Oxford Research Encyclopedia of Criminology

Online Crime

Majid Yar

Subject: Crime, Media, and Popular Culture Online Publication Date: Dec 2016
DOI: 10.1093/acrefore/9780190264079.013.112

Summary and Keywords

The development of the Internet and related communication technologies has had a transformative effect upon social, political, economic, and cultural life. It has also facilitated the emergence of a wide range of crimes that take shape in the spaces of virtual communication. These offenses include technology-oriented crimes such as hacking and the distribution of malicious software; property-oriented crimes such as media piracy, theft, and fraud; and interpersonal offenses such as stalking, harassment, and sexual abuse. In many instances, these crimes serve to entrench and exacerbate existing patterns of victimization, vulnerability, and inequality, along lines of difference related to gender, sexuality, ethnicity, age, and income. The anonymized and globally distributed nature of the Internet creates huge challenges for crime prevention, detection, and prosecution of online offenses.

Keywords: cybercrime, hacking, malware, piracy, stalking, hate speech, sexual offenses, surveillance, policing

Internet Crime: History, Contexts, and Definitions

It is now commonplace to observe that the development of Information and Communication Technologies (ICTs) has transformed the world, impacting upon many and diverse areas including the social, cultural, economic, and political.[1] Analysts and commentators have attempted to capture these changes by suggesting that we now live in an “information society,” an “information era,” a “virtual society,” a “post-industrial” society, a “knowledge society,” or a “network society.” All such accounts place central emphasis upon the transformative power of ICTs to reconfigure and reorganize human action and interaction, thereby creating a new social order that differs markedly from what has come before. With respect to matters of crime and deviance, criminologists have of late started to direct concerted attention to the ways that the informational era changes both the nature and patterns of lawbreaking behavior, and how it presents new and unprecedented challenges for crime prevention and crime control. Central to these new dynamics is the role played by the Internet (and related technologies) in driving processes of globalization; in altering the relations between our local lives and experiences, and the wider transnational realm; and in simultaneously reproducing patterns of power, inequality, and harm on the one hand, while also providing means through which some of those relations and patterns might be challenged in the name of greater equality and freedom.

This essay introduces the main debates around online crime, most commonly discussed in the criminological literature under the concept of "cybercrime." It begins by attempting to define just what is meant by cybercrime, before turning to consider what is known about the nature and extent of such crime, and how its emergence is connected to the process of global social change. This is followed by an overview of the main forms or "types" of cybercrime, considering how each in turn is connected to patterns of power, inequality, and harm. It concludes by exploring the possible future trends and developments in cybercrime, alongside a reflection on the various competing strategies that have been proposed to combat cybercrime, protect victims, apprehend and punish offenders, and to reduce the scale of harm that it may cause.

Before turning to consider cybercrime, it is worth reflecting on the rapid growth of electronic communication technologies over recent decades. The Internet, as its name suggests, is in essence a computer network; or, to be more precise, a "network of networks." A network links computers together, enabling communication and information exchange between them. Many such ICT networks have been in existence for decades—those of financial markets, the military, government departments, business organizations, universities, and so on. The Internet provides the means to link up the many and diverse networks already in existence, creating from them a single network that enables communication between any and all "nodes" (e.g., individual computers or other similar devices) within it. Originally developed as a communications network by U.S. military researchers in the 1960s, by the 1990s it had been handed over to civilian control and underwent rapid development, primarily in universities and scientific research institutions. This period saw the development of the "World Wide Web" (www), software that provided a common "language" through which computers could share information such as text and images. The first commercial web browsing software, called Netscape, was launched in 1994, with Microsoft launching its own Internet Explorer the following year. These browsers made Internet access possible from personal computers (PCs). In the mid-1990s, numerous commercial Internet Service Providers (ISPs) entered the market, offering connection to the Internet for anyone with a computer and access to a conventional telephone line. This was later followed by the development of broadband technologies that massively increased the speed at which information could be shared across the Internet, alongside the popularization of mobile Internet connectivity using "personal digital assistants" (PDAs), smartphones, and tablets.

Since the commercialization of the Internet in the mid-1990s, its growth has been incredibly rapid. Between 1994 and 1999 the number of countries connected to the Internet increased from 83 to 226.[2] In December 1995 there were an estimated 16 million Internet users worldwide; by May 2002, this figure had increased to over 580 million, almost 10% of the world's total population.[3] As of November 2015 the total number of Internet users had reached an estimated 3.3 billion, comprising some 46.4% of the global population.[4] However, it is crucial to bear in mind that, despite this phenomenal growth, access to the Internet remains highly uneven both between countries and regions, and within individual nations. The technical capacity enabling Internet access (PCs, software, reliable telecommunications, and electricity grids) is unevenly distributed—for example, more than 70% of households in Europe have Internet access, while the comparable figure for the African continent is less than 6%.[5] Similarly, while Europe boasts 200 broadband Internet connections for every 1,000 people, in Africa there is only one such connection per 1,000 people.[6] Within individual nations, connection densities vary between more and less prosperous regions and between urban and rural areas.[7] Access is also differentiated according to levels of state control, restriction, or censorship exercised by states, alongside surveillance of usage and punishment for accessing prohibited content.[8] Unequal access also follows existing lines of social exclusion within individual countries—factors such as employment, income, education, ethnicity, and disability are reflected in the patterns of Internet use.[9] These inequalities are criminologically important, as they tell us something about the likely social characteristics of both potential cybercriminal offenders and their potential victims.

Next it is necessary to define, as clearly as possible, just what is meant by "cybercrime." This term does not refer to a single type of criminal behavior (such as theft, fraud, or sexual abuse). Instead, it covers a very wide range of offenses, which nevertheless share an important defining feature—they are committed using digital electronic technologies, such as the Internet, new social media (platforms such as Facebook and Twitter), email, and instant messaging. The term cybercrime has come to be used as a convenient shorthand to denote patters of criminal and rule-breaking activity that are associated in some fashion with the new electronically based information environment. Criminologists have considered how the growth of the Internet has transformed patterns of criminal activity, possibly generated new forms of crime and deviance, and created unprecedented challenges for policing and security.

From the outset, criminologists have debated whether cybercrime marks the emergence of a "new" form of crime or criminality, and if so, would such novelty require us to set aside (or at least modify, supplement, or extend) the existing theories and concepts that criminologists use to explain crime. Unsurprisingly, answers to such questions vary widely. Some criminologists have suggested that the emergence of "virtual crimes" marks the establishment of a new and distinctive social environment ("cyberspace" as opposed to "real space") with its own structures, forms of interaction, roles and rules, limits and possibilities. In this alternate social space, new and distinctive forms of criminal activity emerge, requiring the development of a matching and innovative criminological vocabulary.[10] Skeptics, in contrast, see cybercrime at best as a case of familiar criminal activities pursued with some helpful (at least for the offender) new tools and techniques—in Peter Grabosky's (2001) metaphor, largely a case of "old wine in new bottles."[11] If this were the case, then cybercrime could still be explained, analyzed, and understood using established criminological concepts and theories.

In light of these disagreements, it is important to gain a clearer idea about what may or may not be new or different about cybercrime. One of the most useful classifications for tackling these matters has been developed by David Wall.[12] In analyzing the emergence of cyber offenses, Wall distinguished between "computer integrity crimes," "computer assisted crimes," and "computer content crimes." Each of these forms of offending depends upon exploiting information and communication technologies in different ways. Briefly, they can each be defined as follows.

Computer Integrity Crimes

Computer integrity crimes are those aimed at the network of electronic communications itself, targeting both its computer hardware and the software that enables it to function. These crimes include hacking (unauthorized access, intrusion, and potential interference with a computer system); the distribution of "malware" (malicious software, such as viruses, worms, and Trojans) that can affect the operation of the devices targeted; and "denial-of-service" attacks that take web-based services offline, often by flooding them with an unmanageable number of communication requests. What is noteworthy about such integrity crimes is that they can be seen as wholly new forms of offending—they are only made possible by the existence and architecture of the computer network itself, and in the absence of that ICT-based order they could not exist.

Computer-Assisted Offenses

The second kind of offenses amounts to a reworking of established forms of offending in the new informational environment. They include various forms of theft and fraud—they may target goods and services, money and finance, or information itself (such as confidential data, personal details, private communications, or, as is extremely common, the various forms of legally protected intellectual properties that are bought and sold online). They also include a variety of forms of interpersonal victimization, such as sexual harassment, virtual abuse, trolling, and stalking.

Computer Content Crimes

The third type of crime centers on the content of computerized communication itself. Of particular note are those communications that breach legally defined limits on speech, where, for example, certain types of communication and representation are considered harmful to society and its various communities. These include high-profile and widely debated practices such as the circulation of obscene and violent images; sexualized images of children; expressions that incite political violence (such as “terrorism”); and messages that express and incite hatred against ethnic, religious, sexual, and other minorities.

All three of these types of cybercrime will be considered in more detail in the next section, focusing in particular upon the patterns of power, violence, and harm they entail. However, before such exploration, it is necessary to note some important features of such cybercrimes. While computer-assisted and computer content crimes may “repackage” familiar types of criminal behavior, in doing so they change the nature of these offenses, and create new dynamics that challenge attempts to control crime. They may not be unprecedented, but their relocation to the space of digital communication does transform them in significant ways that must be recognized. For example, fraudsters are now enabled to make their “pitches” electronically to millions of potential victims though spam emailing, text messages, and social media, and can do so simultaneously and at virtually no cost. The increasing use of ICTs for financial transactions (ranging from e-shopping to e-banking) makes users vulnerable to theft of sensitive information, including details of credit cards and bank accounts. Through communication channels such as email, instant messaging, and social media, individuals are made vulnerable to abuse, bullying, and threats. The ability to reproduce and virtually distribute digitized content creates seemingly ungovernable levels of unauthorized copying and sharing of musical recordings, motion pictures, and computer software. Moreover, all of these offenses can be committed at-a-distance—an offender does not need to come into direct contact with a victim in order to commit an offense. As a consequence, the local and private become vulnerable to actions and intrusions emanating from across the globe. Similarly, the kinds of communications involved in content crimes may be familiar, but take on a new lease of life in the online environment. Networked communications enable such content to be globally disseminated, allow the bypassing of restrictions imposed on established media channels, enable the exploitation of legal differences around restricted speech in different countries, and also grant those responsible a degree of anonymity that makes them difficult to identify and act against. This kind of communication is not, of course, entirely negative, as it can also enable a variety of social actors to bypass state censorship and ensure the circulations of truths and opinions that authorities may otherwise be able to silence. In sum, the development of the Internet is a prime driver of the globalization process—“The process of increasing interconnectedness between societies such that events in one part of the world more and more have effects on peoples and societies far way."[13] Just as the Internet has played a key role in globalizing the economy, politics, and culture, it has also played an important part in globalizing crime, instantaneously connecting victims and offenders across huge distances.

Exploring the Varieties of Cybercrime

This section considers in more detail the different types of cybercrime, in an attempt to explicate the patterns of offending and victimization they involve, and how these connect with issues of power, inequality, and harm in a globalized world.

Computer-Oriented Crimes: Hacking, Viruses, and Denial-of-Service Attacks

The term "hacking" has become almost synonymous with computer crime, an association that is bolstered by popular representations in film and television. Such fictions propagate an image of hacking as a powerful and rather mysterious art used by computer virtuosos and geniuses to manipulate computers in seemingly limitless ways. The reality of hacking may in fact be rather more mundane, but is nonetheless far-reaching in its impacts, as examined below.

"Hacking" has a long history that has embraced multiple and shifting meanings. It was originally used to describe the act of creative problem solving when faced with complex technical problems. However, this sense has been overtaken by a more negative meaning, namely, the illicit and usually illegal activities associated with unauthorized access to, or interference with, computer systems. The word is now widely used as shorthand for a range of illicit activities that manipulate networked computers and other devices, either by taking direct control of those computers, or otherwise changing or damaging their normal operations. Thus, for example, the creation and distribution of malicious software or "malware" (such as viruses), and the "crashing" of websites (through so-called "denial-of -service attacks") form part and parcel of the wider span of activities associated with hackers and hacking. Not only has the meaning of the term shifted over time, but the profile and purposes of those engaged in such activities have also undergone significant change alongside the development of the Internet. In its early years, hacking was very much associated with disparate and loosely organized groups of (mainly young, male) computer enthusiasts who used it to test their knowledge and skills, and as a form of exploration of the emerging online realm.[14] The successful engineering of hacks was also a means for individuals to seek status and esteem from others in the hacker subculture, and to create and sustain a sense of collective belonging not dissimilar to that found among other "deviant" youth subcultures.[15] However, over time, a wide range of other actors have entered the arena, including individual criminal entrepreneurs, disgruntled employees, organized crime groups, state military and security services, social protest movements, and "terrorist" organizations.

Financial gain appears to be an important motive for hacking, both on an individual and more of a collective, organized basis.[16] Hackers may exploit unauthorized access in order to steal or copy information including software, business secrets, personal information about an organization's employees and customers, and credit card details that can subsequently be used for fraudulent purposes. Theft of proprietary information is cited as the greatest source of financial losses by business and other organizations.[17] There have even been cases in which seemingly reputable business organizations have allegedly commissioned hackers to steal confidential information from their competitors.[18] Incidents also abound in which thousands of customer credit card details have been stolen as a result of hacking incidents, or in which hackers were able to exploit banks' systems to arrange illegal electronic transfers of funds.[19]The financial harms resulting from hacking are further increased through the widespread distribution of viruses and other forms of malicious software. By the end of 2013, there were an estimated 196 million unique variants of malware in existence, with millions of new viruses appearing every year.[20] It is further worth noting that the risks of victimization are likely to be unevenly shared, with the least experienced and knowledgeable users (the very young, the elderly, and those with poor educational levels) being more likely to fall prey to illicit exploitation of their computers.

In addition to the victimization of businesses and individual computer users by criminals, hacking and related techniques are also used by state actors, targeting other governments and foreign citizens, as well as their own populations. The use of hacking by state security and military organizations against rival governments is nowadays referred to as "cyberwarfare." Such attacks may be used to gather intelligence about other states' economic, political, and military capabilities and strategies, as well as undermining their capabilities through the sabotage and disruption of computer systems. For example, in 2010 an Iranian nuclear facility found its computer systems infected by a piece of malicious software called "Stuxnet." The development and dissemination of Stuxnet has been widely attributed to the United States and Israel, an attempt to disrupt Iran's nuclear weapons development program. More recently, the former U.S. National Security Agency contractor Edward Snowden claimed that the United States infiltrated the systems of a major Chinese computer manufacturing company with the ultimate aim of being able to access the computers of other nations who purchased their hardware from the Chinese firm. The possession of extensive capacities for using such techniques may serve to shape the balance of political power between states in a globalized world, favoring already powerful nations, and further disadvantaging others.[21]

However, the availability of techniques for hacking, intrusion, and disruption may not simply entrench existing patterns of power. Rather, it has been suggested that they also enable otherwise relatively powerless actors to engage in conflict and resistance with more powerful states. Small states may not be able to match their powerful counterparts in military or economic terms, but could utilize the tools of cyberwarfare to launch effective attacks. Indeed, technologically advanced nations’ huge dependence upon computer systems across all walks of life makes their “critical information infrastructure” all the more vulnerable to cyberattacks that could cripple financial and economic activity and cause huge disruption to essential services such as transport, electricity, and telecommunications.[22] The ability to use such methods in conflicts that are otherwise “asymmetrical” (in which opponents are unevenly matched in terms of power and resources) also lend itself to mobilization by both “terrorist” organizations and social protest movements. In the case of the former, we might see “the execution of a surprise attack by a subnational foreign terrorist group or individuals with a domestic political agenda using computer technology and the internet to cripple or disable a nation’s electronic and physical infrastructures.”[23] It should be noted that there are at present few, if any, concrete instances of terrorist groups resorting to such tactics, preferring instead to pursue their goals through more “conventional” forms of violence and intimidation. However, this has not prevented many states’ from introducing laws to combat cyberterrorism and spending substantial amounts of money to protect computer systems against possible terrorist actions. In contrast, there are many and diverse instances of social and political protest movements using hacking and related techniques to publicize their cause and offer resistance to what they see as forms of oppression and injustice. As early as 1998, the Electronic Disturbance Theatre used denial-of-service attacks to shut down Mexican government websites in support of the Zapatista land rights movement that aims to secure farm land for the country’s impoverished and marginalized rural peoples.[24] Similar attacks were used in 1995 by the “Strano Network,” an anti-nuclear group that targeted French Government websites.[25] In 2010, financial services providers including PayPal, Visa, and MasterCard suspended payments made in support of the controversial whistle-blowing organization WikiLeaks; within days, the Anonymous hacktivist group launched retaliatory attacks on those companies, crashing websites and rendering them temporarily inoperative.[26] In sum, computer-focused crime generates new kinds of victimization, targeting various states, businesses, and individual computer users. In a complex and contradictory dynamic, it simultaneously has the ability to entrench exiting patterns of power while also offering avenues for subaltern resistance from the global margins.

Computer-Assisted Offenses

The growth of the Internet has seen a massive increase in offenses that transpose familiar kinds of criminal behavior to the space of online communication. These are many and varied spanning frauds and “cons,” thefts, trade in illicit and prohibited goods such as drugs,[27] and interpersonal offenses (such as stalking, bullying, sexual harassment). Discussion here reflects on some well-known and important instances of computer-assisted offenses in order to glean insights into the patterns of harm and victimization they involve.

Online frauds take a number of forms, one of the most widespread being auction and retail fraud. Retail frauds involve the online sale of goods that may have been stolen, counterfeit, damaged, or otherwise misrepresented in terms of their quality or features—or simply never delivered to the paying customer.[28] Other frauds involve offenders misrepresenting themselves as government officials, so as to extort or scam money from their victims. For example, in 2011 the U.S. Internet Crime Complaint Centre (IC3) received more than 14,000 complaints from victims of such frauds, with an average reported loss of $245 each.[29] Notably, older individuals (60 years plus) were overrepresented among the complainants, and suffered much higher average losses ($484 each) as compared to younger victims. This may simply be an effect of the fact that those at the upper end of the age range have more accrued resources (for example, through savings and pensions) and so make a more attractive target for fraudsters; this would be consistent with the gender pattern among victims, with males (those with relatively greater financial resources at their disposal) being more frequent targets than females. However, it has also been suggested that older individuals are more likely to be trusting and deferential toward authority, making them more responsive to those posing as government officials.[30]

Another form of online fraud that exploits individuals' trust takes the form of dating or romance "scams." Typically, the fraudsters "hook" their victims by feigning romantic interest, then exploit the victims' emotional investment in the "relationship" to procure monies and gifts. A commonplace strategy is to claim personal hardships and family tragedies so as to pressure the victim into offering financial "support." In 2011, the ICCC received more than 5,600 complaints from victims of these scams, who lost an average of $8,900 each, amounting to a total of $50.4 million.[31] In addition to these financial losses, victims suffer significant emotional distress, feeling both foolish and betrayed. Given these emotional dynamics, it is thought that there a huge number of such offenses that go unreported; one recent study estimated that there could be as many as 200,000 victims of dating scams annually in the United Kingdom alone.[32] The statistics collated by IC3 again offer interesting insights into the demographics of victimization. The elderly, divorced, and widowed were more likely to be victims of romance scams, which prey upon loneliness and isolation to "hook" the vulnerable. There is also a clear-gendered dimension to such scams, with women over 50 being three times as likely to report falling victim to these frauds than their male counterparts.[33]

In addition to the kinds of financially oriented offenses discussed above, there are a range of interpersonal offenses such as stalking and harassment that make use of computerized communications. The term "stalking" first can to prominence in the 1980s to describe "persistent harassment in which one person repeatedly imposes on another unwanted communications and/or contacts."[34] Stalking is held to be characterized by repeated behaviors including making phone calls to victims; sending them letters, gifts, or offensive material; following and watching the victim; trespassing on the victim's property; loitering near and approaching the victim; contacting and approaching the victim's family, friends, and coworkers.[35] Stalking may be a prelude to serious physical assault and even homicide. Cyberstalking, as an extension of such behavior, has been defined as "the repeated use of the Internet, email, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual."[36] Early studies of cyberstalking suggested that it most commonly took place via the repeated sending of offensive or threatening emails,[37] and to a lesser extent on Internet chat rooms and through instant messaging services. For example, one U.S.-based study spanning the years 1996–2000 found that email served as the channel for cyberstalking in 92% of reported incidents.[38] However, subsequent developments in online communication have shifted patterns of stalking away from email and toward new social media platforms such as Facebook. In one recent study, it was estimated that 6.3% of social network users experience sustained online harassment.[39] It is important to stress the underlying patterns of victimization in such incidents; confirming the findings of previous studies, Dreßing et al. found a clear gendering of incidents, with males featuring much more frequently as perpetrators (70%) than females (30%). When it comes to victims, this ratio is reverses, with 80% of those reporting stalking being female. Therefore, cyberstalking can be viewed as an extension of long-standing patterns of harassment (sexual and otherwise) in which women are subject to unwanted attentions, abuse, and threats by men. Online behavior of this kind has received considerable attention recently, with discussion of the rise of so-called revenge porn. In such incidents "Angry exes with intimate photos or videos of their former significant others weaponize that media after the breakup by uploading it to the internet, sometimes alongside the victim's name and other identifying information."[40] Again, it is estimated that 90% of victims of such malicious postings are female.[41] Such is the concern of the phenomenon that 12 U.S. states have enacted laws to outlaw it,[42] as has the United Kingdom following provisions in Section 33 of the Criminal Justice and Courts Act 2015. It has also been noted that such gendered patterns of harassment and abuse are increasingly apparent in non-Western countries such as India, where victims' vulnerability is exacerbated by a lack of legal protection.[43]

The gendered patterns of online victimization discussed above also intersect with the disproportionate targeting of young people, through behaviors associated with cyberbullying and "trolling" via social media and mobile phones. Cyberbullying can be defined as "An aggressive, intentional act carried out by a group or individual, *using electronic forms of contact*, repeatedly and over time against a victim who cannot easily defend him or herself."[44] Studies of children and young people (most often female) subjected to cyberbullying suggest that it generates significant psychological and emotional distress, and is linked to an increased likelihood of entertaining suicidal thoughts.[45] There are now numerous recorded incidents in which young people have taken their own lives following concerted online victimization. Cyberbullying is almost invariably perpetrated by the victim's peers, and typically focuses upon concerted mockery and humiliation, often related to the individual's sexual behavior, weight, appearance, or other similar characteristics. Research indicates that the increase in such behaviors is international and cross-cultural, with patterns of victimization in countries such as China mirroring those in the West.[46]

A further dimension of online abuse, also centered upon children and young people, relates to sexual abuse and exploitation. Since the 1980s, child sexual abuse has been brought increasingly to light, with revelations about previously hidden crimes committed across many different sites—in care homes, nurseries, hospitals, churches, and schools. In the late 1990s, the focus upon pedophilia turned increasingly to the online environment. Online child sex abuse can be differentiated between that which remains "virtual" (restricted to communicative abuses committed via the Internet) and that which serves as a preparation method for later physical contact and abuse (so-called grooming of potential physical abuse victims).

Researchers claim to have uncovered a wide range of "cybersexploitation" practices taking place in Internet chat rooms and other forums. In such cases, adults or older adolescents with a sexual interest in young children use online communication in order to "identify, deceive, coerce, cajole, form friendships with and also to abuse potential victims." This may entail, first, adults engaging children in sexually explicit conversations; examples include asking questions of the child such as "Have you ever been kissed?" or "Do you ever touch yourself?"[47] Second, such behavior may entail the "fantasy enactment" of sexual scenarios through online conversation with a child. Third, it may entail what is described as "cyber-rape," in which coercion and threats are used to force a child into acting out the sexual scenarios proposed by the abuser. It has been suggested by many commentators that adult abusers exploit the Internet to disguise their identity, posing as children or adolescents in order to win the friendship and trust of their victims.[48] Children may thus be blissfully unaware that their Internet "friend" is in fact an adult whose aim is to deceive them into participation in sexual conversation and interaction. O'Connell et al. claim that surveys of children's online interaction show that 53% of chat room users aged between 8 and 11 reported having had sexual conversations online.[49] Alarm over these trends has led to legislative change in an attempt to tackle to the problem. The United Kingdom's Sexual Offences Act (2003) makes it a criminal act to incite a child to engage in sexual activity, "such as, for example, persuading children to take their clothes off, causing the child to touch themselves sexually, sending indecent images of themselves, etc." Thus those online child–adult interactions in which the child may be encouraged to engage in sexual acts is defined as "non-contact abuse" and punishable by up to 10 years imprisonment.[50]

The second area of online pedophile activity is linked to the commission of offline "contact abuse." Recent years have witnessed a growing concern that pedophiles are using Internet chat room contacts with children in order to establish a relationship of apparent friendship and trust, which can then be exploited to arrange face-to-face meetings in which sexual abuse can take place. O'Connell (2003) identifies a number of "stages" to such "grooming," starting with friendship formation (getting to know the child), progressing to relationship formation (becoming the child's "best friend"), leading to the exclusivity stage (where intimacy, trust and secrecy are established).[51] It is only when such a bond has been formed that the pedophile will move on to suggesting sexual contact. One U.Ss-based survey of 10–17-year-old Internet users found that 19% reported having been approached for sex online.[52] In response to such findings, the United

Kingdom's Sexual Offences Act (2003) introduced an offense of Internet grooming, "designed to catch those aged 18 or over who undertake a course of conduct with a child under 16 leading to a meeting where the adult intends to engage in sexual activity with a child."[53] Conviction for this offense can result in a custodial sentence of up to 5 years.

Across the range of computer-assisted interpersonal offenses, we see a complex dynamic that brings together the global and the local. These Internet crimes may confront users with acts of victimization that emanate from distant (and often anonymous) others, but may also be closely connected to local relationships (as in the case of stalking by ex-intimates and cyberbullying by peers). Whether local or global in origin, such crimes serve to reproduce "real world" patterns of power, inequality, and harm, reinforcing the exploitation associated with gender and age-related discrimination.

Computer Content Crimes

In addition to computer-focused and computer-assisted offenses, we must consider what are called content crimes—those involving the online distribution of communications that are legally prohibited. Such content crimes take three main forms, each of which will be examined in turn: obscenity (including violent pornography and child sex abuse imagery), hate speech, and terrorist discourse.

In tandem with the concerns about the online sexual exploitation of children and young people, the issues of child pornography has become the focus for a great deal of public, political, and mass media attention. The term "child pornography" (and the alternative term "child sexual abuse imagery") refers to representations featuring a child or children (minors) depicted in an explicitly sexualized manner and/or engaging in sexual activity. Such images have been classified according to different types or "levels." For example, Taylor et al. (2001) furnish a 10-fold typology of such images, ranging from the "indicative" (prima facie non-erotic images of children that are used "inappropriately" for sexual gratification), through "nudist" and "erotic posing," to the most extreme representations entailing assault, sadistic, violence and bestiality.[54] Gauging the precise extent of child pornography online is itself a difficult task. An early study, conducted in January 1998, found that 0.07% of 40,000 news groups examined (28 sites) contained "child erotica" or pornography; in addition, the study found 238 "girl-related child pornography or erotica" web pages.[55] A subsequent study claims that in the period between 2002 and 2004, the number of child pornography and pedophile websites doubled to 19,246.[56] This same study found that over half of reported websites were hosted in the United States, with Americans also figuring as the most prominent visitors to such web pages, comprising over 32% of global users. The majority of such sites were commercial in character, and it was estimated that the online trade in child pornography was worth some $3 billion per annum in 2004[57] (IFR, 2004); more recent estimates place economic returns of the trade in the region of $20 billion per year.[58] A 2009 report by the United Nations agency UNICEF estimated that there were more than 4 million websites featuring child pornography,[59] and it is claimed that there are 116,000 requests for "child pornography" every day on the Gnutella peer-to-peer file-sharing network alone.[60] Data provided by a variety of Internet monitoring organizations in recent years certainly indicates an increasing number of sites hosting such content being reported by the public.[61]

The problem of illegal sexual content is not restricted to child pornography, but also involves the online circulation of obscene and violent imagery involving adults. Generally speaking, when it comes to sexual representation involving adults, a distinction is made between the "indecent" and the "obscene." An image may be deemed indecent if it is objectionable to some viewers, yet in many (though not all) Western democracies, expressions that may be considered indecent are nevertheless tolerated and not subject to strict legal prohibition. In contrast, obscenity is used to denote representations, expressions, or actions that are held to be generally offensive and thus unacceptable by society at large. Obscenity is almost invariably subject to legal prohibition and formal, criminal sanctions. Alongside sexualized representations of minors, there are some kinds of sexual representation of adults that are considered obscene and thus meriting prohibition. The massive amount of sexual content available online (almost from the point of the Internet's inception) led, for example, to U.K. laws being updated through the 1994 Criminal Justice and Public Order Act to take account of such material in an electronic form.[62] British obscenity laws have been most recently extended to counter the production, circulation, and possession of "extreme and violent pornography." What is at stake here is not so much the depiction of acts of actual sexual violence against victims, as consensual performance in scenarios that "realistically" depict sexual violence. This issue came to prominence in the United Kingdom following the sexual assault and murder of Jane Longhurst, a 31-year-old schoolteacher at the hands of Graham Coutts. At Coutts's trial a concerted link was made between the murder and his consumption of violent pornography online, including simulated strangulation, rape, and necrophilia. The media outcry following Coutts's conviction, combined with a campaign led by the victim's mother, resulted in a petition with some 50,000 signatories being submitted to government, calling for the banning of "extreme internet sites promoting violence against women in the name of sexual gratification." This led ultimately to legislation criminalizing the possession of "extreme pornography," making such possession punishable by up to three years imprisonment.[63] Extreme pornography is defined (in the Criminal Justice and Immigration Act 2008) as that which "portrays, in an explicit and realistic way, any of the following—(a) an act which threatens a person's life,(b) an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals, (c) an act which involves sexual interference with a human corpse." These provisions have not gone unopposed, since they criminalize consensual enactments of fantasy scenarios that only *appear* to entail harm to participants. Nevertheless, such legislation changes provide clear testimony to the level of concern about the kinds of sexual imagery that now circulates online, and about the impact it may have on those who consume it.

A second form of content crime relates to what is commonly called “hate speech”—any form of speech or representation that depicts individuals or groups in a derogatory manner with reference to their “race,” ethnicity, gender, religion, sexual orientation, or physical or mental disability in such a manner as to promote or provoke hatred. Particular attention has been directed toward such speech that targets members “of a historically oppressed group,”[64] thereby reproducing patterns of social, political and cultural exclusion and marginalization. The most noticeable online hate speech takes the form of websites (and associated chat rooms and bulletin boards) established by organized political groups. These are typically far right, ultra-nationalist, white supremacist and/or neo-Nazi in orientation. In addition, the United States has seen an extensive online presence of extreme Christian fundamentalists, anti-abortion, and anti-government militia groups. Such sites contain offensive and hateful representations of Blacks, Jews, Muslims, Arabs, other people of non-European origin, women, homosexuals, and persons with physical and mental disabilities. The precise number of such websites is difficult to gauge, as they often appear, disappear, and move location.[65] However, it is clear that their number has grown rapidly over time. Ken Stern claimed that in 1997 there were some 300 such sites in the United States; by 1999, the Simon Wiesenthal Center in Los Angeles had documented the existence of 600 “hate sites” on the Internet;[66] this figure had risen to 11,500 by 2010.[67] A study by U.K.-based Internet security company Surf-Control claims that the number of “hate and violence” sites increased 300% over a four-year period—from 2,756 in 2000 to 10,926 in April 2004.[68] Moreover, the circulation of such speech online appears to have moved from “marginal” spaces associated with extremist groups to more mainstream forums such as new social media like YouTube and Facebook. For example, Citron and Norton (2011) note the existence of Facebook pages such as *Kill a Jew Day* and *We Hate GAY People*, while YouTube has featured videos with titles such as *How To Kill Beaners*, *Execute the Gays*, and *Murder Muslim Scum*.[69] There is some (albeit limited) empirical research evidence that exposure to such hateful messages can be “persuasive in changing inter-group attitudes” and thereby reinforce discrimination and prejudice.[70]

While there are legal provisions in place against hate speech, the global nature of the Internet presents significant difficulties to its effective enforcement. What happens, for example, when the target or victim of hate speech is in one country, the group or individuals responsible for that speech are in another, and the online content is hosted on web servers located in a third territory? Questions of jurisdictional responsibility for dealing with hate speech in such situations pose serious challenges. Since the mid-1990s, the European Union has been taking steps to harmonize provisions dealing with illegal and harmful content online, including the improvement of international cooperation on enforcement across member countries.[71] The Council of Europe’s Convention on Cybercrime was amended in 2003 to include an additional protocol to tackle the “dissemination of racist and xenophobic material through computer systems.”[72] However, significant problems arise when confronting national differences in laws regulating speech. For example, the European approach to prohibiting hate speech contrasts sharply with the situation in the United States, where the First Amendment to the Constitution prohibits lawmakers from encroaching upon the freedom of expression, even where that speech is racist, sexist, homophobic, or otherwise discriminatory in character. The only exemption to First Amendment protection arises when the speech contains a *serious* and *imminent* threat of violence against *identifiable persons*, or *directly* incites others to commit specific criminal acts against those persons. Anything "falling short of incitement to imminent violent action" enjoys constitutional protection.[73] For those advocating the legal restriction of hateful speech, the U.S. Constitution gives a "virtually unlimited license for hate speech."[74]

Earlier in this chapter we noted concerns that terrorist organizations could turn to computer-focused crimes as a tool for staging attacks. However, perhaps a more tangible threat emanates from such groups and their sympathizers turning to the Internet in order to share prohibited communications that further their cause. Firstly, the Internet may be used as an efficient means of intra-organizational communication and coordination of terrorist activities, through the use of technologies such as email and bulletin boards.[75] Here, terrorist groups (like other organizations, be they political, commercial, or criminal) use the Internet to help secure their goals.[76] Use of online tools offers a number of advantages over conventional communications: they enable ease of communication on a transnational basis; they afford greater anonymity; and they afford security. Second, the Internet offers huge opportunities for disseminating propaganda, garnering publicity, and recruiting supporters. The Internet offers an inexpensive means to address a worldwide audience, bypassing the dependence on intermediary news organizations. Numerous terrorist organizations now maintain their own websites. Third, the Internet provides a valuable tool for terrorist fundraising. Websites are used, for example, to post details of bank accounts via which sympathizers can make payments to organizations. The web also provides a useful means for soliciting donations. Internet user demographics are used to identify potential supporters who can then by approached via email and other means. Solicitations are typically made via a front organization (such as a charity) that can then be used to channel finance to the terrorist organization.[77] More generally, the expansion of Internet banking makes it more difficult for authorities to detect suspicious transactions,[78] and its transnational nature enables prohibited organizations to exploit international inconsistencies and gaps in the legal regulation of finance.[79]

Emerging Trends and Social Responses

This third and final section considers two important issues: the possible or likely emerging trends that are reshaping cybercrime in new directions, and the ways that society is responding to cybercrime in terms of policing and controlling the Internet.

Predicting the future of technological development and its social implications is a notoriously difficult enterprise. However, we can note some current trends and consider how these may drive the emergence of new cybercrime threats. The first significant trend in recent years has been the move from accessing the Internet via PCs to 24/7 connectivity using mobile devices such as smartphones and tablets. It is estimated that by 2017, 87% of connected devices sold will be smartphones and tablets, relegating conventional personal computers to a marginal position.[80] Smartphones in particular have become powerful handheld computers offering an ever-expanding range of applications and services, and this is starting to make them a prime target for hackers and other cybercriminals. While the security measures for desktop and laptop computers have become increasingly elaborate and effective over time, smartphone security lags well behind, making them especially vulnerable. Recent studies have shown that a number of the major mobile phone platforms are vulnerable to hacking, enabling unauthorized access to various accounts that users connect with on their mobile devices, or to data stored on the phone itself.[81] Smartphone users are made more vulnerable because, while on the move, they are more likely to use unsecured wireless Internet access points, such as Wi-Fi “hotspots.” This means that information flowing to-and-from the phones can be intercepted and/or impersonated. Current developments to smartphones will also likely bring new vulnerabilities in their wake. For example, the latest generation of phones are being equipped with “near field communication” (NFC) chips—these enable devices to transmit and exchange information with other devices over short distances. The idea is that NFC will enable us to use smartphones to make instant payments by simply “waving” the phone near a properly equipped checkout registers, or for sending “electronic money” to other users of similar devices. While this may undoubtedly bring a new level of speed and convenience for shoppers, it also means that this highly sensitive payment data might be intercepted, altered, or faked by hackers—the tools that could be used for such hacks have already been identified by computer security experts.[82]

The second noteworthy trend is the development of the so-called cloud as means for storing and accessing electronic data. In the past, the data needed by computer users was stored in the devices themselves, using hard drives, and more recently removable digital media such as SD cards. However, as the data needs of users have been ever greater, it has become more cost effective to store data using remote services and access it, as and when needed, via an Internet connection. This has a particular advantage for users of mobile devices who can instantly access all their content (documents, images, video, music, and so on) from wherever they are. There are now numerous cloud storage services offered by companies such as Apple (with its “iCloud”), Google (with its “Google

Drive”), Microsoft (with its OneDrive), and Dropbox to name just a few. However, these storage services, used by government, businesses, and individuals to store and access potentially sensitive data, make them a tempting target for cybercriminals.[83] To offer one illustrative example, in September 2014 the popular press was awash with a news story relating how some 100 actors, musicians, and celebrities (mainly female) found that their private and intimate photographs appeared to have been illicitly obtained and circulated across the Web. I emerged that the source of the images was a popular cloud storage service used by these individuals to back up photographs taken using smartphones, which had been hacked or otherwise illegally accessed.[84] This incident exemplifies the kinds of vulnerabilities that might become commonplace as cloud storage continues to gain popularity among users.

The third emergent area of risk relates to the growth of the so-called Internet of things. This refers to “the pervasive presence around us of a variety of *things* or *objects*—such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc which … are able to interact with each other and cooperate with their neighbours to reach common goals.”[85] Examples range from surgical implants and wearable devices that monitor, record, analyze, and upload biometric measures related to health (such as heart rate, temperature, blood pressure, blood glucose levels, and so on); interconnected home automation systems such as heating, ventilation, lighting, security systems, as well as domestic appliance such as cookers, fridges, and entertainment systems; and transport systems including self-driving vehicles. The development of such technologies, which will be electronically linked and remotely controllable, promises tremendous gains in efficiency and flexibility. However, they bring in their wake significant issues related to security and privacy.[86] For example, personal biometric data might be stolen, altered, or erased, placing individuals’ health at risk; domestic devices will collect huge amounts of data about users’ everyday activities in microscopic detail, data that may be used by state actors to monitor citizens’ activities and corporate actors to covertly profile consumers; devices may be hacked and hijacked with potentially fatal consequences. In short, the more pervasive the web of communication becomes, the “vectors” of attack and vulnerability are created, multiplying opportunities from criminal victimization.

In light of the cybercrime problems discussed thus far, it is important to consider societal responses in terms of policing and crime control measures. Given that the remit of the police is to uphold and enforce criminal law we might expect them to investigate the entire range of Internet-based offenses—hacking, distribution of malicious software, frauds, thefts, hate speech, stalking, and the circulation of offensive and illegal content such as child pornography. In reality, however, the sheer volume of online offenses requires a significant degree of selectivity, with police resources being targeted to those offenses deemed most serious in terms of their scale and the harms that are caused to victims. This selectivity relates to what Wall (2007)[87] calls “the *de minimis* trap”—referring to the dictum that *de minimis non curat lex*, meaning that “the law does not deal with trifles.” Given that many cyberoffenses are low impact in nature, entailing minimal harm to many discrete victims, they tend to fall below the threshold of seriousness that will activate involvement from the police and other criminal justice agencies. Police efforts in relation to cybercrime have tended to focus mainly upon offenses such as child pornography, hacking, political offenses related to terrorism, and interpersonal offenses where the risk of "real world" harm to victims is deemed significant. As the scale of cyberoffenses has grown, and the risks of online victimization have become more widely acknowledged, police forces have incrementally developed the capacity to deal with these problems. All such responses have been constrained not only by resource limitations but also by the established culture and ethos of policing that may be resistant to redefining its remit away from a traditional diet of terrestrial and street-based offenses.[88] However, if we take the United Kingdom as an example, all of the territorially based police forces now have some kind of specialist units that are tasked with addressing at least some variants of Internet-based crimes. At a national level, the perceived need for centralized expertise and coordination of e-crime investigations gave birth to the United Kingdom's National Hi-Tech Crime Unit (NHTCU) in 2001 (subsequently absorbed into the Serious and Organised Crime Agency (SOCA) when the latter was created in 2006). In 2009, the Police Central e-crime Unit (PCeU) was established. The unit, based in the Metropolitan Police Service, provides specialist training and coordinates investigative responses across various regional forces. The PceU's remit is confined to "the most serious incidents" relating to computer hacking, malicious software, denial of service and fraud.[89] Additionally, the Child Exploitation and Online Protection Centre (CEOP), undertakes investigation into child-related offenses, as well as providing education, training, and advice. In light of the globalized character of the Internet, there have also been efforts to create forms of transnational cooperation and coordination of cybercrime investigation, for example, through INTERPOL, EUROPOL, and the EU's high-tech crime agency, ENISA.

Despite the evolving scope of official responses to cybercrime, it is notable that much policing and crime control activity related to the Internet is undertaken by a range of non-state actors, including businesses, charities, and computer users themselves. For example, the aforementioned CEOP, despite being a part of SOCA, in fact includes experts from other organizations such as child protection charities, ISPs, and computer software companies. More broadly, we see organizations such as the Internet Watch Foundation (IWF), which was established in the United Kingdom in 1996 by an association of ISPs, with government backing, although it operates as a self-regulating charitable trust; its membership has subsequently expanded to include operators of mobile telecommunications services, content providers, filtering companies, search engine providers, and financial companies. Its initial brief was to combat child pornographic material, but its brief was later expanded to cover both criminally obscene (but non-child-oriented) content and instances of hate speech (material inciting racial hatred). The IWF operates a "hotline" to which interested parties (be they representatives of organizations or individual members of the Internet-using public) can report illegal content. The IWF produces a "blacklist" of websites or pages it deems to contravene relevant U.K. laws on child sex abuse, obscenity, and race hatred, and this list is used by many ISPs to block access to, or remove from the Web, offending content. Finally, we see the involvement of individual computer users who are "responsibilized" to take measures that protect themselves from victimization, for example, through purchasing and using anti-virus software, firewalls, and password management programs. This plurality of actors (public and private) involved in policing the Internet creates inevitable tensions. Firstly, there may be problems of coordination and inefficiency with numerous organizations involving themselves in crime control activities. Second, the involvement of private organization such as the IWF raises questions about the degree of public accountability we can expect when it comes to their actions. Third, by making individual users responsible for protecting themselves from cybercrime, we may end up favoring those with the most resources and know-how, and disadvantaging those who lack the means to secure themselves from victimization.[90]

Review of the Literature and Primary Sources

Given the wide-ranging and multidisciplinary character of cybercrime studies, it is difficult to identify a core literature for the area that simultaneously addresses the concerns and orientations of researchers approaching the topic from very different angles. For example, the technical issues addressed by those working within the fields of computer science, information security, and electronic engineering are likely to be of far less significance for researchers concerned with the human (social and psychological) questions of etiology, motivation, and the meaning of offending behavior, and vice versa. However, we can note some significant texts that have contributed notably to the development of criminological debates about cybercrime. In step with a growing public and political awareness about Internet crime, Paul Taylor's *Hackers: Crime in the Digital Sublime* (1999) helped stimulate criminological interest and demonstrated the value of qualitative, ethnographic, and broadly sociological approaches to the topic. In the early 2000s, a number of edited collections appeared, which drew together contributions from social scientists to address emerging questions and problems related to crime and the Internet, such as child pornography, fraud, digital piracy, hate speech, and political extremism, while also considering regulatory challenges and legal responses. These works include David S. Wall's *Crime and the Internet* (2001) and Douglas Thomas and Brian Loader's *Cybercrime: Security and Surveillance in the Information Age* (2000). There followed a number of texts that attempted to provide a systematic survey of the emerging subfield of cybercrime studies such as Majid Yar's *Cybercrime and Society* (2006) and David S. Wall's *Cybercrime: The Transformation of Crime in the Information Age* (2007). Meanwhile, a rapid growth in research from a legal perspective has also been reflected in key publications such as Jonathan Clough's *Principles of Cybercrime* (2010) and Susan Brenner's *Cybercrime and the Law* (2012). Influential work on specific, high-profile cybercrime issues includes Philip Jenkins's *Beyond Tolerance: Child Pornography on the Internet* (2001), Maxwell Taylor and Ethel Quayle's *Child Pornography: An Internet Crime* (2003), and Paul Bocij's *Cyberstalking* (2004). Cybercrime research has also made significant inroads into scholarly journals, with publications such as *Deviant Behavior, Crime Media Culture*, and *The British Journal of Criminology* now regularly featuring original contributions addressing Internet crime. The growth of the area has also lead to the creation, in 2007, of the *International Journal of Cyber-Criminology*, the first journal dedicated to research and discussion about crime and the Internet.

Primary sources for cybercrime data broadly comprise four main kinds. First, there are data about the nature and frequency of cybercrimes (such as computer intrusion incidents and malware distribution) that are collected and published by commercial actors, such as information security companies. Annual reports from the likes of Symantec, McAfee, and Verizon provide useful baseline data for tracking incident numbers and trends. However, such sources are doubly limited in that they are, first, produced by those who have a vested interest in establishing the seriousness of cyberthreats; and second, it is difficult to establish either the precise methodology underpinning the data collection or to independently assess its validity. A second source comprises quasi-official surveys of cybercrime incidents, often collected and published by (or in collaboration with) law enforcement agencies. For example, the Computer Security Institute/FBI annual Computer Crime and Security Survey (published between 1996 and 2011) furnished valuable longitudinal data about the scale and cost of computer intrusion incidents experiences by U.S.-based businesses and public agencies; the National White-Collar Crime Center's annual surveys detail trends in cybercrime as experienced by individual victims. A third primary source for cybercrime data comprises large-scale and broad-based victimization surveys such as *Crime in England and Wales* (formerly *The British Crime Survey*), which have belatedly started to routinely include questions about online offenses experienced or witnessed by respondents. The fourth and final source of primary data emerges from qualitative and quantitative data gathered by criminologists in the course of research. Taken together, these sources provide a rich repository for analysis, theory development, and hypothesis testing, which is helping to drive forward the study of Internet crime.

Further Reading

Clough, J. (2015). *Principles of cybercrime*. (2d ed.). Cambridge, U.K.: Cambridge University Press

Gillespie, A. (2015). *Cybercrime: Key issues and debates*. Abingdon, U.K.: Routledge.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offences*. London: Routledge.

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet crime*. Cullompton, U.K.: Willan.

Wall, D.S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge, MA: Polity.

Williams, M. (2007). *Virtually criminal: Crime, deviance and regulation online*. Abingdon, U.K.: Routledge

Yar, M. (2013). *Cybercrime and society*. (2d ed.). London: SAGE.

Notes:

(1.) Castells, M. (2009), *The rise of the network society: Information Age: Economy, society, and culture* (vol. 1, 2d ed.) (Malden, MA: Blackwell).

(2.) Furnell, S. (2002), *Cybercrime: Vandalizing the information society* (London: Addison-Wesley).

(3.) NUA Internet Statistics, (2003), How many online?, retrieved from http://www.nua.ie/surveys/how_many_online

(4.) Internet World Statistics, (2015), World Internet users and 2015 population stats, retrieved from http://www.internetworldstats.com/stats.htm

(5.) International Telecommunications Union, (2012), ICTs in households, retrieved from http://www.itu.int/ITU-D/ict/statistics/

(6.) ITU (International Telecommunications Union), (2009), The world in 2009: ICT facts and figures, retrieved from: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2009.pdf

(7.) Hindman, D. B. (2000), The rural-urban digital divide, *Journalism & Mass Communication Quarterly*, *77*(3), 549–560.

(8.) Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J. G. (2008), *Access denied: The practice and policy of global internet filtering* (Boston: MIT Press).

(9.) Miller, V. (2011), *Understanding Digital Culture* (London: SAGE).

(10.) Capeller, W. (2001), Not such a neat net: Some comments on virtual criminality, *Social & Legal Studies*, *10*, 229–242.

(11.) Grabosky, P. (2001), Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*, 243–249.

(12.) Wall, D. S. (2007), *Cybercrime: The transformation of crime in the information age* (Cambridge, MA: Polity).

(13.) Baylis, S., & Smith, S. (1997), *The globalization of world politics* (Oxford: Oxford University Press).

(14.) Taylor, P. (1999), *Hackers: Crime in the digital sublime* (London: Routledge).

(15.) Yar, M. (2005), Computer hacking: Just another case of juvenile delinquency? *Howard Journal of Criminal Justice*, *44*(4), 387–399.

(16.) Choo, K. K. R. (2008), Organised crime groups in cyberspace: A typology, *Trends in Organized Crime*, *11*(3), 270–295.

(17.) CSI/FBI, (2003), *CSI/FBI computer crime and security survey* (San Francisco: Computer Security Institute).

(18.) Eichenwald, K. (1998), Reuters subsidiary target of U.S. inquiry into theft of data from Bloomberg, *Computers and Security*, *17*(2), 157.

(19.) Wilding, E. (2003), Corporate cybercrime trends, *Computer Fraud and Security*, 6, 4–6.

(20.) McAfee Labs, (2014), *McAfee land threat report: Fourth quarter 2013*, retrieved from: http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2013.pdf

(21.) Kirshner, J. (2008), Globalization, American power, and international security, *Political Science Quarterly*, *123*(3), 363–389.

(22.) Sharma, A. (2010), Cyber wars: A paradigm shift from means to ends, *Strategic Analysis*, *34*(1), 62–73.

(23.) Verton, D. (2003), *Black ice: The invisible threat of cyber-terrorism* (Emeryville, CA: McGraw-Hill/Osborne).

(24.) Pickerill, J. (2006), Radical politics on the net, *Parliamentary Affairs*, *59*(2), 266–282.

(25.) Taylor, P. (2004), Hacktivism—Resistance is fertile? In C. Sumner (Ed.), *The Blackwell companion to criminology* (p. 488) (Oxford: Blackwell).

(26.) Hampson, N. (2012), Hacktivism: A new breed of protest in a networked world, *Boston College International and Comparative Law Review*, *35*(2), 511–542.

(27.) Martin, J. (2014), Lost on the silk road: Online drug distribution and the “cryptomarket.” *Criminology and Criminal Justice*, *14*(3), 351–367.

(28.) Gavish, B., & Tucci, C. (2008), Reducing Internet auction fraud, *Communications of the ACM*, *51*(5), 89–97.

(29.) Internet Crime Complaint Centre, (2012), *2011 Internet Crime Report*, retrieved from: http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf, p. 10

(30.) FBI, (2014), Fraud target: Senior citizens, retrieved from: http://www.fbi.gov/scams-safety/fraud/seniors

(31.) Internet Crime Complaint Centre, (2012), p. 12.

(32.) Whitty, M. T., & Buchanan, T. (2012), The online romance scam: A serious cybercrime, *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181–183.

(33.) Internet Crime Complaint Centre, (2012), p. 12.

(34.) Mullen, P., Pathé, M, & Purcell, R. (2001), Stalking: New constructions of human behaviour, *Australian and New Zealand Journal of Psychiatry*, *35*, 9–16.

(35.) Brewster, M. (2003), Power and Control dynamics in prestalking and stalking situations, *Journal of Family Violence*, *18*(4), 207–217.

(36.) D’Ovidio, R., & Doyle, J. (2003), A study on cyberstalking, *FBI Law Enforcement Bulletin*, *72*(3), 10–17.

(37.) Ogilvie, E. (2000), Cyberstalking, Trends and Issues in Criminal Justice, No. 166. Canberra: Australia Institute of Criminology.

(38.) D’Ovidio, R., & Doyle, J. (2003).

(39.) Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014), Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims, *Cyberpsychology, Behavior, and Social Networking*, *17*(2), 61–67.

(40.) Stokes, J. K. (2014), The indecent Internet: Resisting unwarranted Internet exceptionalism in combating revenge porn, *Berkeley Technology Law Journal*, *29*(4), 929–952.

(41.) Proudman, C. R. (2014, July 2). Revenge porn: Enough still isn’t being done to stop it, *The Independent*, Retrieved from http://www.independent.co.uk/life-style/health-and-families/features/revenge-porn-enough-still-isnt-being-done-to-stop-it-9578892.html

(42.) NCSL (2014, August 15). State “revenge porn” legislation, retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/state-revenge-porn-legislation.aspx

(43.) Saha, T., & Srivastava, A. (2014), Indian women at risk in cyberspace: A conceptual model of reasons and victimization, *International Journal of Cyber Criminology*, *8*(1), 57–67.

(44.) Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008), Cyberbullying: Its nature and impact in secondary school pupils, *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385.

(45.) Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide, *Archives of Suicide Research*, *14*(3), 206–221.

(46.) Li, Q. (2008), A cross-cultural comparison of adolescents’ experience related to cyberbullying, *Educational Research*, *50*(3), 223–234.

(47.) O’Connell, R. (2003), *A typology of cybersexploitation and online grooming practices* (Preston, U.K.: Cyberspace Research Unit), p. 2.

(48.) National Criminal Intelligence Service, (1999), Project Trawler: Crime on the information highways, retrieved from http://www.cyber-rights.org/documents/trawler.htm

(49.) O'Connell, R., Price, J., & Barrow, C. (2004), *Cyber stalking, abusive cyber sex and Online grooming: A programme of education for teenagers* (Preston, U.K.: Cyberspace Research Unit), p. 4.

(50.) Home Office, (2002), Home Office Annual Report 2001–2.

(51.) O'Connell, R. (2003), p. 4.

(52.) Stanley, J. (2002), Child abuse and the Internet, *Journal of the Health Education Institute of Australia*, *9*(1), 5–27.

(53.) Home Office, (2002), p. 25.

(54.) Jewkes, Y., & Andrews, C. (2007), Internet child pornography: International responses, In Y. Jewkes (Ed.), *Crime online* (p. 64) (Collumpton, U.K.: Willan).

(55.) Akdeniz, Y. (2000), Child pornography, In Y. Akdeniz, C. Walker, & D. Wall (Eds.), *The Internet, law and society* (p. 233) (Harlow, U.K.: Longman).

(56.) Telofono Arcobaleno, (2004), Monitoring paedophilia on the Internet: 2004 annual report.

(57.) Internet Filter Review, (2004), Internet pornography statistics, retrieved from http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

(58.) Wolf, I. (2010, June 15), Child-porn industry using web-based system to move funds, *East Valley Tribune*, Retrieved from http://www.eastvalleytribune.com/local/cop_shop/article_2ee0f064-7888-11df-9e7a-001cc4c03286.html

(59.) Darlington, R. (2010), Sex on the net, retrieved from http://www.rogerdarlington.co.uk/sexonnet.html

(60.) Ropelato, J. (2010), Internet pornography statistics, retrieved from http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

(61.) Quayle, E. (2010), Child pornography, In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet crime*. (pp. 344–345) (Cullompton, U.K.: Willan).

(62.) Akdeniz, Y., & Strossen, N. (2000), Sexually oriented expression, In Y. Akdeniz, C. Walker, & D. Wall (Eds.), *The Internet, law and society* (p. 170) (Harlow, U.K.: Longman).

(63.) Jewkes, Y. (2010), Public policing and Internet crime, In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet crime* (p. 527) (Cullompton, U.K.: Willan).

(64.) Nielsen, L. (2002), Subtle, pervasive harm: Racist and sexist remarks in public as hate speech, *Journal of Social Issues*, *58*(2), 265–280.

(65.) Schaffer, J. (2002), Spinning the web of hate: Web-based hate propagation by extremist organizations, *Journal of Criminal Justice and Popular Culture*, *9*(2), 69–88.

(66.) Whine, M. (2000), Far right extremists on the Internet, In D. Thomas & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age*(p. 235) (London: Routledge).

(67.) Online hate sites grow with social networks, (2011, July 28), *The New York Times*, retrieved from http://bits.blogs.nytimes.com/2010/03/16/online-hate-sites-grow-with-social-networks/

(68.) Hate websites continue to flourish, (2004, May 10), *The Register*, retrieved from http://www.theregister.co.uk/2004/05/10/hate_websites_flourish/

(69.) Citron, D., & Norton, H. (2011), Intermediaries and hate speech: Fostering digital citizenship for our information age, *Boston University Law Review*, *91*, 1–18.

(70.) Hargrave, A., & Livingstone, S. (2009), *Harm and offence in media content: A review of the evidence* (2d ed.) (Bristol, U.K.: Intellect Books).

(71.) Rorive, I. (2002), Strategies to tackle racism and xenophobia on the Internet—Where are we in Europe? *International Journal of Communications Law and Policy*, 7, 1–10.

(72.) Van Blarcum, C. (2005), Internet hate speech: The European framework and the emerging American haven, *Washington & Lee Law Review*, 62, 781–829.

(73.) Wendel, W. (2004), The banality of evil and the First Amendment, *Michigan Law Review*, 102, 1404–1422.

(74.) Tsesis, A. (2002), *Destructive messages: How hate speech paves the way for harmful social movements* (New York: New York University Press).

(75.) Shelley, L. (2003), Organized crime, terrorism and cybercrime, In A. Bryden & P. Fluri (Eds.), *Security sector reform: Institutions, society and good governance* (p. 305) (Baden-Baden, Germany: Nomos Verlagsgesellschaft).

(76.) Fleming, P., & Stohl, M. (2000), Myths and realities of cyberterrorism, Paper presented at the International Conference on Countering Terrorism Through Enhanced International Cooperation, September 22–24, 2000, Courmayeur, Italy.

(77.) Weimann, G. (2004), *www.terror.net*. United States Institute of Peace, Special Report 116. Washington, D.C.: USIP, pp. 6–7.

(78.) Fitzgerald, V. (2003), Global financial information, Compliance incentives and terrorist funding. *European Journal of Political Economy, 20*(2), 387–401.

(79.) Shelley, L. (2003), p. 304.

(80.) Columbus, L. (2013, September 12), IDC: 87% of connected devices sales by 2017 will be tablets and smartphones, *Forbes.com*. Retrieved from http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/

(81.) AVG Technologies, (2011), Cybercrime futures, retrieved from: http://aa-download.avg.com/filedir/news/2011_09_09_Future%20Poll_Cybercrime_Futures.pdf

(82.) Hopwell, L. (2012, February 9), Hack exposes Google Wallet PIN, *ZDNet*. Retrieved from: http://www.zdnet.com/hack-exposes-google-wallet-pin-1339331400/

(83.) Kaufman, L. (2009), Data security in the World of Cloud Computing, *IEEE Security and Privacy*, July/August, 61–64.

(84.) Vincent, J. (2014, September 1), Is Apple’s iCloud safe after leak of Jennifer Lawrence and other celebrities’ nude photos? *The Independent*, Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/is-apples-icloud-safe-after-leak-of-jennifer-lawrence-and-other-celebrities-nude-photos-9703142.html

(85.) Atzori, L., Iera, A., & Morabito, G. (2010), The Internet of things: A survey, *Computer Networks*, *54*(15), 2787–2805.

(86.) Weber, R. H. (2010), Internet of things—New security and privacy challenges, *Computer Law & Security*, 26, 23–30.

(87.) Wall, D. S. (2007), p. 161.

(88.) Wall, D. S. (2007), pp. 160–161.

(89.) PceU, (2011), PCeU—Police Central e-crime Unit.

(90.) Yar, M. (2010), The private policing of cybercrime, In Y. Jewkes & M. Yar (Eds.), *The handbook on Internet crime* (pp. 556–557) (Cullompton, U.K.: Willan).

Majid Yar

Independent Scholar