaming, for example, may legitimise hatred and derisory performances and encourage a lack of trust and interdependence (Wall and Williams, 2007a: 408). A shift from vigilante to more formal modes of regulation marks the increasing 'civilization' of the online communities; to reduce online deviance, it is important to achieve an appropriate balance between social, technological and legal controls (Williams, 2007: 69-79).

7. Emergent Crimes

The grooming and sexual abuse of children is well known (McGuire and Dowling, 2013a), but image analysis in peer to peer networks reveals many other paraphilias that may encourage other crimes including the rape of older people, bestiality, serious sexual violence and necrophilia (see for example Murray, 2009; Jenkins and Thomas, 2004; Grebowicz, 2010). A distinction between online and offline crimes that is currently upheld in community practices may hinder understanding and detection of cyber related crime: recent cases of the abuse of infants in nurseries, for example, went undetected by professionals who routinely work together with the police and were not understood as being cyber-motivated (BBC, 2013). The interconnections between online and offline harm and risks must be taken into consideration in contemporary child protection practices (May-Chahal et al., 2012). There is a distinction between crimes that are enhanced by the internet and those that are enabled by it (Wall, 2007a; McGuire and Dowling, 2013b); for example, harassment and psychological abuse can be heightened in cyberbullying, whereas hacking big data is made possible through the internet. In both enhancement and enablement scale, scope and the potential for impact are greatly expanded.

8. Networks and Partnerships

The role of the public police has to be understood within a broader and largely informal architecture of networked Internet policing (Wall, 2008: 92; Dupont, 2004: 76). This includes Internet Service Providers, non-governmental, non-police organisations, governmental non-police organisations and law enforcement units, and transnational law enforcement (Wall, 2008). It is essential that these actors work in partnership (Broadhurst, 2006: 416; UNODC, 2013: 120), and although this is becoming a fact of life in some countries (Grabosky, 2007: 221), obstacles to cooperation remain. Importance is attached to intra-agency cooperation within jurisdictions and the need to improve and maintain these in order to enhance mutual legal assistance at the regional and international level (Broadhurst, 2006: 422).

9. Recommendations for Application to Operational Practice

Based on the review, an ideal model for policing cyberspace would be characterised by:

- Pluralism (multiple agencies)
- A flattening of policing structures
- Parity of legal definitions across boundaries
- Broadly accepted frameworks of accountability to the public
- Shared awareness and values, multi-agency and cross-sector dialogues
- Engagement with hard to hear social voices via social media
- Education, training and equipment for continuous anticipation of crime threats
- Reduced amount of inter-agency competition
- Better national unified systems to respond to victim reports
- Specialized investigative powers to address challenges such as the volatile nature of electronic evidence
- Comprehensive legal frameworks that support investigation of cybercrime

10. Some Research Questions Arising from the Cybercrime Workshop

1. How to make better use of existing data, for example that collected by Action Fraud and Ask the Police?
2. Why is there such a high rate of attrition from referral to prosecution? Should more use be made of anti-social behaviour orders in policing cybercrime?
3. What would the optimum cybercrime prevention toolkit look like for which public group/sector (what would be the equivalent of the 'lock your windows' house?)
4. Can profiling of offenders be more specific?
5. How should harm from cybercrime be defined and measured, including in performance indicators?
6. Future proofing: What is being dealt with now, how might it evolve, what is happening next? How does the current police response influence criminal behaviour in the future?
7. Surveying public opinion through the BCS; are current cybercrime priorities the right ones?
8. Prevention: how to apply lessons learned in the past to cybercrime, how to design protection?
9. Managing public expectations: how to communicate cyber-risk and better respond to and manage public perceptions.

Further Information

This report is one of a series that was produced by the N8 Policing Research Partnership with support from the College of Policing's Innovation Capacity Building Fund.

The N8 Policing Research Partnership (N8PRP) enables research collaborations that help address the problems of policing in the 21st century. As a regional hub for research and innovation in policing it provides a platform for collaborations between universities, Police and Crime Commissioners (PCCs), Government, police forces, and other partners working in policing policy, governance and practice.

Read more at www.n8prp.org.uk