Through the Looking Glass: Emerging Understandings of Cybercrime in GMP

A research project by Paul White (Strategy and Police Officer, Greater Manchester Police)
“When I use a word,’ Humpty Dumpty said in rather a scornful tone, ‘it means just what I choose it to mean — neither more nor less.’

‘The question is,’ said Alice, ‘whether you can make words mean so many different things.’

‘The question is,’ said Humpty Dumpty, ‘which is to be master — that’s all.’

* Lewis Carroll, *Through the Looking Glass*
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Literature Review</td>
<td>8</td>
</tr>
<tr>
<td>Research Methodology</td>
<td>18</td>
</tr>
<tr>
<td>Findings and Analysis</td>
<td>24</td>
</tr>
<tr>
<td>Discussion</td>
<td>47</td>
</tr>
<tr>
<td>Conclusion</td>
<td>54</td>
</tr>
<tr>
<td>References</td>
<td>56</td>
</tr>
<tr>
<td>Appendix A – Example of survey questionnaire</td>
<td>61</td>
</tr>
<tr>
<td>Appendix B – Method of obtaining ‘cybercrime’ data from GMP’s Business Intelligence System</td>
<td>67</td>
</tr>
<tr>
<td>Appendix C – Acknowledgments</td>
<td>73</td>
</tr>
</tbody>
</table>
Introduction

As a member of Police Staff, within the Greater Manchester Police (GMP) Strategy Planning and Policy Team, for a number of years I have taken a keen interest in the implications that the concept of cybercrime poses for public safety and policing. I have followed the developments of national strategy and have become particularly interested with the concept of mainstreaming cyber awareness and capability across policing.

In undertaking this Research Fellowship project, my overall aim is to contribute to the discourse about interactions online and offline, specifically in terms of the impact this is having on demand for police services (especially those one might not immediately associate with having to deal with cybercrime) and how officers and staff view their role in this. My research will be conducted at GMP and the project has four specific research objectives. These are to:

1. Outline the extent to which online behaviour leads to demand on GMP;
2. Capture the perception of police officers and staff on the scale and nature of service demand;
3. Capture the perception that police officers and staff have of their role in servicing demand resulting from online behaviour;
4. Contribute to discussions on the use of the term ‘cyber’ in describing particular forms of internet behaviour and the implications that this may have for policing.

This report will outline my findings against these aims. In doing so, I will begin with a review of appropriate and relevant literature. I will then describe my research method and approach before presenting, analysing and discussing my findings, which will include a consideration of the limitations and implications. Finally, I will draw conclusions and outline the references I have drawn upon throughout. In order to contextualise the study, I will begin by examining the origins of the concept of cybercrime, looking at how this has featured within popular culture and how it has come to the attention of the law enforcement.
The origins of the concept of cybercrime “can be traced back to the cyberpunk social science fiction literature of the 1970s and 1980s” (Wall, 2010: 89) Such literature, Wall notes, presented a genre of science fiction that merged thinking about developments in science and information technology, with the potential to undo social order, and that the link between cyberspace and crime was present even in early cyberpunk stories. In his text, Wall illustrates several examples of books, films and media to demonstrate the impact that the concept of cybercrime has had on popular culture.

In a list of ‘the best hacking and computer geek movies ever’, (Internet Movie Database, 2015a) 85 examples are presented of films and television programmes (both fictional and documentary) from the 1980s to the 2010s where cybercrime and virtual online worlds have been the theme. Figure 1 presents an adapted summary.

**Figure 1: Examples of cyber-themed film and television from the 1980s to the 2010s (adapted from Internet Movie Database, 2015a)**

- Tron (1982) – directed by Steven Lisberger
- Wargames (1983) – directed by John Badham
- Real Genius (1985) – directed by Martha Coolidge
- Lawnmower Man (1992) – directed by Brett Leonard
- The KGB, the Computer and Me (1990 documentary) – directed by Robin Bates
- The Net (1995) – directed by Irwin Winkler
- Firewall (2006) – directed by Richard Loncraine
- Die Hard 4.0 (2007) – directed by Len Wiseman
- The Hacker Wars (2014 documentary) – directed by Vivien Leask Weisman
- Deep Web (2015 documentary) – directed by Alex Winter
- Cyberbully (2015 TV movie) – directed by Ben Chapman
In 2015 popular culture received a further dose of cybercrime fiction with the release ‘Blackhat’, a new film from director Michael Mann, which tells the story of a man “released from prison to help American and Chinese authorities pursue a mysterious cyber criminal” (Internet Movie Database, 2015b). So, given the seeming public interest in information and media related to cybercrime related themes, it is perhaps no surprise that “Issues around cybersecurity are never far from the headlines” (Stephens, 2014). Indeed, as 2014 drew to a close, one of the main news circulating in the media was the reported cyber attack against Sony Pictures in the USA (for example Zetter, 2014 and Carroll, 2014).

As well as being of significant interest within popular culture and the news media, cybercrime has been the subject of numerous reports by governmental and law enforcement agencies. The following examples are meant to be illustrative and not exhaustive.

In what was claimed to be the most detailed study ever undertaken of its kind in the European law enforcement community, Europol (2013a) identified an estimated 3,600 organised crime groups currently active in the EU. The report highlighted the emergence of new criminal phenomena, many linked to the current economic crisis and the internet. Europol describes how these new developments are changing the nature of organised crime towards a model based around a networked community of heterogeneous, international groups. Here, the internet is described as being a major driver of criminal activity, enabling organised crime groups to access a large pool of victims, obscure their activities and carry out a diverse range of criminal acts in a shorter period of time and on a much larger scale than ever before. The spread of the internet and technological advances are said to have caused significant shifts in crime areas and the pattern of criminal activity.

Following the publication of this report, Rob Wainwright, Director of Europol said: “These groups are no longer defined by their nationality or specialisation in one area of crime but by an ability to operate on an international basis, with a business-like focus on maximising profit and minimising risk. They are the epitome of our new globalised society” (Europol 2013b)
More recently, on the scale of the issue, Europol has described how “cybercrime itself is a growing problem. Trends suggest considerable increases in the scope, sophistication, number and types of attacks, number of victims and economic damage.” (Europol 2014: 9)

In terms of how the threat of cybercrime is perceived to be impacting upon the UK, the Government’s Intelligence and Security Committee has previously stated: “The threat the UK is facing from cyber attacks is disturbing in its scale and complexity” (Intelligence and Security Committee, 2013: 19). More recently, in its first annual assessment of the serious and organised crime threats faced by the UK, the National Crime Agency prioritised these threats and considered how they are likely to develop for the next year to three years (National Crime Agency, 2014). Among those identified by the Agency were online threats namely:

- Cybercrime – particularly with increases in the targeted compromise and disruption of access to UK networked systems; the volume of cyber-dependent criminality (driven by the ‘as a service’ nature of the cybercrime marketplace); and
- The growth of online streaming of real-time child sexual abuse.

In describing how it assesses the organised cybercrime threat, the National Crime Agency states:

“Technological development - both legitimate and criminal - is dynamic and criminals have long been fast to adapt to changes of technology, the law, and the actions of law enforcement, regulators and the ICT security industry. Criminals use the internet to conspire with other criminals and to trade a wide range of commodities online – e.g. drugs, firearms, indecent images of children. Criminals also trade skills, tools and techniques that enable criminal offences; this is known as the ‘as-a-service’ business model. In cyber crime, the proliferation of the ‘as-a-service’ marketplace has demonstrated collaboration between cyber criminals and groups from different countries and ethnic groups. While there is a strong international dimension to cyber crime, it is important to stress the involvement of UK-based criminals who act against domestic and global networked systems” (National Crime Agency, 2014: 7)
In view of such reports, cybercrime is perceived by the UK Government to be a real and serious threat to national security and public safety. Her Majesty’s Government (2010) has identified cyber attacks against the UK by other states and ‘large-scale’ cybercrime as a ‘tier one’ threat (the highest level of threat) to national security. Following this analysis, the Cabinet Office published the first ever UK Cyber Security Strategy, which sought to identify threats and opportunities presented by an increasingly connected world, and set out the Government’s vision for UK cyber security in 2015. Among its commitments, this strategy highlighted a need to drive and to shape “training for mainstream law enforcement on cyber issues, and making sure the links to related issues such as bullying or child exploitation are made” (Cabinet Office, 2011: 30). This led to a statement within the Strategy of an action stating that the police “will mainstream cyber awareness, capacity and capabilities throughout their service” (Cabinet Office, 2011: 37)

This desire to see cybercrime skills mainstreamed across policing was also highlighted by a Parliamentary Committee which heard evidence stating that the threat of cybercrime is rising exponentially. Among the recommendations made within its final report, the Committee noted that mainstreaming cybercrime investigative skills throughout the police is key to improving capacity across the board. However, with an apparent reference to the UK Cyber Security Strategy, the Committee’s report stated that “commitments to improve mainstream skill levels have been around for years and practice has not so far matched rhetoric” (House of Commons Home Affairs Committee, 2013: 21).

As part of a review into police compliance with the national Strategic Policing Requirement, introduced in 2012 by the Home Secretary, Her Majesty’s Inspectorate of Constabulary (HMIC) inspected police forces to assess preparedness across England and Wales for dealing with the threat of a large-scale cyber incidence (including a criminal one). The inspectorate’s findings report stated: “Senior leaders across police forces were unsure of what constituted a large-scale cyber incident. We found that, where they existed, STRAs [Strategic Threat Assessments] and plans were focused only on investigating
cybercrime; they were silent about preventing it and protecting people from the harm it causes” (Her Majesty’s Inspectorate of Constabulary, 2014a: 13)

HMIC also stressed that: “It is now essential that police officers have the capability to deal confidently with the cyber element of crimes as it is fast becoming a dominant method in the perpetration of crime” and that “The police must be able to operate very soon just as well in cyberspace as they do on the street” (Her Majesty's Inspectorate of Constabulary, 2014a: 14). However, the Inspectorate found that the take up of training “was disappointingly poor, with only a few forces demonstrating a real commitment to improve the skills of their staff to tackle cybercrime. The average take-up for this training in 37 forces was less than two percent of the workforce.” (Her Majesty's Inspectorate of Constabulary, 2014a: 14).

As part of its inspection programme for 2014/15, HMIC had planned to undertake a further, dedicated thematic inspection of cybercrime. However, Inspectorate note that their consultation with stakeholders has revealed that “there remains considerable ambiguity about how the police should respond to this challenge” (Her Majesty’s Inspectorate of Constabulary, 2014b) and has come to the conclusion that it is not appropriate to undertake its proposed inspection at the present time. Instead, HMIC indicated that it is to undertake a study, with the Home Office, the College of Policing, academics and police forces, to better develop the digital technology aspects of crime and policing, focussing on “those offences committed, in full or in part, through a computer, computer network or other computer-enabled device” (Her Majesty’s Inspectorate of Constabulary, 2014b).

It appears that much of the focus on the threat of cybercrime has been on its implications for serious law enforcement issues such as organised crime, financial crime, and child sexual exploitation. However, there appears little discussion or evidence of the impact that this is having on crime and policing issues which are deemed to be less serious.
One such insight however, is described in a College of Policing press release following an interview with its Chief Executive (Chief Constable Alex Marshall), as part of a BBC Radio 4 Law in Action programme. The College notes that “anecdotal evidence from police officers and staff dealing with less serious crime and anti-social behaviour suggests that half of the reports they deal with may be related to some form of social media”. Chief Constable Marshall is quoted:

“As people have moved their shopping online and their communications online, they’ve also moved their insults, their abuse and their threats online, so many more police investigations are having an online element to them... Officers dealing with less serious crimes and anti-social behaviour might deal with a dozen calls in a typical day and they tell us that at least half of reports of this type, whether around abuse or threats of assault, may be related to Facebook, Twitter or other forms of social media…” (College of Policing, 2014).

In summary, reports by governmental and law enforcement agencies seem to acknowledge that the growth of through globalisation and the growth of digital technology, patterns in criminality are changing. The concept of cybercrime appears to be perceived as a growing threat, and it seems that in response to this threat, a strategic response to mainstream cyber-awareness, capacity and capability across law enforcement has been proposed. I will now explore these themes further through a review of relevant academic literature.
Literature Review

Whilst anecdotal evidence suggests the rising importance of cybercrime across different levels of criminality, it is now important to turn to a wider literature to examine claims about the nature and scale of cybercrime.

To achieve this, I will begin by exploring the origins of the internet and how its growth, commercialisation and the increasing ubiquity of digital online technology present opportunities for criminality. Then, I will look at behavioural explanations of why online technology may be susceptible to exploitation for deviant purposes, and will explore research on the scale and nature of cybercrime. Following this I will present examples of discourse which considers the terminology associated with cyber and its usefulness, and I will also note research which has sought to explore how mainstream police officers view their role in responding to cybercrime.

Turner (2006) discusses the way in which computer technology developed from the early 1960s through to the 1990s and the emergence of the internet. Turner describes how, at the height of the cold war in the 1960s, the perception of computers was bleak, that they were weapons of war representative of the inflexible organisation and mechanistic conformity that made the military-industrial complex possible. However, Turner describes how, between the 1960s and the 1990s, an influential group of American entrepreneurs based in the San Francisco Bay area, negotiated a long-running engagement between San Francisco’s ‘hippie’ counterculture and the developing computer technology hub based at Silicon Valley. Turner notes that through this collaboration between counterculturalists and technologists, computers were re-envisioned as technology that enable personal liberation and freedom through the development of online, ‘virtual’ alternative communities, and the opportunity to explore new social boundaries.
Ultimately, Turner argues that by the 1990s, with the emergence of the internet, computer technology embodied a different world view, one which envisaged a ‘digital utopia’ enabled through online collaboration, modelled on communal ideas of the hippie counterculture movement, which had railed against the establishment during 1960s.

According to Umstätter, 1995 was the trigger year for the commercialisation of the internet. Writing around this time he notes that: “Internet idealists are very disappointed about these developments, while financial oriented brokers repeatedly bring to mind the mood of the gold-rush” (Umstätter, 1996: online).

As the internet has become commercialised so we have seen its use grow exponentially in subsequent years, to the extent that now appears we live in a world where people are able to simultaneously have lives online as well as in the real world. So, rather than being a distinct entity and separate the real world, the online world is increasingly ubiquitous. As of this year, there are over fifty-seven million users in the United Kingdom alone, almost 90 percent of the population. By the end of 2014 there will be over three billion internet users across the world (Internet Live Stats, 2014).

With the increasing use of the internet (seemingly driven by commercialisation and consumerism, the proliferation of mobile technology and the perceived ‘liberation’ endowed by social media), we appear to be seeing an increasing promulgation of personally identifiable information such as emails, photographs, names and Internet Protocol (IP) addresses, to the extent that detailed personal profiles can be obtained from publicly available data. Whilst this information about peoples’ identities has commercial value, so it also has value for criminals.

For serious and organised criminals “identity is both a commodity to be traded and used in further crime such as certain fraud offences, and necessary to disguise their true identity... The use of false identities is an important enabler of serious and organised crime”. (National Crime Agency, 2014: 12)
It is also argued (Vidhya, 2014) that the world’s increasing dependence on technology has revolutionised business and communication, but that too much faith in technology has led to complacency about the threat of cybercrime.

In some ways, the reflects the view that “history shows that the relationship between crime and technology is by no means new and that the potential for creating harm never seems to be far away from any apparently beneficial technological development” (Wall, 2007: 2). So, it appears that rather than becoming the emancipating utopia that Turner describes as envisioned in the 1990s, the online world has instead become a reflection of real world society along with the complexities and deviant behaviour that are inherently part of life. Perhaps, in some ways, the communication media presented by online technologies have certain characteristics that mean they in particular can be exploited for deviant purposes (either purposefully or otherwise).

In terms of the relationship between communication and behaviour, it has been proposed (Rushkoff, 2010) that the media through which people engage with the world and each other carry biases. That is they have a tendency to encourage some behaviours over others. For example, writing a letter, writing an email or sending a message through online social media are all different acts that require different approaches and mindsets in their use: “Just as we think and behave differently in different settings, we think and behave differently when operating different technology (Rushkoff, 2010 p. 21). So, it could be argued that with the increasing ubiquity of online, new media technology behaviour may be emerging which has particular biases, perhaps some of which would be deviant.

The concept of the ‘Online Disinhibition Effect’ (Suler, 2004) goes some way to explaining how this could be the case. People, Suler argues, say and do things in cyberspace that they wouldn’t ordinarily say and do in the real, face-to-face world. Wall (2007) notes the term ‘cyberspace’ was first coined by William Gibson in 1982 and became a popular term used to describe the virtual environment within which networked computer activity takes place).
In cyberspace, Suler suggests, people feel less restrained, and express themselves more openly, leading to the *online disinhibition effect*. However, this disinhibition can manifest itself positively and negatively. For example, Suler describes 'benign disinhibition', which works constructively with peoples sharing emotions, fears and wishes, and showing unusual acts of seemingly altruistic behaviour.

On the other hand Suler highlights 'toxic disinhibition' where the effect leads to “rude language, harsh criticisms, anger, hatred, even threats. Or people visit the dark underworld of the internet - places of pornography, crime, and violence - territory they would never explore in the real world” (Suler 2004: p 321). Suler describes six factors involved in the online disinhibition effect, which are presented in Figure 2.

**Figure 2: Factors involved in the online disinhibition effect (adapted from Suler, 2004)**

- **Dissociative anonymity** – When using the Internet it is not easy to see who others actually are e.g. usernames and e-mail addresses may be visible, but may not reveal much about a person. This enables people to separate their actions online from their 'in-person lifestyle' and identity, and can even 'convince themselves that those online behaviours "aren't me at all."' (Suler, 2004: p 322).

- **Invisibility** – This is a factor in online environments where people cannot see each other. 'Invisibility' gives people the courage to go places and do things that they otherwise would not. Even when identity is known people don't have to worry about how they look or sound when they type a message, nor worry how other will look or sound in response – thereby amplifying the effect.

- **Asynchronicity** – This relates to interactions that do not take place in real time e.g. people can become disinhibited when other's replies to their messages may take minutes, hours, days, or even months, meaning they do not have to deal with immediate reactions;

- **Solipsistic introjections** – This describes how the absence of face-to-face cues combined with text communication can alter self-boundaries. Here, people may feel that their mind has merged with the mind of the online companion;

- **Dissociative imagination** – This describes how people may feel that their dissociated, imaginary online persona (along with the online identities of others) live in a 'make-believe' dimension, separate from the responsibilities of the real world;

- **Minimization of authority** - The absence of cues to status of authority figures online e.g. dress, body language etc. and environmental setting of cyberspace, reduces the impact of their authority.

Rather than acting as separate components, Suler describes how, in the main, these factors interact with each other resulting in a more complex, amplified online disinhibition effect. However, Suler also stresses that people's individual differences and personality styles play an important role in how the effect manifests.
Since Suler outlined the online disinhibition effect in 2004, developments in cyberspace and social media (e.g. with the development of platforms such as Skype and Twitter) have perhaps minimised some of the factors Suler describes e.g. invisibility and perhaps to some extent asynchronicity. However, the model may still have value in helping explain the relationship between cyberspace and the potential for deviant behaviour to manifest, sometimes as criminal behaviour.

If online technology does indeed possess a bias towards promoting deviant behaviour, then with increasing online ubiquity, we might expect to see this manifest through increasing criminality. A Home Office study was commissioned in 2013 to provide an overview on the scale and nature of cybercrime in the UK (Dowling and McGuire, 2013). Dowling and McGuire note that, according to the Crime Survey of England and Wales, in 2011/12 over one-third of adult internet users reported experiencing a negative online experience, but that these experiences would often be below the threshold of a recorded crime. They noted that computer viruses were the most common negative experiences reported, although the proportion of adult internet users experiencing them appeared to have declined. Experiences of computer hacking, on the other hand, appeared to have increased

Dowling and McGuire argue that to drive policy interventions with a sound evidence base, there is a critical need for knowledge of the scale and nature of cybercrime, how it is changing over time and whether interventions to tackle the problem are having an impact. However, they acknowledge that there are significant challenges to this, including: “lack of recording mechanisms that accurately distinguish between online and offline crime; under-reporting of cybercrime… a lack of awareness that some cyber incidents are actually crimes (although not all are); inconsistencies in the measurement and definition of cyber crime within the relevant research…” (Dowling and McGuire, 2013: 14).

But what exactly is this phenomenon called ‘cybercrime’. Cybercrime has been explained as “an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes” (Dowling and McGuire 2013: 5). In their review, Dowling and McGuire use cybercrime to refer to both forms of criminal activity, though they distinguish between ‘cyber-dependent
crimes’ (primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud) and ‘cyber-enabled crimes’ (traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other information communications technology).

For the purposes of their review, Dowling and McGuire include the following types of cyber-enabled crimes: fraud; theft (including theft of personal information and identification-related data); and sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery). Within ‘cyber dependent’ crime, their review also considered online stalking (or cyberstalking), but determined that there is limited evidence available regarding the nature and extent of online stalking in the UK. They found even sparser evidence relating online hate crime. This echoes Hernandez-Castro et al (2014), who note that “very little research has been dedicated to the impact of cybercrime in the United Kingdom, in particular beyond financial losses” (p.2).

The issue of ‘cyberbullying’ was excluded from Dowling and McGuire’s review as they note that this is not classed as a crime in law. However, online guidance produced by the Metropolitan Police states: “some types of bullying are illegal and should be reported to us” (Safe, no date), this is said to include harassment and intimidation over a period of time and anything involving hate crimes. Meanwhile, other public advice (Safe Network, 2013), aimed at the public in England and Wales, about what constitutes cyberbullying, also appears to indicate that such behaviour may include that which is criminal, as shown in Figure 3.
**Figure 3: Public advice on what constitutes cyberbullying (adapted from Safe Network, 2013)**

- Sending threatening or discomforting text message to a mobile phone
- Making silent, hoax or abusive call to mobile phones
- Making and sharing embarrassing images or videos via mobile phone or website
- Broadcasting unsuitable web cam footage that is threatening or manipulative
- Leaving hurtful messages on social networking sites or sending the same message to that person’s peer group
- ‘Outing’ people by publishing or disseminating confidential information online
- Stealing an online identity in order to cause trouble in that person’s name
- Deliberately excluding people from online games or groups
- Setting up hate sites or hate groups against an individual
- Sending menacing or upsetting responses in chat rooms, online games, or messenger ‘real time’ conversations
- Voting for someone in an insulting online poll
- Sending someone ‘sexes’ that try to pressure them into sexual acts

Furthermore, following publication of a House of Lords Communications Select Committee report on social media and criminal offences, the Committee’s Chair Lord Best stated: “Cyber bullying, revenge porn, trolling and virtual mobbing are new phrases in our media vocabulary, but they generally describe behaviour that is already criminal.” (Parliament.uk, 2014). This comment, in addition to public guidance, appears to suggest that in some circumstances what could be deemed cyberbullying may indeed constitute a crime.

Ultimately, it would seem that the term cybercrime “has come to symbolize insecurity and risk online” (Wall, 2007: 10). Wall suggests that the term is for the most part an invention of the media, acknowledging that it has no specific reference point in UK law. Nevertheless, he argues that the term “has entered the public parlance and we are stuck with it” (Wall, 2007: 10) and has gathered significant linguistic agency.

Although cybercrime as a term has gathered such agency, Jarvis and MacDonald (2014) offer an indication of a potential problem this may present. It is argued that the use of the word ‘cyber’ as a prefix to coin new terms is leading to “…a profusion of ill-specified and ill-understood vocabulary” (Weimann 2005, cited in Jarvis and MacDonald, 2014: 53) and that: “This profusion of new terminologies throws up
considerable challenges… Not least amongst these is the inconsistent and interchangeable use of such terms” (Jarvis and MacDonald, 2014: 53).

In discussing the classification of cybercrime, in the findings report following its inquiry, the Home Affairs Committee stated: “The ever-increasing incidence of the use of the internet in some form in traditional crimes indicates the futility of special categorisation for such offences” (Home Affairs Committee, 2013: 6). An intriguing glimpse into the changes in criminal behaviour that could be driving the stated trend of the internet being increasingly used in traditional crimes can be seen in the work of Deputy Chief Constable (DCC) Jon Boutcher (cited by Warrell, 2015), who is the Deputy National Lead for Cybercrime. Mr Boutcher has examined how traditional criminals appear to be migrating to cybercrime. His findings seem to suggest that, across the cases he examined, 64 percent of cybercriminals had previous convictions for non-cyber crimes (e.g. for offences such as burglary, theft and even violence). His thesis also considers the extent of cybercrime reporting and his indications suggests that only 11 percent of cybercrime victims report crimes to the police. This would seem to echo the issue of under-reporting noted by Dowling and McGuire.

References to the increasing involvement of online technology in traditional crimes, and a migration by traditional criminals towards using the internet, would suggest that cybercrime is not necessarily the reserve of specialist police resources, but rather that as the technology becomes more ubiquitous, so too must be the police response in addressing it. This would support the UK Cyber Security Strategy’s aim, to mainstream cyber-awareness, capacity and capability across the police.

But, if cyber is to be mainstreamed, how do police officers feel about their role in responding to crimes and incidents related to cyberspace? My literature review has found little evidence in this area, although some insight is provided in an American study by Bossler and Holt (2012). These authors note that, in the US, commentators and police administrators have argued that local law enforcement agencies, including their front line officers, must increase their capability to respond to cybercrimes. This appears to be in accordance with the UK Cyber Security Strategy aim to mainstream cybercrime training across UK law enforcement.
However, Bossler and Holt note that there are few empirical studies which have assessed how local law enforcement has responded to cybercrime. Thus, they concluded that there is a critical need for research exploring local law enforcement awareness, perceptions, and preparation for dealing with cybercrime. To this end, their study sought to determine:

1) The law enforcement agencies that officers believe should be primarily responsible for investigating cybercrime cases;
2) Officer’s perceptions about their agency’s current ability to respond to these offenses; and
3) Officer’s beliefs regarding the best ways to improve the social response to cybercrime.

From their survey of officers from two US police departments (with around 260 survey respondents), Bossler and Holt found that US officers do not believe that local law enforcement should be primarily responsible for handling cybercrime cases and they have little information on how ‘upper management’ is addressing cybercrime. Officers indicated that the best strategies to deal with cybercrime were greater care taken by citizens online and improvements to the legal system.

Further insight into police employee perceptions is provided in a study by PA Consulting (2014). This survey study was conducted in conjunction with the UK police’s National Analyst Working Group (NAWG), and examined the response to cybercrime. It surveyed police intelligence analysts and researchers from 48 law enforcement organisations, notes that around 15 percent of the 1,500 NAWG members (so around 225 people) responded to the survey. According to the findings, police analysts forecast that the time they spend on cybercrime will treble over the next three years, yet only 30% believe they have the skills and tools to do the job effectively. Other findings from the survey included that:

- 57 percent of analysts think cybercrime is increasing significantly;
- 74 percent of analysts have cybercrime as part of their current role but they only spend 10 percent of their time on cyber-related analysis.

From this review of literature I have identified what appear to be gaps in the evidence base which my research project will address. There appears to be a need for more evidence on the nature and scale of
cybercrime and how this is impacting on demand for the police, which I will examine through a review of police records and a survey of mainstream police officers and staff. Whilst it seems that the use of online technology is becoming more prevalent in traditional criminality, and given a perceived requirement to mainstream cyber across the police, there seems to be limited evidence on the perceptions and attitudes of mainstream police officers and staff on their role in responding to cybercrime. This I will explore through a survey of mainstream police officers and staff. I have also identified some debate around how the term cybercrime is used and how useful it is to specifically define criminal activity in terms of cyber. Therefore, my research will explore how mainstream police officers and staff understand the definition of cybercrime, their experiences in using and encountering the term.
Research Methodology

In the following section I will illustrate the methodological approach I have taken in carrying out this project. I will also present the reader with a descriptive explanation of the research methodology I employed to gather data to inform the study.

My research project can be described as exploratory since my objectives aim to: scope out the magnitude or extent of a particular phenomenon, problem, or behaviour; and generate some initial ideas (or ‘hunches’) about that phenomenon (Bhattacherjee, 2012).

Research can be distinguished as being either inductive or deductive (Bhattacherjee 2012). By using an inductive approach, a researcher aims to infer theoretical concepts and patterns from observed data. However, research using a deductive approach seeks to use new data to test concepts and patterns that are already known from existing theory. In this sense, inductive research can be seen as ‘theory-building’ and deductive research as ‘theory-testing’.

My project does not propose to test a particular research hypothesis, and my objectives are purely exploratory in nature. Therefore, my research project takes an inductive, theory-building approach rather than a deductive one.

An inductive approach is often associated with qualitative research methods, whereas a deductive approach is most commonly associated with quantitative methods. However, this apparent quantitative versus qualitative dichotomy is not clearly defined and is unhelpful in many instances because it excludes potentially useful approaches (Welch and Wood, 2010).

In addition, it has been claimed that the ‘crude’ quantitative-qualitative dichotomy ignores many useful methodological possibilities and that: “types of research methods are more diverse than is often assumed, and that the terms ‘quantitative’ and ‘qualitative’ are best avoided” (Welch and Wood, 2010:
56). This seems to be supported elsewhere, where it is argued: “methods should be our servants, not our rulers. Methods are properly used as tools when they are needed”. (Silverman 2013: 11)

With this in mind, my research project primarily takes, what has been described as a statistical induction approach (Welch and Wood, 2010). This approach it is said, appears to be both quantitative because it is statistical, using quantitative measurable data, but qualitative also, because it is inductive.

To collect data from police officers and staff I used a survey questionnaire. Again, sensitive to the idea of using a ‘quantitative’ questionnaire survey to undertake ‘qualitative’ inductive research, I am conscious it has been claimed that questionnaires are not the most prominent tool used in qualitative research, because participants are required to respond to a stimulus (Woods, 2006). However, this same source also notes that they have their uses, especially as a means of collecting information from a wider sample than can be reached by face-to-face interview. A questionnaire, the source argues, may be the first tool used and then followed up by other techniques to gather richer data on a sample to explore issues in the replies.

I elected to use a survey questionnaire approach owing to the inherent strengths of the method, as noted by Bhattacherjee (2012). In summary survey questionnaires are described as:

- An excellent vehicle for measuring unobservable data, such as people’s preferences and attitudes;
- Ideally suited for remotely collecting data about a population that is too large to observe directly.
- Preferable to some respondents owing to their unobtrusive nature;
- Economical in terms of researcher time, effort and cost.

The majority of the questions within the survey were structured in order to gather quantifiable data through the use of interval-level responses, which could be analysed statistically. I developed a series of 5-point Likert style response scales, where respondents were asked to express the extent to which they agreed or disagreed with a statement presented to them.
I elected to use an odd number of values in the interval scale, because “it is important to use an odd number of values to allow for a “neutral” (or “neither agree nor disagree”) anchor” (Bhattacherjee 2012: 48). This is important in that it acknowledges some respondents may indeed have a neutral stance and does not force them to agree or disagree.

I also used two structured, continuous response questions to explore respondents’ experience of the number of crimes/ incidents they dealt with and the amount of time this took. I used continuous (ratio-scaled) values to do this as they have a meaningful zero point, and it was entirely possible that for some respondents, this would be a true reflection of their experience.

At the end of the survey I included an open, unstructured question to obtain an insight into how, in the participants own words, they defined cybercrime.

Prior to this, in other questions exploring respondents experience of crimes and incidents (e.g. in terms of frequency, nature, scale etc.) I purposefully avoided using the term cybercrime. This was because in my literature review, I identified an apparent debate around how the term is used. So, instead I asked about people’s experiences of crimes and incidents that were “the result of the way that someone has behaved on the internet”.

In constructing a survey questionnaire it is important to give careful consideration to question content and wording, question sequencing and other ‘golden’ rules such as keeping surveys as short as possible, with longer surveys lowering response rates (Bhattacherjee, 2012). Therefore, the survey questions underwent several re-writes and edits until a final version, taking only five minutes to complete, was reached (an example of the final questionnaire survey can be found at Appendix A).

Bhattacherjee notes that it is always advisable to pre-test a questionnaire with at least a convenience sample before administering it to respondents in a field testing. Therefore, as part of the drafting
process, a pilot group of respondents was used to identify ambiguity, lack of clarity and biases in wording which were removed. Some examples of changes made were as follows:

- Reframing the introductory information for participants, with a view to encouraging participation, by emphasising the potential benefits of the study for the organisation and its staff;

- Re-ordering questions so that they flowed in a more logical order in the eyes of respondents;

- To remove the potential for unintended bias by asking participants to state the extent to which the agreed or disagreed with statements presented to them (rather than the extent to which they agreed – which some may have interpreted as a direction towards agreeing).

The survey was self-administered and was delivered to respondents in an online (Surveymonkey) format. The benefit of this format is that it is very inexpensive to administer and the results are instantly recorded in an online database.

To support the online survey, a self-administered mail version (through GMP’s internal mail service) of the survey was also made available to respondents as it became clear that in some roles this was more preferable (with access to a computer not being convenient for all).

Therefore, I used what Bhattacherjee describes as a ‘dual-media survey’, with all respondents completing the survey between 28 November and 12 December 2014.

My literature review highlighted the aim of the UK Cyber Security Strategy to mainstream cyber awareness, capacity and capabilities throughout their service. Therefore, my survey was aimed at respondents who I considered performed ‘mainstream’ policing roles. So, my survey was not targeted at officers and staff in specialist police functions, for example in roles dealing in computer forensics, tackling serious organised crime, economic crime, public protection issues, and counter terrorism.

Instead my survey was aimed at officers and staff in neighbourhood policing teams and response units who are likely to encounter a wide variety of policing problems through their work. Respondents from these roles were targeted on two of GMP’s eleven divisional areas.
I also targeted my survey at crime desk and local resolution officers, who on a daily basis deal with a variety of crimes and incidents from across the spectrum. Respondents from these roles were targeted across all of GMP’s divisional areas. I employed a non-probability, ‘purposive sampling’ approach as my survey was aimed at particular units “based on specific purposes associated” (Teddlie and Yu 2007: 77).

The survey was sent directly to respondents in crime desk and local resolution officer roles. However, in order to reach officers and staff working in neighbourhood policing and response, I used a snowball sampling approach. Using the approach described by Bhattacherjee, I began by identifying a few respondents that matched the criteria for inclusion in the project, and then asked that the survey be promulgated to officers and staff who met the same criteria.

To support my research project, crime and hate incident data was also obtained from GMP’s records using the forces own Business Intelligence System (BIS). A full account of the method used to obtain data from BIS and the caveats applied to it can be found at Appendix B.

In summary, a full twelve months worth of data was examined. This included crimes (which included ‘no crimes’) and hate incidents recorded between 1st January and 31st December 2014. Whilst hate incidents and no crimes do not constitute valid crimes for police counting purposes, they were included in this data, as they will still provide an indication of policing activity (e.g. 'no crimes' may have required an investigation to be conducted or other activity to be undertaken).

It is not possible to use GMP’s data systems to make an exact count of crimes/ incidents relating to online behaviour, or which may be deemed ‘cybercrimes’. Therefore, the data obtained for this project was filtered using various selection criteria that were coded into an Excel spreadsheet, where the data was stored and examined. Filtering took account of factors such as crime/ incident type and a variety of keywords that were used at the time the data was input (see Appendix B).
In preparing this project, I was conscious of the need to ensure my approach considered ethical issues that may impact upon the research and its participants. So, to ensure confidentiality, no personal data that could be used to identify victims, offenders or police personnel was purposefully extracted from GMP’s crime and incident records. It is acknowledged that in extracting free text data there may be some reference to names and locations. However, this will not be used as part of the research.

All participants in the research survey questionnaire gave informed consent and were asked to volunteer their responses freely. Whilst information to identify respondents was sought (e.g. personal identification numbers), this was only to be used as a means of contact. Such information was treated with strict confidentiality and there is no reference to identify individual's responses within this paper. Personal data will only ever be used by the researcher to conduct follow-up enquiries with respondents. Finally, to ensure security, all crime data collected during this project was stored and accessed from GMP’s internal, secure IT network only.

Within this section I have described that my study is exploratory in nature and as such I do not propose an experimental hypothesis to test. I have also explained that I will use a mixture of qualitative and quantitative methods to gather data in order to explore my research objectives. I will now proceed to present my research findings and analysis.
Findings and Analysis

In this section I outline my findings from the recorded crime data obtained from GMP’s Business Intelligence System. I then present a descriptive analysis of my survey findings followed by the findings from statistical tests performed upon the data.

Findings from data retrieved from GMP Business Intelligence system

A search of GMP’s Business Intelligence system showed that between 1st January and 31st December 2014, there were 201,897 crimes and hate incidents recorded. This count excludes those records which were ‘No crimes – entered in error’ and ‘Stats continuous records’ (the latter here referring to duplicate records used to record additional information on an existing crime).

Included however, were records shown as ‘No crime – no offence’ and ‘No crime – outside GMP’ and crimes where the ‘non-counting’ flag was present (this relates to fraud crimes which are reported to the national Action Fraud service and do not feature in local GMP crime reporting). These crimes were included as the fact they are recorded on GMP’s system demonstrates some demand upon GMP resources to at least make the record and perhaps to have undertaken enquiries to determine that no offence occurred or to determine the location.

Of these 201,897 records, it was found that 4,309 (2.13%) met the pre-determined criteria (see Appendix B) for potentially indicating a crime was linked to online behaviour. However, whilst it is possible that this may have excluded some online behaviour related crimes from the count, it was perhaps more likely that some were included when they should not have been – as a result of keywords present in the crime record text being used in a context other than to describe online crime.

With this in mind, the crime records were reassessed. A manual review was undertaken of those records where I believed it was highly likely they had been returned because the keyword was present in a context other than online related behaviour (e.g. the high potential for records containing the term
‘computer’ to be returned when in fact the computer had been the target of a theft or damage). Where the number of records returned for a keyword was more than 30, I chose 30 records to sample determine whether the crimes were related to online behaviour. Where there were less than 30, all records were reviewed.

Following this reassessment of the crime records I decided to remove further records from the count. For example, dip-sampling of keywords ‘computer’, ‘laptop’, ‘hard drive’ appeared to be consistently occurring only because these had been the targets of an acquisitive crime. With this in mind all records related to these keywords were removed. Checking other smaller record groups led to the removal of records relating to the keywords ‘delete’, ‘password’, ‘software’, ‘database’, server’, ‘MSN’, and ‘LinkedIn’, as these did not appear to relate to cybercrimes. Records where a computer was shown as a weapon in the crime were also discounted after review, as these crimes were related to physical assaults rather than cyber attacks.

The remaining records were then separated according to their offence type as per level 4 of ‘Crime Tree’ (Her Majesty’s Inspectorate of Constabulary, no date). They were then scrutinised using the same sampling and review approach as before. This lead to the removal of all records relating to ‘criminal damage & arson’, ‘possession of drugs’, ‘possession of weapon’, ‘burglary in a dwelling’, ‘burglary in a building other than a dwelling’, ‘shoplifting’ and ‘bicycle theft’ - as these again did not appear to relate to cybercrimes.

Following these additional layers of manual scrutiny, the number of crimes that appeared to be related to online behaviour reduced to 3,316 (or 1.64% of the total 201,897 crimes and hate incidents). The results and distribution of keywords and offence types is shown in Table 1.
Table 1: Distribution of crime and hate incident records (by keyword and offence type) considered likely to be related to online behaviour, after additional filtering and manual sampling (grey boxes indicate no records)

Whilst I have confidence that after, filtering and manual adjustment, the majority of the records referred to in Table 1 are indeed related to online behaviour, I am not particularly confident in the records for ‘All other theft’ and ‘Violence with injury’. Sampling the records for the former suggests that whilst many do indeed relate to online behaviour (e.g. theft committed using the internet, or stolen property from a theft being sold via an online auction website) there are also many which do not.
In terms of ‘Violence with injury’, it appears that many of the offences in this category are in some way the result of disagreements or comments made online, which have spilled over into real-world violence. Whilst this may be interesting in perhaps demonstrating the potential for social media networks to provide an environment to facilitate online disagreements which may culminate in real-world violence, it would perhaps be stretching the definition too far to consider such violence as ‘cyber-enabled’.

Of those categories that I have more confidence in, some clear themes emerge. Fraud with 1,120 records (33.8% of the 3,316 records relating to online behaviour), is the largest category. However, almost all of these carried the ‘non-reporting’ crime flag. Fraud is closely followed by ‘Violence without injury’ with 901 records (27.1% of records relating to online behaviour). In the case of the latter, it appears that many of the records relate to offences of harassment, threats made online, or instances where offenders have breached orders (such as restraining orders) by contacting victims through social media.

The next largest category is ‘Miscellaneous Crimes Against Society’, with 292 records. Most of these (202) had a sexual element in that the offences involved taking/ possessing indecent images of children. The next largest category which is for records relating to ‘Other sexual offences’ (238). Combined with records of ‘Rape’ (49), this means that there were 489 cases in the sample which may relate to offences of a sexual nature (14.8% of records relating to online behaviour).

After sexual offences, ‘Hate incidents’ (154) and ‘Public order offences’ (129) are the next largest categories. For both categories it appears that many offences occur as a result of offenders contacting victims through social media. In cases of ‘Public order offences,’ it also seems that, as with the ‘Violence with injury’ category, some may be offences that have occurred in the real world as a result of disagreements or comments made online.

Figure 4 shows, in graphical form, the distribution of the final groupings, with those offence types for which I have less confidence in the returns for (‘All other theft’ and ‘Violence with injury’) being excluded.
Figure 4: Distribution of BI crime and hate incident records (by offence type) considered likely to be related to online behaviour, after additional filtering and manual sampling (excluding ‘All other theft’ and ‘Violence with injury’)

*Includes 202 crimes with a sexual motivation relating to indecent images
Descriptive findings from survey data

In total there were 106 respondents to my survey. Table 2 shows the distribution of respondents by their reported role in GMP.

**Table 2: Count of survey respondents by their reported role at GMP**

<table>
<thead>
<tr>
<th>Respondent reported roles</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbourhood Police Officer</td>
<td>24</td>
<td>22.64</td>
</tr>
<tr>
<td>Response Police Officer</td>
<td>23</td>
<td>21.70</td>
</tr>
<tr>
<td>Local Resolution Officer (LRO)</td>
<td>13</td>
<td>12.26</td>
</tr>
<tr>
<td>Crime Evaluator/ Crime Desk</td>
<td>10</td>
<td>9.43</td>
</tr>
<tr>
<td>Police Community Support Officer (PCSO)</td>
<td>10</td>
<td>9.43</td>
</tr>
<tr>
<td>Detective</td>
<td>8</td>
<td>7.55</td>
</tr>
<tr>
<td>Operational Support Officer (OSO)</td>
<td>6</td>
<td>5.66</td>
</tr>
<tr>
<td>Customer Service Desk (CSD)</td>
<td>4</td>
<td>3.77</td>
</tr>
<tr>
<td>Currently on ‘operational attachment’</td>
<td>1</td>
<td>0.94</td>
</tr>
<tr>
<td>Administrative Support</td>
<td>1</td>
<td>0.94</td>
</tr>
<tr>
<td>Not stated</td>
<td>6</td>
<td>5.66</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>106</td>
<td>100</td>
</tr>
</tbody>
</table>

Almost half of respondents were either Neighbourhood Police Officers (n=24, 22.64%) or Response Police Officers (m=23, 21.70%). But, as the data shows, a variety of mainstream roles were represented. Six respondents (5.66%) did not provide details of their role.

Unfortunately I was unable to survey call takers (staff who receive reports of crimes and incidents directly from the public) owing to the survey being conducted at a particularly busy time for GMP’s Operational Communication Branch. This meant that staff in the Branch could not be allocated time to complete the survey.

The distribution of respondents by gender, age and length of service are shown in Tables 3 to 5. Table 3 shows the distribution of respondents by gender, whilst Table 4 shows length of service. These show
that respondents were largely male (n=67, 63.21%), aged under 45 years (n=75, 70.76%) and had six or more years service with GMP (n=82, 77.36%).

**Table 3: Distribution of survey respondents by gender**

<table>
<thead>
<tr>
<th>Respondent gender</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>38</td>
<td>35.85</td>
</tr>
<tr>
<td>Male</td>
<td>67</td>
<td>63.21</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>1</td>
<td>0.94</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>106</td>
<td>100</td>
</tr>
</tbody>
</table>

**Table 4: Distribution of survey respondents by age**

<table>
<thead>
<tr>
<th>Respondent age</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-24</td>
<td>5</td>
<td>4.72</td>
</tr>
<tr>
<td>25-34</td>
<td>37</td>
<td>34.91</td>
</tr>
<tr>
<td>35-44</td>
<td>33</td>
<td>31.13</td>
</tr>
<tr>
<td>45-54</td>
<td>24</td>
<td>22.64</td>
</tr>
<tr>
<td>55-65</td>
<td>4</td>
<td>3.77</td>
</tr>
<tr>
<td>Over 65</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>3</td>
<td>2.83</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>106</td>
<td>100</td>
</tr>
</tbody>
</table>

**Table 5: Distribution of survey respondents by length of service with GMP**

<table>
<thead>
<tr>
<th>Respondent length of service</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than one year</td>
<td>6</td>
<td>5.66</td>
</tr>
<tr>
<td>One to five years</td>
<td>17</td>
<td>16.04</td>
</tr>
<tr>
<td>Six to ten years</td>
<td>35</td>
<td>33.02</td>
</tr>
<tr>
<td>More than ten years</td>
<td>47</td>
<td>44.34</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>1</td>
<td>0.94</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>106</td>
<td>100</td>
</tr>
</tbody>
</table>
It should be noted that after the initial demographic questions, 18 (16.98%) respondents did not complete any of the other questions in the survey. There does not appear to be any commonality to suggest why these respondents chose not to provide further information. For example, Table 6 shows that these respondents were from a variety of roles, suggesting that role was not a factor in why participants did not respond.

Table 6: Count of respondents (by role) who provided demographic information only

<table>
<thead>
<tr>
<th>Respondent role</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbourhood Police Officer</td>
<td>5</td>
</tr>
<tr>
<td>Crime Evaluator/ Crime Desk</td>
<td>5</td>
</tr>
<tr>
<td>Other (role not stated)</td>
<td>3</td>
</tr>
<tr>
<td>Detective</td>
<td>2</td>
</tr>
<tr>
<td>On operational attachment</td>
<td>1</td>
</tr>
<tr>
<td>Local Resolution Officer</td>
<td>1</td>
</tr>
<tr>
<td>Operational Support Officer</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>18</strong></td>
</tr>
</tbody>
</table>

Findings for survey question 5: “In an average week how many times do you deal with incidents and crimes that are the result of the way someone has behaved on the internet?”

88 (83.01%) respondents answered the question “In an average week how many times do you deal with incidents and crimes that are the result of the way someone has behaved on the internet?” The distribution of responses is shown in Figure 5.
It can be seen from Figure 5 that the data is skewed. It is noted that: "When you have skewed data you should report non-parametric descriptive statistics which do not assume a normal distribution," (Pallant, 2013: 60), including the median. These are shown in Table 7.

**Table 7: Non-parametric descriptive statistics for frequency distribution described in Figure 5**

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>4.57</td>
</tr>
<tr>
<td>Mode</td>
<td>1.00</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>1.50</td>
</tr>
<tr>
<td>Median</td>
<td>5.81</td>
</tr>
<tr>
<td>Skewness</td>
<td>1.69</td>
</tr>
<tr>
<td>Quartile 1 (25th Percentile)</td>
<td>1.00</td>
</tr>
<tr>
<td>Quartile 3 (75th Percentile)</td>
<td>7.25</td>
</tr>
<tr>
<td>Interquartile range</td>
<td>6.25</td>
</tr>
</tbody>
</table>
The mode value (1.00) shows that the data is skewed to the lower frequency of occurrence. Indeed, 43 (48.86%) of respondents reported dealing with 0 to 1 crimes or incidents in an average week. However, the median is 5.81, and 33 (37.50%) – over a third – of respondents to this question said that they dealt with incidents and crimes that are the result of the way someone has behaved on the internet 5 or more times in an average week. Or, cutting the data another way, 21 (23.86%) – over a fifth – of respondents reported the frequency as 10 or more times per week.

Findings for survey question 6: “On average, what percentage of your total working week do you spend dealing with incidents and crimes that are the result of the way someone has behaved on the internet?”

87 (82.08%) respondents answered the question “On average, what percentage of your total working week do you spend dealing with incidents and crimes that are the result of the way someone has behaved on the internet?” The distribution of responses is shown in Figure 6.

*Figure 6: Frequency distribution of participant responses to the survey question 6*
Again the data here is skewed, with many respondents reporting scores at the lower end of the scale. Non-parametric descriptive statistics of the frequency distribution are shown in Table 8.

**Table 8: Non-parametric descriptive statistics for frequency distribution described in Figure 6**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>9.38</td>
</tr>
<tr>
<td>Mode</td>
<td>10.00</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>5.00</td>
</tr>
<tr>
<td>Median</td>
<td>11.85</td>
</tr>
<tr>
<td>Skewness</td>
<td>2.95</td>
</tr>
<tr>
<td>Quartile 1 (25th Percentile)</td>
<td>11.00</td>
</tr>
<tr>
<td>Quartile 3 (75th Percentile)</td>
<td>1.00</td>
</tr>
<tr>
<td>Interquartile range</td>
<td>10.00</td>
</tr>
</tbody>
</table>

Respondents reported spending a median of 11.85% of their time in an average week dealing with incidents and crimes that are the result of the way someone has behaved on the internet. Indeed, 37 (42.53%) of respondents to this question reported 10% or more of their time was spent on this.

**Findings for question 7 in relation to the types of incidents and crimes dealt with**

Participants were presented with a series of seven different types of crimes and incidents resulting from behaviour on the internet, and were asked to rate on a scale how often they dealt with them (very frequently, frequently, occasionally, rarely, never). 88 respondents gave ratings for five of the series, whilst 87 rated the remaining two (‘Offences related to indecent images of children on the internet’ and ‘Online abuse (e.g. bullying, harassment, stalking)’). The respondents' ratings are shown in Figure 7.
Respondents to this question rated ‘Online abuse’ as the type of incident or crime they dealt with most frequently, with 37 respondents (42.53%) saying they dealt with this at least frequently. 62 respondents (71.26%) said they dealt with this at least occasionally (this includes those who answered ‘frequently’ or ‘very frequently’). The next most frequently dealt with offences were ‘Online fraud’ (53 respondents, or 60.23% reporting at least occasionally) and ‘Sexual offences and grooming’ (44 respondents, or 50.00% reporting at least occasionally).
Findings for question 8: Respondents perceptions on increasing crime and incidents; their knowledge and skills; and support available

88 (83.01%) respondents recorded their level of agreement with a series of statements (shown in Figure 8), rating either ‘Strongly agree’, ‘Agree’, ‘Neutral’, ‘Disagree’, or ‘Strongly disagree’.

Figure 8: Respondents’ expressions of agreement/ disagreement in response to statements presented in survey question 8

57 respondents (64.77%) expressed agreement with the statement “The amount of time I spend dealing with incidents and crimes that are the result of the way someone has behaved on the internet is increasing”. 19 (21.59%) remained neutral on this. 12 (13.64%) respondents expressed disagreement with the statement.
18 respondents (20.45%) agreed with the statement “I have the knowledge and skills needed to deal with the incidents and crimes I encounter, which are the result of internet behaviour”. 37 (42.0%) expressed disagreement, whilst 33 (37.50%) were neutral.

Meanwhile, 19 (21.59%) agreed with the statement “Should I need it, support and training is available to assist me in dealing with crimes resulting from people’s internet behaviour”. 38 (43.18%) expressed disagreement, whilst 31 (35.23%) remained neutral.

Findings for question 9: Respondents’ perceptions relating to roles and responsibility for dealing with incidents and crimes resulting from online behaviour

85 (80.19%) respondents recorded their level of agreement with a series of statements (shown in Figure 9), rating either ‘Strongly agree’, ‘Agree’, ‘Neutral’, ‘Disagree’, or ‘Strongly disagree’.

*Figure 9: Respondents’ expressions of agreement/disagreement in response to statements presented in survey question 9*
21 (24.71%) respondents to this question expressed agreement with the statement “In my current role I should be dealing with incidents and crimes which are the result of the way someone has behaved on the internet”. 29 (34.12%) respondents disagreed, whilst 35 (41.18%) remained neutral.

Meanwhile, 44 (51.76%) respondents expressed agreement with the statement “Crimes and incidents resulting from internet behaviour should only be dealt with by specialist units who are trained to investigate them”. 17 (20.00%) of respondents expressed disagreement and 24 (28.24%) remained neutral.

There was less agreement with the statement that “Crimes and incidents resulting from online behaviour should only be investigated by regional and/or national law enforcement agencies”. 19 (22.35%) respondents expressed agreement, 26 (30.59%) expressed disagreement, with 40 (47.06%) remaining neutral.

Findings for questions 10 and 11: Respondents perceptions on the use of the term ‘cyber’ to describe crimes and incidents
Participants were asked to rate the frequency (very frequently, frequently, occasionally, rarely, never) with which they (question 10) and other people (question 11) used the term ‘cyber’ to describe crimes or incidents. 82 (77.36%) respondents gave ratings for both questions. The results are shown in Figure 10.
9 (10.98%) respondents reported using the term ‘cyber’ at least regularly and 18 (21.95%) reported using the term occasionally. 55 (67.07%) respondents reported rarely/never using the term.

The results for experience of the term being used by other people were similar. 8 (9.76%) respondents encountered other people using the term ‘cyber’ at least regularly, with 21 (25.61%) reporting this happened occasionally. Meanwhile, 53 (64.63%) respondents reported rarely/never encountering others using the term.
Findings for questions 12 and 13: Respondents understanding of the term ‘cybercrime’

81 (76.42%) respondents recorded their level of agreement/disagreement (‘Strongly agree’, ‘Agree’, ‘Neutral’, ‘Disagree’, or ‘Strongly disagree’) with the statement “I am clear about the definition of cybercrime”. The results are shown in Figure 11.

Figure 11: Respondents’ expressions of agreement/disagreement with the statement “I am clear about the definition of cybercrime”

21 (25.93%) respondents expressed a level of agreement (agree/strongly agree) with the statement. Meanwhile, 37 (45.68%) respondents reported a level of disagreement (disagree/strongly disagree) and 23 (28.40%) remained neutral.

Question 13 enabled participants to provide a free text description of how they would describe to someone else what a cybercrime is. 62 (58.49%) respondents gave their descriptions (one of these included a Response Police Officer who stated, “No idea”). Reviewing these showed that 53 (85.48%) described a general use of the internet or digital/computer technology to commit crime, with little specificity around the nature of the crime or its impact. Illustrative examples of these statements are presented in Figure 12.
Meanwhile, the remaining eight respondents expanded their definitions somewhat, to include reference to particular offence types and the impact upon victims. A common factor across the majority of these was the potential for ‘cybercrime’ to be linked in some way to harassment or some form of intimidation. The eight definitions are shown in Figure 13.

Figure 12: Examples of descriptions of cybercrime as general use of the internet or digital/computer technology to commit crime

- “A crime using the internet in any way” (Response Officer)
- “Internet/ computer based crime” (Crime Desk/ Evaluator)
- “Any crime using the internet or computer tech etc” (Response Officer)
- “Crime online” (Neighbourhood Police Officer)
- “Crime via the internet” (Response Officer)
- “Use of computers or the internet to commit an offence” (Neighbourhood Police Officer)
- “Offences taking place online through use of a computer or online device” (Response Police Officer)
- “Crime committed using, or on, the internet/ computer systems” (Detective)
- “Its [sic] a crime that has been committed [sic] using the internet or other computer software.” (Police Community Support Officer)
- “Crime over the internet” (Operational Support Officer)
It should be noted that 44 (41.51%) of respondents did not complete question 13. As with other missing values, there does not appear to be a common factor across the non-respondents and again they were from a variety of roles (see Table 9).

**Table 9: Count of respondents (by role) who did not state how they would describe to someone what a cybercrime is**

<table>
<thead>
<tr>
<th>Respondent role</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Police Officer</td>
<td>5</td>
</tr>
<tr>
<td>Operational Support Officer</td>
<td>4</td>
</tr>
<tr>
<td>Local Resolution Officer</td>
<td>3</td>
</tr>
<tr>
<td>Neighbourhood Police Officer</td>
<td>11</td>
</tr>
<tr>
<td>Crime Evaluator/ Crime Desk</td>
<td>7</td>
</tr>
<tr>
<td>Police Community Support Officer</td>
<td>4</td>
</tr>
<tr>
<td>Administration Support</td>
<td>1</td>
</tr>
<tr>
<td>Detective</td>
<td>2</td>
</tr>
<tr>
<td>Currently on 'operational attachment'</td>
<td>1</td>
</tr>
<tr>
<td>Not stated</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>18</strong></td>
</tr>
</tbody>
</table>
**Statistical analysis of survey data**

Data gathered from the survey was subject to statistical analysis using SPSS software. Non-parametric tests were used as the data did not fit the conditions for parametric tests. For example, the data did not follow a normal distribution, and the sampling method was not random [Pallant: 2013].

A Mann-Whitney U test revealed a significant difference in the percentage of the total working week spent dealing with incidents and crimes that are the result of the way someone has behaved on the internet for those who agreed (median = 10, n = 20) and those who disagreed (median = 5, n = 37) with the question "to what extent do you agree or disagree with the statement 'I am clear what the definition of cybercrime is'?" [U = 250.500 z = -2.018 p = 0.044 r = -2.018/ SQRT(57) = -0.26 (small effect size)]. This was the case when neutral responses to the statement were excluded from the analysis. However, when neutral responses were included in the disagree category there was no significant difference.

A Chi-squared test revealed that there was no significant difference between respondents' length of service (test undertaken between two groups – those with 0-5 years service and those with 5 or more years) and how much they agreed/disagreed that they were clear on the definition of cybercrime. This was the case when neutral responses to the statement on the definition of cybercrime were both included (as describing non-agreement) and were excluded.

The data appears to show that those respondents with longer service tend to report dealing deal with more crimes and incidents that are the result of the way someone has behaved online. A Mann-Whitney U test revealed a significant difference in the average number of crimes and incidents dealt with in the total working week that are the result of the way someone has behaved on the internet for those with 0-5 years’ service (median = 1, n = 21) and those with more than 5 years’ service (median = 3, n = 67) [U = 463.500 z = -2.399 p = 0.016 r = -2.399/ SQRT(88) = -0.26 (small effect size)].
Chi-squared tests were used to examine whether there was an association between respondents’ length of service (again two groups, 0-5 years’ service and those with 5 or more years) and their agreement that:

- they had the knowledge and skills to deal with the crimes and incidents resulting from online behaviour that they encounter; and
- support and training is available to assist them in dealing with crimes resulting from people’s internet behaviour.

However, no evidence of an association was found.

A further series of Chi-squared tests were undertaken to test whether there was an association between the degree to which respondents agreed that they were clear on the definition of cybercrime, and the frequency they reported dealing with the various types of crimes and incidents resulting from behaviour on the internet (as described in Figure 7). No evidence of an association was found.

Chi-squared tests were also used to test whether there was an association between respondents’ length of service (test undertaken between two groups – those with 0-5 years’ service and those with 5 or more years) and the frequency with which they reported using the term cyber to describe crimes and incidents they deal with. However, there was no evidence of a significant difference in frequency between the two groups. The same result was found when testing the frequency with which respondents encountered others using the term cyber.

However, a Chi-square test for independence (with Yates Continuity Correction) indicated a significant association between use of the term 'cyber' to describe crimes or incidents and agreement with the statement 'to what extent do you agree or disagree with the statement 'I am clear what the definition of cybercrime is' Chi-square [(1, n = 58) = 4.442, p = 0.035, phi = -0.315 (medium effect size)]. This was the case when neutral responses to the statement were excluded. However, when these were included (as a statement of non-agreement) no association was found.
A Chi-square test for independence (with Yates Continuity Correction) also indicated a significant association between encountering others using the term 'cyber' to describe crimes or incidents and agreement with the statement 'to what extent do you agree or disagree with the statement 'I am clear what the definition of cybercrime is' Chi-square [(1, n = 58) = 4.907, p = 0.027, phi = -0.328 (medium effect size)]. Whilst this was true when neutral responses were excluded, a significant association was also found when neutral responses were included as statements of non-agreement [Chi-square (1, n = 81) = 4.434, p = 0.035, phi = 0.263 (small effect size)].

**Research limitations**

The findings and analysis I have described should be considered alongside the limitations of the research and the methodology I have employed. There were limitations with the approach I used to extract and analyse data from GMP’s Business Intelligence system. For example, the keywords used in the search criteria are subjective (other researchers may have chosen to include/exclude some or others) and whilst I have tried to keep the approach to sampling and refining the records returned consistent, here too I have made subjective decisions regarding including and excluding records from the sample. Therefore, I do not feel confident that this analysis necessarily presents a completely accurate picture of the demand experienced by GMP from crime related to online behaviour. However, given that my research is exploratory, I have succeeded in establishing a starting point for further research to build upon. This data may also be affected by the potential for “under-reporting of cybercrime” (Dowling and McGuire, 2013: p14).

The fact I chose to use a survey questionnaire approach to gather responses from officers and staff also has limitations. This approach has some unique disadvantages including: non-response bias, sampling bias, social desirability bias, and recall bias (Bhattacherjee 2012). So, these limitations may explain why 18 survey respondents provided no more information other than demographics. Whilst I have acknowledged that my sample was not random and that particular groups of officers and staff were targeted, the nature of the survey approach will only capture the views of those who choose to respond,
potentially leading to under-coverage even amongst the selected groups. There are further limitations in that respondents may have felt the need to provide answers which they felt were socially desirable and would have had opportunity to discuss their responses with colleagues. This opportunity to discuss with colleagues and given that respondents were being asked to reflect on previous events could also have meant that their responses were not always accurate.
In beginning this discussion on my research findings, I need to reiterate that in scoping, developing and undertaking the project, I envisaged the work as a purely exploratory piece and not one which sought to provide evidence in support, or otherwise, of a hypothesis I proposed. After I completed my initial literature review and conducted my research and analysis, the first national police demand analysis report (College of Policing 2015) was published.

This demand analysis presents a national picture of the scale and complexity of police work, but acknowledged that there is limited data available to provide robust estimates of emerging crime problems, such as cyber-enabled crime. However, in the absence of estimates on the scale of demand, instead the College presents a series of hypotheses. These propose that whilst such crimes are increasing in volume, they are coming to the attention of the police in low numbers compared with ‘conventional crime’. They also propose that many such crimes are associated with vulnerability, public protection and safeguarding and will require more policing resources as they are generally more complex to investigate.

Whilst I did not formulate my own hypothesis for my exploratory research, those presented by the College of Policing will be referred to alongside my discussion on the findings made against my research offers a framework around which to discuss some of my research objectives. To reiterate briefly, these were:

1. Outline the extent to which online behaviour leads to demand on GMP;
2. Capture the perception of police officers and staff on the scale and nature of service demand;
3. Capture the perception that police officers and staff have of their role in servicing demand resulting from online behaviour;
4. Contribute to discussions on the use of the term ‘cyber’ in describing particular forms of internet behaviour and the implications that this may have for policing.
My findings from GMP data suggest that only around 1.6% of the records in the 201,897 contained in the sample, appeared to be related to online behaviour, and in some way 'cyber-enabled'. This appears to support the College of Policing hypothesis that emerging crimes, such as cyber-enabled crime, are coming to the attention of the police in low numbers compared with conventional crime.

Perhaps unsurprisingly, of the records I examined, I found that the largest single group of crimes were for fraud with these accounting for 34% of the records. The next largest category was ‘violence without injury’ (these were crimes such as harassment), which accounted for 27%. However, if to the later were added the crimes recorded as public order (examples being where offenders had broken a restraining order and contacted victims online) and hate incidents, then around 36% of the records seemed to involve some kind of online harassment or abuse – and accounted for a slightly higher proportion of the records than fraud did. Also, among the records returned, around 15% of the sample related to crimes that had a sexual element.

Together, this seems support the College of Policing hypothesis that many emerging crimes such as cyber-enabled crime, are associated with vulnerability, public protection and safeguarding and will require more policing resources as they are generally more complex to investigate.

In terms of patent, apparent demand then, it would seem that crime resulting from online behaviour forms only a small fraction of that falling upon GMP and its resources to respond to, but that within this there is an element of vulnerability and safeguarding. Whilst the sampling methodology and framework I did indeed have limitations, it is perhaps unlikely that any other significantly sizeable chunk of demand from online behaviour exists elsewhere within the records I reviewed.

However, this may not be the complete demand picture. As I have previously noted, it has been suggested that data on the scale of cybercrime may likely be affected by the potential for it to go unreported (e.g. Dowling and McGuire, 2013 and the work of DCC Jon Boutcher, cited by Warrell, 2015). If this is the case, there may well be much demand relating to online behaviour that is as yet latent and
unseen by police and law enforcement. If so, this could present an emerging threat which could lead to an increasing demand upon police resources, and one which GMP and the Police Service would benefit from understanding more accurately, so that the potential impact can be assessed. This would seem especially important in terms of the potential implications for vulnerability and safeguarding.

From the survey I conducted, it appears that on average mainstream officers and staff are dealing with around 6 crimes and incidents a week which are cyber-enabled in their nature. Respondents reported that they also spending on average around 12% of their time in dealing with these. Of the crimes and incidents that they encounter, those they most commonly deal with are related to ‘Online abuse’ (e.g. harassment, bullying, stalking etc), followed by ‘Online fraud’ and ‘Sexual offences and grooming’.

It is instructive, and perhaps reassuring in terms of my research methodology, that these findings appear to reflect those I drew from my analysis of GMP records, and that the survey too seems to support the College of Policing hypotheses that cyber-enabled crime is seen in low numbers compared to conventional crime, but that many are associated with vulnerability, public protection and safeguarding, which are more complex and require more policing resources to investigate.

Also of particular note, from respondents to my survey, was that 65% of them felt that the time they spend dealing with cyber related crimes is increasing. This would seem to reflect findings from other research (PA Consulting, 2014) which found that 57% of law enforcement analysts think cybercrime is increasing significantly. It may also provide some support to the College of Policing hypotheses that cyber-enabled crimes are increasing in volume.

However, it should be noted that the responses to my survey indicate that the amount of time officers and staff amount spend dealing with such crimes and incidents is increasing, and not that they are necessarily seeing an increase in the volume in which they are reported. Whilst this may well be the case, my findings may also reflect a growing complexity in the crimes and incidents relating to online behaviour that officers and staff are dealing.
This again would appear to emphasise the importance for GMP and the wider Police Service to develop a clearer understanding of the potential demand impact from cyber-enabled crime, and the implications this has in terms of vulnerability and safeguarding.

Whilst my research suggests a prevailing perception, among many mainstream police officers and staff, that the amount of time they spend dealing with crimes and incidents resulting from online behaviour is increasing, it is particularly noteworthy that when asked if they felt this is something they should be doing in their current role, only 25% agreed.

Instead, there was more support (52% agreement) for crimes and incidents related to online behaviour being dealt with by specialist units within the police service. My findings here appears to reflect previous research (Bossler and Holt, 2012), which found that officers in the US did not believe that local law enforcement should be primarily responsible for handling cybercrime cases.

If my findings are accurate, in that there is little support among mainstream police officers and staff for having a role in dealing with crimes and incidents resulting from online behaviour, this may present an obstacle to the UK Cyber Security Strategy (Cabinet Office, 2011) objective to mainstream cyber awareness, capacity and capabilities throughout the police service. For example, if mainstream officers and staff still do not believe that they have a role to play, this might limit their interest in and thereby the effectiveness of training being offered and delivered in this area and may ultimately impact upon the service received by victims.

However, my research also found that 41% of respondents were neutral on the subject of them having a role in dealing with crimes and incidents resulting from online behaviour. This seems to suggest that there is a sizeable proportion of mainstream police resources who might be particularly receptive to being ‘nudged’ into understanding that they do indeed have a role to play in this area..
To this end, it may be of import and benefit to the Police Service to consider why some of its mainstream resources may be resistant to accepting that dealing with cyber-enabled crime and incidents are part of their role. Speculating on this, it could be that as police resources continue to be reduced in line with reductions in public spending, mainstream resources view cyber-enabled crime as an additional responsibility being place upon them, in addition to the other tasks they perform.

Alternatively, or perhaps in addition to this, it could be that for many the ‘online world’ is still viewed as something which is separate and different to the ‘real world’, and as such should be treated as something that is different and more specialist from the mainstream. However, such a view does not take into account that online is becoming increasingly ubiquitous and that the lines between it and the real world are becoming increasingly blurred. Also, such a view does not take into account research that suggests traditional crime and criminals appear to migrating to cybercrime.

It may also be the case that there is a perception among mainstream officers and staff that crimes and incidents resulting from online behaviour are of less importance than those committed wholly in the real world, and that they have less impact upon victims. This, alongside my previous speculations, may be an issue which benefits from further research and exploration in order to better understand how issues relating to online vulnerability are identified, assessed and resourced.

As noted in my literature review, it has been suggested that the use of the word ‘cyber’ as a prefix to coin new terms is leading to a wealth of ill-specified and ill-understood vocabulary. In the case of crime and policing, this could have significant implications in relation to the use of the term cybercrime.

My research found that, when asked about their understanding of the term cybercrime, only 26% of survey respondents felt they were clear on the definition, whilst 47% felt they were not clear on what the definition was. Meanwhile, 67% of respondents indicated that they rarely or never use the term ‘cyber’ to describe the crimes and incidents that they deal with, and a similar proportion, 65%, said they never encounter others using the term.
Therefore, from my research it would appear that the term cybercrime is not particularly well understood by mainstream police officers and staff, and that the term is in the main rarely used. This lack of understanding would appear to present GMP with a particular problem in terms of how cyber-enabled crimes are recorded and ultimately how they are measured and the scale of demand understood. In April 2014 GMP introduced a ‘cyber-flag’ indicator which officers and staff must select when recording a crime, if they believe that it is cyber-enabled. If staff are unclear on how to define cybercrime, this could mean that the cyber-flag indicator will not be correctly used meaning that GMP may not have a true picture of demand from cyber-enabled crime.

The apparent lack of understanding of the term cybercrime among mainstream police officers and staff, sits alongside another example of apparently ill-specified and ill-understood cyber-prefixed terminology was highlighted in my literature review. Here I noted conflicting descriptions and interpretations around the term ‘cyberbullying’. For example, whilst some studies on cybercrime (e.g. Dowling and McGuire, 2013) have exclude cyberbullying from their analysis, as bullying is not a crime in law, advice available to the public has indicated that sometimes behaviour described as bullying can indeed be criminal (e.g. Metropolitan Police, online; Safe Network, online).

Whilst this may be part of a dilemma which is wider in scale than the scope of my research paper allows me to address (namely the relationship between bullying and criminality), there is still, it seems, an issue that a lack of clarity about what defines and constitutes cyberbullying, may present an obstacle to the police service developing a better understanding of the scale of demand for policing. This could prove particularly problematic for those analyses which seek to exclude cyberbullying given that these may be excluding crimes of harassment, those involving hate, and those where people are persuaded to perform sexual acts (which are all included in advice to the public as examples of bullying/ cyberbullying). Within such crimes there may be particular issues of vulnerability and safeguarding which analyses could miss.

Perhaps there is need for more discussion and debate on how useful the term cyber is to the Police Service in defining behaviours as cybercrimes or indeed cyberbullying. It may be, as I have previously
suggested, that the term cyber conjures a perception of something separate from the real world and which, as a result of its perceived remoteness, is seen as having less significance in terms of the threat, risk and harm it presents, than other ‘real world threats’.

If I were to continue this research, at the start of a new project I would ensure that the current findings were followed up through interviews and focus groups with survey respondents to further explore their insights. Also, as my findings in relation to the scale and nature of cybercrime are emergent, further research could be undertaken to try and replicate them and determine whether the patterns I have found are consistent across other areas. Furthermore, the data I obtained from GMP systems presents a snapshot of one period in time. Future research could examine whether trends in recorded crime data over time suggest that crimes and incidents resulting from online behaviour are increasing.

Whilst my project focused on experiences of GMP and its personnel, I believe it would be beneficial for future research to explore the experiences and perceptions of victims of online crime. This would seem to be particularly important from the perspective of vulnerability and safeguarding.
Conclusion

In conclusion, my research suggests support for the College of Policing hypotheses that cyber-enabled crime is coming to the attention of the police in low numbers compared with traditional crime, but that it is increasing in volume.

However, there does not appear to be much appetite amongst officers and staff in mainstream policing roles for having a part in dealing with so-called cybercrime. This, it would seem, is problematic given that: an objective of the UK Cyber Security Strategy is to mainstream cyber awareness, capacity and capabilities across the police; analysts expect demand from cybercrime to increase; and indications appear to suggest that the nature of everyday crime is shifting online.

Cybercrime does not appear to be widely talked about nor understood by mainstream police officers and staff, and it may be the case that this is contributing to reasons why confidence in the knowledge and skills to deal with the issue is not widespread among them. It may be the case that the term ‘cybercrime’ conjures up an impression of something that is separate and different to everyday crime – something which is not relevant to mainstream policing, but instead something which only needs to be understood and dealt with by specialists who deal with issues emanating from the online, cyber world.

To some degree, certainly in terms of ‘cyber dependent’ and technically complex crimes this may be correct. However, such a view also misses the fact that as more and more of the real world ‘goes digital’, and as people become increasingly connected and live their lives online, the nature of everyday crime is changing and that, potentially, mainstreaming awareness and capability to deal with this will become increasingly important.

As GMP and the wider Police Service undergoes transformation in the coming years, in line with more austere public spending and with reduced budgets and resources, it will become increasingly important to focus upon areas of demand that present the most significant threat, harm and risk, and where
vulnerability and safeguarding are paramount. So, it will be important to ensure that where crimes are perceived as being ‘cyber’ in nature they are not seen to present less threat, risk or harm simply because they have been conducted through the online medium.

Perhaps there needs to be a change in the discourse to help drive a perception shift among mainstream police resources, towards a recognition that dealing with the cybercrime is not actually a new or additional task being placed upon them, and that it is not the responsibility of ‘cyber-specialist’ resources alone. Maybe we need to drop the term ‘cyber’ and instead highlight that the requirement for mainstream police to deal with crimes and incidents committed through the online world is just a reflection of the fact that the nature of everyday crime is changing, and that their toolkit for dealing with crime needs enhancing to reflect this. Conceivably one day we’ll get back to just talking about crime and policing.
References

http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks


http://www.theguardian.com/technology/2014/dec/05/sony-style-hack-attack-could-hit-anywhere


Europol (2013b) *Europol identifies 3,600 organised crime groups active in the EU* [Online] [Accessed on 23rd May 2014]


Her Majesty’s Inspectorate of Constabulary (2014a) *The Strategic Policing Requirement: An inspection of how police forces in England and Wales deal with threats of a large-scale cyber incident (including criminal attack).* [Online] [Accessed 3rd January 2015]


http://www.cybersec.kent.ac.uk/Survey2.pdf

http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf


https://books.google.co.uk/books?id=e2YCuxBjkq0C&pg=PA20&lpg=PA20&dq=rushkoff++guns+dont+kill+people&source=bl&ots=GVli-rAnK5&sig=ebGv29-ziP3Rrf8hIhxW-EDJzw&hl=en&sa=X&ved=0CDMQ6AEwBmoVChMIrcKh9O3xwiVy-sUCH1_QqR0#v=onepage&q=rushkoff%20%20guns%20%20kill%20people&f=false

Safe (no date) *Bullying and the law*. [Online] [Accessed on 13th March 2015]
http://safe.met.police.uk/bullying/consequences_and_the_law.html

Safe Network (2013) *Helping you understand what cyberbullying is and how it can be prevented*. [Online] [Accessed on 25th May 2014]
http://www.safenetwork.org.uk/help_and_advice/Pages/cyberbullying.aspx

https://books.google.co.uk/books?id=LySjM0tY-tEC&pg=PA7&lpg=PA7&dq=silverman+2013+what+you+can+and+cant+do+with+qualitative&source=bl&ots=kE33lGIEtV&sig=aOGVI96fvO385xI5VN7-EwEM4TU&hl=en&sa=X&ved=0CCUQ6AEwA2oVChMI75nKjei4xwiVqRbbCh01Owvd#v=onepage&q=silverman%202013%20what%20you%20can%20and%20cant%20do%20qualitative&f=false

http://www.bbc.co.uk/news/education-28096723


http://hub.ib.hu-berlin.de/~wumsta/pub95.html
http://www.icrjms.in/applications/CYBER%20CRIME%20AS%20SOCIAL%20ISSUE.pdf


https://books.google.co.uk/books?id=GSPhAQAAQBAJ&pg=PA89&lpg=PA89dq=%22cybercrime+in+popular+culture%22&source=bl&ots=gV3uKEXGBp&sig=J2HhNHTMngjubQGbCE6RYMim4to&hl=en&sa=X&ei=nhKoVMacFcqt7gawzoD4Dg&ved=0CBQQ6AEwAA#v=onepage&q=%22cybercrime%20in%20popular+culture%22&f=false

http://www.ft.com/cms/s/0/673a98d0-eccc-11e4-a81a-00144feab7de.html


http://www.edu.plymouth.ac.uk/resined/qualitative%20methods%202/qualrshm.htm#Inductive%20analysis%20and%20grounded%20theory

http://www.wired.com/2014/12/sony-north-korea-hack-experts-disagree/
Appendix A
Example of survey questionnaire

Participant Information
This project is part of a new collaboration between GMP, the College of Policing and Manchester Metropolitan University.

The research aims to find out more about the extent to which people’s online internet behaviour leads to demand on GMP, what perceptions officers and staff have of this and how they view their role in responding to it. It will also look to consider the way people talk about crime and incidents that arise online and the implications that this might have on how we look at the subject.

By completing this questionnaire you will be helping to develop GMP’s understanding of this emerging area of police business and thereby helping to shape our response, which may well influence the training and resourcing of you and your colleagues.

Please be assured that all your responses will be treated confidentially and no comments will be attributed to individuals.
Demographic information

How old are you?
16-24
25-34
35-44
45-54
55-65
Over 65
Prefer not to say

What is your gender?
Male
Female
Prefer not to say

How long have you worked for GMP?
Less than 1 year
1-5 years
6-10 years
More than 10 years
Prefer not to say

What is your current role?
Response Police Officer
Neighbourhood Police Officer
Call Handler
Other (please specify)
1) In an average week how many times do you deal with incidents and crimes that are the result of the way someone has behaved on the internet?

__________ times per week

2) On average, what percentage of your total working week do you spend dealing with incidents and crimes that are the result of the way someone has behaved on the internet?

__________ %

3) How often do you deal with the following types of incidents and crimes where they are the result of the way someone has behaved on the internet? (Please tick as many as applies to you)

<table>
<thead>
<tr>
<th>Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks against a computer, online network or services (e.g. virus/ malicious software)</td>
</tr>
<tr>
<td>Sexual offences or grooming</td>
</tr>
<tr>
<td>Offences related to indecent images of children on the internet</td>
</tr>
<tr>
<td>Abuse (e.g. bullying, harassment, stalking)</td>
</tr>
<tr>
<td>Fraud</td>
</tr>
<tr>
<td>Theft</td>
</tr>
<tr>
<td>The supply of illegal commodities (e.g. drugs, people trafficking)</td>
</tr>
</tbody>
</table>
4) To what extent do you agree or disagree with the following statements?

“The amount of time I spend dealing with incidents and crimes that are the result of the way someone has behaved on the internet is increasing”.

“I have the knowledge and skills needed to deal with the incidents and crimes I encounter, which are the result of internet behaviour”

“Should I need it, support and training is available to assist me in dealing with crimes resulting from people’s internet behaviour”

5) To what extent do you agree or disagree with the following statements?

“In my current role I should be dealing with incidents and crimes which are the result of the way someone has behaved on the internet”

“Crimes and incidents resulting from internet behaviour should only be dealt with by specialist units who are trained to investigate them”

“Crimes and incidents resulting from online behaviour should only be investigated by regional and/ or national law enforcement agencies”
6) How often do you use the term ‘cyber’ to describe crimes or incidents you deal with (e.g. cybercrime, cyber bullying, cyber stalking etc.)?

7) How often do you encounter other people using the term ‘cyber’ to describe crimes or incidents?

8) To what extent do you agree or disagree with the following statement?

“I am clear about what the definition of cybercrime is”

9) How would you describe to someone else what a cybercrime is?

Respondent contact details
If you are happy to be contacted by me in the future to take part in either a one-to-one interview or a focus group, please leave your personal contact details below. If you choose to provide these details and consent to participating in an interview or focus group, please be assured that all your answers within this survey and any future contact will remain confidential and no comments will be attributed to individuals.

If you agree to be contacted further and participate in an interview or focus group check this box ☐

Division/ Department ________________________________
Team/ Unit ________________________________
PIN ________________________________
Telephone number ________________________________
Appendix B
Method of obtaining ‘cybercrime’ data from GMP’s Business Intelligence System (BIS)

General caveats

The data contained crimes (including hate incidents and no crimes) recorded between 1st January and 31st December 2014. Hate incidents and no crimes do not constitute valid crimes but were included in the data set, as it is intended to provide an indication of policing activity associated with online behaviour and hate incidents and (some) no crimes may require an investigation to be conducted or other activity to be undertaken.

A number of BIS fields included in the data (such as ‘weapons’ and ‘instruments’ related to a crime/ incident) are not mandatory, and so may not be completed for all crimes.

Definition

Potential ‘cybercrimes’ have been selected using various criteria. The most accurate of these criteria is Computer Misuse Act offences, but the majority of crimes where one of the three ‘instrument’ fields contains the word COMPUTER, and crimes where the ‘deception’ field contains ‘COMPUTER’ are also likely to be relevant.

The majority of the criteria used to select potential cybercrimes are based on the occurrence of keywords in the MO (modus operandi) BIS text field. However, it should be noted that the use of keywords is very unlikely to produce data which is completely accurate as:

- The list of keywords is limited to those identified by a small number of individuals, and there are likely to be a large number of keywords which have not been considered;
- This methodology does not account for variations or spelling errors made when the data was originally input; and
Keywords may appear in the MO text in a variety of contexts and, without an extensive manual review (which cannot be undertaken due to the number of records), it is not possible to confirm that crimes are relevant to this request.

To reduce the number of irrelevant crimes included in the data, the criteria within the definition have been ordered, and those which are considered to be more accurate are applied in preference. For example, all crimes under the Computer Misuse Act are relevant to this request, whereas crimes where the MO text contains the word ONLINE may not be relevant, and, consequently, the former is applied in preference to the latter. The order of the criteria is subjective, and unlikely to remove all irrelevant crimes.

A small number of criteria were amended to increase the accuracy (for example, spaces have been included at the beginning of some keywords to ensure that words where the keywords appear as a string of characters in another word are excluded). For example, 85 crimes contain ‘E_BAY’ (the underscore indicates a space). But, this would include phrases such as THE BAY WINDOW. Adding a leading space to this keyword (_E_BAY) reduces the number of crimes from 85 to 2. Key words searched for and additional criteria used where deemed relevant were as follows:

<table>
<thead>
<tr>
<th>Key words</th>
<th>Additional criteria relating to keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ALIBABA)</td>
<td>ALIBABA or ALI_BABA</td>
</tr>
<tr>
<td>(ALIEXPRESS)</td>
<td>ALIEXPRESS or ALI_EXPRESS</td>
</tr>
<tr>
<td>(AMAZON)</td>
<td></td>
</tr>
<tr>
<td>(ASK.FM)</td>
<td>ASK.FM, ASKFM, ASK-FM or ASK_FM</td>
</tr>
<tr>
<td>(BEBO)</td>
<td></td>
</tr>
<tr>
<td>(EBAY)</td>
<td>EBAY, E-BAY or _E_BAY</td>
</tr>
<tr>
<td>(E-HARMONY)</td>
<td>E-HARMONY, EHARMONY or E_HARMONY</td>
</tr>
<tr>
<td>(FACEBOOK)</td>
<td>FACEBOOK, FACE_BOOK, F/BOOK or FBOOK</td>
</tr>
<tr>
<td>(FACETIME)</td>
<td>FACETIME or FACE_TIME</td>
</tr>
</tbody>
</table>

69
<p>| <strong>(FLICKR)</strong> |  |
| <strong>(GRINDR)</strong> |  |
| <strong>(GUMTREE)</strong> | GUMTREE or GUM_TREE |
| <strong>(INSTAGRAM)</strong> |  |
| <strong>(LINKEDIN)</strong> | LINKEDIN or LINKED_IN |
| <strong>(LOOT)</strong> |  |
| <strong>(MSN)</strong> |  |
| <strong>(MYSPACE)</strong> | MYSPACE, MY-SPACE or MY_SPACE |
| <strong>(PAYPAL)</strong> | PAYPAL or PAY_PAL |
| <strong>(SNAPCHAT)</strong> | SNAPCHAT or SNAP_CHAT |
| <strong>(SKYPE)</strong> |  |
| <strong>(TINDER)</strong> |  |
| <strong>(TWITTER)</strong> | TWITTER or TWEET |
| <strong>(VIBER)</strong> |  |
| <strong>(WHATSAPP)</strong> | WHATSAPP or WHATS_APP |
| <strong>(YOUTUBE)</strong> | YOUTUBE or YOU_TUBE |
| <strong>(.CO.UK or .COM)</strong> |  |
| <strong>(CHATROOM)</strong> | CHATROOM or CHAT_ROOM |
| <strong>(CYBER)</strong> |  |
| <strong>(DATABASE)</strong> | DATABASE or DATA_BASE |
| <strong>(DDOS)</strong> |  |
| <strong>(DOWNLOAD)</strong> |  |
| <strong>(EMAIL)</strong> | E-MAIL, _EMAIL or _E_EMAIL |
| <strong>(FILE SHARING)</strong> |  |
| <strong>(INTERNET)</strong> |  |
| <strong>(PEER TO PEER)</strong> | PEER TO PEER, PEER-TO-PEER or PEER 2 PEER |
| <strong>(PHISH)</strong> | |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(REMOTE ACCESS)</td>
<td>REMOTE ACCESS or REMOTELY ACCESS</td>
</tr>
<tr>
<td>(SERVER)</td>
<td>excluding CONSERVER, OBSERVER, SERVERAL and SERVERING</td>
</tr>
<tr>
<td>(SOCIAL MEDIA OR SOCIAL NETWORK)</td>
<td></td>
</tr>
<tr>
<td>(USERNAME)</td>
<td>USERNAME or USER_NAME</td>
</tr>
<tr>
<td>(VIDEOLINK)</td>
<td>VIDEOLINK or VIDEO_LINK</td>
</tr>
<tr>
<td>(VIRUS)</td>
<td></td>
</tr>
<tr>
<td>(WEBCAM)</td>
<td>WEBCAM or WEB_CAM</td>
</tr>
<tr>
<td>(WEBSITE)</td>
<td>WEBSITE or WEB_SITE</td>
</tr>
<tr>
<td>(PLAYSTATION NETWORK)</td>
<td>PLAYSTATION NETWORK or PLAY_STATION NETWORK, excluding crimes where COMPUTER, COMPUTER GAME, COMPUTER HARDWARE, COMPUTER SOFTWARE, CONSOLE or LAPTOP are attached as items of property</td>
</tr>
<tr>
<td>(XBOX LIVE)</td>
<td>XBOX LIVE, X-BOX LIVE or X_BOX LIVE, excluding crimes where COMPUTER, COMPUTER GAME, COMPUTER HARDWARE, COMPUTER SOFTWARE, CONSOLE or LAPTOP are attached as items of property</td>
</tr>
<tr>
<td>(COMPUTER)</td>
<td>Excluding crimes where COMPUTER, COMPUTER GAME, COMPUTER HARDWARE, COMPUTER SOFTWARE, CONSOLE or LAPTOP are attached as items of property</td>
</tr>
<tr>
<td>(LAPTOP)</td>
<td>Excluding crimes where COMPUTER, COMPUTER GAME, COMPUTER HARDWARE, COMPUTER SOFTWARE, CONSOLE or LAPTOP are attached as items of property</td>
</tr>
<tr>
<td>(HARD DRIVE)</td>
<td></td>
</tr>
<tr>
<td>(DELETE)</td>
<td></td>
</tr>
<tr>
<td>(DATA)</td>
<td></td>
</tr>
<tr>
<td>(ONLINE)</td>
<td>ONLINE or ON_LINE</td>
</tr>
<tr>
<td>(PASSWORD)</td>
<td>PASSWORD or PASS_WORD, excluding robbery and theft from the person</td>
</tr>
<tr>
<td>(SOFTWARE)</td>
<td>SOFTWARE or SOFT_WARE, excluding robbery and theft from the person</td>
</tr>
</tbody>
</table>

Also included in the initial collection were crimes where a computer was referred to in the ‘weapon’ field of the crime report.
Appendix C
Acknowledgments

I would like to thank my mentor, Clive McGoun (from the Faculty of Health, Psychology and Social Care at Manchester Metropolitan University), for all his support during throughout this research project. I am extremely grateful for the guidance and encouragement Clive has provided, and which has been of immense value to me.

My gratitude and thanks are also extended to colleagues from Greater Manchester Police who provided assistance. Thank you to Frank Rutter for his expertise in converting my survey questionnaire to Survey Monkey format, and to Alexandra Thomson for her support in collating responses from police officers and staff to the survey. Many thanks also to Lauren Clifton and Philip Li for their assistance in accessing GMP’s crime records data and in using SPSS software to prepare the statistical analysis.

Finally, my warmest thanks go to my family for all their support and for understanding that daddy has not been available as much as usual on evenings and weekends.