Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policing

David S. Wall

The Oxford Handbook of Law, Regulation and Technology
Edited by Roger Brownsword, Eloise Scotford, and Karen Yeung

Print Publication Date: Jul 2017
Subject: Law, IT and Communications Law, Crime and Criminology, Criminal Law
Online Publication Date: Feb 2017 DOI: 10.1093/oxfordhb/9780199680832.013.65

Abstract and Keywords

Networked digital technologies have transformed crime to a point that 'cybercrime' is here to stay. In the future, society will be forced to respond to a broad variety of networked crimes that will increase both the complexity of crime investigation and prevention, whilst also deepening the regulative challenges. As cybercrime has become an inescapable feature of the Internet landscape, constructive management and system development to mitigate cybercrime threats and harms are imperatives. This chapter explores the changing cybersecurity threat landscape and its implications for regulation and policing. It considers how networked and digital technologies have affected society and crime; it identifies how the cybersecurity threat and crime landscape have changed and considers how digital technologies affect our ability to regulate them. It also suggests how we might understand cybercrime before outlining both the technological developments that will drive future cybercrime and also the consequences of failing to respond to those changes.

Keywords: cybercrime, Internet crimes, policing cybercrimes, information communications technologies, hacking, data theft

1. Introduction

CONTEMPORARY media headlines about cybercrime boldly suggest that we are still coming to terms with the Internet a quarter of a century or so on from its introduction.[1] Yet, we have actually come far since those early years, at least in terms of understanding the Internet's ill effects and how to respond to them. During the Internet's early years many apocalyptic predictions were made about cybercrime (p. 1076) without any real evidence of it actually happening on the scales predicted (Wall 2008). We knew, for example, all about cybercrime long before we had really experienced any and our understanding of

the issues were largely shaped by, what were effectively, the equivalent of 'weather reports from umbrella salesmen' (Wall 2008: 53). In other words, without any contemporary counterfactual information, the emerging cybersecurity industry and others used fear as a marketing tool to increase sales of their products, which raises important epistemological questions about how we understand the reality, or realities, of cybercrime. We will return to this question later.

In terms of predicted threats, the jury is still out on Y2K and contemporary security concerns (Bilton 2009) and whether or not the many billions of dollars, pounds, euros or roubles spent on preventative measures was a wise investment, or just an over-reaction to an unknown risk. What is certain is that some of those early predictions about the invasiveness and impact of cybercrime are now being realized and have become part of our everyday reality. As the Internet continues to permeate almost every aspect of our everyday life, so the opportunities for cybercrime grow, often mimicking developments in online e-commerce. But the impacts of online activity often appear contradictory and sometimes unexpected; for example, the scale of the impact of social network media was not anticipated a decade ago and nor were its good or bad consequences. Social Network Media evils, such as sexting, bullying, and the resultant suicides, deceptions and so on, are well reported, but headlines trumpeting the Internet's contribution to the positive well-being of millions of people or its 'civilising' effect are largely absent from the news.[2] Knowing about cybercrime is one thing, but responding constructively to that knowledge is another.

As the growth of criminal opportunities relating to digital and networked technologies continues, then so do the regulatory challenges for law, industry, police, and the courts. One of those challenges lies in managing public expectations of security to keep them in line with the levels of protection that police and government can realistically deliver. The ability of police and government to manage those expectations is important because the police, as upholders of law and gatekeepers to the justice system not only have to respond to reported victimizations, but how they do so is also increasingly important. This is because the politics of policing cybercrime is almost as important as the policing process itself. Furthermore, not only are policing agencies having to respond to public demands to act, but very often the laws they use are either outdated, mis-applied, or not yet formed—see, for example, the three case studies mentioned later in this chapter. Case studies which highlight that Police agencies cannot respond to cybercrimes alone and it is arguable that they should not do so where the solution or resolution cuts across criminal justice and other agencies. Yet a potential paradox emerges whereby on the one hand it could be counter-productive to involve the police as the sole agency involved in dealing with some of the more minor types of cybercrimes because they lack (p. 1077) financial and human resources to deal with the increased volume of crime. Yet, not involving the police would leave judges out of the equation with a detrimental effect on interpretations of the common law developments relating to cybercrime. This is because police decisions over what to investigate are increasingly important factors in the subsequent decisions over whether to prosecute or not and filter what goes before the court. For these reasons, together with the need for transparency and oversight, police agencies must develop col-

laborative models with other key stakeholders, such as the financial industries and telecommunications service providers. Such models are not only counterintuitive to traditional police organizational cultures (see Reiner 2010), but they will have to go way beyond being merely collaborative. Any new partnerships will have to be co-productional in order to create a USP (unique selling point) in terms of new intelligent security products and norms.

This reflective essay draws upon 20 years of experience (from Wall 1997 onwards) in researching and commentating upon the developing area of crime and technology. It also encompasses recent research conducted for the RCUK Global Uncertainties programme[3] to consider how networked and digital communication technologies have changed, and are continuing to change,[4] the world in terms of crime and expectations of security. The chapter looks, firstly, at the impact of networked and digital technologies upon society and crime. The second section specifically examines how the cybersecurity threat and crime landscape have changed. The third section considers how digital technologies are affecting the ability to regulate them and the corresponding challenges for law and its enforcement. The next section explores what cybercrime is and how we understand it. Section five describes the technological developments that will likely impact upon the regulation of cybercrime over the next five to ten years, and section six reflects upon the consequences if we fail to respond to these changes. The final section concludes with some ideas about what needs to be done, and how.

2. How have Network and Digital Technologies Transformed Criminal Behaviour Online?

In three significant ways, digital and networked, technologies have brought about a fundamental transformation of social behaviour across the networks they create. They have caused it to become *global, informational*, and *distributed* (see further Castells 2000). The same technologies have also transformed criminal behaviour in much the same ways, although to achieve different ends (Wall 2007). (p. 1078) Firstly, network technologies not only globalize the communication of information, ideas, and desires, but they also impact locally by causing a ‘glocalizing’ effect—the global impact upon local policing services. For example, a new type of scam committed by offenders in one country upon victims in another will create the need to expand the capacity of their local police to deal with that crime—as was the case with pyramid scams committed by offenders in the UK upon victims in South America.[5] Secondly, network technologies create the potential for new types of asymmetric relationships where one offender can victimize many individuals across the planet at the same time. Thirdly, network technologies and associated social network media are creating new forms of networked and non-physical social relationships that act as the source of new criminal opportunities (Wall 2007; 2013). Such opportunities lead to emerging crimes such as stalking, grooming, bullying, fraud, sexting, and sextortion,[6] etc. —forms of offending that challenge law and its procedures. The upshot is that crime can now be simultaneously panoptic and synoptic in that a few offenders can not only victim-

lize the many, but the many can also victimize the few; especially in cases involving social network media crime. Cybercrime can be committed at a distance, much more quickly, and in much greater volume than offline crime and this 'cyber-lift' marks out the fundamental differences between the two.

New forms of criminal opportunity are being created that are also changing the way that crime is taking place. Criminal labour—because committing crime is a form of labour—is rapidly becoming deskilled and reskilled simultaneously by the networked and digital technologies (see arguments in Wall 2007: 42); in much the same way that everyday work has become rationalized via process a process of automating labour. In terms of criminal labour, one person can now control a complete crime process, such as a robbery which once required many people with a range of criminal skills. Furthermore, the entry level skills of cybercrime have fallen because crime technologies have become so automated that malware can now operate by itself, or be rented, or be bought off the shelf via crimeware-as-a-service (Sood and Enbody 2013; Wall 2015a). The 'technology' used has effectively 'disappeared' in that its operation is now intuitive and offenders no longer require the specialist programming skills they once did. Another significant development has been the drop in the cost of technologies, which has dramatically reduced the start-up costs of crime, thus increasing the level of incentive, especially with the advent of cloud technologies (see later).

Put in more simplistic terms, networked and digital technologies create an environment in which there is no need for criminals to commit a large crime at great risk to themselves anymore, because one person can now commit many small crimes with lesser risk to themselves. The modern day equivalent of the bank robber can, for example, contemplate committing 50m £1 low-risk thefts themselves from the comfort and safety of their own home, rather than commit a single £50m robbery with its complex collection of criminal skill sets and high levels of personal (p. 1079) risk (Wall 2007: 3, 70). The impact of these transformations upon crime is that the average person can, in theory, now commit many crimes simultaneously in ways not previously imagined possible, and on a global scale. If not a bank robbery, then they can commit a major hack, a DDOS (Distributed Denial of Service)[7] attack (De Villiers 2006), a hate speech campaign, or suite of frauds; see for example, the case of Lomas who scammed 10,000 victims out of £21m (BBC 2015a) or the 15-year-old TalkTalk hacker who (with others) allegedly hacked the TalkTalk database and stole personal information on 1.2 million customers (Wall 2015b; BBC 2015c). The fact that one or two people can now control whole criminal processes has profound implications for our understanding of the organization of cybercrime. In a rather cynical way, the Internet has effectively democratized crimes such as fraud that were once seen as the crimes of the powerful and the privileged. There is, however, an underlying and almost ideological (mis)assumption that a new Internet mafia is forming (Wall 2015a). As mentioned earlier, all crime is organized in one way or another, but all crime is not 'organized crime', so we need to briefly understand how cybercrime differs from other crimes, but firstly we need to look at the Cyberthreat landscape.

3. How has Network and Digital Technology Changed the Cyberthreat Landscape?

Two and a half decades since the birth of the Internet, it is clear that the cybersecurity threat landscape has changed considerably as networked technologies have progressively transformed the way that online crime is organized. These threats have been further escalated in recent years as cybercrime has become more professional (see, for example, the case of Stuxnet[8]) and stealthier via Rootkit[9] malware, such as Zeus[10] and the BEEBONE Botnet[11] (Robot networks) (Simmons 2015). In this post-script kiddie[12] world, the offenders no longer want to be known or even admired as they once did. Cybercrimes have also become more automated, for example, Ransomware[13] and Fake AV,[14] and larger, as recent distributed denial of service (DDOS) attacks illustrate. They have also become more complex with the maturing of social network media and the crime potential of Cloud technologies which increase computing power, storage space, and reduce overall costs.[15] Furthermore, these trends are compounded by emerging networked technologies that are currently being planned or in progress (see later). Before looking at how we can understand the many accounts of cybercrime, it is important to also look briefly at the (p. 1080) ways that the same technologies that create criminal opportunity can also assist police public service and criminal justice delivery.

3.1 Regulating and Policing: How are Technologies Helping?

The same technologies that are transforming crime are also transforming policing, which is the gateway to the criminal justice system – a factor often forgotten. Not only can these technologies help police investigate and catch criminals, but they can also help victims report their victimization and help police to respond to victims, especially if no further police action is to be taken. Or they enable victims to be referred to another agency, for example, the UK Action Fraud National reporting site which takes reports of economic and certain types of cybercrime.

In addition to the above, Social network media can not only help police and other agencies engage with the public to communicate outwards, but they can also help capture essential specialist community knowledge even encouraging community sleuthing in support of police. The same technologies also help increase police accountability to the public, the police profession itself, and also to law (Chan 2001: 139). Furthermore, new technologies are also assisting police forces to administer their organization more effectively and help individual officer’s process cases more efficiently, in greater volume and also at a distance—ironically, in much the same way that criminals commit crime. In so doing, new digital and network technologies increase individual worker accountability to police management whilst also helping to enforce the rules of the organization. The indications for the policing future is that networked technologies are causing individual UK police forces to think nationally by creating national policing norms, whilst remaining local. Yet, with a twist because there is also early evidence that policing models are developing that

are increasingly less dependent on the local police station system itself, than local online services. But, the rest of this chapter focuses upon cybercrime.

4. What is Cybercrime: How Can We Best Understand It?

The definition of cybercrime is highly contentious because everybody agrees that it exists, but not everybody agrees what it is, even after so many years (p. 1081) (Wall 2007; 2014). The following outline of cybercrime helps us understand how it is organized, but we must first separate the cybersecurity debates over risk and threats from the cybercrime debates over *actual* harms (to individuals, businesses, and nation states). These issues are often confused, yet not all threats and risks manifest themselves as harms and not all harms are crimes, but some do, so how do we make sense of them?

The 'transformation test' (Wall 2007) is one way of separating cybercrimes from non-cybercrimes. This is where the impact of networked technologies (earlier referred to as the 'Cyber-lift') is removed from the crime to see what would be left. This can be done either scientifically or metaphorically. But this process helps reflect upon how the crime was committed and the levels to which networked and digital technology have assisted the criminal behaviour. We can use this 'transformation test' to understand how crimes have been transformed in terms of their *mediation by technologies*. At one end of the spectrum is 'cyber-assisted' crime that uses the Internet in its organization and implementation, but which would still take place if the Internet was removed (e.g. murderers Googling for information about how to kill someone or dispose of the body). At the other end of the spectrum is 'cyber-dependent' crime, which exists *because* of the Internet, such as DDoS attacks or spamming.[16] If the Internet (networked technology) is taken away, then the crime simply disappears. In between the cyber-assisted and cyber-dependent crime is a range of hybrid 'cyber-enabled' crime. This range of cyber-enabled crimes includes most types of frauds (but not exclusively) and are existing crimes in law, previously committed locally but are given a global reach by the Internet, see for example, Ponzi frauds and pyramid selling scheme scams. If the Internet is taken away, these crimes still happen, but at a much more localized level and they lose the global, informational, and distributed lift that is characteristic of 'cyber' (see further Wall 2005).

Once the level of mediation by technology has been established then the *modus operandi* needs to be considered. We therefore need to distinguish between 'crimes *against* the machine', such as hacking and DDOS attacks, etc., which are very different from 'crimes *using* the machine', such as fraud, etc. Both also differ from 'crimes *in* the machine', such as extreme pornography, hate speech, and social networking-originated offences, and others. Yet, the distinction between them is rarely made in practice, even though the three types of *modus operandi* each relate to different bodies of law in most modern jurisdictions. Finally, the treatment of cybercrime also needs to be differentiated by victim group. Despite similarities in 'attack type', individual victimsations are different from organizational victimsations (including businesses), who in turn are different from nation state vic-

tims (national infrastructure) (see Wall 2005; 2014). Each involve different offender motivations and victimization tactics.

Each of these dimensions of cybercrime in terms of influence of technology, *modus operandi* and victim group have different implications for understanding the (p. 1082) nature of the victimization experience, but also differences in the types offenders and the way the cybercrimes are organized. The process of separating out the different organizing concepts of cybercrime also helps differentiate between the different debates, different impacts of technology and different types of crime. It helps our understanding of them and also reconciles different accounts of cybercrime and cybersecurity in the literature that are often presented in conflicting ways. By mapping out, say, impacts of technology on crime against *modus operandi*, by, say, different victim group, the different resources required to respond to cybercrime can be identified. The resulting matrix also helps identify the intelligence and evidential challenges and also the responsible agencies. Moreover, it can also help identify when police do or do not get involved, or pass a particular type of case on to another agency, and the following section on cybercrime statistics illustrates why this may be important.

5. Which Cybercrimes are Actually Affecting Police and the Criminal Justice System?

There has been much speculation over the years about the extent of cybercrime victimization and a considerable disparity exists between the millions of cyberthreats circulating at any one time compared to the low level of prosecution, say, for computer misuse (see for example Wall 2007: 42). Cyberthreat analyses are numerous and Semantec's 2015 Internet Security Threat Report is one useful example of many such regular reports and it has a long track record of reporting change in the threat landscape. The report identified in 2014, for example, that 500,000 web attacks are blocked daily and that 6549 new vulnerabilities were identified. Malware and ransomware attacks increased in volume 2014, with a noticeable four thousand-fold increase in crypto-ransomware attacks. McAfee estimated that the global cost and impact of cyber attacks was about $400 billion a year (Latiff 2014). Kaspersky and others provide similar threat analyses. The problem with these threat reports is that estimates of losses in terms of numbers and costs contrast dramatically with the number of prosecutions, especially for computer misuse. In the UK, for example, approximately four hundred or so prosecutions have been made under the Computer Misuse Act 1990 in the past twenty-five years since its introduction (Wall and Cockshut 2015).

(p. 1083) 5.1 The Divide between Cybercrime Estimates and the Prosecutions

Simply put, the estimates and alleged reports of cybercrimes are often breath-taking in their claims and excite dramatic media headlines. However, these reports can be equally confusing, because they regularly conflate risks with threats, harms, and crimes, and very

often in the way that media sources report their findings rather than the way the data is presented. The difference between each source is very important epistemologically when seeking to understand cybercrime. Whereas risks are the things that in theory *could* happen, such as the meteorite that might destroy life on earth, 'threats' are those risks that are in circulation at any one time, such as meteorites flying around the cosmos but not necessarily hitting anything (yet!). These risks and threats both contrast with harms and crimes, which (following the meteor analogy) actually hit something, but do not necessarily cause significant damage. In the case of crimes, however—and the meteor analogy stops here, they may either do damage that needs resolving, or in the case of inchoate crimes,[17] exhibit behaviour that needs to be prevented from reoccurring. It is therefore very important to distinguish between reports relating to risk and threats; reports of harms made to the police; harms the police decide to investigate; and offenders who the Crown Prosecution Service prosecute.

The estimates that most excite the media are usually representative of threats and risks, rather than the actual harms committed against victims (unless there is a strong human interest victim story) because of their dramatic volume or novel news value. At the courts end of the criminal justice process, prosecutions are very unreliable indicators of overall crime levels as they simply represent the end of the long legal process. Also, as the above analysis of cybercrime has illustrated, there are also many different types of cybercrime other than computer misuse. Moreover, there are also many different groups of victims—individual victims, as stated earlier, are very different from business victims, and within each group are sub-groups who have different reporting practices and understandings of the harms against them. There are also different public or private sector regulators who may vary as to whether they see the resolution of the crime as public or private affair. Despite the media tendency to over-sensationalize, some cybercrime are likely to be underreported, for example in the case of business victims, or victims of cybercrime with a sexual motivation (as they tend to be offline also). It is also the case that many computer misuse crimes are eventually prosecuted under other laws. As a rule, computer-related fraud, for example, tends to be prosecuted as fraud alone under the Fraud Act 2006 (the main offence), and any Computer Misuse Act 1990 aspect will tend to be lost from the debate or dialogue.

To reiterate, in order to understand the cybercrime issue, it is important to separate risks and threats from the actual harms. Harms are an important tipping point (p. 1084) in the justice process as they indicate when a crime begins to be experienced by the victim as a crime, rather than simply be as a technical victimization. One such example might be the receipt of a scam email where the recipient has not responded to it. It is technically an attempted fraud (an invitation to be defrauded), but unlikely in most circumstances to be either experienced or prosecuted as a fraud. So, crime has a technical state, a breach of certain legal conditions, but for it to progress through the criminal justice system it has in most circumstances to substantially harm a victim in order for it to be reported, as well as to satisfy various legal and procedural criteria in order for it to be investigated and prosecuted. These criteria include the Home Office Counting Rules,[18] the Code of Practice for Criminal Procedure and Police Investigations,[19] or the Code for Crown Prosecu-

tors.[20] As state earlier, crimes very often described as cybercrime are technically crimes, in so far as they are a breach of the law, but for various reasons they often do not fall within the legal criteria of a crime that can be investigated and pursued through the courts.

Sometimes cybercrimes are simply *de minimis non curat lex;* too small to pursue or prosecute in the public interest, or they fall outside routine police activities, or the criteria for recording and investigating crime (Wall 2007: ch8). This is especially the case if the crime now comprises of 50 million £1 thefts instead of a £50 million bank robbery. Whilst this is a hypothetical example, the previously discussed case of Lomas (BBC 2015a) graphically illustrates a new and real dynamic to policing cybercrime, especially then need to join up the intelligence from each offence in order to identify the offender. This intelligence not only includes information about who is committing mass amounts of small victimisations, but also the various inchoate offences related to them, such as the Spamming that delivers the threat via fraudulent email—which tends to be currently ignored in most cases. In this new set of policing dynamics, intelligence and evidence become very closely intermingled.

Finally, there is the definitional question as to when a morally outlawed deviant behaviour actually becomes a crime in law, because many of the harms that concern the public are not actually computer misuse, but related to bad Internet behaviour, or breaches of what was once called ‘netiquette’. A phenomenon arises that is not unlike the ‘dog-shit syndrome’ found in research into perceptions of street safety, where people fixate upon incivilities such as dog excrement on the pavement, rather than on more serious criminal threats affecting their life and limb. This emphasis on Internet bad behaviour can be illustrated by comparing prosecutions under s. 127 of *The Communications Act 2003* with those under the *Computer Misuse Act 1990* since 1990. Between 2004 and 2015 there were 21,320[21] s.127 prosecutions: a considerable contrast to the very small number of computer misuse prosecutions (four hundred over twenty-five years). The finding suggests that police are responding to increased demands to resolve Social Network Media behaviours and online communications issues, rather than offences under the Computer Misuse Act 1990. The following three case studies each explore the types of crimes regularly being found in the police workload today.

(p. 1085) 5.1.1 Facebook and Flirting

The first case study is reminiscent of the Twitter Joke Trial (*DPP v Chambers*)[22] and relates to s127 of the Communications Act 2003 and Internet threats. About five years ago a teenaged girl posted on Facebook a holiday picture of herself coming out of the sea wearing a bikini with the text, ‘What do you think boys?’ ‘Fxxxing gorgeous’, came the reply from her 15-year-old boyfriend’s best mate, and a flirty, but witty, banter followed. Jealous, her boyfriend told his best mate to ‘back off’ and a bad-tempered exchange ensued. The boyfriend angrily said (to his, now former best mate) that if he said it again he would hunt him down and kill him—actually paraphrasing Liam Neeson’s speech in the 2008 Pierre Morel-directed film, *Taken*. The former best mate’s parents saw the exchange and, concerned for his safety, mentioned it to his teacher, who did not know what to do.

She referred it to the head of year, and the situation worked its way up to the school's management hierarchy to the headmaster, who also did not know what to do. He asked the local police liaison officer, who asked the Crown Prosecution Service for advice. They considered the words 'I will kill you' to be of a menacing character and a clear contravention of s. 127(1a) of the Communications Act 2003. The police arrested the boyfriend, now deemed a potential killer, with force and seized his computers. In the following investigation the case then started to unravel and fall apart and became very public; the boyfriend was clearly not a killer and when he refused to accept a caution the case was dropped.

5.1.2 Snapchat and 'Sexting'

The second case study was reported by the BBC (2015b) and involved a 14-year-old boy sending a naked photograph of himself via the smartphone application Snapchat to a girl at his school. Snapchat deletes pictures after ten seconds, but the recipient managed to save the picture within that period and sent it on to her school friends. The picture was brought to the attention of the school liaison officer and although no charges were brought it was officially recorded as a crime and the details of both the sender and recipient placed on a police intelligence database. They could be stored for up to ten years and disclosed in a criminal records check. If the original sender of the image had been over eighteen years of age, the boy would have been the victim of 'revenge porn' and the girl who distributed the image prosecuted. Interviewed by the press, the boy's mother said that her son has been 'humiliated' for being 'at best naive' and at worst, just being 'a teenager'. What the case identified was that many young people now take part in so-called 'sexting' as a form of flirting (BBC 2015b). It is a form of behaviour that has become part of 'a new normal' and which requires much more understanding by the older generation and the authorities.

5.1.3 The TalkTalk Hack

The third case study is the 2015 TalkTalk data hack[23] and theft which sparked off a media frenzy and raised questions as to whether the culprit could receive a fair trial (p. 1086) and also whether the proportionality of justice normally found in the courts could ever be applied. In the aftermath of the TalkTalk 'attack' there seemed to be endless, yet information-less hand-wringing apologies from the company's CEO who repeatedly painted a picture of the company as an innocent victim. In the media stampede that followed various pundits liberally speculated over potential terrorist involvement, vast financial losses and an impending cybercrime tsunami. Then apocalyptic warnings followed from the business community and the commissioning of Government enquiries. Additionally, there were many media reports of customers losing money through secondary victimization to opportunist fraud. Quite independent of the data hackers, fraudsters made random phone calls purporting to be from TalkTalk and asking 'victim' subscribers to change their login details over the phone whilst confirming their payments for a refund or discount—therefore giving away their personal financial information. These events confirmed many folk myths about cybercrime and escalated the culture of fear around cybercrime (see Wall 2015b). And then there was an anti-climax following the sudden arrest of a 15-year-old boy from

Northern Ireland who presumably masterminded this heinous international crime from his bedroom and two 16-year-olds and a 20-year-old in connection with the case. Subsequently bailed, the 15 year old and accomplices were alleged to have hacked into the Internet service provider by using a DDoS attack as a smokescreen to hide an SQL injection in order to steal data containing information about four million or so TalkTalk customers (the actual number varies according to different reports). Not only do DDoS attacks fall under s36(3) of the Police and Justice Act 2006, but the way the data was stolen also contravenes s1(1) and s1(3) of the Computer Misuse Act 1990; so in this case, the law was very clear as to the crime. The hackers are then alleged to have contacted TalkTalk to ransom the data for about £80,000,[24] presumably threatening to release or sell the data if the ransom demand was not paid. The Metropolitan Police Cybercrime Unit (FALCON) tracked them down and arrested them before the data could be released or sold on. FALCON also confirmed that although some personal information could have been stolen, credit and debit card numbers had not been taken.

In fact, much of the initial speculation about the hack turned out to be unfounded and the whole affair began to look rather amateurish. But not before the backlash. More enquiries were announced and embarrassing questions asked about where TalkTalk's security people were at the time and exactly what was learned from TalkTalk's two previous attacks? Were they being fair to their customers? But the elephant in the room was the question over how could a 15-year-old and his 16- and 20-year-old associates could commit such serious crimes and cause so much damage from their bedrooms, simply 'because they could' and not because of a deeper criminal motive. In explaining his actions to Magistrates, one of the hackers said: 'I didn't think of the consequences at the time. I was just showing off to my mates' (BBC 2016). So, the answer to this question about how they could cause such damage lies in the earlier analysis of the how the Internet changes criminal behaviour by (p. 1087) providing new opportunities for crime at a distance, at speed, and in great volume (Wall 2015b). The answer to 'why' in this case may be much simpler.

5.1.4 Deciphering the Threat of Cybercrime

Each of the three cases mentioned above raises some very important questions about the role of police and authority today in dealing with disputes and issues arising from the internet and social network media. None are particularly unusual, but each present Police agencies with a new set of circumstances that fall outside their normal routine activities. In the threats and sexting cases, there are questions about whether police should have become involved so directly. There are also important questions about the responsibilities of the other parties involved. Did the parents over react? Were the teachers over-cautious or under-informed, or both? Did the prosecution lawyers consider the full context of the cases in their assessment of criminal responsibility? Did the police over-react because of pressure from parents or teachers? In the TalkTalk case, however, almost the opposite questions could be asked: were the parents under-cautious? Should they, or the teachers, have picked up warning signs, or involved police earlier? And the question common to all three cases is whether or not the authorities involved fully understood the nature of, what

is, apparently 'normal' teenage behaviour around the use of networked and mobile devices, a point raised earlier. All things seem to point here to the increasing importance of mainstreaming cybercrime in policing and, for example, developing roles like the police school liaison officer as key players in the resolution of cybercrime, rather than just developing specialist cybercrime units.

5.2 Policing the Reassurance Gap

Various victim surveys show a disparity between high levels of fear of cybercrime compared with lower levels of actual victimization (National Statistics 2012; Levi and Williams 2012; Wall 2013: 16–17). As alluded earlier, a 'culture of fear' about cybercrime has emerged from a combination of confused media reportage which mixes up potential cybersecurity risks and threats and actual cybercrime harms, against a background of dystopic conceptualizations of cybercrime that were written in social science fiction before cybercrime had ever existed (see Wall 2008). This inflation of fear has arguably led to demands for levels of security that the police agencies and government cannot realistically deliver alone (Wall 2008). The knock-on effect is that police and government have embarked upon a process of reassurance policing to bridge the gap between the demands for, and supply of, security and safety. But the results have been mixed, because some of the tactics employed amount to important and novel developments in policing (e.g. disruptive policing models), whereas others seem to be little more than PR exercises to (p. 1088) appease the public. What seems to be happening is that in the current politicization of cybercrime with the lack of legal focus and practical guidance, police agencies often tend to respond to the micro-politics of the situation, especially to the 'voices of concern', rather than to the justice needs of individual victims. Because of the general uncertainty in relating the involvement of police agencies to actual policing of cybercrime, forces and their officers find it hard to distinguish between those crimes which cause real harm to victims and those which people *perceive* as harmful. The upshot here, it is argued, is that the loudest voices tend to prevail and policing agencies feel pressure to police the reassurance gap, rather than police cybercrimes in order to achieve justice. This phenomenon is supported by an analysis of local police data which shows emphasis towards policing internet bad behavior (under s.127 Communications Act 2003) rather than Computer Misuse, but can be seen more broadly, for example, locally and nationally in the various responses to the three case studies outlined in the previous section.

The culture of fear about cybercrime and the reassurance gap arising from the mismatch between expectations of security and its delivery means that police and related agencies will have to work towards managing public and business expectations of the levels and types of security that police and government can deliver. The public's first point of contact, the police call centre, for example, is the most logical starting point for this. Current practice in many police force call-centres with regard to reports of frauds and cybercrime seems to be to re-direct callers to report them to Action Fraud (the UK national economic and cybercrime reporting centre). It is arguable that if call-centre staff across the UK spent one or two minutes more with each caller to give advice and reassurance and explain to victims that their information is very important even though less serious cases

may not result in a police investigation, then the public might be more inclined to report a cybercrime. In so doing, important strategic intelligence is also collected, including vital information about the many attempted frauds and related inchoate offences, which can be used by the National Fraud Intelligence Bureau to develop the UK Fraud Strategy and also to identify the tactical information that is needed to investigate online crimes (see Wall 2013: 18 and references below).[25]

5.3 Which Cybercrimes are Impacting upon Local Police Forces?[26]

The disparity between the politics and reality of cybercrime illustrated above is supported by an analysis of primary police data (from two UK police forces).[27] What is strikingly absent from local incident and 'crimed' datasets are the tier-one threats that cybercrime allegedly poses to the nation, as well as the cyber-dependent (p. 1089) malicious malware and cyber-enabled frauds so often reported in the media. But this lacunae is not surprising, because reports relating to these incidents are steered away from local police forces by call-centre responders, for example, directly to Action Fraud—the central repository for reports of economic and cybercrime. The data is therefore found in different databases, such as the Action Fraud dataset held by the City of London Police and intelligence feeds from GCHQ. But what is being found in the local police data, however, is an impact of the Internet that has rarely been the focus of public discussion. Local police forces receive many reports of low-level social network media aggravated crime (cyber-assisted crime) in which networked technologies play an important part and which increases demands upon police time. There are two main forms of this type of offending: social network media aggravated threats and assaults, and social network media aggravated frauds.

Social network media aggravated assaults occur where person A has insulted person B on a social network media site and person B, their partner or friend, retaliates by insulting or even physically assaulting person A. A variant of this behaviour is 'trolling' or Internet bad behaviour, where an individual takes pleasure in repeatedly upsetting others online. The victims in both types of offending are very often former friends or family members, though not always, and the actions cause considerable upset and disruption to victims' lives. Often, the offending online behaviour breaches an offline restraining order and typically occurs when an ex-partner harasses the victim online, incorrectly thinking the behaviour is not covered by the order. In each of these variants of threats and assaults, the online behaviour has offline implications and creates localized and resource-intensive demands on local police forces to meet with the parties involved.

Social network media aggravated frauds occur when peer to peer (P2P) online relationships lead to fraud both online and usually offline at some point. Many are variations of advance-fee fraud[28] of which the 419 scams have been the classic model. The offender typically entices a victim into taking part in an activity in order to extract fees in advance of services which do not take place. Before the Internet existed, these types of scams took place offline by using the postal system and letters, but they quickly moved online with the advent of the Internet to offer victims' large sums of money if they help the fraudster

move funds from one country to another. This 'alleged' transfer of funds is usually to be achieved by the victim agreeing to provide either an advanced fee to 'release funds', or allowing the perpetrator access to the victim's bank account, or sometimes both. Although victims are risk averse and rarely seem to fall for advanced fee frauds, when they do they are at considerable personal risk, especially if the online behaviour goes offline.

Advanced fee fraud has recently evolved into the Lottery Scam, which requires advance fees to release the 'winnings' and also the dating scam, which is claiming many victims. Fraudsters meet and groom victims through online dating sites and as the relationship progresses they extract monies, often in anticipation of the (p. 1090) meeting date and the fulfilment of emotional or sexual desires (see further Whitty and Buchanan 2012). The third type of advanced fee fraud is the auction fraud, where fraudsters lure victims by enticing them into buying goods that either don't exist or are not as advertised. These, and other relevant, offences are initially dealt with by Action Fraud, Trading Standards, or the commercial sector, and are then referred back to local police forces where a clear evidence trail exists. Some of the more straight-forward scams, mainly where both victim and offender are in the police force locality, will be handled directly by local police (see further Levi and others 2015).

These two basic types of cyber-assisted (or cyber-aggravated) crime are not particularly dramatic developments in the profile of crimes to which the police respond, but they do indicate a marked and gradual change in police response behaviour, which raises the question as to how police and police forces need to develop in terms of volume and resource demands. Currently local police forces and the National Crime Agency at a national level handle cyber-assisted crime, depending upon the severity of the harassment and volume of the offending.

6. Technological Development: Five–Ten Year Impact on the Police

One or more of three current technological developments will possibly challenge law enforcement and keep police managers and policy makers awake at night during the next ten years[29]. Mesh technologies will join our digital 'devices' to develop lateral communication networks; self-deleting communications, such as Tiger texts or Snapchat will eradicate evidence of communications; and crypto-currencies such as Bitcoin, Robocoin, Dodgecoin, Litecoin, and especially Zerocoin, which claims to be anonymous (Greenberg 2015), will create alternative value-exchange systems that could challenge the authority of banking systems. Amplified in time by the 'Internet of things' (see Ward 2014), these three technologies will collectively challenge policing and attempts at imposing governance, especially cross-jurisdiction governance. Moreover, there are also new forms of new criminal service delivery which mimic online business services and enable non-specialist criminals to commit crimes. Crimeware-as-a-service enables criminals to organize cybercrime attacks without requiring expert knowledge of computers or systems, as was once the case (Wall 2015a). The general concern about these developments is that the

public fear of crime that they give (p. 1091) rise to will reduce incentives for legitimate businesses to invest in networked activities, whilst further encouraging the infiltration of online markets by offline organized criminals. This development could further widen the reassurance gap between the levels of security that are being demanded by the public and the levels of security that governments and police bodies can realistically deliver. The widening of the reassurance gap is further exacerbated by the additional fear of an Internet take-over by organized crime groups present in media reporting, which raises questions about how the police will respond to these potential changes (Wall 2015a).

6.1 Failing to Respond to These Changes: the Consequences

What will happen if the police are unable to, or fail to, respond to cyber-criminals and cybercrime? Firstly, there would be no ‘certainty of apprehension’ and therefore no deterrence effect, which could encourage more online offending. This highlights the need to think about how to deal with cybercrime offender groups, which are distinctly different from other offender groups. Since there is little evidence to show that traditional organized crime groups have migrated their activities online, in fact online offender groups seem to have a different social and educational profile to traditional organised crime groups. As a consequence, it is probably unwise to directly imprison young online offenders who have succumbed to the seductions of cybercrime and drifted into serious (cyber) crime without ever leaving their bedroom. Typically, these offenders will have heavily played computer games before graduating to using game cheats and then learning how to disable their opponent’s computers in order to win, before developing further cybercrime skills from various criminal forums, often to see if they could do it? Not only are they psychologically unprepared for criminal justice processes and punishments, but whilst in prison they could easily fall under the protection of organized criminals, who will likely as not, then own them and call in cybercrime favours later! They do, however, require some alternative punishment to utilise their skills to the common good. Yet, without sufficient deterrence, the reassurance gap mentioned earlier will increase between public demands for security (the culture of fear) and what police and government can or cannot deliver. The perceptions of greater insecurity will, in turn, likely further discourage strategic investment in the Internet to improve services and citizen participation. The worst case scenario is that the perceived failure of police agencies will give rise to vigilante groups both online and offline, which could result in a growth in virtual or networked societies away from the Westphalian (p. 1092) state model, and towards affinity-based networked societies, like that occurring in the Middle East with IS.

7. Conclusion: What Can Be Done about Cybercrime, and How?

One certain fact about cybercrime is that it cannot be eradicated and there is no kill switch (literally or metaphorically) to turn these technologies off. More laws are also not the answer because existing computer misuse law, seemingly in all jurisdictions, is ar-

gually under-utilized. Furthermore, pure technological counter-measures are not purely the answer because they so often restrict other freedoms. Instead, we can only seek to manage cybercrime constructively and mitigate the risks and harms that it poses as soon as practically possible. So police, government and the private sector, as the 'capable guardians' (see Hollis and others 2013), will each need to respond intelligently to increasingly dynamic and varied forms of networked crime. To achieve this goal, a more nuanced and connected approach is required to address the challenges, and at a number of difference levels, but how?

The traditional response has been to develop collaborative models that bring together policing agencies, the computer security industry and other private sector bodies. The overview of cybercrime presented here, however, would suggest that such bodies also need to work closely with a broad range of other types of parties, such as, teachers, parents and the Crown Prosecution Service (CPS) to name but a few. One of the main weaknesses of collaborations, however, is that they tend to promote, at best, a form of tolerance, so there is the need for a more dynamic type of collaborative relationship that follows a co-productive or co-creative model. One that is co-owned by each of the stakeholder groups and aligned with a more intelligent capacity-building programme to help police leaders, officers, support staff, and other stakeholders understand, respond, and manage the behaviours that lead to developments in crime both off- and online crime. Furthermore, police agencies will need to work with their partner agencies and key stakeholders in their own countries as well as overseas towards developing new systems and standards for understanding changes in crime as they happen, and then immediately sharing the information about these changes. Developments in 'big data' analytic capacities indicate possibilities for informing strategy and policy in near real-time, although they introduce new risks and ethical concerns, especially to privacy. All this suggests that a major conversation is necessary between the private and public sectors, especially as we are at the dawn of the 'Internet of things', which will connect most (p. 1093) of our domestic and professional objects to the Internet and drastically expand the information flows about and between us.

References

BBC, 'Promoter of £21m pyramid scam ordered to pay back £1' (*BBC News Online*, 15 July 2015a) **<www.bbc.co.uk/news/uk-england-bristol-33536824>** accessed 30 April 2016

BBC, 'Sexting' boy's naked selfie recorded as crime by police' (*BBC News Online*, 3 September 2015b) **<www.bbc.com/news/uk-34136388>** accessed 30 April 2016

BBC, 'TalkTalk hack: Boy, 15, arrested in Northern Ireland released on bail' (*BBC News Online*, 27 October 2015c) **<www.bbc.co.uk/news/uk-northern-ireland-34646196>** accessed 30 April 2016

BBC, 'Boy, 17, admits TalkTalk hacking offences' (*BBC News Online*, 15 November 2016) **<http://www.bbc.co.uk/news/uk-37990246>** accessed 15 November 2016

Bilton N, 'The Y2K That (Thankfully) Never Happened' (*New York Times*, 30 December 2009) **<http://bits.blogs.nytimes.com/2009/12/30/the-y2k-that-thankfully-never-happened/?_r=0>** accessed 30 April 2016

Castells M, 'Materials for an explanatory theory of the network society' (2000) 51(1) British Journal of Sociology 5

Chan J, 'The technological game: How information technology is transforming police practice' (2001) 1(2) Criminal Justice 139

De Villiers M, 'Distributed Denial of Service: Law, Technology & Policy' (2006) 39(3) World Jurist Law/Technology Journal **<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952177>** accessed 30 April 2016

Greenberg A, 'Zerocoin Startup Revives the Dream of Truly Anonymous Money' (*WIRED*, 4 November 2015) **<www.wired.com/2015/11/zerocoin-startup-revives-the-dream-of-truly-anonymous-money/>** accessed 30 April 2016

Hollis M and others, 'The capable guardian in routine activities theory: A theoretical and conceptual reappraisal', (2013) 15(1) *Crime Prevention & Community Safety* 65

Latiff S, 'Cyber Attacks Cost $400 Billion A Year, Wrecking Global Economy' (The TechJournal, 11 June 2014) **<http://thetechjournal.com/internet/web-security/cyber-attacks-wrecking-global-economy.xhtml>** accessed 30 April 2016

Levi M and others, *The Implications of Economic Cybercrime for Policing* (City of London Corporation, 2015) **<www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf>** accessed 30 April 2016

Levi M and Williams M, *eCrime Reduction Partnership Mapping Study* (NOMINET/ Cardiff University, 2012)

National Statistics, *2010/11 Scottish Crime and Justice Survey: Main Findings*, (National Statistics/ Scottish Government, 2012) **<http://www.scotland.gov.uk/Resource/Doc/361684/0122316.pdf>** accessed 1 February 2013

Reiner R, *The Politics of the Police* (4th edn, OUP 2010)

Simmons D, 'Europol kills off shape-shifting 'Mystique' malware' (*BBC News Online*, 9 April 2015) **<www.bbc.co.uk/news/technology-32218381>** accessed 30 April 2016

(p. 1096) Sood A and Enbody R, 'Crimeware-as-a-service—A survey of commoditized crimeware in the underground market' (2013) 6(1) ScienceDirect 28 **<www.sciencedirect.com/science/article/pii/S1874548213000036>** accessed 30 April 2016

Wall D, 'Policing the Virtual Community: The Internet, Cyber-crimes and the Policing of Cyberspace' in Peter Francis, Pamela Davies, and Victor Jupp (eds), *Policing Futures: The Police, Law Enforcement and the Twenty-First Century* (Palgrave Macmillan 1997)

Wall D, 'The Internet as a Conduit for Criminal Activity' in April Pattavina (ed), *Information Technology and the Criminal Justice System* (2015 revised version on SSRN, Sage 2005) **<http://ssrn.com/abstract=740626>** accessed 30 April 2016

Wall D, 'Cybercrime: The transformation of crime in the information age' (Polity Press 2007)

Wall D, 'Cybercrime and the Culture of Fear: Social Science fiction and the production of knowledge about cybercrime' (Article revised in May 2010, 2008) 11(6) Information Communications and Society 861 **<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155>** accessed 30 April 2016

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

Wall D, ' "High risk" cyber-crime is really a mixed bag of threats' (The Conversation, 17 November 2014) **<https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091>** accessed 30 April 2016

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

Wall D, 'The TalkTalk hack story shows UK cybersecurity in disarray' (*The Conversation*, 28 October 2015b) **<http://theconversation.com/the-talktalk-hack-story-shows-uk-cybersecurity-in-disarray-49909>** accessed 30 April 2016

Wall D and Cockshut L, 'Prosecuting Cybercrime: Achieving Justice or Reassurance?' (European Society of Criminology Annual Conference, September 2015)

Ward M, 'CES 2014: Connected tech raises privacy fears' (*BBC News Online*, 8 January 2014) **<www.bbc.co.uk/news/technology-25662006>** accessed 30 April 2016

Whitty M and Buchanan T, 'The Psychology of the Online Dating Romance Scam' (ESRC Research Report, University of Leicester 2012) **<www2.le.ac.uk/departments/media/people/monica-whitty/Whitty_romance_scam_report.pdf>** accessed 30 April 2016

Notes:

(1.) This chapter was originally presented as a paper to the *Cyber crime: Research, practice and roadmaps panel* of the 2015 CEPOL Annual European Police Research and Science Conference, 5-8 October, Edíficio Polícia Judiciária, Lisbon, Portugal. It mainly draws upon the UK experience, but the general issues are global. I thank Karen Yeung and reviewers for their valuable comments.

(2.) These statements are based upon observations made by myself from the UK National Wellbeing Survey which shows an increase in well-being (especially among young women) during a period of austerity, an increase that could be attributed to the impact of social network media. See <https://www.gov.uk/government/publications/wellbeing-policy-and-analysis>. Also based upon observations of young social network users who appear to morally censure each other when one of them 'oversteps the mark'.

(3.) EPSRC Global Uncertainties Programme (EPSRC CeRes Project EP/K03345X/1).

(4.) This paper is also informed by the early findings of another (new) project under the EPSRC Global Uncertainties Programme is which is looking at the impact of Cloud Technologies upon Cybercrime (EPSRC CRITiCal EP/M020576/1).

(5.) **Pyramid selling scams** (or Ponzi schemes) have migrated online and are elaborate confidence tricks that promise a good return on investment. The return on investment is, however, paid from money derived from new investors rather than profits and the schemes mathematically eventually run out of investors.

(6.) **Sextortion** is when intimate knowledge or pictures of a victims sexual activity is used to threaten their reputation in order to extort revenge, money, or favours.

(7.) **Distributed denial of service** (DDOS) attacks prevent legitimate users from gaining access to their web space (networks and computer systems) by bombarding access gateways with a barrage of data.

(8.) The **Stuxnet** worm is a form of malware that was used in 2010 to sabotage industrial control systems (SCADA) in an Iranian Nuclear Powerplant. The worm was introduced via a USB stick and sought out a particular configuration of hardware and control system before deploying. It is often regarded as an example of information warfare.

(9.) **Rootkit malware** is lodged in the 'root' of the operating system and enables hackers to obtain remote access to the computer. It is essential in the execution of, amongst other cybercrimes, botnets.

(10.) **Zeus** is a form of malware distributed by spammed email to infect the computers of small businesses and individuals in order to steal bank login information and make the computers part of a botnet.

(11.) **Botnets** comprise lists of the Internet protocol (IP) addresses of 'zombie' computers that have been infected by remote administration tools (malcode) and which can subsequently be controlled remotely.

(12.) **Script kiddies** are inexperienced and unskilled hackers who seek peer respect for their audacity by infiltrating or disrupting computer systems by using cracking scripts that they have designed.

(13.) **Ransomware** is malicious software that hijacks a computer system until it is neutralized by a code provided by a blackmailer once a ransom has been paid.

(14.) **Fake AV** (Anti-Virus) malware informs users, using signs that emulate the operating system, that illegal files are found on their computers and that they need to download a free ‘patch’ to prevent them reappearing. Users are then told that they need to purchase a professional version of the ‘patch’ in order to make the repair permanent.

(15.) I am avoiding using the term ‘The Cloud’ here because it is conceptually problematic and hard to differentiate from what existed before, but the phrase cloud technologies encapsuates the change in terms of increased computing power, storage, and reduced costs.

(16.) **Spamming** is the distribution of unsolicited bulk emails. They choke up bandwidth and present risks to the recipient, should they respond.

(17.) An Inchoate offence is typically an action that is taken in preparation to commit a crime and it may not in itself be harmful.

(18.) Counting rules for recorded crime <https://www.gov.uk/government/publications/counting-rules-for-recorded-crime>

(19.) Code of Practice to the Criminal Procedure and Investigations Act 1996 <https://www.app.college.police.uk/app-content/investigations/introduction/#principles-of-investigation>

(20.) Code for Crown Prosecutors <http://www.cps.gov.uk/publications/code_for_crown_prosecutors/codetest.html>

(21.) Data obtained from requests made under the Freedom of Information Act 2000 (my thanks to Dr Ladan Cockshut and Dr Laura Connelly).

(22.) In the Twitter Joke Trial, Chambers sent a tweet saying that he would destroy Doncaster airport while in a fit of pique and was subsequently prosecuted under s 127 of the Communications Act 2003. The conviction was quashed after a third appeal, as it was deemed to be ‘a message which does not create fear or apprehension in those to whom it is communicated, or who may reasonably be expected to see it, falls outside this provision’ (of the CA 2003 Act) See *DPP v Paul Chambers* [2012] EWHC 2157 <https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/chambers-v-dpp.pdf>

(23.) **Data theft** (hack) is the theft of bulk data by hackers who have, to date, tended to perform a DDoS attack as a decoy to confuse the computer security before breaching the system (via an SQL injection) to steal the data.

(24.) Which is a small sum compared to the value of the data to the company.

(25.) At the time of writing, many UK police forces are reviewing their call-centre advice to the public with regard to cybercrimes. There is also talk of a review of the Action Fraud system being undertaken.

(26.) These observations are of trends drawn from an analysis a combination of aggregated individual police force data for an EPSRC project (EP/K03345X/1) obtained under data processing agreements which, because the research is still underway, only allow for discussion in principle, and also an analysis of Action Fraud Data by the author (see Levi and others 2015).

(27.) Because of the data processing agreements governing the use of this data the findings of the analysis are only discussed broadly and in principle at this stage.

(28.) **Advanced fee frauds** (419 Scams) are fraudulent tactics that deceive victims into paying fees in advance to facilitate a transaction which purportedly benefits them and never materializes.

(29.) These issues were first raise in (Norman Baker's) Home Office Ministerial Working Group on Horizon Planning 2020–2025 in 2013.

David S. Wall

David S. Wall, Centre for Criminal Justice Studies, School of Law, University of Leeds, UK