Sean Brennan

University of Portsmouth

Institute of
Criminal Justice Studies

May 2017

Dissertation submitted in partial fulfilment for the requirements of the BSc (Hons) Crime and Criminology Degree

Institute of Criminal Justice Studies

BSc (Hons) Crime and Criminology Degree

Dissertation submitted as partial requirement for the award of BSc (Hons) Crime and Criminology Degree

Title: Cybercrime and the 'Peelian Model' of Policing: A Literature Review

Submitted by: Sean Brennan

Declaration:

I confirm that, except where indicated through the proper use of citations and references, this is my own original work. I confirm that, subject to final approval by the Board of Examiners of the Institute of Criminal Justice Studies, a copy of this Dissertation may be placed upon the shelves of the library of the University of Portsmouth and may be circulated as required.

Signed:

Date: 4th May 2017

Abstract

‘Cybercrime’ is the term used to describe the use of internet and computer technology to engage in unlawful activity. Through its scale, anonymity and portability, the internet has revolutionised the way we live our lives while in turn giving rise to new forms of crime and deviance. Policing must adapt to this unique environment while continuing to meet conventional demand. This review summarises and critically evaluates existing research on how the internet has changed society and the demands on policing. It examines the effectiveness of cybercrime policing apparatus in England and Wales, and explores a trifurcated method of improvement. Relevant literature was identified, reviewed and synthesised into three main themes to meet the objectives. Findings indicate that cybercrime is a complex and poorly defined concept which poses challenges to traditional modes of law enforcement, resulting in a poorly co-ordinated response. Conclusions are drawn that the rise of the internet in England and Wales appears to correspond with changes in criminal behaviour, but further research and improved recording practices are needed to prove a relationship. In the absence of a dedicated ‘cyber-force’, the police response is exiguous to the current threat, harm and risk. Recommendations include a shift towards multilateral and pluralised models of policing and a re-engagement of current resources through the professionalism agenda.

Keywords: cybercrime; Peelian model; literature review

Table of Contents

List of Figures

Introduction

The internet has become a parallel form of life for millions of people around the globe and wherever there is human social activity, there is altruism, and there is crime (Forst, 1993). 'Cybercrime' is the term used to describe the use of internet and computer technology to engage in unlawful activity. This can mean using computer networks or devices to commit crime or targeting them in a criminal way, for example, through hacking, the spread of viruses or denial of service attacks (Wall, 2007). In addition, the term may refer to crimes that could be conducted without computer technology, but which are enabled by the internet, such as fraud, stalking and child pornography (Brown, 2015).

Whilst there is disagreement on the scale and financial cost of these crimes, it is widely accepted that the problem has escalated into a global epidemic with profound implications for society (Levi, 2012a). The rapid growth and spread of cyber-related offences presents challenges for the prevention and detection of crime, where it is argued that traditional modes of control are insufficient for dealing with crimes unbounded from the limitations of physical proximity and scale (Brenner, 2013). Amid concerns that cybercrime "will present some of the biggest policing challenges in the immediately foreseeable future" (Stenning & Shearing, 2015, p.7), it is imperative for policy makers to review the effectiveness of current policing arrangements in England and Wales, and to reflect on future improvements.

Aim:

This literature review will summarise and critically evaluate existing research concerning policing methods, systems and apparatus in countering cybercrime in England and Wales.

Objectives:

(a) to analyse the effects of the cyber-environment on crime in England and Wales;

(b) to outline the architecture of cybercrime policing in England and Wales and to examine its strengths and weaknesses;

(c) to consider the future of law enforcement in England and Wales in response to the threat of cyber-crime.

To meet these objectives the review is organised into three chapters.

Chapter One will examine how the cyber-environment has effected crime in England and Wales, identifying challenges in defining cybercrime and theories applied to understanding and explaining the phenomenon.

Chapter Two will critically examine current methods, systems and apparatus of tackling cybercrime in England and Wales, identifying the strengths and weaknesses of applying the traditional 'Peelian model' of policing to new and emerging threats.

Chapter Three will explore how a future policing model might be configured to better meet the demands of cybercrime, including taking a multilateral, pluralised and evidence-based response.

Chapter One

Understanding Cybercrime

This chapter will critically examine the effect of the internet on crime and consider how its expansion coincides with a reduction in traditional property crimes alongside a rise in sexual crimes and fraud. The nature of cybercrimes will then be discussed alongside policy and practitioner efforts to reduce it. Finally, it will evaluate theoretical frameworks and explore the divergence between scholars who paint cybercrime as a unique construct and those who argue that it is merely "old wine in new bottles" (Grabosky, 2001, p.244).

The Effect of the Internet on Crime

In 1989, Sir Berners-Lee proposed a vision of a world-wide web that would become integrated into everyday life to the extent where it would no longer be separate from reality (Berners-Lee, 1989). Almost thirty years later and 82% of the British adult population (41.8 million) accesses the internet daily or almost daily (ONS, 2016a), while internationally, over 40% (3.4 billion) of the world's population enjoys some form of access (Pick & Sarkar, 2015). As parity of global connectivity improves (Gelvanovska, Rogy & Rossotto, 2014), the internet is becoming an integral part of modern British life, with our most popular activities being e-mail (79% of users), finding information about goods or services (76% of users), reading the news (60% of users) and internet banking (60% of users) (ONS, 2016a).

Blanton and Kegley (2016) mark the introduction of the internet as a cultural revolution in the acquisition and diffusion of information however, such progress may be comparable to other patterns of human contact which have led to a globalised world. For instance, Friedman (2005) argues that when trade opened between the New and Old Worlds in the fifteenth century, the world shrank from large to medium as countries globalised; then came the technologies of the Industrial Revolution that shrank the world from medium to small as companies globalised; now in the deindustrialised era, the creation of fibre-optic networks appears to have shrunk the world from small to tiny as individuals themselves

globalise. Arguably, the difference between this and earlier forms of globalisation is that people and technology are now closely intertwined through an instantaneous network that "reflects [human] interests, obsessions and imperatives over a very wide range of value sets, cultures and assumptions" (Berners-Lee, et al, 2006, p.80).

As the landscape of interaction expands, further transformation is observed in the decline of national identity, where the ability of government to exert control over its territory and citizens is impaired (Ariely, 2012). These two phenomena are highlighted by Castells (2009) in his 'networked society' theory, whereby the physical spaces of production, decision-making and participation are shifted into global spaces of information flows. At this point the internet offers a duality of existence; a world where the virtual becomes a platform for all forms of human labour, recreation and transgression (Ferrell, Hayward & Young, 2015). The question then, is how can a decentralised architecture be understood through social science, when it retains traditional terms of bounded units and forms of analysis (Kirby & Penna, 2011)?

Rapid expansion of the internet has provided free and open access to information while creating new opportunities for criminals to exploit (Decker, 2008). The National Crime Agency (NCA) (2014, p.4) claims that "if there is a single cross-cutting issue that has changed the landscape for serious and organised crime, it is the growth in scale and speed of internet communication technologies". Wall (2007) further argues that the global impact of the internet has altered traditional modes of delinquency and created new demands on the police; a theory which, on the face of it, is supported by data on recorded crimes in England and Wales. In 1990, there were a total of 28,970 sexual offences, 529,161 domestic burglaries, 1,267,288 vehicle related thefts and 147,909 fraud offences (ONS, 2016b). By contrast, in 2015 there were a total of 88,219 sexual offences (+205%), 197,021 domestic burglaries (-63%), 351,452 vehicle related thefts (-72%) and 230,630 fraud offences (+56%) (ONS, 2015) (see Figure 1).

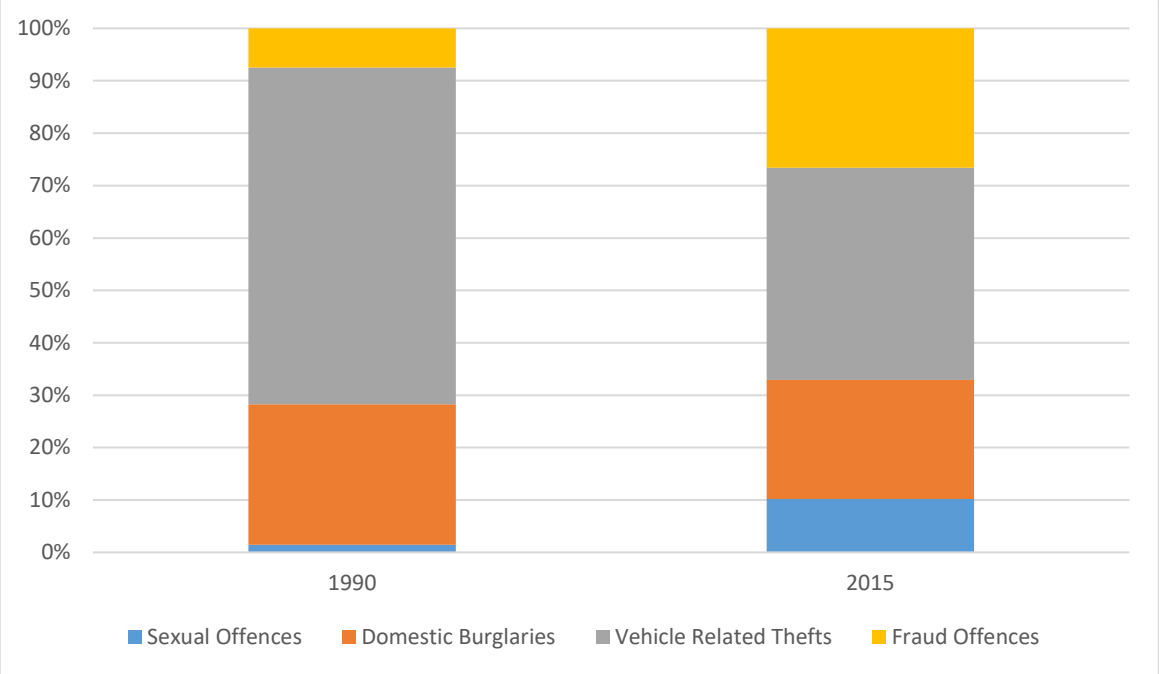

Figure 1: Changes in Home Office Recorded Crime Data in England and Wales 1990 - 2015

The reduction in traditional property crimes alongside a rise in sexual crimes and fraud suggests that crime in England and Wales has altered significantly over the last 25 years. Nevertheless, tempting as it may be to conclude a link with technology, there are alternative theories for this transformation, including socio-economic influences (Rosenfeld & Fornango, 2007), changes to police recording practices (Thomas, 2016), increased incarceration of offenders (Levitt, 2004), innovative control strategies (Ratcliffe, 2016) and the reduction of lead in the atmosphere (Stretesky & Lynch, 2004).

Beyond recorded crime, the College of Policing (2015) analysed demand on policing by incorporating calls for service together with local preventative work not captured by forces or national datasets. This revealed a reduction in discretionary activity such as patrolling; an increase in non-crime demands (e.g. concern for welfare calls) that account for 84% of all command and control logs; an increase in the number of indictable cases heard at Crown Court attributed to a growth in complex crimes; a two-fold increase in the number of indecent images of children being shared over the internet; an increase in the number of human-trafficking referrals and an increase in child safeguarding demand. Crucially, the

report identified limited data on new and emerging crimes, mainly because data returned to the Home Office relate to the crime itself rather than the context in which it was committed. Despite acknowledging this, the authors appear to overlook similar limitations with data from the Crime Survey of England and Wales (CSEW) since questions relating to fraud and cyber offences were not included before October 2015 (ONS, 2016b). It could be argued then, that the failures of both the CSEW to include cybercrimes in surveys conducted prior to 2015, and of the Home Office to delineate true computer crimes from those where the context included peripheral use of technology, means that the impact of internet technology on crime is poorly understood.

Defining Cybercrime

Whilst the link between technology and crime is unclear, a review of literature suggests that crime has transformed since the 1990s, attaining new dimensions and creating an array of new challenges and demands on policing (Brown, 2015; Pyrooz, Decker & Moule, 2013; Brenner, 2008). The nature of online criminal activity means that skilled criminals have acquired a transnational reach in conducting illicit intrusions into computer networks to gather information, deface websites or carry out distributed denial of service (DDoS) attacks (Clough, 2015b). Fraud specialists employ social engineering techniques including spamming, domain squatting and phishing to manipulate peoples' actions (Broadhurst, Grabosky, Alazab & Chon, 2014). Bullying has moved beyond traditional spheres as cyberbullies subject their victims to flaming (abusive posts), malware (deliberate sharing of viruses) and outing (posting of personal information) (Gillespie & Weare, 2015). The spread of online child pornography worldwide exposes children to the dangers of sexual assault and re-victimisation that occurs in the knowledge that through the internet their images are kept alive (Taylor & Quayle, 2003). Examples can be broadened further to include concepts of organised cybercrime, corporate espionage and cyber-terrorism (Brenner, 2010).

The social and economic costs of cybercrimes may be hard to define as a lack of reliable empirical data means that no study can ever be definitive (Levi, 2012a). The scope of the challenge may be increased by an underreporting of cybercrime

from the public and businesses and a lack of transparency and comparability from industry sources (McGuire & Dowling, 2013). In the former case, a survey by the Institute of Directors (2016) found that 49% of firms believed the most significant damage from cybercrime was the interruption to business, but only 28% of incidents were reported to police. In the latter case, Lagazio, Sherif and Cushman (2014) suggest that UK financial institutions are affected by a feedback loop, where a higher number of reported cyber-attacks is linked to a higher potential for reputational damage. It is therefore claimed that companies under-report cyber incidents in the UK, which drives down government estimations of the problem and leads to a lower state effort to reduce it. Nonetheless, a recent official estimate (Action Fraud, 2016) suggested that the cost of cybercrime to the UK economy was £10.9bn. Prior to this, a report by Detica (2011) estimated the annual cost to be £28bn, while a study by Anderson, et al (2012), broadened to include traditional (e.g. tax fraud), transitional (e.g. online payment card fraud) and new crimes (e.g. malware), found the cost of genuine cybercrime to the UK economy was a much lower £108m.

Beyond the monetary costs of cybercrime are the political and social effects (Kshetri, 2010). First, are implications for education, employment and wealth creation. In the UK, in 2010, approximately 16,500 young people aged 11–15 were absent from school where bullying was cited as the main factor (Brown, Clery & Ferguson, 2011). Of the total number who experience bullying, 65% report some form of cyberbullying (Ditch the Label, 2016). This is significant, as a longitudinal study found that Britons who were bullied in childhood had poorer cognitive functioning at the age of 50 and lower education levels, with male victims more likely to be unemployed and earn less (Takizawa, Maughan & Arseneault, 2014).

Second are implications for child protection. Holloway, Green & Livingstone (2013) remark on the substantial rise in internet usage by children under nine years between 2007 (67%) and 2012 (87%), with children using online and mobile technology to access virtual worlds and social networks. The potential dangers within these domains can be categorized as content-risks (child receives mass produced content, e.g. pornography), contact risks (interaction commenced

by an adult, e.g. sexual grooming) and conduct risks (child participates in peer-to-peer interaction, e.g. cyberbullying). However, as sensible as it may seem to affiliate the increase in internet usage with an increase in risk, it is worth noting that long-term measures over the same period in the UK and USA indicate little or no increase of harm to children (Madge & Barker, 2007; Maughan, Collishaw, Meltzer & Goodman, 2008), and a slight decrease in bullying and victimisation (Finkelhor, 2014). Examining the mantra that new technologies expose children to greater risk (College of Policing, 2015; Unicef, 2011), Livingstone & Smith (2014) question whether older forms of risk have instead been displaced (e.g. children accessing pornography online rather than offline), whether the receipt of hostile words or content is amplified by the ease or anonymity of new technologies, and whether technology is now so entrenched into children's communicative activities that it is likely to be implicated along with (rather than instead of) real-world interactions. They also suggest that the intensification of practitioner and policy efforts to raise awareness has resulted in children becoming more resilient, hence measures of harm have not increased commensurately.

Third are implications for liberty and security. As the internet raises new risks for criminal victimisation, it inevitably raises questions about control. The UK National Cyber Security Strategy (HM Government, 2016) aims to expand the focus on cyber threats through the development and deployment of technology and the creation of a National Cyber Security Centre. This is cemented by the 2016 Investigatory Powers Act, which, according to sponsors, provides a framework to govern the official use of covert powers (House of Commons, 2015). However, critics of the legislation (MacAskill, 2016) point to a provision that requires communication service providers to retain internet connection records for a period of 12 months. Reasons for this include the prevention or detection of crime, interests of public safety, assessing and collecting taxes and the regulation of financial services (Schafer, 2016). While law enforcement argue that such powers are necessary in the fight against crime (UK Parliament Joint Committee, 2016), Anderson (2016) identifies that the shift from monitoring communications based on individual suspicion to the indiscriminate collection of personal data has a "chilling effect on people's willingness and ability to lawfully

express dissent" (p.6). Thus, it argued that repression in the physical world is realised through the regulation of cyberspace, in what Cohen (1985) describes as the 'soft line' mode of social control.

Theoretical Cybercrime Framework

Despite consensus that cybercrimes exist, there remains debate on "what they are and what risks they pose" (Wall, 2007, p.185). Over the last two decades, criminological research has expanded to develop understanding of these new modes of deviance, but without a unified definition many scholars are conceptually divided (Holt & Bossler, 2014). On one side is the perspective that cybercrimes are traditional crimes applied through new means, but driven by the same intrinsic human emotions that underlie corruption in the real world. Describing cybercrime as "old wine in new bottles" (Grabosky, 2001, p.244), or at best "old wine in bottles of varying and fluid shape" (Yar, 2005, p.424), scholars such as Newman & Clarke (2003) and Taylor, Caeti, Loper, Fritsch & Liederback (2006) cite 'routine activities' theory (Cohen & Felson, 1979) in asserting that the basic tenets of motivation, opportunity and the absence of a capable guardian are as applicable to cyberspace as they are to street-crimes.

Nevertheless, in their analysis of studies on victimisation using 'routine activities' as a theoretical framework, Luekfeldt and Yar (2014) found divergence between diverse types of cybercrimes and the impact of each tenet. For example, examination of victim impact factors (opportunity) found that women, people with a higher education and those with a paid job were exposed to the most risk of hacking and malware, whereas the risk of identity theft bears no correlation to any of those factors. The authors therefore question whether cybercrimes have changed the traditional elements of 'routine activities' theory to the extent that they can no longer explain victimisation. Similarly, a study by Bossler and Holt (2009) identified that strong computer skills and careful password management did not reduce the threat of malware infection, suggesting that the presence of a capable guardian holds little influence over cybercrime victimisation.

Other criminologists paint cybercrime as a unique construct, focusing on the social-structural aspects of the environment in which they occur. Furnell (2002)

and Brenner (2009) argue that conventional spatial-temporal theories are unable to comprehend activities such as hacking or the disruption of computer functionality (viruses and DDoS attacks) since they exist purely within the infrastructure of information technology systems. In this novel environment, the scale and scope of offending is inexorably transformed, as are the relationships between victims and offenders (Capeller, 2001). Here attention is given to sociological accounts of globalisation as a form of time-space compression (Harvey, 1989), with internet theorists suggesting that near-instantaneous encounters between spatially distant actors in cyberspace render us vulnerable by creating new methods of connection and exchange (Shields, 1996). In discerning their ontological structures, it is suggested that while people, objects and activities can be easily located in the fixed and ordered 'real world', such assets are chronically disorganised in the cyber environment. Thus, the ecologically oriented theories of crime that require convergence between likely perpetrators and suitable targets in time and space are of limited value in explaining cybercrime (Yar, 2005).

Supplementing these perspectives is a less binary approach that addresses the question of whether cybercrime is a new form of offending or merely traditional crime in a novel environment. By reconceptualising cybercrime so that it exists on a continuum, it could be argued that the answer is both, depending on how criminals apply technology in the commission of the crime (Gordon & Ford, 2006). It is broadly acknowledged that there are two distinct but closely related forms of computer crimes. At one end are cyber-dependent acts that exist purely within the virtual realm and can only be committed using a computer, the internet or other technology. Such acts are directed towards other computer networks and may include hacking and the spread of viruses. At the other end are cyber-enabled acts that are increased in scale or reach using computer networks but remain people related at their core (Clough, 2015b). While they may occupy an equal share of the definitional spectrum, in 2015 there were a reported 16,349 cyber-dependent crimes in the UK, compared with more than 700,000 cyber-enabled incidents (NCA, 2015c). Thus, it is argued that cybercrime is a firmly human phenomenon irrespective of the ontological debate.

In addition, Manky (2013) offers an insight into how the internet is changing the strata of offenders through the development of crime-as-a-service, where the technical barrier to individual participation is removed and replaced by a low-cost service based model. In other words, whereas cybercrime offenders were traditionally highly skilled individuals acting in pursuit of their own goals, they now offer cybercrime-as-a-service that can be obtained for a fee. The unique ecosystem of the internet provides an environment where anonymity infers a lack of consequence and therefore a lack of personal responsibility (Europol, 2014). This arguably presents new challenges for traditional theories of deviance and systems of control pointed toward an easily identifiable, and therefore manageable subset of the population, and facilitates those lacking in technical knowledge and experience to commit crimes on a scale disproportionate to their ability.

The internet has changed the landscape of human interaction. Its free and open access to information has altered traditional modes of delinquency and created new demands on the police. Arguably, this may have contributed to a change in crime in England and Wales between 1990 and 2015, as crimes that were limited to physical spaces have shifted to those that can inhabit the online domain. The control of cybercrime is made difficult, not simply because of its reach, but also because of its form, and the solutions for child sexual exploitation are not necessarily suited to fraud. It is argued that the state of cybercrime policing corresponds to a discord in academia, and that designing an appropriate response first requires the problem to be understood. The next chapter will examine how a traditional policing model is confronting the demands of cybercrime.

Chapter Two

Cybercrime within a 'Peelian Model' of Policing

This chapter traces the history of the 'Peelian paradigm' to discover the logic behind its territorial nature. Situated in the modern policing framework are the NCA and Regional Organised Crime Units (ROCUs), whose role in dealing with cybercrime will be critically discussed. Next the role of local police officers dealing with bulk cybercrimes will be examined, before analysis of specialist capabilities pointed at higher risk crimes asks if space exists to incorporate digital vigilantism into this arena. Finally, mechanisms for reporting and recording cybercrime will be reviewed.

Towards a 'Peelian Paradigm'

The Metropolitan Police Act was introduced in England in 1829 by Sir Robert Peel amid concerns about social dislocation, moral decay and rising crime (Reiner, 2010; Emsley, 2014). Fear of the dangerous classes was reinforced by annual statistics purporting a seven-fold increase in the number of persons committed for indictable trials. Crimes of the day were often driven by social and economic necessity (Taylor, 2005) and included petty thefts, prostitution, drunkenness, and vagrancy (Emsley, 2011). Public knowledge of criminal activity was limited to their own and vicarious experiences gained through the press. In this context, Peel sought to introduce an ethical, transparent and democratic police force that would gain public support. In doing so, he reformed the parochial system of the night-watchmen and parish constables (Critchley, 1978), leaning instead, toward a local approach, focusing upon public co-operation and crime prevention. Hitherto social and quasi-criminal activities such as drinking, gambling, animal cruelty, and even the collection of family maintenance were incorporated into police control (Taylor, 1997). The social dynamics of crime were thus transformed and despite public opposition to professional, centrally organised law enforcement, Peel's model was implemented throughout England and its Colonies, underlining the approach used to control crime today (Brenner, 2010).

Brenner (2010) argues that the 'Peelian model' was created to deal with the problems of urbanisation and was consequently fashioned by the distinct characteristics of real-world crimes: first, in the physical world both victim and perpetrator are proximate to one another, occupying the same geographic space. Second, real-world crimes frequently occur on a one-to-one scale where the perpetrator must focus attention on consummating a crime before moving to the next. A burglar for example, cannot break into more than one house at one time. Third, real-world crime is subject to physical constraints, requiring some level of planning to succeed. Fourth is the ability to track crimes insofar as victimisation tends to fall into geographic or demographic patterns, causing much of society's routine crime to be concentrated in identifiable areas. It is argued that Peel's model takes for granted the persistency of this ecosystem and assumes that the task of law enforcement is to deploy force to respond to a threat in a specific territorial area (Brenner, 2014).

Although the characteristics and constitutional position of English and Welsh policing has altered, for example, with the post-war shift from a service-oriented to a crime-fighting model, many original principles remain firmly intact. Police today still adopt a leading role in the investigation of crimes, holding responsibility for interviewing victims and arresting suspects (Hodgson, 2010). Moreover, modern policing continues to be ordained within bureaucratic hierarchical structures that are responsive to local crime, identifiable from the public and accountable to law (Wall, 2007). Nevertheless, scholars suggest that policing systems in developed economies, including Britain, continue to undergo radical change through the expansion of private and community-based agencies (Bayley & Shearing, 1996); a growth in transnational governance and institutions (Sheptycki, 2007) and; the emergence of evidence-based policing (Sherman, 2013). It is within this pluralised environment that Stenning and Shearing (2015, p.7) observe that cybercrime "will present some of the biggest policing challenges in the immediately foreseeable future".

The National and Regional Picture

In England and Wales, the response to cybercrime is led by the National Cyber

Crime Unit (NCCU) within the NCA. Born from the UK Cyber Security Strategy (HM Government, 2011), the NCCU investigates the most serious incidents of cybercrime, offers technical, strategic and intelligence support to local and regional law enforcement and advises private industry on control measures (NCCU, 2017). Its priorities are to suppress the market for cybercrime-as-a-service and deal with specific threats that meet an undefined threshold of national and international harm (Morbin, 2014). Analysis of the NCA website and online news reports suggests that the unit has enjoyed limited success in terms of prosecutions, while research evidence on its efficacy remains unpublished.

Situated beneath the NCCU are ten ROCUs that provide specialist capabilities including cybercrime investigation. These regional police units are distinct from the NCA and form part of the government strategy to prevent serious and organised crime (HM Government, 2013). A review of their capability and effectiveness identified inconsistencies in their structure, with some forces unwilling to commit resources (HMIC, 2014b). Thus, while each ROCU has the capacity to investigate cybercrime, their response is often limited and detached from efforts to tackle traditional organised crimes. Not only are the roles and responsibilities of police forces and ROCUs in relation to cybercrime poorly understood (HMIC, 2014b), the objectives of NCCU, ROCU and local policing overlap significantly. For example, while the NCCU leads operations against the most serious cybercrimes while "working in partnership with ROCUs to arrest cyber criminals" (NCA, 2015a p.3), ROCUs investigate serious and organised cybercrimes while supporting local forces, and local Police Cyber Crime Units have a mandate to "tackle those responsible for the most serious [cyber] incidents" (IBT, 2011, p.1).

In determining the effect of strategic overlaps, an ethnographic study on inter-agency responses to child abuse observed how professional collaboration was frequently impeded by gate keeping and domain disputes that occur through blurred boundaries between partner organisations (Scott, 1997). However, a cross-sectional survey of child protection and mental health workers identified that structural impediments, such as inadequate resources and gaps in inter-agency methods were more important than individual level barriers to collaboration, such

as professional knowledge areas and boundaries (Darlington, Feeney & Rixon, 2005). To what extent then the intersection of agency roles holds implications for investigating cybercrime is unclear.

Increased funding for national and regional cybercrime units (NCA, 2015b; HM Government, 2015) is built on the premise that "developments in organised crime, notably the emergence of cybercrime, mean [that the UK] needs to improve NCA and police capabilities" (HM Government, 2013, p.10). Lavorgna and Sergi (2016) are sceptical about the extent of cybercrime organisation, arguing that evidence of criminal groups operating in cyberspace (Lusthaus, 2013; Hutchings, 2014; Kleemans, 2014) is mostly speculative or anecdotal. It is suggested that constructing cybercrime as 'organised' plays with the concept, to raise the seriousness of online threats and invoke powerful regulatory frameworks (Leukfeldt, Lavorgna & Kleemans, 2016). In the UK, this is seen in the Investigatory Powers Act 2016, the announcement of cybercrime as a tier one threat to national security, and allocation of Government Communications Headquarters (GCHQ) resources to a Joint Operations Cell in collaboration with NCCU (Paganini, 2015).

In exploring the role of GCHQ in combatting cybercrime, the interplay between policing and intelligence is understood through the doctrine of risk management applied in a similar way to the war on terror, where enemies are elusive and the aim is to avoid harm without the prospect of closure (Heng, 2002). There, as in here, the emphasis of criminal justice shifts from gathering evidence for prosecution to identification of targets based on risk calculations derived from the surveillance of meta-data. But how did a spying agency gain control over crime? Lea (2015) argues that once the principles of anti-terrorism stratagems are established, they begin to contaminate other areas of criminal justice and state security. It could be argued that with cybercrime, this process was ameliorated with the institution of cyber threats as a focal point to national security where two interlinking factors convened: first a belief that modern societies are imperiled by growing numbers of catastrophic vulnerabilities; second, a perception that dangerous actors are prepared to ruthlessly exploit those vulnerabilities (Furedi, 2008).

Dunn-Cavelty (2012) posits that the handling of cybercrime in the UK is linked directly to the level of knowledge, or rather non-knowledge, of a highly diffuse problem. As a result, speculative forms of vulnerability-based analyses are relied upon for the identification of weaknesses (in this case the UK National Security Strategy). Inevitably these become reified in the political process so that potential threats are turned into actual threats, and in the UK, a military response becomes the answer to a law enforcement problem. This culminates in a strong human rights argument to return primacy of cybercrime investigation to the framework of local policing.

General Practitioners and Bulk Cybercrimes

Flannery and Graham (2014) suggest that in the control of cybercrime, most investigative work is carried out by general practitioners, where typical cases include cyberbullying, small value frauds and the possession and distribution of indecent images (Bryant & Kennedy, 2014). Determining the effectiveness of local practitioners in responding to cybercrime through literature is challenging. In 2015, the National Police Chiefs Council (NPCC) published a framework for internet investigations at force level that for first responders included increased awareness of digital scene preservation, standardised cybercrime prevention advice to victims, the ability to conduct online patrols and new ways to engage with the public online. Translating this into practice may prove difficult however, as the new policing architecture requires managers and practitioners to adhere to Authorised Professional Practice (APP) set by the College of Policing (2013).

Analysis of published APP on cybercrime and related issues suggests that guidance on digital investigation is still under development. Since research indicates that most officers hold no opinion on their current and future roles in confronting the cybercrime problem (Bossler & Holt, 2012), the absence of standardised cybercrime policy and procedure presents a significant barrier to the implementation of the NPCC framework and its idealised front end response. This situation contrasts with experience in the commercial sector, demonstrating that "in increasingly globalised and high-risk industries, internal communications and training are the first frontiers where the battle for the consumer is fought and won – or lost" (Chong, 2007, p.210).

According to Brenner (2013), emerging crimes, including cybercrimes, exponentially exceed traditional crimes, yet they have simply been added to the list of problems with which law enforcement must deal. Consequently, the ability of police to react effectively is eroded because resources that were barely adequate in dealing with real-world crimes are wholly inadequate in dealing with cybercrime-plus-real-world-crime. In policing, where demand is prioritised, the consequences are manifested in two studies, observing how local investigators considered the social impact of cybercrimes as inferior to traditional forms of crime (Leukfeldt, Veenstra & Stol, 2013), and similarly, that officers found it difficult to empathise with cyber-victims compared with victims of traditional crimes (HMIC, 2015). This may suggest that victims of low harm cybercrimes receive a poorer service within the framework of local policing.

Moreover, evidence suggests that local police agencies have neither the training nor the resources to investigate cyber-offences properly. The solution often proposed is for police to work more effectively with other agencies that provide security on the internet (Brenner, 2008; Hinduja & Patchin, 2008). However, it could be argued that in the UK, police attitudes are reinforced, not through a lack of funding, awareness or collaboration, but by a National Intelligence Model (NIM), which uses information on criminal acts to determine where to intervene on the strategic and tactical level. Since the protocol relies on the throughput of information, it centres on the idea that crime only becomes relevant when it is visible and therefore detectable by the police (Sergi, 2015).

In this regard NIM is consistent with the English legal principle of *de minimism non-curat lex:* 'the law does not deal with trifles' (Gillespie & Weare, 2015, p.264), and it is here that Wall (2007) observes a conflict between prioritisation and cybercrimes that are small-impact with bulk victimisation spread across multiple jurisdictions. As policing strategies in England and Wales are often reduced to decisions made in the public interest, it becomes harder to justify expenditure on cybercrimes, and thus in times of austerity, police attitudes are perpetuated by the NIM and the principle of *de minimism*.

Specialist Capabilities and High Harm Cybercrimes

For lower volume, higher harm cybercrimes (e.g. high value fraud, industrial espionage, extortion), police rely on specialist departments that broadly fall into three categories (Jewkes & Andrews, 2013). First, Hi-Tech Crime Units (HTCUs) that perform forensic data recovery and image analysis on seized computer equipment. In UK forces, these tend to be small teams with a mix of digital analysts and forensic imagers, with an increasing number of police staff rather than officers (Bryant & Stephens, 2014). Amid growing numbers of cybercrimes, it is argued that most forces are failing to keep pace with investment in HTCUs (Conway, 2014; HMIC, 2014a; Goldberg, 2015) with significant delays reported in computer and mobile forensic analysis. This is exacerbated by challenges from skills retention, rapid pace of technological change, encrypted data, cloud storage and anti-forensic awareness (Houses of Parliament, 2016).

Second are units that gather intelligence on major crimes, named the Force Intelligence Bureau, Intelligence and Specialist Operations, Crime Squad or similar. These covert units work on cross-border investigations and organised crime, but are not dedicated cybercrime specialists. In determining whether the remit of these teams could be adjusted to include emerging crimes such as cybercrime, Jewkes and Andrews (2013) question their overall technical competence and suggest that the police in general are resistant to change. Multiple studies show that organisational culture plays a key role in the change process (Rashid, Sambasivan & Johari, 2003; Lorenzo, 1998; Ahmed, 1998), but in policing, a challenge lies in identifying clear behaviours that cut across jurisdictions and time.

In his analysis of the impact of police culture on cybercrime, Wall (2007) argues that cybercrime outcomes are affected by issues of routinisation. Police culture is understood as an accumulation of routine events that enable officers to interpret the world around them. In other words, the police respond to routine activities that define their occupational culture. Difficulties arise when non-routine events occur, such as cybercrime. However, in reaching this conclusion, it could be argued that Wall draws on outdated evidence (Reiner, 2000; Sussman, 1995; Shearing & Ericson, 1991; McBarnet, 1979), and that his analysis reflects the cognitive-burn

associated with much police cultural research (Sklansky, 2007). This deflates complex modern systems of policing into a caricature (Manning, 2007). With questions being raised on whether orthodox views on police culture continue to hold value, up-to-date research may be needed on specialist police team culture to determine any likely resistance to incorporating cybercrime into traditional remits.

Setting aside concerns about change resistance and addressing the importance of technical competence, research by Marcum, Higgins, Freiburger & Ricketts (2010) found that specialised task forces increased the number of investigations and arrests for certain cybercrimes compared with forces without such units (they also found that cybercrime training was not linked to increase in arrests). On the issue of whether human (as in specialist police units) or technical (as in HTCU) skills are more suited to the investigation of cybercrime, Brown (2015) posits that technology expands the capacity to acquire vast arrays of evidence, but "it is the human side of a cybercrime inquiry which is pivotal" (p.64), as an investigative mindset is needed to interpret information and initiate dialogue with key individuals. This contradicts the idea that a new policing model requires not "the 50-year old sweaty detectives" (Flannery and Graham, 2014, p.27) of the kind observed by Loftus (2012), "but 20-plus year olds who have grown up using computers on a daily basis". Instead, it suggests that both are relevant in the fight against cybercrime.

The third group of specialists are those who deal with obscene images of children and investigate paedophile networks, often called Public Protection Units. In many forces, internet child abuse investigation is complicated by organisational structures where specialist departments contain units with overlapping responsibilities (Jewkes, 2013). The West Midlands Police (2017), for instance, possesses both a dedicated Online Child Sexual Exploitation Team tasked with "identifying and prosecuting [online] sexual predators" (p.6) and a Technical Intelligence Development Unit tasked with "conducting covert online operations" (p.7). Both target offenders through online chat rooms, social networking sites and Darknet forums (Dubord, 2008), interacting directly with perpetrators to witness crimes as they occur (Tetzlaff-Bemiller, 2011).

Undercover officers require comprehensive understanding of covert policy and legislation, but in return such operations typically succeed because the obstacle of attributing online criminal activity for law enforcement makes it equally difficult for perpetrators to recognise undercover agents (Lusthaus, 2012). In a policing architecture described as pluralised, networked and post-regulatory (Bayley & Shearing, 2001; Johnston & Shearing, 2003; O'Malley & Palmer, 1996), it is argued that the ability to operate clandestinely without the physical difficulties of attribution may influence and alter the relationship with actors elsewhere in the policing sphere. The control of internet sex offences already involves a multi-layered assemblage of cyber-policing actors (Yar, 2013). For example, internet service providers carrying out pre-emptive actions in response to parental concerns about child safety (Jones, 2009). These are Walls' (2007, p.188) "online virtual environment security managers". Then there are internet users themselves, who are mobilised to generate invisible flows of actionable intelligence to intermediary organisations, such as the Internet Watch Foundation, who receive and process reports of child grooming and sexual imagery (Clough, 2015b). In evaluating the consequence of Lusthaus' (2012) attribution phenomena in terms of reordering specialist policing services however, it is the third strand, known as digital vigilantism (Campbell, 2016) that features most prominently.

In England and Wales, and elsewhere, so-called 'paedophile hunters' (Kosseff, 2016) employ methods outside of traditional policing practices, raising questions about where the normative bounds of citizen involvement might be drawn. Set against a moral panic that online paedophiles are at epidemic levels (Barford, 2013), the emergence of digital vigilantism coincides with new opportunities for citizens to exact their own forms of criminal justice (Wall, 2007). Digital vigilantism occurs in response to actual or perceived failings of policing, but is usually supportive of the state and allied to the concept of law and order (Trottier, 2016). In contrast to their growth, Yar (2013) argues that the extent of public concern reserved for internet sex offending generates demands that their policing should not be "surrendered to voluntarism, chance or the initiative of users" (p.492) and serves to counter the trend toward pluralisation and privatisation. This may seem clear, but the question of whether digital vigilantism could ever pass the test of legitimacy within the existing policing framework is equivocal

(Campbell, 2016). As Ashenden (2002) explains, in a liberal society the socio-political imaginaries of law and due process can be excused in the pursuit of child protection. This is seen in Gamble's (2014) proposal to harness the spirit of vigilantism into an army of digital volunteer detectives, comparable to the Special Constabulary, but patrolling online spaces rather than towns and cities.

However, this notion overlooks a key aspect of digital vigilantism; that it essentially weaponises the visibility of its targets (Trottier, 2016) and "legitimates accompanying forms of violence, including the structural foreclosure of life chances" (Gandy, 2009, p.59) (paedophile hunters typically name and shame their targets publicly before handing evidence to police). Nevertheless, how can an aim to render the problem visible be reconciled with calls from the NPCC to rehabilitate, rather than imprison paedophiles who view indecent images, but go no further (Sawer, 2017)? Furthermore, a citizen can only progress a case so far, until it falls to traditional policing to arrest and process a suspect. Unless due process safeguards are surrendered then incorporating online volunteers into the policing framework may only add to the burden on policing, thus reducing public confidence further and increasing the frustration that fuels vigilantism in the first place. As cost-saving as it may be to incorporate digital vigilantism into the policing assemblage, the idea poses risks to consensual, accountable and legitimate policing within liberal democratic societies (Tan, 2012). This new wave of vigilantism may never become stabilised within policing proper, but it nonetheless describes how future cybercrime policing could be delivered "elsewhere and otherwise" (Campbell, 2016, p.360) than in existing policing structures.

Cybercrime Reporting and Recording Mechanisms

The task of identifying victims and preparators of cybercrimes is complex and may significantly impair the capacity of the police to respond effectively (Brown, 2015). In 2016, the CSEW included experimental statistics on fraud and cybercrime that were published alongside Action Fraud data and police recorded offences flagged as having an online element (ONS, 2017). In the UK, Action Fraud has been the central reporting mechanism for fraud and cybercrime since

2014 and is the single point of contact for businesses and individuals (Ryder, 2011). It provides users with a crime number but does not investigate cases or update victims (Gillespie, 2015). Instead, it maps patterns and trends and disseminates crime packages to police forces, who guide the response and in some cases, initiate investigations (Clough, 2015b). This means that cybercrime victims are disadvantaged compared to traditional victims who can at least be assured of a basic police investigation.

Moreover, while Action Fraud statistics incorporate cyber-enabled frauds, they may not accurately reflect the cybercrime problem since they overlook its many other forms. As there is no specific offence of 'cybercrime', measures rely upon the flagging of police recorded data. Contrary to the objective of the UK Cyber Security Strategy (HM Government, 2016) to increase mainstream awareness however, research with front line officers in an English metropolitan area found that only 26% of officers felt clear on the definition of cybercrime, with 67% indicating that they rarely or never use the term 'cyber' to describe the crimes with which they deal (White, 2015). This poor understanding could lead to the cyber-flag indicator being used incorrectly, thus presenting a false picture of the demand from cybercrime.

While the UK provides some transparency on fraud losses through data published by Financial Fraud Action UK (FFA UK) (Levi, 2012b), the effect of cybercrime within the financial industry remains opaque as FFA UK data excludes attempts prevented through banking detection systems. These factors combined, result in a disparate picture of an emerging crime problem. Those who suffer loss are disadvantaged compared to victims of traditional offences and may be confused by the array of organisations involved in the regulation of cyberspace behaviour (Wall, 2007). Reliable data is essential to the allocation of government funding (Armin, Thompson, Ariu, Giacinto & Roli, 2015) and without sufficient resources the current policing paradigm cannot evolve to meet the emerging threats of today.

The 'Peelian model' of policing was created to deal with the problems of urbanisation and is fashioned by the characteristics of real-world crimes.

Overlapping objectives of the NCA, ROCU and police may stem from a framework that retains this ethos, resulting in poorly coordinated services. The allocation of military resources to cybercrime is understood through the doctrine of risk management as applied to a similar front on the war on terror. While this leads to a strong human rights argument to return primacy of cybercrime investigation to local policing, it may also reduce the quality of service for victims. A review of specialist police units indicates that policing and technical skills are equally valuable in the fight against cybercrime. Finally, accommodating digital vigilantism into policing would require significant due process safeguards to be surrendered, and while this may seem implausible, in a liberal society the socio-political imaginaries of law and due process can be excused in the pursuit of child protection. The concluding chapter will examine how the traditional policing model could be improved to better meet the demands of cybercrime.

Chapter Three

Analysis and Conclusion: Towards A New Cyber Paradigm

This concluding chapter will critically examine macro, meso and micro-level solutions for improving the current model of policing. It will suggest that historical precedent exists for bringing cybercrime under international control; that a pluralised response must somehow overcome the philosophical difference between public and private actors; and that policing in England and Wales should align itself with a medical model of professionalism to counter the prevailing dogma on cybercrime.

The Macro: A Multilateral Response to Cybercrime

The discussion on cybercrime has identified major constraints in respect of the principle of territoriality, where the decentralised architecture of the internet and the dynamic transfer of data across multiple jurisdictions has impaired the ability of governments to exert control over their territory and citizens (Ariely, 2012). This provides new opportunities for criminals, while simultaneously challenging traditional methods of control that have evolved to counter threats in a territorial area (Brenner, 2014). In the milieu of globalisation, a juxtaposition is observed between the moral, political and constitutional differences of sovereign states (Swire, 2005) and the highly diffuse but interconnected assemblage of global information and communications infrastructure that transcends geographic borders (Putman & Elliott, 2001).

Analysis on the effectiveness of state actors operating inside this domain suggests that sophisticated criminal networks maintain a substantial advantage by employing layers of technical abstraction (Kellerman, 2010), and that efforts to locate and apprehend offenders are frequently impeded by a lack of formalised protocol on information sharing and the prosecution of offenders. Scholars in international jurisprudence (Clough, 2015a; Furnell, 2002) point to the Council of Europe's Convention on Cybercrime (2001), or the Budapest Convention, as being the nearest thing to a multilateral treaty in the fight against cross-border

crime. While the treaty aims to increase co-operation between law enforcement in the collection of computer evidence, it also lays the foundations for a minimum legislative framework (Viano, 2016). However, it is criticised for being a piece of "symbolic legislation" (Marion, 2010, p.702) intended to console public demand for something to be done about the cybercrime problem. This view is reinforced by Gillespie (2015) and Walden (2004) who observe limited effects of the Convention's harmonising measures in the absence of a binding requirement for signatory nations to incorporate them into domestic legislation.

Furthermore, it is argued that the addition, in 2006, of a protocol dealing with the publication of racist and xenophobic material raises a political impediment to international co-operation on cybercrime (Carr, 2016), with the USA refusing to limit freedom of expression by ratifying what it regards as the antithesis to the First Amendment of the Constitution (Banks, 2011). Here a divergence in security philosophy can be observed between European top-down regulation and the USA's decision not to interfere with governance of the internet since its early design, with distance assured by the creation of the Internet Corporation for Assigned Names and Numbers (Froomkin, 2013). This non-profit corporation held a memorandum of understanding that guaranteed that market forces would control the evolution of cyberspace through bottom-up policy, global representation and competition in the domain name server market. Consequently, the European Councils' suppression of racist and xenophobic cybercrimes away from activities where a military or economic imperative exists, may have proven a step too far. As Williams (2011) contends, the strength of the Convention in its potential to deliver cyber security may have been its most limiting factor, potentially preventing broader ratification.

With the recent vote in Britain to leave the EU and the election of Donald Trump in the USA, there is increasing concern that nations are becoming less co-operative and more isolationist (The Economist, 2016). In this context, achieving multilateral regulation of cyberspace may necessitate a common framework with the capacity to move beyond "like-minded coalitions" (Hurwitz, 2014, p.330). Rhaman, Khan, Mohammad and Rhaman (2009) argue that new institutions are required at the national and international level: a uniform international cyber law

to define what constitutes a cybercrime; the re-adjustment of existing principles of international law; an international regulatory body to monitor cyber activities under a UN framework; and the establishment of an international cyber court to try cyber offences of an international character. As a method of control however, this notion is critiqued from the point of view that significant difficulties may arise in homogenising the international response to cybercrime, where the boundaries between deviant and illegal behaviour are often influenced by social context and moral points of view (Ghernaouti, 2013). For example, the age of sexual consent varies significantly between countries; it is seventeen in Cyprus, fifteen in France and fourteen in Serbia. Thus, what is illegal in Cyprus is permissible in Serbia. In a similar way, cyber activities that are considered anti-social in one territory may be framed as criminal in another (Goodman, 2010).

Moreover, the theory of 'universal jurisdiction' derives from the idea that a crime must reach a certain level of harm, or threaten the interests of the international community, before it can displace national law (Tehrani & Manap, 2013). Examples of normative criteria include war crimes, slave trading, piracy and apartheid (Bassiouni, 2006). Arguably, while this threshold is met by acts of cyber terrorism, the international community would travel beyond the principle in exerting itself in cases of less harmful cybercrimes, such as identify theft, on the idea of them being on par with genocide.

On the other hand, in a critical assessment of piracy as an international crime, Song (2015) and Slaughter (2006) assert that its classification as a heinous act is counterintuitive, in the sense that robbery on the sea is somehow deemed worthier than robbery on the land. This leads to a conclusion that piracy was made subject of universal jurisdiction in order to solve a co-ordination issue, and so, contrary to Tehrani and Manap's (2013) bifurcated justificatory structure, it is viewed as a response to an enforcement gap rather than a jurisdictional gap. With its borderless shape and form, cybercrime in many ways mirrors the problem of maritime piracy, where the universal threshold principle has long been diminished to fill an enforcement gap in international waters. By framing international jurisdiction in an historical context, it is argued that methods of traditional

policing create a similar gap on the seas of the internet, and that new laws and models of control are required to manage crime in a networked society.

The Meso: A Pluralised Response to Cybercrime

In literature, the evolution of policing in England and Wales can be traced to three predominant eras that reflect different changes to the core function based on the mandates and priorities of the time (Nhan, Huey & Broll, 2017). The first of these is the political era in the mid to late 1800s, when policing aimed to preserve political order through moral control and social service; then came the reform era in the early to mid-20th century, when the eradication of corruption was sought through professionalism and crime control; to be replaced by the community era from the 1970s, which developed community support through prevention and problem-solving strategies (Kelling & Moore, 2005). Sceptics assert that there is nothing new in modern policing (Bullock & Tilley, 2009) but other scholars now recognise that 21st century policing encapsulates a fourth era of information policing (Luscombe & Walby, 2015; Hooper, 2014; Oliver, 2006) driven by research evidence, diverse forms of intelligence, and predictive strategies.

Despite a move towards information-based techniques and incorporating technology into their practices, the police still find themselves struggling to meet increasing demands for service (Brenner, 2014), particularly as the internet raises significant new risks for victimisation. Thus, as the capacity of traditional law enforcement is outpaced, so a number of private actors, ranging from citizens to large businesses, are starting to play a role in the administration of online security (Wall, 2007); a phenomenon described as the pluralisation of cybercrime control. Whilst the internet is becoming an increasingly vital front for state and global security, contrawise to the information on conventional threats, much of the data on cybercrime is held on commercial internet servers and it is often this sector that has a leading role and interest in its defence (Levi & Williams, 2013). Without a clear and capable guardian serving to regulate cyberspace (Tokunaga 2010), it could be argued that police strategists must learn to embrace the limitations, as well as the benefits of pluralisation (Loader, 2000), as legitimacy

can only be acquired through the unique expertise of public and private actors working together to form a security quilt (Ericson, 1994).

The provision of pluralised policing is conceptualised through Johnston and Shearing's (2003) 'nodal governance' theory, as a set of interconnected organisational and individual nodes that distribute functions, resources and problems with an effectiveness not matched by homogenous command-and control-structures (Shearing & Johnston, 2010). In theory, a cybercrime reduction network would consist of nodes of government, law enforcement, private industry and the public working collaboratively towards similar security goals (Levi & Williams, 2013). While each of these nodes may share a similar worldview, they would retain idiosyncratic agendas, and have their own form of unequally distributed capital, meaning there would be dominant and dominated actors (Dupont, 2004).

A node's economic capital would determine its ability to secure financial resources; political capital to its ability to influence strategy; cultural capital to its unique knowledge; social capital to its ability to create and maintain relations with other nodes; and symbolic capital to its perceived legitimacy in directing other members of the network (Dupont, 2004). At present, policing holds a monopoly over powers of arrest and forensic services that afford it a high degree of symbolic and economic capital (Holley & Shearing, 2017), but its peripheral position in terms of governance provides only a small degree of political capital with which to exert strategic influence (Broll, 2016). This holds serious implications for current approaches to the policing of cyber-crime.

Nonetheless, the effectiveness of nodal partnerships across public and private sectors in combatting cyber-crime is difficult to determine (Wall, 2007), with several challenges and limitations having already been raised. In their study examining the role of the public in policing cybercrime, Huey, Nhan and Broll (2012) identify barriers to nodal partnerships with civilians as legal liabilities, police perceptions that the public add little or no value to the investigative process, and police mistrust of civilian efforts. Even where this relationship is successful, concerns are raised on the 'transformation thesis' (Jones & Newburn, 2002), that as the proportion of private nodes to police nodes increases in any

given security network, the direction of the network shifts from the logic of common good to the logic of the market (Nhan, et al, 2017).

Sparrow (2014) suggests that this incompatibility can be overcome if the police consider themselves less as the deliverers, and more as the orchestrators of security provision. But what about a more radical solution? What if, instead of trying to align these two philosophies, policing strategists accept that the internet is, and always will be driven by commercial interests (Zook, 2008), and, instead of controlling crime using traditional methods, they withdraw altogether and allow online spaces to be governed by market forces? While possibly overcoming philosophical difference, such an approach would depend upon the moral perspective of each crime, and inevitably meets the argument that some crimes are so serious that only the police should deal with them. Instead, compromise could be achieved by configuring strategies that vary between crimes "following the wider contours of public and political sensibilities" (Yar, 2013, p.494). For example, by relinquishing control over online harassment and e-fraud, but retaining oversight of child sex offences and digital terrorism, policing could address moral concerns as well as capacity issues.

The Micro: An Evidence-Based Response to Cybercrime

As our understanding of the impact of networked technologies on human social behaviour increases (Burford & Park, 2014; Misra, Cheng, Genevie & Yuan, 2014), so new and emerging forms of deviance are being added to the list of conventional problems with which law enforcement must continue to deal (Brenner, 2014). In local policing, where demand is prioritised, the consequences of adding new types of cyber-enabled and cyber-dependant crimes to increasing workloads are manifested in the attitudes and behaviours of investigators toward low-level cybercrime victimisation. Consequently, sufferers may receive a poorer service compared with victims of traditional crimes (HMIC, 2015; Leukfeldt, Veenstra & Stol, 2013). This may be intensified by proposals such as that by Sherman (2015) that not all crimes are equal, meaning that different types of crimes can be weighted according to their perceived harm. Indeed, in the Cambridge Crime Harm Index (Sherman, Neyroud & Neyroud, 2016) and

subsequent Crime Severity Score (ONS, 2016c), offence categories focus on traditional crimes to the exclusion of cyber-related crimes. While these may be argued to come under the bracket of fraud for example, they nonetheless fail to highlight cybercrime as a priority.

The view that cybercrime lies low on the agenda of police officers is strengthened by data from the USA, which found that half (50%) of front line officers held no opinion on the subject of cybercrime, with only a small minority (18%) agreeing that cybercrime should be dealt with by local law enforcement (Bossler & Holt, 2012). Similarly, research on an English metropolitan force suggests that only 21% of front line officers agree that "in their current role they should be dealing with incidents or crimes which are the result of the way someone has behaved on the internet" (White, 2015, p.37), with three quarters remaining neutral or disagreeing that they were "clear about the definition of cybercrime" (p.40).

At the start of their careers, police officers are assigned to serve a geographic area, thus socialising them to understand that the role of policing is coupled to territorial and physical space (Huey, Nhan & Broll, 2012). Evidence also suggests that motivations to join the police are still couched in terms of wanting to be in a practical and physically demanding job that is predominantly outside (Lander, 2013). It would be interesting to conduct the same research using police trainees prior to initiation, to examine if these findings point to a subculture or the core beliefs of recruits, as this would enable interventions to be targeted at either the individual or organisational level.

In determining the plasticity of this and similar forms of dogma, attention turns to healthcare, where a comparison can be drawn with the way in which medical professionals have traditionally conceptualised health and illness. Until recently, disease was treated by doctors within a biological model where ill-health was exclusively treated by medical means. In the face of criticism for failing to acknowledge the influence of psychological and social factors on health and illness, a new, expanded biopsychosocial model was proposed (Engel, 1977). Evidence suggests that new methods of clinical training have challenged the dominance of the traditional medical model (McInerney, 2015), contributing to

the uptake of a broader and more holistic approach in a way that changes professional attitudes and beliefs (Jenkins & Fallowfield, 2002). While the opinions of front-line police officers toward cybercrime victimisation may be intrinsic to their territorial role, the experience of the medical profession sets a clear precedent in altering conventional dogma to deliver better outcomes for service users, without extensive structural reform.

The success of medicine in reaching a more holistic perspective may be attributable to its longstanding development as a profession, which, unlike policing, can be characterised by its own self-regulation, membership and registration; a requirement for appropriate qualifications on entry; a commitment to lifelong learning; and a body of research that underpins the practice of its members (Epstein & Hundert, 2002). In England and Wales, a drive toward professionalising the police service is supported by central government and the College of Policing, which, as part of its national role has a mandate to set and improve policing standards. Professionalising initiatives fall in line with those set out by Epstein and Hundert (2002) and include the introduction of a Code of Ethics in England and Wales (Holdaway, 2017); developing a Policing Education Qualifications Framework to address national inconsistencies in recruitment and training and; advocating for degree-level entry into the police (Home Affairs Select Committee, 2016).

This drive towards the professionalisation of policing is further supported by the concept of evidence-based policing (EBP) practices through practitioner-led research and evaluation (Thomas, 2014). Prior to now, the vacuum of shared policing knowledge was filled by external multi-disciplinary attention that substituted the practitioner-led inquiry common to many other professions (Rosenbaum, 2010). Theoretical discourse was not seen as important by police practitioners and rigour in methodology and evaluation were frequently abandoned in favour of the need to demonstrate success (Cockcroft & Beattie, 2009). Practitioners who engaged in research often did so in response to a single issue and not conducting research for its own sake (Wilkinson, 2010).

However, as much of the existing cybercrime literature remains theoretical, it could be argued that the professionalism agenda presents an opportunity to increase evidence on 'what-works' to reduce internet based crime. Drawing on the College of Policing Crime Reduction Toolkit (2017), future policing strategies and interventions targeting cybercrime would be empirically tested, leading to more a more effective and cost-effective response and better outcomes for cybercrime victims (Heaton & Tong, 2015). Moreover, empowering police officers to undertake research and create their own practice-based evidence may improve workforce understanding of cybercrime in all its contexts, while encouraging officers to take interest in, and ownership of cybercrime as a legitimate police responsibility. Evidence to support this can be found in research on body-worn video (BWV) (Ariel, Farrar & Sutherland, 2015), where the Chief of the Rialto Police Department conducted a randomised control study that confirmed a reduction in police use of force and complaints against the wearers. Consequently, Rialto police officers are issued with BWV as standard (Carroll, 2013).

In the face of resistance to the implementation of EBP (Hope, 2009), Sherman (2015) argues that the move towards taking a more evidence-based approach has three prerequisites: "(1) a powerful advocate for EBP; (2) an "evolutionary" dimension to add on to any "smothering paradigm" that resists the addition of evidence to decision-making; and (3) strong external demands for change" (p.11). While the College of Policing already advocates strongly for EBP (Sherman, 2013), the introduction and subsequent evolution of degree qualified police officers may contribute to the cultural shift towards evidence based practice, in which officers are trained with the knowledge and skills required to undertake workplace research as a normal part of practitioner-led enquiry. In the context of cybercrime, critical events such as the well-publicised theft of 500 million Yahoo users' personal details (Walters, 2016) may lead to calls for an evidence-based approach to combatting cyber offences.

This dissertation has reviewed existing literature to analyse the effect of the internet on crime and evaluate the capacity and capability of the 'Peelian model' to confront new risks and forms of victimisation. The introduction of the internet

has been marked as a cultural revolution in the acquisition and diffusion of information that surpasses all previous forms of globalisation. The rise of the internet appears to correspond with changes in criminal behavior in England and Wales, with increases in offences where online facilitation is made possible, and decreases in crimes that are fixed to the conventional realm of time and space. However, further research and improved recording practices are needed to corroborate the link and to preclude alternate theories. Existing structures and methods of policing in England and Wales are based on a formula that takes for granted the persistency of the criminal ecosystem, where the task is, and always has been, to deploy force to respond to a threat in a specific territorial area. Without a dedicated 'cyber-force' the police response is exiguous to the risk. The NCCU exists to counter national and international cyber threats, but where does this leave the bulk of cases that fail to meet these criteria? The reality is that most cybercrime victims are left to flounder in the framework of local policing, where research reveals a disturbing lack of empathy and resistance to owning the problem.

In terms of improving cybercrime policing in England and Wales, macro-analysis reveals potential difficulties in homogenising the international response to cybercrime, but examination of maritime piracy suggests that precedent exists for a multilateral solution to solve the co-ordination issue. At the meso-level, policing may need to embrace its position within a pluralised reality as it finds itself unable to contain future demand. Opposition to commercial philosophy could be reconciled if police leaders regarded themselves as orchestraters, rather than delivers of security. The option of retreating from cyberspace is alternatively proposed, but there are likely to be strong moral arguments against this, and so a compromise based on the hierarches of standing principle (Yar, 2013) could be reached, where police relinquish control over low-harm cybercrimes to increase their capacity to deal with less, but more serious online activities. On the micro-level, the views of local investigators toward cybercrime may be influenced by the Cambridge Crime Index that prioritises traditional crimes to the exclusion of cyber-related offences. This could be overridden by the introduction of a professionalism agenda that empowers officers to undertake research and improve

their understanding of cybercrime in all its contexts, encouraging them to embrace it as a legitimate policing responsibility.

The reluctance of policing to respond to new forms of human social patterns can be traced throughout history, and fundamental structural and cultural change is often reactive, and in response to dramatic events or public outcry. The findings of this review suggest an urgent need for policymakers to seize the initiative and create a new policing architecture; one that is responsive to the public's needs today, to prevent criticism tomorrow.

References

Action Fraud. (2016). *Fraud & Cybercrime Cost UK Nearly £11bn in Past Year.* Retrieved from http://www.actionfraud.police.uk/news/fraud-and-cybercrime-cost-UK-nearly-11bn-in-past-year-oct16

Ahmed, P. (1998). Culture and Climate for Innovation. *European Journal of Innovation Management, 1*(1), 30 – 43.

Anderson, P. (2016). *Fighting Terrorism, Repressing Democracy: Surveillance and Resistance in the UK.* Working Paper. Coventry: School of Law, University of Warwick. Legal Studies Research Paper (Unpublished).

Anderson, R., Barton, C., Bohme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T. & Savage, S. (2012). Measuring the Cost of Cybercrimes. In R. Bohme (Ed.), *The Economics of Information Security and Privacy* (pp. 265 – 300). London: Springer Publishing.

Ariel, B., Farrar, W. & Sutherland, A. (2015). The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomised Controlled Trial. *Journal of Quantitative Criminology, 31,* 509 – 535.

Ariely, G. (2012). Globalisation and the Decline of National Identity? An Exploration Across Sixty-Three Countries. *Nations and Nationalism, 18*(3), 461 – 482.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F. (2015). *2020 Cybercrime Economic Costs: No Measure No Solution.* Paper presented at 10th International Conference on Availability, Reliability and Security (pp. 701 – 710).

Ashenden, S. (2002). Policing Perversion: The Contemporary Governance of Paedophillia. *Cultural Values, 6*(1), 197 – 222.

Banks, J. (2011). European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation. *European Journal of Crime, 19,* 1 – 13.

Barford, V. (2013, 19th September). Who are Vigilante Group Letzgo Hunting? *BBC News*. Retrieved from http://www.bbc.co.uk/news/magazine-24143991

Bassiouni, M. (2006). The History of Universal Jurisdiction and Its Place in International Law. In S. Macedo (Ed.), *Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes Under International Law* (pp. 39 – 64). Pennsylvania: University of Pennsylvania Press.

Bayley, D. & Shearing, C. (1996). The Future of Policing. *Law and Society Review, 30*(3), 585 – 606.

Bayley, D. & Shearing, C. (2001). *The New Structure of Policing.* Washington DC: The National Institute of Justice.

Berners-Lee, T. (1989). *Information Management: A Proposal.* CERN Report. Retrieved from http://faculty.georgetown.edu/irvinem/theory/Berners-Lee-HTTP-proposal.pdf.

Berners-Lee, T., Hall, W., Hendler, J., O'Hara, K., Shadbolt, N. & Weitzner, D. (2006). A Framework for Web Science. *Foundations and Trends in Web Science, 1*(1), 1 – 30.

Blanton, S. & Kegley, C. (2016). *World Politics: Trend and Transformation.* Boston: Cengage Learning.

Bossler, A. & Holt, T. (2009). On-Line Activities, Guardianship and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology, 3*(1), 400 – 420.

Bossler, A. & Holt, T. (2012). Patrol Officers' Perceived Role in Responding to Cybercrime. *International Journal of Police Strategies & Management, 35*(1), 165 – 181.

Brenner, S. (2008). Cybercrime Jurisdiction. *Crime Law Social Change, 46,* 189 – 206.

Brenner, S. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State.* Oxford: Oxford University Press.

Brenner, S. (2010). Cybercrime: *Criminal Threats from Cyberspace.* Oxford: Praeger.

Brenner, S. (2013). Cybercrime: Re-thinking Crime Control Strategies. In Y. Jewkes (Ed.), *Crime Online* (pp. 12 – 29). Abingdon: Routledge.

Brenner, S. (2014). *Cyberthreats and the Decline of the Nation State*. Abingdon: Routledge.

Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014). Organisations and Cyber Crime: An analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology, 8*(1), 1 – 20.

Broll, R. (2016). Collaborative Responses to Cyberbullying: Preventing and Responding to Cyberbullying Through Nodes and Clusters. *International Journal of Research and Policy, 26*(7), 735 – 752.

Brown, C. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology, 9*(1), 55 – 119.

Brown, V., Clery, E. & Ferguson, C. (2011). *Estimating the Prevalence of Young People Absent from School Due to Bullying.* Retrieved from http://www.natcen.ac.uk/media/22457/estimating-prevalence-young-people.pdf

Bryant, R. & Kennedy, I. (2014). Investigating Digital Crime. In R. Bryant and S. Bryant (Eds.), *Policing Digital Crime* (pp. 123 – 147). Farnham: Ashgate Publishing Ltd.

Bryant, R. & Stephens, P. (2014). Policing Digital Crime: The International and Organisational Context. In R. Bryant and S. Bryant (Eds.), *Policing Digital Crime* (pp. 111 - 123). Farnham: Ashgate Publishing Ltd.

Bullock, K. & Tilley, N. (2009). Evidence-Based Policing and Crime Reduction. *Policing, 3*(4), 381 – 387.

Burford, S. & Park, S. (2014). The Impact of Mobile Tablet Devices on Human Information Behaviour, *Journal of Documentation, 70*(4), 622 – 639.

Campbell, E. (2016). Policing Paedophilia: Assembling Bodies, Spaces and Things. *Crime Media Culture, 12*(3), 345 – 365.

Capeller, W. (2001). Not Such a Neat Net: Some Comments on Virtual Criminality. *Social and Legal Studies, 10,* 229 – 242.

Carr, M. (2016). Crossed Wires: International Co-Operation on Cyber Security. *Journal of International Affairs, 2,* 2 – 14.

Carroll, R. (2013, 4th November). California Police Use of Body Cameras Cuts Violence and Complaints, *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/nov/04/california-police-body-cameras-cuts-violence-complaints-rialto

Castells, M. (2009). *The Rise of the Networked Society* (2nd ed.). London: Wiley-Blackwell.

Chong, M. (2007). The Role of Internal Communication and Training in Infusing Corporate Values and Delivering Brand Promise: Singapore Airlines' Experience.

Corporate Reputation Review, 10(3), 201 – 212.

Clough, J. (2015a). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation, *Monash University Law Review, 40*(3), 698 – 736.

Clough, J. (2015b). *Principles of Cybercrime* (2nd ed). Cambridge: Cambridge University Press.

Cockcroft, T. & Beattie, I. (2009). Shifting Cultures: Managerialism and the Rise of Performance. *Policing: An International Journal of Police Strategies & Management, 32*(3), 526 – 540.

Cohen, S. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588 – 608.

Cohen, S. (1985). *Visions of Social Control: Crime, Punishment and Classification.* Cambridge: Blackwell Publishers.

College of Policing. (2013). *Leadership and Standards in the Police: House of Commons, Home Affairs Committee, Monday 1st July 2013: College of Policing Response.* Retrieved from http://www.college.police.uk/About/Documents/College_response_HAC_1310.pdf

College of Policing. (2015). *College of Policing Analysis: Estimating Demand on the Police Service.* Retrieved from http://www.college.police.uk/Documents/Demand_Report_21_1_15.pdf

College of Policing. (2017). *Crime Reduction Toolkit.* Retrieved from http://whatworks.college.police.uk/toolkit/Pages/Toolkit.aspx

Conway, Z. (2014, 3rd October). Police 'Overwhelmed' by Number of Child Abuse Images. *BBC News*. Retrieved from http://www.bbc.co.uk/news/uk-29470001

Council of Europe. (2001). *Convention on Cybercrime.* Retrieved from http://www.refworld.org/docid/47fdfb202.html

Critchley, T. (1978). *A History of the Police in England and Wales* (2nd ed.). London: Constable Publishing.

Darlington, Y., Feeney, J. & Rixon, K. (2005). Interagency Collaboration Between Child Protection and Mental Health Services: Practices, Attitudes and Barriers. *Child Abuse & Neglect, 29,* 1085 – 1098.

Decker, C. (2008). Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime. *Southern California Law Review, 81,* 959 – 1016.

Detica. (2011). *The Cost of Cyber Crime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.* London: Cabinet Office.

Ditch the Label. (2016). *The Annual Bullying Survey 2016.* Retrieved from http://www.ditchthelabel.org/wp-content/uploads/2016/04/Annual-Bullying-Survey-2016-Digital.pdf

Dubord, P. (2008). Investigating Cybercrime. In J. Barbara (Ed.), *Handbook of Digital and Multimedia Forensic Evidence* (pp. 77 – 89). New Jersey: Humana Press Inc.

Dupont, B. (2004). Security in the Age of Networks, *Policing & Society, 14*(1), 76 – 91.

Dunn-Cavelty, M. (2012). The Militarisation of Cyberspace: Why Less May Be Better. In C. Czosseck, R. Ottis and K. Ziolkowski (Eds), *Proceedings of the 4th International Conference on Cyber Conflict* (pp. 141 – 153). Tallinn: NATO CCD COE Publications.

Emsley, C. (2011). The Birth and Development of the Police. In T. Newburn (Ed.), *Handbook of Policing* (2nd ed.) (pp. 72 – 89). London: Routledge.

Emsley, C. (2014). *The English Police: A Political and Social History* (2nd ed.). London: Routledge.

Engel, G. (1977). The Need for a New Medical Model: A Challenge for Biomedicine. *Science, 196*(4286), 129 – 136.

Epstein, R. & Hundert, E. (2002). Defining and Assessing Professional Competence, *JAMA, 287*(2), 226 – 235.

Ericson, R. (1994). The Division of Expert Knowledge in Policing and Security. *British Journal of Sociology, 45*(2), 149 – 175.

Europol. (2014). *The Internet Organised Crime Threat Assessment* (iOCTA). The Hague: Europol.

Ferrell, J., Hayward, K. & Young, J. (2015). *Cultural Criminology* (2nd ed.). London: Sage.

Finkelhor, D. (2014). *Trends in Bullying and Peer Victimisation.* Crimes Against Children Research Centre. Retrieved from http://www.unh.edu/ccrc/pdf/CV280_Bullying%20%20Peer%20Victimization%20Bulletin_8-25-14.pdf

Flannery, K. & Graham, J. (2014). *Police Force Collaboration: An Independent Review of the Warwickshire and West Mercia Strategic Alliance.* Retrieved from http://www.policefoundation.org.uk/uploads/holding/projects/police_force_collaboration.pdf

Forst, B. (1993). Socio-economics, Crime, and Justice. In B. Forst (Ed.), *The Socio-Economics of Crime and Justice* (pp. 3 – 19). Abingdon: Routledge.

Friedman, T. (2005). *The World is Flat: A Brief History of the Twenty First Century.* New York: Douglas & McIntyre.

Froomkin, A. (2013). ICANN and the Domain Name System After the Affirmation of Commitments. In I. Brown (Ed.), *Research Handbook on Governance of the Internet* (pp. 27 – 52). Cheltenham: Edward Elgar Publishing Ltd.

Furedi, F. (2008). Fear and Security: A Vulnerability-Led Policy Response. *Social Policy & Administration, 42,* 645 – 661.

Furnell, S. (2002). *Cybercrime: Vandalising the Information Society.* London: Addison Wesley.

Gamble, J. (2014). *Time to Turn the Tables on Child Sex Offenders.* Retrieved from https://ineqe.com/2014/11/13/time-to-turn-the-tables-on-child-sex-offenders/

Gandy, O. (2009). *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage.* Farnham: Ashgate Publishing.

Gelvanovska, N., Rogy, M. & Rossotto, C. (2014). *Broadband Networks in the Middle East and North Africa: Accelerating High-Speed Internet Access.* Washington: The World Bank.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace.* Florida: Taylor and Francis Group.

Gillespie, A. (2015). *Cybercrime: Key Issues and Debates.* London: Routledge.

Gillespie, A. & Weare, S. (2015). *The English Legal System* (5th ed.). Oxford: Oxford University Press.

Goldberg, A. (2015, 8th November). Child Abuse Cases Delayed by Police

Backlog. *BBC News.* Retrieved from http://www.bbc.co.uk/news/uk-34713745

Goodman, M. (2010). International Dimensions of Cybercrime. In S. Ghosh and E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis* (pp. 311 – 339). Heidelberg: Springer Publishing.

Gordon, S. & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology, 2*(1), 13 – 20.

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies, 10*(2), 243 – 249.

Harvey, D. (1989). *The Condition of Postmodernity.* Oxford: Blackwell.

Heaton, R. & Tong, S. (2016). Evidence-Based Policing: From Effectiveness to Cost-Effectiveness. *Policing, 10*(1), 60 – 70.

Heng, Y. (2002). Unravelling the War on Terrorism: A Risk Management Exercise in War Clothing? *Security Dialogue, 33*(2), 227 – 242.

Her Majesties Inspectorate of Constabulary (HMIC). (2014a). *Crime Inspection 2014: Sussex Police.* London: HM Stationary Office.

Her Majesties Inspectorate of Constabulary (HMIC). (2014b). *Regional Organised Crime Units: A Review of Capability and Effectiveness.* London: HM Stationary Office.

Her Majesties Inspectorate of Constabulary (HMIC). (2015). *Real Lives, Real Crimes: A Study of Digital Crime and Policing.* London: HM Stationary Office.

Hinduja, S. & Patchin, J. (2008). Cyberbullying: An Explanatory Analysis of Factors Related to Offending and Victimisation. *Deviant Behaviour, 29*(2), 129 – 156.

HM Government. (2011). *National Cyber Security Strategy 2011 – 2016.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

HM Government. (2013). *Serious and Organised Crime Strategy.* London: HM Stationary Office.

HM Government. (2015). *Home Secretary's Speech at the Serious Organised Crime Exchange.* Retrieved from https://www.gov.uk/government/speeches/home-secretarys-speech-at-the-serious-organised-crime-exchange

HM Government. (2016). *National Cyber Security Strategy 2016 – 2021.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hodgson, J. (2010). The Future of Adversarial Criminal Justice in 21st Century Britain. *North Carolina Journal of International Law and Commercial Regulation, 35,* 319 – 362.

Holdaway, S. (2017). The Re-Professionalisation of the Police in England and Wales. *Criminology & Criminal Justice,* 1 – 17.

Holley, C. & Shearing, C. (2017). A Nodal Perspective of Governance: Advances in Nodal Governance Thinking. In P. Drahos (Ed.), *Regulatory Theory: Foundations and Applications* (pp. 163 – 180). Canberra: ANU Press.

Holloway, D., Green, L. & Livingstone, S. (2013). *Zero to Eight: Young Children and Their Internet Use.* London: EU Kids Online.

Holt, T. & Bossler, A. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behaviour, 35*(1), 20 – 40.

Home Affairs Select Committee. (2016). *College of Policing: Three Years On: Fourth Report of Session 2016 – 2017.* London: HM Stationary Office.

Hooper, M. (2014). Acknowledging the Existence of a Fourth Era of Policing: The Information Era. *Journal of Forensic Research and Crime Studies, 1,* 1 – 4.

Hope, T. (2009). The Illusion of Control: A Response to Professor Sherman. *Criminology & Criminal Justice, 9*(2), 125 – 134.

House of Commons. (2015). *Draft Investigatory Powers Bill.* Briefing Paper Number 7371, 19 November 2015. London: HM Stationary Office.

Houses of Parliament. (2016). *Parliamentary Office of Science and Technology Postnote Number 520 March 2016: Digital Forensics and Crime.* London: HM Stationary Office.

Huey, L., Nhan, J. & Broll, R. (2012). 'Uppity Civilians' and 'Cyber Vigilantes': The Role of the General Public in Policing Cyber-Crime. *Criminology & Criminal Justice, 13*(1), 81 – 97.

Hurwitz, R. (2014). The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests, 36,* 322 – 331.

Hutchings, A. (2014). Crime from the Keyboard: Organised Cybercrime, Co-offending, Initiation and Knowledge Transmission. *Crime, Law and Social Change, 62(*1), 1 – 20.

Institute of Directors. (2016). *Cyber Security: Underpinning the Digital Economy*. IOD Policy Report, March 2016. Retrieved from https://www.iod.com/Portals/0/PDFs/Campaigns%20and%20Reports/Digital%20and%20Technology/Cyber%20Security%20-Underpinning%20the%20digital%20economy.pdf?ver=2016-09-13-171033-407

International Business Times (IBT). (2011, 3rd October). E-Crime Unit Saves UK Economy £140 Million in 6 Months. *International Business Times*. Retrieved from http://www.ibtimes.co.uk/economy-met-pceu-save-crime-harm-reduction-online-223674

Investigatory Powers Act. (2016). Retrieved from http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm

Jenkins, V. & Fallowfield, L. (2002). Can Communication Skills Training Alter Physicians Beliefs and Behaviour in Clinics? *Journal of Clinical Oncology, 20(*3), 765 – 769.

Jewkes, Y. (2013). Public Policing and Internet Crime. In M. Yar and Y. Jewkes (Eds.), *Handbook of Internet Crime* (pp. 525 – 546). Abingdon: Routledge.

Jewkes, Y. & Andrews, C. (2013). Internet Child Pornography: International Responses. In Y. Jewkes (Ed), *Crime Online* (pp. 60 – 81). Abingdon: Routledge.

Johnston, L. & Shearing, C. (2003). *Governing Security: Explanations in Policing and Justice.* London: Routledge.

Jones, S. (2009, 4th February). MySpace Removes 90,000 Sex Offenders. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2009/feb/04/myspace-social-networking-sex-offenders

Jones, T. & Newburn, T. (2002). The Transformation of Policing? Understanding Current Trends in Policing Systems. *British Journal of Criminology, 42*(1), 129 – 146.

Kellerman, A. (2010). Mobile Broadband Services and the Availability of Instant Access to Cyberspace. *Environmental Planning, 42,* 2990 – 3005.

Kelling, G. & Moore, M. (2005). The Evolving Strategy of Policing. In T. Newburn (Ed.), *Policing: Key Readings* (pp. 88 – 108). London: Routledge.

Kirby S. & Penna, S. (2011). Policing Mobile Criminality: Implications for Police Forces in the UK. *International Journal of Police Strategies & Management, 34*(2), 182 – 197.

Kleemans, E. (2014). Organised Crime Research: Challenging Assumptions and Informing Policy. In J. Knutsson and E. Cockbain (Eds.), *Applied Police Research: Challenges and Opportunities* (pp. 57 – 68). Abingdon: Routledge.

Kosseff, J. (2016). The Hazards of Cyber-Vigilantism. *Computer Law & Security Review, 32*(4), 642 – 649.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* London: Springer Publishing.

Lagazio, M., Sherif, N. & Cushman, M. (2014). A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector. *Computers & Security,* 1 – 32.

Lander, I. (2013). Obstacles for Changes Within the (Swedish) Police Force: Professional Motivations, Homosociality, and Ordering Practices. *Journal of Scandinavian Studies in Criminology and Crime, 14*(1), 43 – 61.

Lavorgna, A. & Sergi, A. (2016). Serious, Therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom. *International Journal of Cyber Criminology, 10(*2), 170 – 187.

Lea, J. (2015). From the Criminalisation of War to the Militarisation of Crime Control. In S. Walklate and R. McGarry (Eds.), *Criminology and War: Transgressing the Borders* (pp. 198 – 212). Abingdon: Routledge.

Leukfeldt, E., Veenstra, S. & Stol, W. (2013). High Volume Cyber Crime and the Organisation of the Police: The Results of Two Empirical Studies in the Netherlands. *International Journal of Cybercriminology, 7*(1), 1 – 17.

Luekfeldt, E. & Yar, M. (2014). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behaviour, 37*(3), 263 – 280.

Leukfeldt, E., Lavorgna, A. & Kleemans, E. (2016). Organised Cybercrime or Cybercrime That is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research,* 1 – 20.

Levi, M. (2012a). Measuring the Cost of Cybercrimes. *Cybercrime and Policy Issues, 90,* 12 – 13.

Levi, M. (2012b). Trends and Costs of Fraud. In A. Doig (Ed.), *Fraud: The*

Counter Fraud Practitioner's Handbook (pp. 7 – 19). Abingdon: Routledge.

Levi, M. & Williams, M. (2013). Multi-Agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Co-operation Space. *Information Management & Computer Security, 21*(5), 420 – 443.

Levitt, S. (2004). Understanding Why Crime Fell in the 1990s: Four Factors That Explain the Decline and Six That Do Not. *Journal of Economic Perspectives, 18*(1), 163 – 190.

Livingstone, S. & Smith, P. (2014). Annual Research Review: Harms Experienced by Child Users of Online and Mobile Technologies: The Nature, Prevalence and Management of Sexual and Aggressive Risks in the Digital Age. *Journal of Child Psychology and Psychiatry, 55*(6), 635 – 654.

Loader, I. (2000). Plural Policing and Democratic Governance. *Social & Legal Studies, 9*(3), 323 – 345.

Loftus, B. (2012). Covert Surveillance and the Invisibilities of Policing. *Criminology & Covert Policing, 12*(3), 275 – 288.

Lorenzo, A. (1998). A Framework for Fundamental Change: Context, Criteria and Culture. *Journal of Research and Practice, 22*(4), 335 – 348.

Luscombe, A. & Walby, K. (2014). High Policing and Access to Information. *Journal of Police Practice and Research, 16*(6), 485 – 498.

Lusthaus, J. (2012). Trust in the World of Cybercrime. *Global Crime, 13*(2), 71 – 94.

Lusthaus, J. (2013). How Organised is Organised Cybercrime? *Global Crime, 14*(1), 52 – 60.

MacAskill, E. (2016, 19th November). Extreme Surveillance Becomes UK Law with Barely a Whimper. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

Madge, N. & Barker, J. (2007). *Risk & Childhood.* London: The Royal Society for the Encouragement of Arts, Manufactures & Commerce.

Manky, D. (2013). Cybercrime as a Service: A Very Modern Business. *Computer Fraud & Security, 6,* 9 – 13.

Manning, P. (2007). A Dialectic of Organisational and Occupational Culture. In M. O'Neill, M. Marks and A. Singh (Eds.), *Police Occupational Culture: New*

Debates and Directions (pp. 47 – 85). Oxford: JAI Press.

Marcum, C., Higgins, G., Freiburger, T. & Ricketts, M. (2010). Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime. *International Journal of Police Science & Management, 12,* 516 – 525.

Marion, N. (2010). The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation. *International Journal of Cyber Criminology, 4*(1), 699 – 712.

Maughan, B., Collishaw, S., Meltzer, H. & Goodman, R. (2008). Recent Trends in UK Child and Adolescent Mental Health. *Social Psychiatry and Psychiatric Epidemiology, 43,* 305 – 310.

McBarnet, D. (1979). Arrest: The Legal Context of British Policing. In S. Holdaway (Ed.), *The British Police* (pp. 24 – 40). London: Arnold.

McGuire, M. & Dowling, S. (2013). *Cybercrime: A Review of the Evidence, Research Report 75.* London: HMSO.

McInerney, S. (2015). Introducing the Biopsychosocial Model for Good Medicine and Good Doctors, *British Medical Journal*, 324:1533.

Misra, S., Cheng, L., Genevie, J. & Yuan, M. (2014). The iPhone Effect: The Quality of In-Person Social Interactions in the Presence of Mobile Devices, *Environment & Behaviour, 48*(2), 275 – 298.

Morbin, T. (2014, 1st November). Cybercrime: The New Normal. *SC Magazine*. Retrieved from https://www.scmagazineuk.com/cybercrime-the-new-normal/article/541540/

National Crime Agency (NCA). (2014). *National Strategic Assessment of Serious and Organised Crime 2014.* Retrieved from http://www.nationalcrimeagency.gov.uk/publications/207-nca-strategic-assessment-of-serious-and-organised-crime/file

National Crime Agency (NCA). (2015a). *A Co-Ordinated Response to Cyber Crime: March 2015.* Retrieved from http://www.nationalcrimeagency.gov.uk/publications/528-a-coordinated-response-to-cyber-crime-march-2015/file

National Crime Agency (NCA). (2015b). *National Crime Agency Annual Reports and Accounts 2015 – 16.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/583545/NCA_Annual_Report_and_Accounts_2015-16__web_.pdf

National Crime Agency (NCA). (2015c). *NCA Strategic Cyber Industry Group: Cyber Crime Assessment 2016.* Retrieved from http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

National Cyber Crime Unit (NCCU). (2017). *About the National Cyber Crime Unit.* Retrieved from http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

National Police Chiefs Council (NPCC). (2015). *Digital Investigation and Intelligence: Policing Capabilities for a Digital Age.* Retrieved from http://www.npcc.police.uk/documents/reports/Digital%20Investigation%20and%20Intelligence%20Policing%20capabilities%20for%20a%20digital%20age%20April%202015.pdf

Newman, G. & Clarke, R. (2003). *Superhighway Robbery: Preventing E-Commerce Crime.* Cullompton: Willan Press.

Nhan, J., Huey, L. & Broll, R. (2017). Digiantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings. *British Journal of Criminology, 57,* 341 – 361.

Office of National Statistics (ONS). (2015). *Crime in England and Wales: Year Ending June 2015.* Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/2015-10-15

Office for National Statistics (ONS). (2016a). *Statistical Bulletin: Internet Access – Households and Individuals 2016.* Retrieved from http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016#activities-completed-on-the-internet

Office of National Statistics (ONS). (2016b). *Offences Recorded by the Police in England and Wales by Offence and Police Force Area from 1990 – 2001/02.* Retrieved from https://www.gov.uk/government/statistics/historical-crime-data

Office for National Statistics (ONS). (2016c). *Research Outputs: Developing a Crime Severity Score for England and Wales Using Data on Crimes Recorded by the Police.* Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/researchoutputsdevelopingacrimeseverityscoreforenglandandwalesusingdataoncrimesrecordedbythepolice/2016-11-29#annex-1-proportional-composition-of-unweighted-offence-rate-and-crime-severity-score

Office for National Statistics (ONS). (2017). *Crime in England and Wales: Year Ending September 2016.* Retrieved from https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingsept2016

Oliver, W. (2006). The Fourth Era of Policing: Homeland Security. *International Review of Law, Computers and Technology, 20*(1), 49 – 62.

O'Malley, P. & Palmer, D. (1996). Post-Keynesian Policing. *Economy and Society, 25*(2), 137 – 155.

Paganini, P. (2015, 11th November). GCHQ and NCA Hunting Criminals in the Dark Web. *Security Affairs.* Retrieved from http://securityaffairs.co/wordpress/41883/cyber-crime/gchq-nca-joc.html

Pick, J. & Sarkar, A. (2015). *The Global Digital Divides: Explaining Change.* London: Springer.

Putman, T. & Elliott, D. (2001). International Responses to Cyber Crime. In S. Goodman and A. Sofaer (Eds.), *The Transnational Dimension of Cyber Crime and Terrorism* (pp. 35 – 69). Stanford: Hoover Institution Press.

Pyrooz, D., Decker, S. & Moule, R. (2013). Criminal and Routine Activities in Online Settings: Gangs, Offenders and the Internet. *Justice Quarterly, 32*(3), 471 – 499.

Rashid, Z., Sambasivan, M. & Johari, J. (2003). The Influence of Corporate Culture and Organisational Commitment on Performance. *Journal of Management Development, 22*(8), 708 – 728.

Ratcliffe, J. (2016). *Intelligence Led-Policing* (2nd ed.). London: Routledge.

Reiner, R. (2000). *The Politics of the Police* (3rd ed.). Oxford: Oxford University Press.

Reiner, R. (2010). *The Politics of the Police* (4th ed.). Oxford: Oxford University Press.

Rhaman, M., Khan, M., Mohammad, N. & Rhaman, M. (2009). Cyberspace Claiming New Dynamism in the Jurisprudential Philosophy: A Substantive Analysis of Conceptual and Institutional Innovation. *International Journal of Law and Management, 51*(5), 274 – 290.

Rosenbaum, D. (2010). Police Research: Merging the Policy and Action Research Traditions. *Police Practice & Research, 11*(2), 144 – 149.

Rosenfeld, R. & Fornango, R. (2007). The Impact of Economic Conditions on Robbery and Property Crime: The Role of Consumer Sentiment. *Criminology, 45*(4), 735 – 769.

Ryder, N. (2011). *Financial Crime in the 21st Century: Law and Policy.* Cheltenham: Edward Elgar Publishing Ltd.

Sawer, P. (2017, 28th February). Police Chief Calls for Paedophiles Who View Child Abuse Images to be Spared Prosecution as Officers 'Can't Cope' With Volume of Reports. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/2017/02/28/police-chief-calls-low-risk-paedophiles-spared-jail-officers/

Schafer, B. (2016). Surveillance for the Masses: The Political and Legal Landscape of the UK Investigatory Powers Bill. *Datenschutz und Datensicherheit, 40*(9), 592 – 597.

Scott, D. (1997). Inter-Agency Conflict: An Ethnographic Study. *Child and Family Social Work, 2,* 73 – 80.

Sergi, A. (2015). Divergent Mind-Sets, Convergent Policies: Policing Models Against Organised Crime in Italy and in England Within International Frameworks. *European Journal of Criminology, 12*(6), 658 – 680.

Shearing, C. & Ericson, R. (1991). Culture as Figurative Action. *British Journal of Sociology, 42*(4), 481 – 506.

Shearing, C. & Johnston, L. (2010). Nodal Wars and Network Fallacies: A Genealogical Analysis of Global Insecurities. *Theoretical Criminology, 14*(4), 495 – 514.

Sheptycki, J. (2007). Transnational Crime and Transnational Policing. *Sociology Compass, 1*(2), 485 – 498.

Sherman, L. (2013). The Rise of Evidence Based Policing: Targeting, Testing and Tracking. *Crime and Justice, 42*(1), 377 – 451.

Sherman, L. (2015). A Tipping Point for ''Totally Evidenced Policing'': Ten Ideas for Building an Evidence-Based Police Agency. *International Criminal Justice Review, 25*(1) 11-29.

Sherman, L., Neyroud, P. & Neyroud, E. (2016). The Cambridge Crime Harm Index: Measuring Total Harm from Crime Based on Sentencing Guidelines, *Policing, 10*(3) 171–183.

Shields, R. (1996). *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies.* London: Sage.

Sklansky, D. (2007). Seeing Blue: Police Reform, Occupational Culture, and Cognitive Burn-In. In M. O'Neill, M. Marks and A. Singh (Eds.), *Police Occupational Culture: New Debates and Directions* (pp. 19 – 47). Oxford: JAI Press.

Slaughter, A. (2006). Defining the Limits: Universal Jurisdiction and National Courts. In S. Macedo (Ed.), *Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes Under International Law* (pp. 168 – 193). Pennsylvania: University of Pennsylvania Press.

Song, J. (2015). Pirates and Torturers: Universal Jurisdiction as Enforcement Gap-Filling. *The Journal of Political Philosophy, 23*(4), 471 – 490.

Sparrow, M. (2014). *Managing the Boundary Between Public and Private Policing.* Retrieved from https://www.ncjrs.gov/pdffiles1/nij/247182.pdf

Stenning, P. & Shearing, C. (2015). Privatisation, Pluralisation and the Globalisation of Policing. *Research Focus, 3*(1), 1 – 8.

Stretesky, P. & Lynch, M. (2004). The Relationship Between Lead and Crime. *Journal of Health and Social Behaviour, 45,* 214 – 229.

Sussman, V. (1995, 23rd January). Policing Cyberspace. *U.S. News & World Report,* 54 – 61.

Swire, P. (2005). Elephants and Mice Revisited: Law and Choice of Law on the Internet. *University of Pennsylvania Law Review, 153*(6), 1975 – 2001.

Takizawa, R., Maughan, B. & Arseneault, L. (2014). Adult Health Outcomes of Childhood Bullying Victimisation: Evidence from a 5-Decade Longitudinal British Cohort. *American Journal of Psychiatry, 171*(7), 777 – 784.

Tan, L. (2012). Museums and Cultural Memory in an Age of Networks. *International Journal of Cultural Studies, 16*(4), 383 – 399.

Taylor, D. (1997). *The New Police in Nineteenth-Century England: Crime, Conflict and Control.* Manchester: Manchester University Press.

Taylor, D. (2005). Beyond the Bounds of Respectable Society: The "Dangerous Classes" in Victorian and Edwardian England. In J. Rowbotham and K. Stevenson (Eds.). *Criminal Conversations: Victorian Crimes, Social Panic and Moral Outrage* (pp. 3 – 22). Ohio: Ohio State University Press.

Taylor, M. & Quayle, E. (2003). *Child Pornography: An Internet Crime.* London: Routledge.

Taylor, R., Caeti, T., Loper, D., Fritsch, E. & Liederbach, J. (2006). *Digital Crime and Digital Terrorism.* New Jersey: Pearson Prentice Hall.

Tehrani, P. & Manap, N. (2013). A Rational Jurisdiction for Cyber Terrorism. *Computer Law & Security Review, 29,* 689 – 701.

Tetzlaff-Bemiller, M. (2011). Undercover Online: An Extension of Traditional Policing in the United States. *International Journal of Cyber Criminology, 5(*2), 813 – 824.

The Economist. (2016). Trump's World: The New Nationalism. *The Economist*. Retrieved from http://www.economist.com/news/leaders/21710249-his-call-put-america-first-donald-trump-latest-recruit-dangerous

Thomas, G. (2014). Research on Policing: Insights From Literature. *Police Journal: Theory, Practice and Principles, 87,* 5 – 16.

Thomas, T. (2016). *Policing Sexual Offences and Sex Offenders.* London: Palgrave MacMillan.

Tokunaga, R. (2010). Following You Home From School: A Critical Review and Synthesis of Research on Cyber Bullying Victimisation. *Computers in Human Behaviour, 26*(3), 277 – 287.

Trottier, D. (2016). Digital Vigilantism as Weaponisation of Visibility. *Philosophy & Technology*, DOI 10.1007/s13347-016-0216-4

UK Parliament Joint Committee. (2016). *Joint Committee on the Draft Investigatory Powers Bill: Written Evidence.* Retrieved from https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf

Unicef. (2011). *Child Safety Online: Global Challenges and Strategies.* Retrieved from https://www.unicef-irc.org/publications/pdf/ict_eng.pdf

Viano, E. (2016). Cybercrime: Definition, Typology and Criminalisation. In E. Viano (Ed.), *Cybercrime, Organised Crime, and Societal Responses: International Approaches* (pp. 3 – 23). Washington: Springer Publishing.

Walden, I. (2004). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice, 12*(4), 321 – 336.

Wall, D. (2007). Policing Cybercrimes: Situating the Public Police in Networks of

Security Within Cyberspace. *Police Practice & Research, 8*(2), 183 – 205.

Walters, R. (2016). *Cyber Attacks on U.S. Companies in 2016.* Retrieved from http://thf-reports.s3.amazonaws.com/2016/IB4636.pdf

West Midlands Police. (2017). *WMP Cyber Crime Presentation.* Retrieved from http://www.westmidlands-pcc.gov.uk/media/411906/WMP-Cyber-crime-presentation-18116.pptx

White, P. (2015). *Through the Looking Glass: Emerging Understandings of Cybercrime in GMP.* Retrieved from http://library.college.police.uk/docs/WHITE-through-the-looking-glass-2015.pdf

Wilkinson, S. (2010). Research and Policing – Looking to the Future. *Policing: A Journal of Policy and Practice, 4(*2), 146 – 148.

Williams, C. (2011). Police Governance: Community, Policing and Justice in the Modern UK. *Taiwan in Comparative Perspective, 3,* 50 – 65.

Williams, K. (2011). Transnational Developments in Internet Law. In Y. Jewkes and M. Yar (Eds.), *Handbook of Internet Crime* (pp. 466 – 492). Abingdon: Routledge.

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407 – 427.

Yar, M. (2013). The Policing of Internet Sex Offences: Pluralised Governance Versus Hierarches of Standing. *Policing and Society*, *23*(4), 482 – 497.

Zook, M. (2008). *The Geography of the Internet Industry: Venture Capital, Dot Coms and Local Knowledge.* Oxford: Blackwell Publishing.