Routledge
Taylor & Francis Group

Contemporary Social Science

Journal of the Academy of Social Sciences

ISSN: 2158-2041 (Print) 2158-205X (Online) Journal homepage: http://www.tandfonline.com/loi/rsoc21

A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online

Mary Aiken, Ciaran Mc Mahon, Ciaran Haughton, Laura O'Neill & Edward O'Carroll

To cite this article: Mary Aiken, Ciaran Mc Mahon, Ciaran Haughton, Laura O'Neill & Edward O'Carroll (2015): A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online, Contemporary Social Science, DOI: 10.1080/21582041.2015.1117648

To link to this article: http://dx.doi.org/10.1080/21582041.2015.1117648

Published online: 10 Dec 2015.

Contemporary Social Science, 2015
http://dx.doi.org/10.1080/21582041.2015.1117648

A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online

Mary Aiken*, Ciaran Mc Mahon, Ciaran Haughton, Laura O'Neill and Edward O'Carroll

CyberPsychology Research Centre, Royal College of Surgeons in Ireland, Dublin, Ireland

(*Received 20 October 2015; final version received 2 November 2015*)

Contemporary news headlines seem to play regular host to treatments of one form of *cybercrime* or another, whether it be fraud, hacking, malware, piracy or child abuse material online. In this paper, the meaning of that term is unpacked, social impact is considered and possible future developments are discussed. Given the pervasive and profound influence of the Internet, it is important to acknowledge that in terms of criminology, what happens online can impact on the real world and vice versa. Consequently, real-world and cyber social impacts in relation to cybercrime will be examined.

Keywords: cyberpsychology; cybercrime; social impact; hacking; piracy; child abuse material

Introduction

Technology is now ubiquitous, the Internet specifically is an increasingly pervasive phenomenon with approximately 3.2 billion people (almost 40%) of the world's population now online (International Telecommunications Union, 2015). While the Internet offers abundant opportunities for education, networking and communication as an information superhighway, it can also manifest risk particularly regarding criminal activity, which in turn has implications in both real and virtual worlds. As such, the purpose of this article is to discuss the social impact of forensic phenomena in this new sphere: *cybercrime*.

Social impact and social context of cybercrime

'Social impact' per se is a fickle concept, which can be treated on both a macro scale – for example, the 'economic and social impact of the arts' (Reeves, 2002), the political effects of rumors (Huang, 2015) – and a micro scale – ' … changes in physiological states and subjective feelings, motives and emotions, cognitions and beliefs, values and behavior, that occur in an individual, human or animal, as a result of the real, implied, or imagined presence or actions of other individuals' (Latane, 1981, p. 343). Consequently, there lies within our exploratory toolkit a whole range of factors to hand – from economic, cultural, psychological and interpersonal – which is useful, because, as will be discussed cybercrime explodes the notion of social impact. It is an implicit argument within this paper that such an explosion of the understanding of

*Corresponding author. Email: maryaiken@rcsi.ie

'social impact' is necessary in the study of cybercrime, because, quite frankly, of the nature of the environment in which it occurs.

Human interaction in cyberspace, while usually carried out in physical isolation, is almost immediately public and permanent: users are both alone and hyper-connected, all at once. As such, given the social context of cybercrime, its social impact has quite unusual properties. Slane (2007, p. 97) has noted:

> Claims for the independence of cyberspace sound quaint and idealistic, largely because they are based on a false dichotomy between virtual and physical phenomena. Physical and virtual are not opposed; rather the virtual complicates the physical, and vice versa.

This complication of virtual and physical – a sort of 'augmented reality' (Jurgenson, 2011) – represents a new problem for the study of environmental behaviours such as crime. The difficult task is therefore to study problems as they are naturally occurring in everyday life (Proshansky, 1987), a point which is particularly relevant in the study of cybercrime. Proshansky states that it is important, however, for the environmental researcher to utilise all aspects of research and analysis of the findings and to take into account both the general and individualised aspects of the problems. However, Proshansky (1987) only considered environment in terms of a 'real-world' construct, understandably his research at the time did not extend into cyberspace. Subsequently, Suler (2004) presents an evolving conceptual framework for understanding how people react to and behave in cyberspace, arguing that the experience created by computers and computer networks should in many ways be understood as a psychological 'space' – ergo, 'cyberspace'. How the learnings of environmental psychology, like Proshansky (1987), be applied to Suler's (2004) remains to be seen, though this paper, like some other tentative steps (Aiken & Mc Mahon, 2014), should be seen in that light.

Such theoretical developments naturally produce corollary methodological issues. For example, Aiken and Mc Mahon (2014, p. 3) assert that 'traditional research methodology … is beginning to look quaint' in the light of rapid developments in information communication technology and how that effects the social science research process. There are important questions which researchers must reflect upon, such as the level of digital literacy of the researcher, the source of their ethical guidance, the evangelism which envelopes public messaging on the use of technology and how close the researcher can or should come to the lived experience of the research subjects (Aiken & Mc Mahon, 2014). Such reflections are particularly useful in the context of the social impact of cybercrime, but equally so in a broader conversation on the academic treatment of its social context. Vishik (as cited in '4th World Cyber Security Technology Research Summit Report,' 2014) noted that 'the multi-disciplinary nature of cyber security attacks is important, attacks happen for different reasons, only some of which are technical, other reasons include, for example, socioeconomic issues' (p. 8). What is also important, in addition to inter-disciplinarity, is the construct of trans-disciplinarity in cyberspace (Suler, 2013). There is a long-standing tradition of this in the context of cybercrime, in the guise of applied studies such as forensic and investigative psychology, and as such, cyberpsychology is yet another exemplification of how this can be achieved, drawing from social science and computer science, but also similarly recent enterprises such as network science and digital humanities.

With regard to the current treatment, the most salient cyberpsychological theoretical perspective to note is the concept of online disinhibition (Suler, 2004). In exploring how people tend to do and say things while on the Internet, which they would not be likely to do in a real-world face-to-face context. Suler (2004) details several factors at play in this phenomenon, including dissociative anonymity, and minimisation of status and authority online. Suler notes that the text-heavy nature of online environments occludes many of the effects of authority as presented in the

physical environment – dress, physical stature, trappings of officialdom and so on. Moreover, there is a long-standing Internet social philosophy which holds that 'everyone is an equal, that the purpose of the net is to share ideas and resources among peers' (Suler, 2004, p. 324). Consequently, with society's normal hierarchies and powers flattened somewhat, it could be argued that the online environment is one which naturally lends itself to criminal or at least unusual behaviour. Minimisation of authority should be viewed in addition to what Suler terms 'dissociative imagination' – the idea that 'one's online persona along with the online others live in a make-believe dimension, separate and apart from the demands and responsibilities of the real world' (2004, p. 323). As such, even without tackling the problematic issue of anonymity, scenarios may manifest online which are quite unlike those where real-world physical crimes occur.

When the notion of authority is developed more specifically with regard to cybercrime, there are a number of corollaries. On the one hand, with no observable authority figures, or in an apparently hierarchy-free context, a lower barrier to crime participation may be envisaged. Moreover, where there is the possibility that all participants in this environment may not fully appreciate it as a real environment, the words of the infamous hacker, Kevin Mitnick may be appreciated: ' … the human factor is truly security's weakest link' (Mitnick & Simon, 2002, p. 16). Fundamentally, even following installation of sophisticated information security technology, practices and training, a company will still be vulnerable. This is because people tend to underestimate the severity of potential cyber threats and this complacency may lead to successful cyber-attacks (Paganini, 2012).

As such, from the perspective of the victims of cybercrime, concepts such as *herd immunity* may need to be considered (Rosenzweig, 2013) – where not every member of a population needs to be inoculated to prevent the spread of infection – with regard to human behaviour in cyberspace. Some work has been done with regard to modelling the spread of viruses in computer networks (Asllani & Ali, 2012), but this concept should be considered in relation to a wider variety of phenomena: perhaps people fall victim to cybercrime because they assume that the rest of the herd will take care of security for them? This also has parallels with what is known as the Peltzman effect (1975) – whereby paradoxically increased safety regulation seems to reduce safety behaviours. Fundamentally, while not wishing to engage in digital dualism (Jurgenson, 2011), people should be open to the possibility that denizens of cyberspace, either not fully believing it to be 'real', or assuming that its security will be taken care of elsewhere, may leave themselves open to some forms of criminal attack. At the outset, a preliminary social impact of the phenomenon of cybercrime should be noted: a culture of unreality and novelty still pervades in cyberspace, which continues to be readily exploited by adversaries.

Such an illusory context however, has concomitant risk. Wilde (1998) proposed the hypothesis of risk homeostasis, suggesting that people maximise their benefit by comparing the expected costs and benefits of safer and riskier behaviour. Thus, any situation which is perceived as safe will allow people to take more risks, resulting in equilibrium: as the dangers of the Internet can be intangible, a false sense of security can develop. This allows cybercriminals to take bigger risks online, while at the same time, in a social context, enables their victims to be less protective of themselves and their information online. In an industry context, a lot of cybercrimes go unreported to authorities and thus, the majority of information is held in the private sector by businesses or their IT partners (Bradley, 2014). Businesses seek to minimise public panic when they are attacked, and are concerned about liabilities from disclosing internal information (Groenfeldt, 2013). In early 2015, the British telecommunications company, Talktalk, had a security breach and lost valuable customer data. The hack was not publically disclosed and therefore hackers were then able to contact customers, quote personal information, gain remote access to their computers, thus allowing the hackers to steal in excess of £3000 per customer (Brignall, 2015). Some feel that they cannot risk reporting to the authorities, and instead opt for 'frontier

justice' – counter attacks (which shut down the server an attack is originating from) known in cyber security industry as 'active defence' or 'striking back' (Deloitte, 2014). To combat rogue security and encourage sharing with law enforcement, Deloitte, amongst others, has suggested a clearinghouse model (2014). Private companies worried about seizure of servers, public trust and competitors taking advantage could submit data to the clearinghouse, which would analyse it to share with action-taking authorities and also to warn other companies in similar industries of potential risks (Deloitte, 2014). Information sources such as SurfWatch are on this path, collecting data to better inform industries and allow them to compare information about cybercrime and related issues (SecurityWeek, 2015). But there is very much a sense of primitiveness in how this is being dealt with: as if all are still in the early days of understanding how to collectively organise a response to these threats.

Cybercrime defined

At the outset, it is worth noting that the relatively recent phenomenon of cybercrime is steadfastly resisting an accepted definition. Popular media treatments mentioning cybercrime usually involve imagery of masked hackers typing green screen text in dark rooms, but scholarly treatment of the concept is far more mundane. On the one hand, there is the general understanding that cybercrime refers to ' … any activity occurring online which has intended negative consequences for others … ' (Kirwan & Power, 2012, p. 2). To specify in some more detail, a three-stage classification is provided by the US Department of Justice:

(1) Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and Distributed Denial of Service (DDoS) attacks.
(2) Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud.
(3) Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime (Clough, 2010, p. 10).

Alternatively, Kirwan and Power (2013, p. 3) state that ' … cybercrime can be divided into "property crimes" (such as identity theft, fraud and copyright infringement) and "crimes against the person" (such as cybercrimes involving the sexual abuse of children)'. Kirwan and Power (2013, p. 3) outline a basic typology of cybercrime, classified as 'Internet-enabled crimes', 'Internet-specific crimes' and 'Crime in virtual worlds'. For the purposes of this article, via a cyberpsychological lens, a wide variety of phenomena will be examined along an ad hoc structure: while these definitions and typologies are useful, none have considered cybercrime from a perspective of social impact.

Hacking, malware, dark net, black markets and more

One of the more highly publicised categories of cybercrime involves hacking, which can be defined as ' … activities involved in attempting or gaining unauthorised access to IT systems' (Furnell, 2009, p. 173). Hacking is used as a broad term in the media and could be considered as too simplistic as there are a number of different sub-groups. For example, a white hat or ethical hacker infiltrates a system without causing any damage in the process and such an individual can be hired by companies to find weaknesses in security systems. Alternatively, some hackers unrequested, infiltrate systems in order to highlight frailties and report it to the organisation in order for them to improve their security. While there is obviously a benign motivation for such activity, it is still an illegal act (as a form of trespassing) and hackers can be prosecuted even

without having done any damage. Conversely, black hat hackers penetrate computer systems with the specific purpose of causing damage or accessing unauthorised information. Grey hat hackers may seek opportunities to exploit systems in the hope of obtaining a monetary reward and may cause malicious damage to an individual or organisation they deem to be unethical. Kirwan and Power (2012, p. 57) discuss the 'dark figure' of hacking – that is, the difficulty of knowing just how much hacking occurs due to issues in completing methodical surveys, attackers not wanting to incriminate themselves, victims' disinclined to report hacking, and victims who may even be unaware and therefore unable to report.

Given such secrecy and intrigue around the topic, it might be difficult to ascertain any broader social aspects to these phenomena. On the one hand, there exists early research which notes that hacking was associated with 'intellectual curiosity and fascination with the technology' (Bissett & Shipton, 1999, p. 904), and even further back Hayes (1989) suggests that teenage hackers are rarely politically motivated. Yet more recently this has transitioned into an 'obsession to make all information free and accessible to everyone … no secrets' (Kirwan & Power, 2012, p. 55). Moreover, at the same time, this occurs alongside an 'anti-authority impulse [which] begins to manifest itself in response to commercial or legal obstacles – illegal aspects … begin to appear' (Kirwan & Power, 2012, p. 55).

Labelling theory (Becker, 1997), from the sociological theory of crime, may be applicable in that defining a person in a certain light may allow the definition to become a means of defence to them (Rock, 2007). For example, Appleby (2010) states that that the way in which muslims are sometimes banded together under the same umbrella as militant Islamists may cause them to feel alienated and eventually cause them to sympathise with said group. Similarly, Kirwan and Power (2012) suggest that it is possible that media coverage of all hackers as black hat hackers might impact white/grey hat hackers and alter their behaviours. Warren and Leitch (2009) draw a comparison between hackers who 'tag' themselves in site they have gained access to, and offline 'taggers' in graffiti culture – an interesting interrelationship between online and offline vandalism.

In terms of social developments, what has emerged in recent years is an unusually strong political culture in hacking. There now exists the figure of the *hacktivist* – an individual who draws 'on the creative use of computer technology for the purposes of facilitating online protests, performing civil disobedience in cyberspace … ' (Gunkel, 2005, p. 595). An example in that light is the Aaron Swartz hacktivism case involving mass downloading JSTOR ('Journal Storage') of scientific research documents, which he believed should be made freely available for everyone, not just those who could afford them (Naughton, 2015). This was deemed a felony by US prosecutors (*United States of America v. Aaron Swartz*, 2012). Facing up to 35 years in prison and a fine of up to $1 million (US Attorney's Office District of Massachusetts, 2011), Swartz took his own life while awaiting trial, his memory has become a *cause celebré* for hacktivists worldwide. There is now an increase politically motivated Denial of Service (DoS) or DDoS attacks (Nazario, 2009), a DoS attack is where a system or website is flooded with requests, slowing or stopping normal operations, whereas a DDoS attack is where a botnet (remote-controlled group of computers, possibly surreptitiously compromised by a hacker) attacks such a service or website (Cid, 2014). As such, whereas hacking began as an 'intellectual curiosity' arguably with hints of vandalistic overtones, it now has distinct overtones of political and social protest.

However, at the same time, such exploits require reasonably high levels of technical expertise – but such is not necessarily required in order to gain access to a system. *Social engineering*, where people are a system's weakest point, has been utilised by hackers such as the aforementioned Kevin Mitnick (Mitnick & Simon, 2011). Examples of exploiting social convention to hack include: finding out someone's birthday and sending them an email with a masked and malicious link and so on. This kind of *socio-technical approach* runs through the whole phenomenon of *malware* (malicious software), and other cybercrime tools such as worms, Trojans,

spyware, keyloggers, ransomware and rootkits to name a few. Bocij (2006) discusses the switch from curiosity to financial motives in malware writers, as well as a move to the more profitable spyware. A white paper published in 2012 by Trend Micro gives insight into cybercrime originating in Russia, showing the prices of popular hacking services and software:

> Trojan for bank account stealing – US$1300
> Credit card checker – US$70
> Fakes of different programs – US$15–25. (Goncharov, 2012)

Cyber criminals offer consulting and programming services, installation options and spamming/phishing schemes and viruses/malware such as Trojans or rootkits. What is curious to note, in terms of a narrow understanding of social impact (Latane, 1981), is the development of CaaS – 'Cybercrime as a Service' (Europol, 2014a; Manky, 2013). In other words, the technical expertise barrier to individual participation in cybercrime has been removed, replaced with a low financial cost and a service-based model.

Such a phenomenon is new, but does not appear to be under threat of law enforcement, perhaps due to the globalised nature of cybercrime. With an apparent lax attitude to IP and copyright, and a disinterest in prosecuting for international cybercrimes (Plesser, 2014), Russia's cybercrime market reached a conservative estimate of US$1.9 billion in 2012 (Volkov et al., 2013). At one global estimate, where victims lose around €290 billion each year worldwide as a result, cybercrime is more profitable than the global trade in marijuana, cocaine and heroin combined (Europol, 2014b). Other estimates put the economic impact of cybercrime at $445 billion worldwide, and between 15% and 20% of the value created by the Internet ('McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies,' 2014) In general, however, it is incredibly difficult to find hard, empirical data on how much profit cybercriminals are making, additionally an often cited estimate of $1 trillion global cost of cybercrime has been queried (Maass & Rajagopalan, 2012).

In a financial and corporate context, the threat of cybercrime has been a substantial fear for quite some time, with references to the Internet being a 'wild west' type of environment stretching back at least 20 years (Amiran, Unsworth, & Chaski, 1992; Gozzi, 1994; Meyer, 1995). That idea, with its associations with general lawlessness, still recurs in information security literature (Moraski, 2011). The 2014 hack of the multi-billion dollar company Sony offers a prime example of the cost of cybercrime, the attack ended up costing the company over $35 million (Hornyak, 2015; Seal, 2015). Consequently, it is no overstatement to say that cybercrime presents a very clear and present danger to all companies.

Interestingly, according to the Director of the Federal Bureau of Investigation, 'there are only two types of companies: those that have been hacked, and those that will be' (Mueller, 2012, para. 63). What is curious to note is not necessarily how blunt or pessimistic that assessment is – but how odd it would seem if it were made in the context of real-world physical security.

For most private individuals, on finding out their house or car was broken into, or wallet containing money and personal information was stolen, the first call would be to the police. Yet, articles offering information to victims of hacking advise them to contact the group with whom they hold the compromised account, with no mention of contacting law enforcement (e.g. Gibbs, 2014). Similarly, in a business context, advice to private enterprises with regard to information security is quite low on reference to state security. With no real geo-political borders, asking nations to police their own 'area' of cyberspace can be confusing, and next-to-impossible in a lot of cases. If you, as a UK citizen, are in Germany on holidays, and have your Gmail account (with servers in Ireland) hacked by Russians, who are working off servers hosted somewhere in the Caribbean, which country is responsible for protecting you online? Who do you report digital theft to?

Companies have however acted on their own initiative and have made efforts themselves in terms of corporate social responsibility. Microsoft, for example, have taken their own action, founding their Digital Crimes Unit (DCU), focusing on technology-facilitated child sexual exploitation crimes, malicious software crimes and piracy and intellectual property (IP) crimes (Campbell, 2015). Barclays Bank have a link with Europol where they are sharing all information they have of being hacked to help better understand how hackers work. This information is vital for future cyber safety (Nicholls, 2015).

However, for many businesses, IT security companies are the first call when they discover cybercrimes (Selby, 2012). These 'digital bodyguards' are tasked with hunting down intruders and protecting systems from attack when there is no statutory alternative – for example, Mandiant was recently profiled under the Ghostbusters-esque title of 'Who you gonna call?' (Stone & Riley, 2013). While some companies may wish to press legal charges, exposing a security breach may deter them from reporting, and the inherent global nature of the Internet makes it difficult to track down offenders, and even more difficult to prosecute them under local laws (Dye, Ax, & Finkle, 2013). According to Richard Boscovich, senior attorney with Microsoft's DCU, 'the number one issue is that there is simply no homogenous legislation worldwide' (as quoted in Moraski, 2011). It would appear that the risks involved in cybercrime are minimal, especially when compared to other criminal acts. The former Chief Security Advisor for Microsoft UK, Ed Gibson, maintains:

> If you commit a cybercrime there's almost no chance you'll get caught; if caught there's almost no chance you'll get prosecuted; get prosecuted and there's slim chance you'll get time; get time and there's no chance you'll serve anything like the whole ride. Under those conditions, what possible reason would there be not to commit cybercrime? (as cited in Kassner, 2014, para. 11)

As such, with smaller acts of cybercrime (e.g. music piracy, below) a person's attitude to risk is not as important a factor, as the acts are not even perceived as 'real' crimes, and therefore carry little or no risk (Nandedkar & Midha, 2012). For more advanced cybercriminals, the risk is evaluated on a cost basis, 'the greater the overall gain from any particular behaviour, the more likely it is to be carried out' (Feldman & Feldman, 1993, p. 224). The social consequences of this are seen as the cost-benefit of any cybercrime is extremely appealing; it is more likely to be carried out. There is often a disconnect between the potential danger online and the awareness of such danger felt by Internet users, who are often connecting to the Internet from a familiar, safe environment such as home or office. Arguably this may lead to a user base that is notably lax about cyber security, and therefore ripe for exploitation and victimisation. As private companies and authorities try to make the Internet a safer place, it seems that users may defer responsibility for their own security, and take more risks in keeping with the belief that is it safe to do so (McAfee Enterprise, 2013).

On the other hand, cybercriminals have become adept in hiding their illegal activity online. It is important to remember that what is commonly called 'the Web' is really just the surface Internet, beneath that surface content lies a vast, mostly uncharted area known as the 'Deep Web'. It is estimated that the surface web accounts for only about 1% of all content online; the remaining 99% is housed in the deep web (Pagliery, 2014). Tor ('The Onion Router', so-called because of its many layers of security) is one of the gateways to purposefully hidden information in the Deep Web (Kotenko, 2014). Designed to anonymise users, it also has a function for whistleblowers, activists and confidential sources (Kotenko, 2014). Deep web and Tor protocols were arguably originally intended for sensitive communications including political dissent; however, in the last decade they have become hubs for criminal black markets that distribute drugs, counterfeit pharmaceuticals, stolen credit cards, child pornography online, pirated media and more ('Going Dark: The Internet Behind The Internet,' 2014). Open-source software based currency

such as *bitcoins* can be used to facilitate transactions on the deep web, drugs can be purchased, money can be laundered and assassins can be hired (Pagliery, 2014), and consequently there is some speculation it has been compromised by the FBI (Poulsen, 2013).

Up until its closure in 2008 (Davies, 2010), DarkMarket was one of the largest English-speaking online black markets. The Silk Road, residing on the Deep Web and accessible via Tor, was shut down in 2013 (*United States Of America v. Ross Ulbricht*, 2014). Without a doubt, other markets have sprung up to capture their market share (Goodman, 2013). With black markets similar to eBay and Amazon available, cyber criminals can buy and sell credit cards, identities, financial information, as well as new hacking software tools with relative ease (Goodman, 2013). The very odd social feature of these black markets is not only how accurately they copy the 'look and feel' of their surface web, public and legal counterparts, but that apparently, they have great customer service (Bartlett, 2014). Bartlett (2014) notes that, despite them being dens of inordinate criminality, social interactions on deep web illicit markets display a large amount of self-policing and monitoring by it is community of users. Such an observation lends itself to a corollary on the social impact of this cybercrime: the potential normalisation of online drug sales. An example of this phenomenon is highlighted by the fact that many teenagers have been found posting pictures on social media and bragging about the drugs they have purchased on the deep web (O'Neill, 2013).

Piracy

While the preceding section dealt with cybercriminals of a relatively small population of individuals, the most prevailing offences by ordinarily law-abiding citizens concerns illegal file-sharing or piracy (Kirwan & Power, 2012). Piracy therefore probably presents one of the best opportunities to discuss the social impact of cybercrime. Online piracy is understood to involve the unauthorised copying, distribution and selling of works that are in copyright (Yar, 2005). Copyright piracy has existed for decades but relied on hard-copy distribution, for example, physical CDs/DVDs being duplicated and sold on the black market. Modern piracy has been facilitated by the explosion of faster Internet speeds and the availability of popular illegal file-sharing websites such as 'Napster' (now a legitimate site) and 'The Pirate Bay', which were established in 1999 and 2003, respectively. Through sites such as these, the Internet has expanded people's resources to the point where anyone with a basic knowledge of computers has the ability to download any copyrighted material such as music, films and games for free.

In terms of a social context, a 2013 British Phonographic Institute report (BPI) found that 14.5% of Britons were using piracy networks and 4 million people were regularly file-sharing in the UK (2013). The BPI believes that £980 million in physical music sales is lost annually to illegal downloading (Robinson, 2010). The Federation Against Copyright Theft (FACT), as cited in Yar (2005), estimates an annual loss of £400 million for the British Film Industry (BFI). However, it must be noted that the preponderance of facts made publicly available are published by organisations with a vested interest in highlighting the seriousness of the problem and there is some research that suggests that some artists can benefit from illegal downloading (Bounie, Bourreau, & Waelbroeck, 2006; McKenzie, 2009; Shang, Chen, & Chen, 2007). Nevertheless, the majority of the studies in the field tend to find a negative association between illegal downloading and genuine sales (Smith & Telang, 2012). However with illegal downloading affecting the revenues of major corporations it was only a matter of time before online piracy drew significant attention from the law.

Despite highly publicised court cases brought forward by the music industry in order to deter file-sharing, millions of people around the world continue to illegally download and share music.

In 1999, Napster, the first major online file-sharing service, made its debut and at the peak of its popularity could boast 60 million registered users (Goldman, 2010). The Recording Industry Association of America (RIAA) took 'Napster' to court and was successful in forcing the company into liquidation. Individual file sharers have also been pursued. The most recent case involved Paul Mahoney of Northern Ireland being sentenced to four years in prison for facilitating the streaming of movies online, costing the film industry an estimated £120 million (Deeney, 2015).

So why do millions of people continue to break the law? Altschuller and Benbunan-Fich (2009) state that from a social outlook, it might be expected that the laws in place sufficiently reflect the moral perceptions of society and in turn will be observed by the bulk of its citizens. Events however suggest that the law does not reflect what the general public considers to be legal or even moral in the case of digital music downloading. Research suggests that deterrence attempts, such as the legal proceedings mentioned above, are likely to fail in this context because, once again, the chances of being caught are slim and participants perceive the prevalence of the criminal act makes it extremely difficult to take action against every individual file sharer (Wingrove, Korpas, & Weisz, 2011). As long as a punishment seems unlikely, offending behaviour is probably going to continue (Kirwan & Power, 2013). The number of 'neutralisation' techniques as put forward by Sykes and Matza (1957) are also used by offenders to justify offending behaviour. Respondents in some studies state a belief that illegal downloading is a victimless act, that it causes no harm to artists and the record companies could afford the financial loss (Altschuller & Benbunan-Fich, 2009; Selwyn, 2007).

Social learning theory suggests individuals tend to pick up deviant behaviour from their peers (Bandura, 1977). Peer norms have a strong impact on the intentions to illegal download music (Levin, Dato-on, & Manolis, 2007). Individuals may place higher values on their social group norms rather than on legal norms, which is blurring the line between a moral and immoral act. Svensson and Larsson's (2012) study in Sweden found that there are no social norms to back up the judicial system in this field. The question must be posed: how can compliance to the law be maintained when it is not supported by social norms? Such is a continuing observation in the study of the social impact of cybercrime. This would explain why overwhelming evidence suggests that most Internet users view such downloading behaviours as morally acceptable despite the law (Selwyn, 2007; Shang et al., 2007; Sirkeci & Magnúsdóttir, 2011). Individuals may not be able to evaluate or recognise infringing on IP rights as an ethical dilemma when it comes to non-tangible goods such as digital files. Evidence of this is well highlighted in studies such as Lysonski and Durvasula (2008), who examined opposing ethical beliefs systems regarding hard-copy (CD) shop lifting and digital 'soft lifting'. Here researchers found that their participant's ethical beliefs would prohibit them from stealing a CD from a record store; however, the same partakers were ambivalent towards downloading pirated material. Moores and Chang (2006) suggest that there is a disconnection between real-world ethical orientations and online downloading behaviour. Suler's (2004) online disinhibition effect can help us to explain how computer-mediated environments can create ethical ambiguity through dissociative anonymity and lead to a minimisation of authority. The potential disconnect between the law and personal ethics can often be due to fast-pace changes in technology and their impacts on society (Altschuller & Benbunan-Fich, 2009).

The war between the entertainment industries and online file sharers has had a considerable effect on society and the generation who grew up file-sharing. A new technology emerged which on the one hand was heralded by the vast population and on the other, derided as deviant by corporate record companies and the law. Harvard Universities Lawrence Lessig in Winter's (2013) film 'Downloaded' states it created:

> … a war which has basically criminalized a whole generation, it is *culture's Vietnam* … the only people who have gotten paid are the lawyers who have been presiding over expanding legal actions against people who are only using culture the way technology encourages them to use it.

It seemed at one stage that along with the general population, major media organisations were changing their stance on the morality of piracy. This can be highlighted by the HBO show 'Game of Thrones', which broke a piracy world record in 2013 when an episode was shared 1.5 million times within the first 12 hours of its airing (Tassi, 2013). The CEO of Time Warner Jeff Bewkes, as cited in Tassi (2013, para. 5), addressed this piracy and highlighted how it could be portrayed as a positive; '… if you go around the world, I think you're right; Game of Thrones is the most pirated show in the world. Well, you know, that's better than an Emmy'. Fast forward to 2015, this time four out of ten episodes in the Game of Thrones series could be downloaded from torrent sites two days before being aired on HBO. Contrary to their previous stance, HBO promptly sent out legal letters to users who were suspected of downloading the episodes (Kain, 2015). This example highlights the paradoxical nature of attitudes to piracy. If the producers of content cannot make up their minds about whether piracy is good or bad, is it any wonder that the people who download it generally do not feel like they are doing anything wrong.

There has been a decline in illegally copied files and this has been ascribed to the rise of legal alternatives, such as streaming service Spotify for music and Netflix for film, which offer consumers a more reliable experience than peer-to-peer file-sharing sites (Sherwin, 2013). Figures released by the BPI (2013) showed that legally acquired music surpassed file-sharing by 13.2%, and for the first time in history digital music had outsold all other types of physical formats. These statistics seemed to demonstrate that tougher anti-piracy laws, demanded by music and film companies, were no longer required, since the market was driving file-sharing to the margins (Sherwin, 2013). With this in mind, it would appear that the British government has decided to effectively decriminalise the downloading of copyright material. From 2015 onwards, individuals found downloading copyrighted content will be sent four warning letters that are aimed at educating the offender; however no legal action will be pursued even if that individual was to continue downloading illegally (Green, 2014). Society's norms have in a sense dictated the law, in that what was once deemed deviant will now have no legal ramifications in the UK. Perhaps the pirates have won.

Child pornography online, self-produced indecent images of minors and sexting

During the past 10 years over 132 million child pornography images have been seized by police and sent to the National Centre for Missing and Exploited Children (NCMEC, 2015). Of the 5375 victims that have been identified and classified by NCMEC investigators, 70% of these images were classified as child pornography, 16% as online enticement (grooming) and 14% as 'self-production'.

The U.S. Department of Justice (2010) outlined that 'child pornography' refers to the possession, trade, advertising and production of images that depict the sexual abuse of children. The term child pornography is a legal term for images of child sexual abuse; however, a report by the U.S. Department of Justice (2010, p. 8) maintains that,

> … many experts in the field believe that use of that term contributes to a fundamental misunderstanding of the crime – one that focuses on the possession or trading of a picture and leaves the impression that what is depicted in the photograph is pornography. Child pornography is unrelated to adult pornography; it clearly involves the criminal depiction and memorializing of the sexual assault of children and the criminal sharing, collecting, and marketing of the images.

In terms of describing the offence, there is a growing movement to utilise the words 'Child Abuse Material' (CAM) (Aiken, Moran, & Berry, 2011). The term child pornography is however consistently used in the majority of laws and policy documents internationally (Akdeniz, 2008), and attempts to change terminology are thought by some to be inadequate in terms of capturing the complex nature and of the material (Lanning, 2008). Terminology differs by jurisdiction, in the UK the wording 'Indecent Images of Children' is used in The Protection of Children Act (PCA, 1978) and the legislative term 'Prohibited Images of children' is employed in Section 62 of the Coroners and Justice Act (2009). Akdeniz (2008) notes the role of the Internet in the production, collection and distribution of 'Internet Child Pornography', pointing out that in recent years there is a general consensus that the Internet has increased the range, volume and accessibility of child-related pornographic imagery. The delicate social implications of appropriate and acceptable terminology illustrate the complexity of this cybercrime. Given these sensitivities for the purposes of this paper, the term CAM will be utilised.

The use of the Internet regarding this abusive material of minors has been a growing concern, there is a paucity of up-to-date data regarding the volume and criminal value of this material. In 2009 the criminal commercial 'market' for CAM was estimated to be worth in excess of $20 billion annually (Bourke & Hernandez, 2009). Cooper, Delmonico, and Burg (2000) first discussed the accessibility, affordability and anonymity (Triple A Engine) of the Internet and its impact on availability of CAM. Notably, research indicates that complex social networks can form, not dissimilar to peer-to-peer networks, concerning collecting and sharing of CAM online (Moran, 2010). Aiken et al. (2011) describe the social networking phenomenon of 'sharers' and 'leechers' in CAM trading communities online, which are comparable to 'seeders' and 'leechers' on networks such as 'The Pirate Bay'. Regarding these CAM communities, Aiken et al. (2011) point out an apparent *cyber social order* – in that expert groups develop a distinct hierarchy; jobs include administrators, technology advisors, security personnel and intelligence experts: a daunting prospect for law enforcement.

Minors are at risk as a result of the self-production of indecent images/videos, which may be distributed online. While there are cases of children being extorted into producing such media (Hainsworth & Sterling, 2014), others may engage in this behaviour as a result of online disinhibition (Suler, 2004), or simply in the course of normative adolescent social and developmental behaviour (Wolak & Finkelhor, 2011). Leary (2010) stresses the importance of the subject, pointing out that social problems that exist at the intersection of adolescence sex, technology and criminology require immediate investigation. This uploading of self-produced inappropriate material by Internet users, including many children and adolescents, is a growing phenomenon (Lenhart, 2009; Temple et al., 2012), resulting in youth engaging in increasingly risky behaviour (Leary, 2010; Wolak, Finkelhor, & Mitchell, 2011). This can even lead minors to produce and distribute images of themselves that are similar to child pornography (Quayle & Jones, 2011). The self-production of indecent images is also known as *sexting.* Specifically sexting is a form of mobile text messaging in which people send pictures of a sexual nature or sexually explicit text. Youth sexting has been described as the creating, sharing and forwarding of sexually suggestive nude or nearly nude images by minors (Lenhart, 2009). However, in many jurisdictions, senders are in danger of being charged with possession and distribution of child pornography (Leary, 2010), notwithstanding the fact that they are minors, and that the pictures are often of themselves (Zhang, 2010). A recent case in North Carolina highlighted issues in this area when a 17-year-old was prosecuted for having naked photos of himself on his phone (Brennan, 2015). Cormega Copening was sixteen at the time the photos were taken and was accused of committing a sexual offense against himself, he took a plea deal in order to avoid going to prison and having to register as a sex offender (Brennan, 2015).

From a criminal social justice perspective, Ostrager (2010) has suggested that the legal system needs to distinguish between sexting as a serious offence posing a danger to others, and when it is simply normative adolescent romantic activity (Wolak & Finkelhor, 2011). Typically, youths are taking photographs of themselves and posting them on social network sites, in chat room forums, or transmitting them on mobile phones via Multimedia Messaging Services (Ringrose, Gill, Livingstone, & Harvey, 2012).

One of the social challenges of this problem is to attempt to understand why youth engage in this form of cyber behaviour. The Barnes (2006) model of the cyberpsychology 'privacy paradox' suggests that young people may not always be aware of the public nature of the Internet. The privacy paradox is the disconnect between how users feel about privacy online, how they act, and how they react to the consequences of an unintended breach of privacy (Barnes, 2006; Viégas, 2006). Generally teens are aware that the Internet is not private; however, some act as though it is, and freely give up often personal information (Barnes, 2006; Gross, Acquisti, & Heinz, 2005). Additionally people share much of their lives online, revealing intimate thoughts and information, but are often unclear of the boundaries between public and private space (Barnes, 2006). Once an item is placed on the Internet, it can be distributed worldwide especially if it goes viral, while the individual concerned is under the impression that his/her boyfriend/girlfriend is the only recipient of their exchanges of images/ photographs. However the question must be asked if youth can be really be so disconnected from the issue? Phippen (2009) reports that most youth are fully aware of the concept of sexting, and a significant subset are actively engaged in the practice. The author notes that 'what is particularly worrying is the somewhat blasé attitude to the subject' (Phippen, 2009, p. 2). Ringrose et al. (2012) report that quantitative research on sexting has found rates varying from 15% to 40% among young people, depending on age, methodology and the definition of sexting employed. Temple et al. (2012) report that 28% of youth are engaging in the behaviour; however, Mitchell, Finkelhor, Jones, and Wolak (2012) argue that that only 1% of content in their study was actually sexually explicit. Discrepancies in terms of defining, investigating and academic reporting of sexting require clarification. The legal overlap between sexting and child pornography requires further investigation. From a sociological perspective the issue is a complex one, ranging from the production and distribution of child pornography (which is a criminal act) to the self-production and dissemination of indecent images by minors, which is arguably a social as opposed to policing issue; that said, given the nature of the material, it remains de facto a crime. Once again similarly to piracy, it is a question of weight of numbers, there exists a cybercrime which is illegal, that is, the production and distribution of explicit content by minors, but would appear to be socially acceptable amongst those who engage in the practice.

Policy and policing

In terms of addressing cybercrime, Kirwan and Power (2012, p. xvii) point out that 'governments attempt to respond with law, corporations with policies and procedures, suppliers with terms and conditions, users with peer pressure, technologists with code' and this perhaps illustrates one of the core issues, and that is the multiplicity of approaches to the problem space. Physical presence and visibility have been a cornerstone of policing policy to date. The lack of visibility of police online may arguably be a factor in the facilitation of cybercrime (Suler, 2004). An interesting initiative may now address this lack of visibility. In September 2014 Europol launched a trial of the first fully international cybercrime task force, the *Joint Cybercrime Action Taskforce* (J-CAT), results of which are still under review at the time of writing. Based in the Netherlands, it will be led by the deputy head of the UK's National Crime Agency's National Cyber Crime Unit, Andy Archibald (Schwartz, 2014). Paul Gillen (head of operations of the European Cybercrime Centre) has

stated that 'everyone has woken up to the fact that we can no longer stay within our own borders and enforce the law, we have to reach out to each other' (as cited in Schwartz, 2014, para. 4). Referring to the difficulties inherent in multinational cooperation against cybercrime, he states that 'in the European Union we have 28 different countries, 23 different languages, 28 different legal systems, and law enforcement … is not the most integrated part of the European Union' (as cited in Schwartz, 2014, para. 7). This new initiative is a significant step in the right direction in terms of 'joined up thinking' and a globally co-ordinated policing approach in cyberspace.

In terms of deterrents, amendments to UK legislation have increased the seriousness of penalties for certain cybercrime offences, up to life imprisonment (Serious Crime Act, 2015). However, it is yet to be seen if traditional criminal deterrent measures such as incarceration will be effective as digital space evolves. Notably, Chris Burchett of Credant Technologies states, 'Legislative bureaucracies tend to move slowly, whereas the attackers have shown a spectacular capacity for adaptation and innovation' (as cited in Moraski, 2011, p. 21).

There is a vast amount of data and literature regarding real-world crime; however everything has changed concerning the emergence of cybercrime, ranging from hacking to malware, and from piracy to the self-production of CAM by minors. In terms of criminal investigation, arguably there has been a paradigm shift, key police investigative aides such as eye witness testimony, and physical forensic evidence (e.g. DNA and fingerprints) are no longer relevant in cyber contexts. In terms of future research, cyber methodological approach will be critical in order to empirically investigate this new environment, cyberspace. An interdisciplinary or transdisciplinary research and investigative approach may result in optimum results and insights. Additionally, learnings from the field of cyberpsychology to date and going forward will arguably be invaluable in terms of illuminating human behaviour impacted by emerging technologies.

Detailed consideration of the social impact of cybercrime is a complex issue. There exists a vast body of knowledge regarding real-world crime; however, as crime has evolved online some of that knowledge may now be redundant, and therefore more research is required to rebuild the knowledge base. Given the evolving and adaptive nature of the phenomenon, unexpected events such as the increasing decriminalisation of piracy and the spontaneous generation of CAM by minors, evidently there exist significant challenges in terms of investigating cybercrime and any associated social impact. Going forward it may be observed that if a crime even vaguely involves cyber technologies at some point, it could be labelled a 'cybercrime'. Moreover, taking this position to a not-too-distant future, it is quite easy to imagine a context where all crime may be some form of cybercrime (Mc Mahon, 2013). Given the proliferation of networked surveillance devices, the question must be asked, how easy will it be to commit a crime in the future or indeed the present, *without* there being some 'cyber' aspect – that is, without leaving some digital forensic trace? The corollary to such an observation is that when everyone is carrying a smartphone or similar device (loaded with valuable personal data), coupled with an ever increasing presence of privatised Unmanned Aerial Vehicles (UAVs) in the skies, people may hypothetically enter a state of ubiquitous high-risk victimology. Both might seem like straightforward observations from a criminological standpoint, but are considerably more troublesome from a social impact perspective.

Notes on contributors

Mary Aiken is the Director of RCSI CyberPsychology Research Centre. She also held positions such as Academic Adviser (Psychology) in Europol Cyber Crime Centre (EC3); Research Fellow in IBM Swansea University Network Science Research Centre; and Research Fellow in Middlesex University School of Law.

Ciaran Mc Mahon is Research and Development Coordinator in RCSI CyberPsychology Research Centre.

Ciaran Haughton is a Research Assistant in RCSI CyberPsychology Research Centre.

Laura O'Neill is a Research Assistant in RCSI CyberPsychology Research Centre.

Edward O'Carroll is a Research Assistant in RCSI CyberPsychology Research Centre.

References

Aiken, M., & Mc Mahon, C. (2014). A primer on research in mediated environments: Reflections on cyber-methodology. *Social Sceince Research Network*. Retrieved from http://papers.ssrn.com/abstract=2462700

Aiken, M., Moran, M., & Berry, M. J. (2011, September 5–7). *Child abuse material and the Internet: Cyberpsychology of online child related sex offending*. 29th Meeting of the INTERPOL Specialist Group on Crimes against Children (pp. 1–22), Lyon.

Akdeniz, Y. (2008). *Internet child pornography and the law: National and international responses* (4th ed.). Hampshire: Ashgate.

Altschuller, S., & Benbunan-Fich, R. (2009). Is music downloading the new prohibition? What students reveal through an ethical dilemma. *Ethics and Information Technology*, *11*(1), 49–56. doi:10.1007/s10676-008-9179-1

Amiran, E., Unsworth, J., & Chaski, C. (1992). Networked academic publishing and the rhetorics of its reception. *Centennial Review*, *36*(1), 43–58.

Appleby, N. (2010). Labelling the innocent: How government counter-terrorism advice creates labels that contribute to the problem. *Critical Studies on Terrorism*, *3*(3), 421–436. doi:10.1080/17539153.2010.521643

Asllani, A., & Ali, A. (2012). Using simulation to investigate virus propagation in computer networks. *Network and Communication Technologies*, *1*(2), 76–85. doi:10.5539/nct.v1n2p76

Bandura, A. (1977). *Social learning theory*. Oxford: Prentice-Hall.

Barnes, S. B. (2006). A privace paradox: Social networking in the United States. *A Privacy Paradox*, *11*(9). doi:10.5210/fm.v11i9.1394

Bartlett, J. (2014). *Dark net drug markets kept alive by great customer service*. Retrieved September 23, 2014, from http://www.wired.co.uk/news/archive/2014-08/21/buying-drugs-on-the-dark-net/viewgallery/284

Becker, H. S. (1997). *Outsiders: Studies in the sociology of deviance*. New York, NY: Simon & Schuster.

Bissett, A., & Shipton, G. (1999). Some human dimensions of computer virus creation and infection. *International Journal of Human-Computer Studies*, *52*, 899–913. doi:10.1006/ijhc.1999.0361

Bocij, P. (2006). *The dark side of the internet: Protecting yourself and your family from online criminals*. Greenwood Publishing Group. Retrieved from http://books.google.com/books?hl=en&lr=&id=o5h2qwyDzRsC&pgis=1

Bounie, D., Bourreau, M., & Waelbroeck, P. (2006). Piracy and demands for films: Analysis of piracy behavior in French universities. *Review of Economic Research on Copyright Issues*, *3*(2), 15–27. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=936049

Bourke, M. L., & Hernandez, A. E. (2009). The "Butner Study" Redux: A report of the incidence of hands-on child victimization by child pornography offenders. *Journal of Family Violence*, *24*, 183–191.

BPI. (2013). *BPI digital music nation*. London. Retrieved from http://www.ukmusic.org/assets/general/Digital_Music_Nation_2013_LR.PDF

Bradley, K. (2014). *Speech to the finance services' cybercrime summit*. Finance Services' Cybercrime Summit. London. Retrieved from https://www.gov.uk/government/speeches/karen-bradleys-speech-to-the-finance-services-cybercrime-summit

Brennan, C. (2015). *An American teenager has barely escaped prosecution for sexually exploiting ... himself*. Retrieved September 24, 2015, from http://www.thejournal.ie/naked-selfie-prosecution-2344010-Sep2015/?utm_source=facebook_short

Brignall, M. (2015, March 14). TalkTalk won't listen as another fraud victim fights for compensation. *The Guardian*. London.

Campbell, A. (2015). *Inside Microsoft's digital crimes unit*. Retrieved September 25, 2015, from http://smallbiztrends.com/2015/04/microsoft-digital-crimes-unit.html

Cid, D. (2014). *More than 162,000 wordpress sites used for distributed denial of service attack*. Retrieved September 28, 2015, from https://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html

Clough, J. (2010). *Principles of cybercrime*. New York, NY: Cambridge University Press.

Cooper, A., Delmonico, D. L., & Burg, R. (2000). Cybersex users, abusers, and compulsives: New findings and implications. *Sexual Addiction and Compulsivity*, *7*, 5–29.

Coroners and Justice Act 2009 (c 25), s. 62, *The Crown Prosecution Service*, UK.
Davies, C. (2010, January). Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley
Deeney, D. (2015). *Shy fraudster who pocketed almost £300k from his "sophisticated" film-streaming website jailed for four years*. Retrieved September 23, 2015, from http://www.belfasttelegraph.co.uk/news/northern-ireland/shy-fraudster-who-pocketed-almost-300k-from-his-sophisticated-filmstreaming-website-jailed-for-four-years-31512777.html
Deloitte. (2014, February 26). Banding together to fight cyber crime. *The Wall Street Journal*. Retrieved from http://deloitte.wsj.com/cio/2013/02/26/band-together-to-fight-cyber-crime/
Dye, J., Ax, J., & Finkle, J. (2013). *Huge cyber bank theft spans 27 countries*. Retrieved September 4, 2014, from http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cybercrime-idUSBRE9480PZ20130509
Europol. (2014a) *Europol iOCTA: Threat assessment* (*abridged*)*: Internet facilitated organised crime*. The Hague. Retrieved September 10, 2015 https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
Europol. (2014b). *European cybercrime centre cybercrime: A growing global problem*. Retrieved from https://www.europol.europa.eu/ec3old
Feldman, P., & Feldman, M. P. (1993). *The psychology of crime: A social science textbook*. New York, NY: Cambridge University Press. Retrieved from http://books.google.ie/books/about/The_Psychology_of_Crime.html?id=aqjSf3lLMzoC&pgis=1
Furnell, S. (2009). Hackers, viruses and malicious software. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime* (pp. 173–193). New York, NY: Willan.
Gibbs, S. (2014, February 14). What to do if your email gets hacked – and how to prevent it. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/feb/03/what-to-do-email-hacked-how-to-prevent
Going Dark: The Internet Behind The Internet. (2014). Retrieved September 23, 2015, from http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet
Goldman, D. (2010). *Music's lost decade: Sales cut in half*. Retrieved July 23, 2014, from http://money.cnn.com/2010/02/02/news/companies/napster_music_industry/
Goncharov, M. (2012). *Russian underground 101. Trend micro incorporated*. Cupertino. Retrieved from http://dl.packetstormsecurity.net/papers/general/wp-russian-underground-101.pdf
Goodman, K. (2013). *The dark net: The new face of black markets and organized crime*. Retrieved September 4, 2014, from http://www.huffingtonpost.com/kevin-goodman/internet-black-markets_b_4111000.html
Gozzi, R. J. (1994). *The cyberspace metaphor*. Retrieved August 26, 2014, from http://www.thefreelibrary.com/The+cyberspace+metaphor.-a015543199
Green, C. (2014, July 23). New internet piracy warning letters rules dismissed as "toothless." *The Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/new-internet-piracy-warning-letters-rules-dismissed-as-toothless-9623907.html
Groenfeldt, T. (2013). *Hackers collaborate, now white hats can share cybercrime info*. Retrieved September 4, 2014, from http://www.forbes.com/sites/tomgroenfeldt/2013/11/04/hackers-collaborate-now-white-hats-can-share-cyber-crime-info/
Gross, R., Acquisti, A., & Heinz, H. J. (2005). *Information revelation and privacy in online social networks*. Proceedings of the 2005 ACM workshop on Privacy in the electronic society – WPES '05 (p. 71). New York, NY: ACM Press. doi:10.1145/1102199.1102214
Gunkel, D. J. (2005). Editorial: Introduction to hacking and hacktivism. *New Media & Society*, *7*, 595–597. doi:10.1177/1461444805056007
Hainsworth, J., & Sterling, T. (2014). *Dutch man's case linked to Amanda Todd*. Retrieved September 29, 2015, from https://www.bostonglobe.com/news/world/2014/04/18/dutch-man-case-linked-amanda-todd/39eIi53AFtgqc79yqH8JTJ/story.html
Hayes, D. (1989). *Behind the silicon curtain: The seductions of work in a lonely era*. London: Free Association Books.
Hornyak, T. (2015). *Hack to cost Sony $35 million in IT repairs*. Retrieved September 24, 2015, from http://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.html
Huang, H. (2015). A war of (mis)information: The political effects of rumors and rumor rebuttals in an authoritarian country. *British Journal of Political Science*. Advance online publication doi:10.1017/S0007123415000253

International Telecommunications Union. (2015). *ICT facts and figures – The world in 2015*. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Jurgenson, N. (2011). Digital dualism versus augmented reality. *Cyborgology*, *24*. doi:10.1089/cyber.2009.0226

Kain, E. (2015). *HBO is going after* "*game of thrones*" *pirates*. Retrieved September 23, 2015, from http://www.forbes.com/sites/erikkain/2015/04/19/hbo-is-going-after-game-of-thrones-pirates/

Kassner, M. (2014). *TEDx Birmingham: Call the police on cybercrime*. Retrieved September 4, 2014, from http://www.techrepublic.com/article/tedx-birmingham-call-the-police-on-cybercrime/

Kirwan, G., & Power, A. (2012). *The psychology of cybercrime: Concepts and principles*. Cambridge: Cambridge University Press.

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. New York: Cambridge University Press.

Kotenko, J. (2014). *What is Tor*? *A beginner's guide to the underground internet*. Retrieved September 23, 2015, from http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/

Lanning, K. V. (2008). *Child pornography.* Paper presented at the Child Pornography Roundtable, National Center for Missing and Exploited Children, Washington, DC.

Latane, B. (1981). The psychology of social impact. *American Psychologist*, *36*(4), 343–356. doi:10.1037/0003-066X.36.4.343

Leary, M. (2010). Sexting or self-produced child pornography? The dialogue continues – structured prosecutorial discretion within a multidisciplinary response. *Virginia Journal of Social Policy and the Law*, *17*, 486–566.

Lenhart, A. (2009). *Adults and social network websites*. Retrieved September 9, 2014, from http://www.pewinternet.org/2009/01/14/adults-and-social-network-websites/

Levin, A. M., Dato-on, M. C., & Manolis, C. (2007). Deterring illegal downloading: The effects of threat appeals, past behavior, subjective norms, and attributions of harm. *Journal of Consumer Behaviour*, *6* (2–3), 111–122. doi:10.1002/cb.211

Lysonski, S., & Durvasula, S. (2008). Digital piracy of MP3s: Consumer and ethical predispositions. *Journal of Consumer Marketing*, *25*(3), 167–178. doi:10.1108/07363760810870662

Maass, P., & Rajagopalan, M. (2012). *Does cybercrime really cost $1 trillion*? Retrieved September 23, 2015, from http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud & Security*, *6*, 9–13. doi:10.1016/S1361-3723(13)70053-8

McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies. (2014). Retrieved September 23, 2015, from http://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx

McAfee Enterprise. (2013). *SMBs false sense of security: How this is putting their businesses in Jeopardy.* Retrieved September 4, 2014, from https://blogs.mcafee.com/business/smbs-false-sense-of-security-how-is-this-putting-their-business-in-jeopardy/

McKenzie, J. (2009). Illegal music downloading and its impact on legitimate sales: Australian empirical evidence. *Australian Economic Papers*, *48*(4), 296–307. http://doi.wiley.com/10.1111/j.1467-8454.2009.00377.x

Mc Mahon, C. (2013, December 13). *All crime is cybercrime*. An Garda Síochána Analyst Service Annual Conference. Dublin, Ireland.

Meyer, M. (1995, February). Stop! Cyberthief! *Newsweek*, 36–38. Retrieved from http://www.d.umn.edu/~pcannan/mikemeyer.pdf

Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2012). Prevalence and characteristics of youth sexting: A national study. *Pediatrics*, *129*(1), 13–20. doi:10.1542/peds.2011-1730

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* Wiley & Sons. Retrieved from http://books.google.ie/books/about/The_Art_of_Deception.html?id=VR_aVP0KKh8C&pgis=1

Mitnick, K. D., & Simon, W. (2011). *Ghost in the wires: My adventures as the world's most wanted hacker.* New York, NY: Little, Brown and Company.

Moores, T. T., & Chang, J. C.-J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, *30*(1), 167–180. Retrieved from http://dl.acm.org/citation.cfm?id=2017284.2017294

Moran, M. (2010). *Online child abuse material offenders: Are we assigning law enforcement expertise appropriately*? Unpublished manuscript. Dublin, Ireland: University College Dublin.

Moraski, L. (2011). Cybercrime knows no borders. *Infosecurity*, *8*(2), 20–23. doi:10.1016/S1754-4548(11)70021-3

Mueller, R. S. I. (2012). *Combating threats in the cyber world: Outsmarting terrorists, hackers, and spies*. Retrieved from http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Nandedkar, A., & Midha, V. (2012). It won't happen to me: An assessment of optimism bias in music piracy. *Computers in Human Behavior*, *28*(1), 41–48. doi:10.1016/j.chb.2011.08.009

Naughton, J. (2015, February 7). Aaron Swartz stood up for freedom and fairness – and was hounded to his death. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy

Nazario, J. (2009). Politically motivated denial of service attacks. In C. Czosseck & K. Geers (Eds.), *The virtual battlefield* (pp. 163–181). Amsterdam: IOS Press.

NCMEC. (2015). *National Center for Missing and Exploited Children*. Retrieved March 12, 2015 http://www.missingkids.com/home

Nicholls, J. (2015). *Europol backs Barclays as pair commit to cybercrime fight*. Retrieved September 28, 2015, from http://www.cbronline.com/news/cybersecurity/business/europol-backs-barclays-as-pair-commit-to-cybercrime-fight-4612750

O'Neill, P. H. (2013). *Teens on Tumblr can't stop bragging about silk road drug deals*. Retrieved September 23, 2015, from http://www.dailydot.com/crime/tumblr-teens-silk-road-drug-deals/

Ostrager, B. (2010). SMS. OMG! LOL! TTYL: Translating the law to accomodate today's teens and the evolution from texting to sexting. *Family Court Review*, *48*(4), 712–726. http://doi.wiley.com/10.1111/j.1744-1617.2010.01345.x

Paganini, P. (2012). *Why humans could be the weakest link in cyber security chain*? Retrieved August 21, 2015, from http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html

Pagliery, J. (2014). *The deep web you don't know about*. Retrieved September 23, 2014, from http://money.cnn.com/2014/03/10/technology/deep-web/index.html

Peltzman, S. (1975). The effects of automobile safety regulation. *Journal of Political Economy*, *83*(4), 677–726. Retrieved from http://www.jstor.org/discover/10.2307/1830396?uid=17134080&uid=3738232&uid=2&uid=3&uid=67&uid=18761664&uid=62&sid=21104621298313

Phippen, A. (2009). *Sharing personal images and videos among young people*. Exeter. Retrieved from http://www.blackpoollscb.org.uk/contents/documents/sexting-detail.pdf

Plesser, B. (2014). *Skilled, cheap Russian hackers power American cybercrime* – NBC News.com. Retrieved September 4, 2014, from http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371

Poulsen, K. (2013). *FBI admits it controlled tor servers behind mass malware attack*. Retrieved September 9, 2014, from http://www.wired.com/2013/09/freedom-hosting-fbi/

Proshansky, H. M. (1987). The field of environmental psychology: Securing its future. *Handbook of Environmental Psychology*, *2*, 1467–1488.

Protection of Children Act 1978 (c 37), s.1, *The Crown Prosecution Service, UK*.

Quayle, E., & Jones, T. (2011). Sexualized images of children on the Internet. *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 7–21. doi:10.1177/1079063210392596

Reeves, M. (2002). *Measuring the economic and social impact of the arts: A review*. London: Arts Council of England. Retrieved from http://culturability.org/wp-content/blogs.dir/1/files_mf/1271761227measuringtheeconomicandsocialimpactofthearts.pdf

Ringrose, J., Gill, R., Livingstone, S., & Harvey, L. (2012). *A qualitative study of children, young people and "sexting."* London. Retrieved from http://eprints.lse.ac.uk/44216/1/__Libfile_repository_Content_Livingstone, S_A qualitative study of children, young people and "sexting" (LSE RO).pdf

Robinson, J. (2010, December 16). Britons "downloaded 1.2bn illegal tracks this year" | Media | theguardian.com. *The Guardian*. Retrieved from http://www.theguardian.com/media/2010/dec/16/illegal-music-downloading-online-piracy

Rock, P. (2007). Sociological theories of crime. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *The Oxford handbook of criminology* (pp. 3–42). Oxford: Oxford University Press.

Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Retrieved from http://books.google.ie/books?hl=en&lr=&id=teZ8pAHJUa8C&oi=fnd&pg=PP2&dq=rosenzweig+books+cyber+warfare&ots=5-NPcIPT6C&sig=FjIUgIrkbwXEWPmTXcGXVAt-xEA&redir_esc=y#v=onepage&q=rosenzweig books cyber warfare&f=false

Schwartz, M. (2014). *EU to roll out cybercrime taskforce*. Retrieved September 5, 2014, from http://www.bankinfosecurity.com/eu-to-roll-out-cybercrime-taskforce-a-7093/op-1

Seal, M. (2015, March). An exclusive look at Sony's hacking Saga. *Vanity Fair*. Retrieved from http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

SecurityWeek. (2015). *SurfWatch labs enables intelligence sharing across extended enterprise*. Retrieved September 23, 2015, from http://www.securityweek.com/surfwatch-labs-enables-intelligence-sharing-across-extended-enterprise

Selby, N. (2012). *There's No 911 for cybercrime, but would anyone call if there were*? Retrieved September 28, 2015, from http://www.pcworld.com/article/254499/theres_no_911_for_cybercrime_but_would_anyone_call_if_there_were_.html

Selwyn, N. (2007). A safe haven for misbehaving?: An investigation of online misbehavior among university students. *Social Science Computer Review*, *26*(4), 446–465. doi:10.1177/0894439307313515

Serious Crime Act 2015, s. 41–44, *Home Office*, UK.

Shang, R.-A., Chen, Y.-C., & Chen, P.-C. (2007). Ethical decisions about sharing music files in the P2P environment. *Journal of Business Ethics*, *80*(2), 349–365. doi:10.1007/s10551-007-9424-2

Sherwin, A. (2013). *Music and film industries winning war on piracy, says report*. Retrieved July 23, 2014, from http://www.independent.co.uk/arts-entertainment/music/news/music-and-film-industries-winning-war-on-piracy-says-report-8714499.html

Sirkeci, I., & Magnúsdóttir, L. B. (2011). Understanding illegal music downloading in the UK: A multi-attribute model. *Journal of Research in Interactive Marketing*, *5*(1), 90–110. Retrieved from http://www.academia.edu/491842/Understanding_illegal_music_downloading_in_the_UK_A_multi-attribute_model

Slane, A. (2007). Democracy, social space, and the internet. *University of Toronto Law Journal*, *57*(1), 81–105. doi:10.1353/tlj.2007.0003

Smith, M. D., & Telang, R. (2012). Assessing the academic literature regarding the impact of media piracy on sales. *SSRN Electronic Journal*. Retrieved from http://papers.ssrn.com/abstract=2132153

Stone, B., & Riley, M. (2013, February). *Hacked*? *Who ya gonna call*? Retrieved September 4, 2014, from https://dl.mandiant.com/EE/library/businessweek_eprint.pdf

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *7*(3), 321–326. doi:10.1089/1094931041291295

Suler, J. (2013). *Cyberpsychology as interdisciplinary, applied, and experiential*. Retrieved September 4, 2014, from http://cypsy.com/News/Cyberpsychology_as_Interdisciplinary

Svensson, M., & Larsson, S. (2012). Intellectual property law compliance in Europe: Illegal file sharing and the role of social norms. *New Media & Society*, *14*(7), 1147–1163. doi:10.1177/1461444812439553

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670. Retrieved from http://www.jstor.org/stable/2089195?seq=1#page_scan_tab_contents

Tassi, P. (2013, April). "Game of Thrones" sets piracy world record, but does HBO care? *Forbes*. Retrieved from http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care/

Temple, J. R., Paul, J. A., van den Berg, P., Le, V. D., McElhany, A., & Temple, B. W. (2012). Teen sexting and its association with sexual behaviors. *Archives of Pediatrics & Adolescent Medicine*, *166*(9), 828–833. doi:10.1001/archpediatrics.2012.835

The Centre for Secure Information Technologies (CSIT). (2014). *4th world cyber security technology research summit: Securing our digital tomorrow*. Belfast. Retrieved from http://www.csit.qub.ac.uk/News/Events/Belfast2014/Filetoupload,450092,en.pdf

United States of America v. Ross Ulbricht, 1:13-mj-02328. (2014). *New York Southern District Court*. Retrieved from http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR/US v. Ross Ulbricht Indictment.pdf

US Attorney's Office District of Massachusetts. (2011). *Alleged hacker charged with stealing over four million documents from MIT network*. U.S. Department of Justice. The U.S. Attorney's Office Massachusetts. Retrieved from http://www.justice.gov/archive/usao/ma/news/2011/July/SwartzAaronPR.html

U.S. Department of Justice. (2010). *The national strategy for child exploitation prevention and interdiction: A report to congress*. Retrieved from http://www.justice.gov/sites/default/files/psc/docs/natstrategyreport.pdf

Viégas, F. B. (2006). Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated Communication*, *10*(3). doi:10.1111/j.1083-6101.2005.tb00260.x

Volkov, D., Grudinov, S., Skripkar, T., Kislitsin, N., Belov, V., & Kalinin, A. (2013). *Group-IB Threat Intelligence Report 2012-2013 H1*. Retrieved from http://report2013.group-ib.com/

Warren, M., & Leitch, S. (2009). Hacker taggers: A new type of hackers. *Information Systems Frontiers*. doi:10.1007/s10796-009-9203y

Wilde, G. J. S. (1998). Risk homeostasis theory: An overview. *Injury Prevention*, *4*(2), 89–91. doi:10.1136/ip.4.2.89

Wingrove, T., Korpas, A. L., & Weisz, V. (2011). Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy. *Psychology, Crime & Law*, *17*(3), 261–276. http://dx.doi.org/10.1080/10683160903179526

Winter, A. (2013). *Downloaded*. United States: Trouper Productions.

Wolak, J., & Finkelhor, D. (2011) '*Sexting: A typology*'. Research Bulletin (March), University of New Hampshire: Crimes Against Children Research Center.

Wolak, J., Finkelhor, D., & Mitchell, K. (2011). Child pornography possessors: Trends in offender and case characteristics. *Sexual Abuse : A Journal of Research and Treatment*, *23*(1), 22–42. doi:10.1177/1079063210372143

Yar, M. (2005). The global "epidemic" of movie "piracy": Crime-wave or social construction? *Media, Culture & Society*, *27*(5), 677–696. doi:10.1177/0163443705055723

Zhang, X. (2010). Charging children with child pornography – using the legal system to handle the problem of "sexting." *Computer Law & Security Review*, *26*(3), 251–259. doi:10.1016/j.clsr.2010.03.005