available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment

*Paul Hunton**

Cleveland Police, Ladgate Lane, PO Box 70, Middlesbrough, Cleveland TS8 9EH, UK

ARTICLE INFO

Article history:
Received 20 January 2010
Received in revised form
2 November 2010
Accepted 10 January 2011

Keywords:
Cybercrime
e-Crime
Internet Crime
Hi-tech Crime
Police
Policing
Law enforcement
Criminal investigation
Investigation framework
Investigation model

ABSTRACT

As the Internet evolves and continues to become a compelling part of our everyday lives, individuals, communities and nations alike are becoming increasingly exposed to the growing threat of the cybercriminal. The aim of this paper is to widen the discussion surrounding the many global issues and challenges of cybercrime investigation with specific reference to UK law enforcement. This paper first discusses the vast transnational landscape now associated with cybercrime and the rapid growth in cyber offences and other unacceptable Internet behaviours. The emerging characteristics of cybercrime are then presented as a Cybercrime Execution Stack. This logical model of cybercrime demonstrates an objective view and is aimed at identifying the common characteristics of cyber criminality that are likely to occur during the commission of an offence or other illicit behaviours. The concepts of a cybercrime investigation framework focussing on a UK law enforcement environment are introduced following the stages of Initiation, Modelling, Assessment, Impact and Risks, Planning, Tools, Action and Outcome. The benefits of such a framework are intended to provide a cybercrime investigator with a much richer understanding of the complex technical elements of networked technology and the Internet that must be considered when conducting a rigorous cybercrime investigation.

1. Background

In 1989 Sir Tim Berners-Lee made one of the most significant and influential advancements in modern technology with the invention of the World Wide Web. Twenty years on and the Internet has grown beyond imagination and provides digital communication and interaction to almost two billion global users, which accounts for nearly a third of the world population (Digital Britain, 2009).

The phenomenon of the Internet is argued by governments and businesses across the globe as directly impacting upon and even underpinning many fundamental aspects of modern society and critical national infrastructures (Cyberspace Policy Review, 2009; Cabinet Office, 2009a,b; Digital Britain, 2009; e-Crime Congress, 2009; Europol, 2007; McAfee, 2009; Estonia, 2008). Technology and more specifically the Internet is now considered as the global platform for opportunity and innovation (Digital Britain, 2009; Cyberspace Policy Review, 2009; BERR, 2008; Gowers, 2006) having already 'transformed the global economy and connected people in ways previously never imagined' (Cyberspace Policy Review, 2009).

One example of the sheer magnitude and increasing global acceptance of the Internet is demonstrated by the growing volume of online shopping transactions. Worldwide, online

* Tel.: +44 (0) 7747111602.
E-mail address: Paul.Hunton@cleveland.pnn.police.uk.
1742-2876/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2011.01.002

sales have increased from £3.5 billion in 2000 to over £40 billion in 2008 (APACS, 2009), with online retail transactions in the UK expected to account for 10% of all retail sales by the end of 2009 (BRC, 2009). The scale of our cyber existence becomes even more apparent when considering that an estimated three billion e-mails are sent everyday in the UK (BBC News, 2009b). The growing global obsession with a virtual existence is further demonstrated by the concept of virtual goods that only exist as data. An estimated one billion dollars is likely to be spent in the US during 2009 on virtual goods such as social gaming, online gifts and smartphone add-ons (BBC News, 2009c).

The reliance now placed upon the Internet is further demonstrated by the recent Youthnet survey that found 75% of 16–24 year-olds felt they could not live without the Internet (BBC News, 2009a,b,c). The Internet has become an intrinsic and compelling part of our everyday lives.

However, as technology continues to develop and evolve so do new opportunities for criminal and undesirable behaviours (Bryant et al., 2008). The open nature and ease of access to the Internet make it vulnerable to attack (HM Government, 2009). The Internet provides criminals with a simplified, cost effective and repeatable means to conduct rapid, large scale attacks against a global cyber community (Bryant et al., 2008). The ease of access and increased anonymity facilitated by the Internet (Fletcher, 2007) allows unscrupulous individuals to interact freely with a vast global community and behave in ways that would be completely unacceptable in the physical world (Garlik, 2008). It is now argued that with the exception of direct physical attack, the potential risks, threats and harm we are exposed to in the real-world are equally applicable on the Internet (Digital Britain, 2009).

2. Crime and the internet

The term now commonly associated with the undesirable and illicit behaviours when using the Internet is cybercrime (Bryant et al., 2008; Cross, 2008; Moulton, 2008; Wall, 2007; Yar, 2006). 'Cybercrime' is often used as a convenient label to describe the global phenomenon of crime and other undesirable behaviours that involve the use of networked technology and more specifically the Internet. The ability to distinguish or quantify the true scale and criminal nature of cybercrime is not a simple task. Commonly accepted is the difficulty in gathering meaningful and accurate data in relation to cybercrime (ACPO, 2009; New Zealand Police, 2009). This issue is further compounded when considering that under UK sovereignty, there is no definitive classification of technology related crime (House of Lords, 2008) and not all so-called cybercrimes are crimes under criminal law (Wall, 2007).

With cybercrime hitting the news headlines on a daily basis it is not surprising that the Garlik (2009) cybercrime report estimated that 3.6 million criminal acts were committed online against UK victims during 2008. The report further shows that identity fraud increased by 207%–217, 323 incidents compared to the previous 12 months and online banking fraud had increased by 132%, which now accounts for illegal transactions totalling £52.5 million. Internet related card fraud has continued to increase, with UK issued card fraud reaching £181.7 million in 2008 (APACS, 2009). The 2008 British Retail Crime Survey (BRC, 2009) also found that 85% of the businesses surveyed had experienced Internet fraud during the previous 12 months and 64% had experienced an increase. The research into cybercrime by Symantec (2009) further supports the above findings and argues that the primary aim of the technical activities deployed by cybercriminals is to attack end users for financial gain.

Common examples of cyber related crimes can be demonstrated by such offences as fraud, identity theft and theft of Intellectual Property Rights. However, the motive behind cybercrime is not entirely about financial gain. The young and vulnerable are also targeted, being subjected to online crimes such as grooming, cyber-bullying, pornography and paedophilia. A recent survey of 11–18 year-olds by the charity BeatBullying found that nearly a third of those surveyed had experienced some form of online bullying (BeatBullying, 2009). In response to the technical capability facilitated by the Internet, cybercriminals are capitalising on the opportunity for computer misuse and are utilising a wide range of techniques including spamming, phishing, viruses, malicious code, hacking, denial of service attacks, network intrusion and the distribution and supply of illicit data to commit acts of both criminal and undesirable behaviour. Examples of cybercrime can be broadened even further with the concepts of cyber warfare and cyber terrorism, industrial espionage and disinformation ranging from information warfare to propaganda and political attack.

However, with such a vast array of diverse criminal activities, the difficulty and complexity law enforcement face in determining and tackling cybercrime is a major challenge. This issue is further compounded when considering the interchangeable state of the terms cybercrime, e-Crime, Internet crime and high-tech or digital crime. In response to the growing issue of crime and the Internet and the lack of clarity surrounding cybercrime in the UK, the Association of Chief Police Officers (ACPO) has recently defined the term e-Crime as 'the use of networked computers or Internet technology to commit or facilitate the commission of crime' (ACPO, 2009). The ACPO definition moves away from the catch all terms of high-tech or electronic crime, and focuses specifically on networked computers and the Internet in line with the criminal element of the term cybercrime. Although the ACPO definition provides clarity in relation to crime under criminal law, other commentators continue to argue that national legislators around the globe have yet to keep pace with the already broad and growing range of other unacceptable Internet related behaviours, for which there is no consistent definitive criminal legislation or regulatory control (Brenner, 2007; Bryant et al., 2008; COE, 2009; McAfee, 2009; Yar, 2006).

Hidden among the technical magnitude, compounded by the physical boundaries of legal sovereignty and the sheer complexity of the Internet is a vast opportunity for either, the lone cybercriminal, organised crime gangs or terrorist networks to commit crime and other illicit and undesirable behaviour using the Internet. Therefore, for the purpose of this discussion the terms cybercrime, Internet crime and e-Crime are all considered as generalised labels used to describe criminal and undesirable or harmful behaviour that is assisted