Handbook of Internet Crime

Yvonne Jewkes, Majid Yar

On the globalisation of crime

Publication details
Barry Sandywell
Published online on: 01 Nov 2009

How to cite: Barry Sandywell. 01 Nov 2009, On the globalisation of crime from: Handbook of Internet Crime Routledge
Accessed on: 10 Mar 2019

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
Chapter 3

On the globalisation of crime: the Internet and new criminality

Barry Sandywell

Introduction

I write this chapter in the midst of one of the most severe financial crises that the developed world has experienced. The so-called ‘credit crunch’ – the crisis of the global system of financial capitalism – has its sources and causes in the more general globalisation of socioeconomic, political and cultural relationships that have developed over the past three decades. In response to the extreme rapidity and extent of ‘capital loss’ – what might be called global decapitalisation – the popular press are full of apocalyptic commentaries on the ‘end of capitalism’, the prospects of a total collapse and the abyss of uncontrollable recession with estimates of up to 20 million people unemployed in the industrial nations by the end of 2009. Indeed the deputy governor of the Bank of England, Charles Bean, has described the slump as ‘possibly the largest financial crisis of its kind in human history’.

For our purposes, however, the financial crisis is doubly instructive in firstly revealing the cyclical ‘reflexive’ instabilities of the global capitalist market and in clearly marking a configuration of social and technological conditions that have also facilitated the globalisation of criminal activity and practices over the same period. In other words, the forces that have precipitated the global financial crisis are the same generic conditions of unregulated interdependence, digital connectivity, and deterritorialisation that constitute the diverse phenomena of cybercrime.

These conditions include:

- the global reach of instantaneous digital communications technologies (the Internet, World Wide Web, video conferencing, multimedia digitisation, wireless technologies, ‘cloud computing’, and so on);
- globalisation or the emergence of a global network society in which information, social relations, services and institutions are increasingly networked (the era of cyberspace or global telecommunications connectivity);
On the globalisation of crime: the Internet and new criminality

- the radical ‘compression’, ‘disembedding’, and ‘re-embedding’ of local and everyday events and practices with global social processes (for example the creation of databanks covering national and international populations, digitally coded geo-demographic information on populations, extraterritorial policing and surveillance systems);

- the increasing interdependence and mobility of manufacturing, commerce and financial capital in the context of global forces of commodification and consumerism;

- the spread of digitalised mass media, particularly news media and journalism, that intensively document and report upon global events on a continuous 24/7 basis;

- the ‘blurring’ of traditional normative boundaries, for example the blurring of distinctions between sanctioned and non-sanctioned activities as these have become normal features of a deterritorialised economic and political order.

Taken as a totality this constellation provides the historical setting for our specific topic, the globalisation of crime in the era of capitalist cyberculture.

1. Crime and criminality?

Some commentators see e-criminality as the most significant threat facing an increasingly globalised world. The Internet, the Web and cyberspace have been described as the ‘wild west’ of new forms of criminality organised on a planetary scale. Of course, to speak of ‘crime’ is to invoke a highly charged normative category. Like taxes and death, rule breaking, deviance and antisocial behaviour will always be with us. Every organised society has, in Durkheimian terms, its own quota of transgressive acts and, correlated to these, its own socially regulated forms of sanction, deterrence and punishment. ‘Criminal behaviours’ are typically singled out and semiotically marked as among the most threatening and destabilising manifestations of societal deviance. This also entails a discourse of punishment and redress typically involving juridical and state institutions. In general terms whatever contests the authority and continuity of the dominant institutions tends to be labelled as ‘deviant’ and regulated through various types of authorised sanctions. ‘Deviance’ and ‘crime’, in other words, are profoundly social phenomena, embedded in the wider cultural, economic and political contexts of a given society.

In thinking about the present global crisis, our normal categories of crime and criminality seem wholly inadequate. We need to ask the more reflexive question of what kind of knowledge can be gained by researching criminal activities on a global scale? What forms of compliance and ‘normalisation’ are implicit in a society’s sanctioning regimes? To this end we need to think more critically about the assumptions underlying such categories as ‘deviance’, ‘crime’, ‘law-breaking’ and ‘subversion’. In what follows it is important to approach criminality in socio-discursive terms as those actions, practices
and relationships that are judged to be transgressive by the normative standards of a powerful group, class or whole society. A reflexive criminology would be one that brackets the ‘real’ or ‘ontological’ nature of crime and instead examines what, how, when and where human activities are treated as ‘deviant’ and ‘criminal’ by powerful agents and agencies. If criminality is ‘socially constructed’ in and through the mediations of powerful social practices the central theoretical topic of a more reflexive criminology should be *criminalisation practices* as these are institutionally embodied in a given social order.

The phenomena labelled ‘criminality’ are thus mediated by the social categorisation procedures of a particular society’s systems of risk management and social control. Furthermore, as the morphology of ‘criminality’ will vary with the changing economic, political and cultural contexts of perceived threat and risk, critical criminology needs to adopt a radically historical approach. For example, a society with a well-demarcated, hierarchical and resourced ‘establishment’ would be expected to have a powerful set of paradigms operating to ‘criminalise’ and ‘control’ anti-establishment threats to its authority and power. For analytical purposes such classificatory ascriptions of deviance would both identify and differentiate some of the dominant meaning systems and conflicts in a given society (thus what we are calling ‘criminal discourse’ might be generated by a range of societal agents and agencies), it might also be typically interwoven with political discourses concerned with inclusion and exclusion of ‘others’ and be embedded in moral and social policy discourses based upon anxieties to perceived threats to the existing social order.²

One interesting area that is rarely explored in traditional criminology and social theories of deviance is the interplay between transgression and the ‘technologies of transgression’, the techniques and material forms that create the possibility of digital databanks and networks also facilitate and mediate cyber-attacks and deviant practices with regard to those systems. Here I will argue that the same processes of global connectivity that have seen a revolution in communication and social exchange also facilitate criminal activities on a planetary scale. This phenomenon has been variously conceptualised as Web crime, digital criminality, e-criminality or, at its most generic, *cybercrime* (Wall 2003a, 2007).

A related phenomenon revealed in all its starkness and radicalism by the current global financial meltdown is the extent to which the deterritorialised business culture of banking and financial corporations has become intensely interdependent and reliant upon new technologies and globalised digital media. Contemporary capitalism is perhaps better described as cyber-capitalism. Thus, for example, traditional patterns of financial investment and speculation are now typically directed towards future states of capital and market movements (Web futures based upon circuits of intangible assets). Whole sectors of credit and finance have become wired up to markets trading in national currencies, government bonds, future economic conditions, ‘derivatives’ and other intangibles (creating what might be called a global economy of intangible capital and associated transactional ‘instruments’). In this way the traditional commercial practices of capitalism have been
increasingly ‘virtualised’ as corporate organisations outside of the traditional
stock markets – banks, mortgage brokers, etc. – trade in ‘futures’ and ‘hedge
funds’ based directly upon anticipated future states of the economy. With
the support of institutional deregulation and the philosophy of ‘market
fundamentalism’, the financial heart of the major industrial economies has
assumed the form of interlocking information-based casinos, multiplayer
speculative games carried out in the ether of cyberspace. We now live in a
planetary civilisation in which the social formation of ‘capital’ increasingly
takes the form of instantaneously transmissible electronic information (where,
for example, ‘runs on the bank’ occur in nanoseconds and, amplified by
mass-media publicity networks, become powerful generative ‘vicious circles’
that expand and deepen the original problem to create chaotic macro events
and processes). In being enmeshed in new digital media and the abstract
instrumentality of financial derivatives the banking and financial sector no
longer merely reacts to changes in markets but actively, if unintentionally,
produces and magnifies those changes.

Contemporary globally interconnected capitalism has thus become
profoundly reflexive, computer-mediated, and chronically unstable. Thus it
is not only ‘hackers, punk capitalists, graffiti millionaires and other youth
movements’ that are transforming the landscape of modern capitalism (Mason
2008), but the ‘pump ‘n’ dump’ and ‘short selling’ strategies of hedge fund
managers, anonymous corporate investors, and pension fund millionaires.
All of these practices are examples of reflexive circuity that have become
embedded in the normal operations of global financial markets.

The 1990s is littered with the ominous harbingers of these market
instabilities. The phenomenon of rogue traders like the derivatives trader
Nick Leeson (whose fraudulent activities led to £700 million losses and the
destruction of Barings Bank in 1995), the bond trader Toshihide Iguchi (losses
of $1.1 billion), and Jerome Kerviel (whose fraudulent dealings in equities lost
the French company Société Générale £3.5 billion in 2008) are symptomatic of
this new constellation. On a more global scale, much more extensive losses are
involved in recent cases of corporate corruption (Enron, Tyco and WorldCom
in the US being paradigm cases of the extent of corporate malfeasance made
possible by deregulated energy markets). Global deregulation has created an
interlocking system that is chronically prone to crisis. It also makes possible
levels of corruption on an equally planetary scale. In other words, we have
the basic conditions for what George Soros describes as a cycle of self-
reinforcing processes that introduces chaos into market systems. Moreover
it is this particular branch of speculative capital that appears to be one of the
causal elements in a complex chain of reflexive relationships that has
precipitated what many see as a total collapse of legitimacy in stock markets
and the global economy. Not surprisingly, some commentators have come to
view corporate corruption as a generic condition of the American economic
and political system. Corporate corruption on a hitherto unimaginable scale
has, in other words, become a ‘normal phenomenon’ of global capitalism.

In this transformed situation we clearly need to reflect on the unprecedented
changes in the sociocultural conditions and new information technologies of
globalised modernity.
2. Criminality without borders

In what follows I will use the following acronyms and shorthand: information and communication technology (ICT), computer mediated communication (CMC), new electronic media (NEM), and cybercrime (computer-based crime, electronic crime or e-criminality).

While in the past these technologies have been relatively invisible (and have been treated as such in mainstream discussions of criminality), today they have begun to take centre stage; and among the most insistent of these technologies are new digital information technologies like MP3 players, iPod and multimedia cellular phones and, more particularly, the emergent communications media associated with the second and third generation Internet (what today is generally referred to as Web 2.0 and beyond). We are increasingly moving into an era of ubiquitous, mobile, distributed multimedia information appliances that ‘wire’ individuals to distant and anonymous networks (exemplified by the availability of free software such as Skype and Linux and the impact of ‘cloud computing’ organised by such major players as Google and Microsoft). E-crime presupposes such a distributed universe of information infrastructures as its fundamental technical and material condition.

The basic sociological thesis here is that as we move from the electronic to the digital age, from analogue technologies to CMCs, as we enter a truly globalised world of corporate capitalism, we correspondingly witness the mutation of analogue to electronic and digital forms of deviance and crime on a transnational scale. In other words, with the coming of digital communication networks we not only witness the creation of ubiquitous multimedia but also experience an explosion of online criminality, particularly of illegal accounting practices and corporate criminal activities made possible by the new information networks. It is also of some relevance that commentators on the current global economic crisis routinely resort to the language of viruses that spread ‘toxic contagion’ when describing the ‘financial contagion’ infecting the world’s economies (just as ‘computer virus’ emerged with the first phase of information globalisation, phrases like ‘toxic debts’ and ‘toxic liabilities’ have become media clichés in descriptions of the latest crisis of global capital). Stated baldly this conjecture suggests a technological determinist approach to social life; however, in what follows I wish to avoid this interpretation by promoting a more ‘mediated’ and dialectical version of this general argument linking cybercrime to some of the major forces that are transforming contemporary society and consciousness in the global era.

As a longer-term project, a general socio-cultural theory of globalised cybercrime would have to address the following conceptual issues:

1. how to theoretically describe the constitutive differences between pre-digital and digital criminality;
2. how to explain the continuities between analogue and digital crime;
3. how to analyse the formative role of the new information technologies in transforming the global culture of crime while avoiding technological determinism.
4 how to model the emergent forms and characteristics of cybercrime (distinguishing, for example, between individual, corporate and state-centred forms of global criminality);

5 how to explain the societal, cultural and governmental responses to emergent forms of anonymous, automated and virtual criminality and their consequences for the wider society in different national and geographical contexts;

6 how these phenomena are leading to new attitudes towards personal and collective security, new forms of surveillance, and new forms of transnational regulation and policing.

Needless to say, while these theoretical issues form the background of the present paper, the articulation of a systematic theory of e-crime in relation to cyberculture more generally is beyond the scope of this essay. As a step in this direction I shall concentrate upon the emerging forms of Internet crime and the public and private responses to these new threats to personal and collective space.5

3. Old and new criminality: the distinctive features of e-criminality

At the outset we need a broad, if necessarily schematic, descriptive account of the phenomenon of ‘new criminality’. Such a phenomenology of Internet malfeasance must not only locate the essential features of digital crime but also capture some of the emergent characteristics of the new criminality. We first need to conceptualise the Internet as a distinctive globalised socio-cultural system and then formulate a description of e-crime in its essential aspects.

The Internet is typically defined (and modelled) in fluid and network metaphors: as a ‘fast’ technology of global information ‘flows’, ‘mediations’, ‘translations’ across human–machine networks; as a sphere of hypermobility that reflects the global pace of hypermodernity; as an open-ended, decentralised and non-hierarchical technology (expressed by the popular imagery of ‘the Net’ or ‘Web); as the source of loosely connected virtual realities (‘cyberspace’).

By deploying these images cyberspace can be imagined as the virtual topography created by the Internet as a system of interactive, multimedia websites. In sociological terms cyberspace is both a conceptual site and a force of social reconfiguration and personal experience (a technological formation that constitutes new modes of production, appropriation and transnational connectivity). Thus:

The Internet, in fact, is not just a global computer network, but a network of networks, the actualization of a set of design principles entailing the interoperability of heterogeneous information systems. Not only, that is, is there no central control of the Internet (although there are many control centres), but the whole space of communication has been designed and conceived in terms of dynamic and variable
relations between different communication networks. (Terranova 2004: 53–4)

Even considered at a technical level as a border-defying communication technology many commentators regard the boundary-dissolving and trespassing powers of the Internet and Web as profoundly anarchic, transgressive and threatening (see Jordan 1998; Lyon 1994; Plant 1998; Sandywell, 2006).6

**Cybercrime**

What, then, are the characteristics of cybercrime?

First, digitisation through Internet networks makes possible virtually instantaneous information transmission. As the Internet morphs with other digital apparatuses this makes possible mobile access on a transnational scale (storage power is reduced from building- and room-sized facilities to laptops and hand-held mobile phones). With the globalisation of space and time the mobility of information transmission brings with it the ‘instantaneity’ of viruses and malware (‘If one carries forward the metaphor of “virus” from its original public health context, today’s viruses are highly and near-instantly communicable, capable of causing world-wide epidemics in a matter of hours’ (Zittrain 2008: 51; cf. Rochlin 1997)).

Second is the anonymity or ‘facelessness’ of cyberspace as an effect of the deterritorialisation of social encounters and online relationships in cyberspace. In media influenced by Web 2.0 platforms like MySpace, YouTube, Facebook, cyberspace identities are wholly constructed through the information that users provide – typically in the form of lines of text or visual imagery (which can themselves be ‘mashed’, morphed and manipulated to create specific image profiles – the 14-year-old schoolgirl in a chat room turns out to be a 50 year-old male with a documented history of paedophilia).

Third, the feature of material incorruptibility: being digital rather than analogue, information capital can be ‘lifted’ and replicated without altering its original (hence copying digital information does not ‘degrade’ or ‘deteriorate’ the prototype); this non-degradation feature also adds another dimension to the structure of anonymity producing a situation where data can be stolen without any trace of the violation (thus in identity theft I am still left with the same coded information even though this is now in circulation and being used as a surrogate of my own electronic ‘signature’).

Fourth, the ‘manipulability’ of digitally coded electronic information (in principle any coded software is ‘open’ software and therefore susceptible to modification with minimal costs and overheads).

Fifth, the correlative expansion of diverse, geographically decentralised and multifarious forms of criminal activity accompanying the global extension of the new information technologies (we might characterise this as the move from analogue crime involving ‘linear’ and ‘hierarchical’ relations between perpetrators and victims to digital crime involving anonymous, networked and rhyzomatic relations between perpetrators and victims).

When combined these features create ubiquitous digital platforms that facilitate information-based borderless crime on a planetary scale and
On the globalisation of crime: the Internet and new criminality

hence prefigure the emergence of a situation of permanent information warfare.

Just as the appearance of ‘gated communities’ encourages ‘gated crime’, so the gated communities of cyberspace will encourage gated cybercrime. In this way every organisation and institution that is ‘wired’ through digital means becomes open to information violation, to ‘attack’ by a diverse and disparate range of ‘intruders’ – in this way analogue stealing that defines such legal categories as theft and burglary become globalised into identity theft, the violation of copyright and, at the highest level, cyber-terrorism against a whole society’s information infrastructures. Not surprisingly the language of the information society adopts military rhetorics as a matter of course. For those concerned with digital security we now live in societies that are ‘besieged’ by hackers and digital warriors, we live in a state of permanent information insecurity, we are fighting an ‘information war’ on many levels and fronts. Articulated into a theoretical model, we have the elements of a new globalised risk economy. The ‘theatre’ of this new warfare – this new form of global criminality – is the field of information itself.

E-crime as a social construction

The fundamental social-epistemological problem posed by both analogue and digital crime can be stated simply: how do we come to know the world of crime? Or expanded and generalised: how do we come into contact with the various social constructions of criminal activity. Expressed more reflexively: what are the modes of discourse and forms of representation constituting criminal forms of life?

E-crime emerges with its distinctive epistemology and ontology in terms of the emergence – the ‘reality’ and ‘thinkability’ – of criminal organisations and activities on a planetary scale. It would be a basic failure of reflexivity to ignore the complex loops that flow between such social phenomena and their representation in the media and popular imagination. Hence a critical framework must also include the issue of the active rhetorical and ideological representations of deviance, of the rapid circulation of images, categories and representations by means of which certain behaviours, relations, and practices are labelled as ‘criminal’, ‘antisocial’, ‘corrupt’, and so forth (we might call this the ‘discourse of criminality’ available to a given community or society).

Approaching these questions from a more reflexive perspective we are directed towards the representations and discourses that constitute the phenomenon of globalised criminality in the context of twenty-first-century social relations, technologies and the transnational reconfiguration of time and space.

Where the larger part of personal and collective life is ‘translated’ into software and this software is ‘wired’ into impersonal electronic networks, the creation of new forms of hardware and software and their public ‘accessibility’ becomes a major political question for all advanced societies. The new ‘political economy’ of information is increasingly one of securing codes, regulating software applications, monitoring ‘malware’ and ensuring ‘normal applications’ of technologically intensive investments. In a
globalised world traditional issues of societal control, power and domination increasingly assume the form of agencies and organisations engaged in the reflexive regulation of societal and trans-societal information governance. Just as central governments strive to control transnational networks and ensure ‘safety’ for legitimate uses of these networks, so the new criminality attempts to manipulate and misuse these networks for illicit ends.7

4. Empirical forms of the new criminality

Analysts of cybercrime have distinguished three subcategories of e-crime:8

1 traditional criminal activities that are expanded or enhanced by CMCs and NEM (for example criminal exploitation of ATM machines, the expansion of ‘analogue’ industrial espionage to include industrial espionage facilitated by unauthorised copying of branded commodities and reverse engineering);

2 traditional criminal activities that are generalised and ‘radicalised’ by the availability of NEM (money laundering, drug smuggling, cyberstalking, paedophilia activities, cyber-pornography, online gambling, assisted suicide, terrorism, etc.);

3 criminal activities that are created by CMCs and NEM (crimes directed towards computer systems or computer-based networks, e.g. hacking and digital piracy; crimes directed towards collective databases and infrastructural systems such as ‘spamming’, information espionage, global information warfare and cyber-terrorism).

While all of these categories are interrelated, it is the third category of emergent criminality that will be central to the following analysis. This category exemplifies phenomena that we regard as fundamental to discussions of the ‘new criminality’.

One way into this emergent phenomenon is given with the idea of boundary transgression or ‘border crossing’. Because of its global and transnational structure cyberculture is vulnerable to a wide range of boundary transgressive invasions of local cultures and lifeworlds (Sandywell 2006). We have seen that online crime is typically presented in invasive metaphors (hacking, hijacking, bombing, and so on). Not surprisingly the discourse of online deviance has become organised around the idea of ‘alien Others’ invading private and public space as we move from gated communities to gated cyberspace protected by electronic barriers (cybergates). Traditionally the wealthy and the privileged tend to cluster together and create boundaries that cannot be readily crossed. The same dynamic now operates in cyberspace, where the rich and powerful construct ‘firewalls’ and ‘encryption’ barriers to ensure the privacy and protection of their digital ‘property’. Information becomes the new form of capital. The same forces that drive the privatisation of life in advanced industrial countries (extreme inequalities of wealth and access to life chances, accumulation of property, deregulated competition, and marketisation of services) also produce ‘knowledge-based’ ecologies and,
with these, *cybergate* security industries. Information ('knowledge capital') is the new frontier that must be encrypted and defended with impenetrable barriers and anti-spyware systems (and increasingly the sociological operation of physical ‘gates’ and cybergates interact and coalesce to create new maps of social exclusion and inequality).

In what follows we will briefly discuss four types of ‘border crossing’ associated with e-crime. Taken together they define the new global culture of cybercrime:

1. identity theft and related security threats (hacking/cracking, distributed denial-of-service attacks (DDOS));
2. digital piracy (violation of intellectual property rights, copyright and culture theft stemming from the explosion of what might be called Internet piracy technologies: file-sharing, digital copying, scanning, sampling and mixing, remixing and morphing);
3. punk capitalism;
4. cyber-terrorism.

### 4.1 Identity theft

The world of new electronic mobility routinely problematises the issue of identity as a contested domain. While we can now communicate and carry out almost every activity of everyday life on a global scale so we can also be defrauded by the same technological means. The new, anonymous and fluid world of e-criminality is itself an example of deterritorialised ‘smart mobs’ – volatile, centred, non-locatable groups made possible by the new technologies (Rheingold 2002). As people increasingly carry out everyday activities through online identities new forms of border transgression necessarily assume the form of identity theft. While precise empirical evidence of these volatile transformations is difficult to assemble surveys suggest that people are more anxious about having their online identities compromised than they are of being mugged (*Guardian*, 10 August 2007).

The phenomenon of global online insecurity is experienced first hand in the phenomenon of identity theft and forms of criminality associated with the misuse of personal information, personal identity codes and personal networks (from the theft of banking codes to more insidious forms of hacking, malicious spyware that ‘seed’ remote code execution programs and pre-installed keylogging devices, and cyberstalking). In the wake of global consumerism, identity theft scams and online fraud (for example credit card fraud, the theft of banking codes and PINs) is estimated to have cost British consumers £414 million in 2007 (*ibid.*). Wherever monetary transactions are coded as information and virtual money circulates across borders we create the opportunity of criminal intervention exemplified by phishing attacks. Fraudsters have developed ways of automatically accessing bank accounts through ‘packet reading’ to siphon off money from vulnerable accounts. In this way the electronic risk to privacy (the general problematic of network infiltration and insecure passwords) has moved on from the isolated attacks...
of ‘lonely hackers’ and the physical theft of credit cards to the world of organised criminal rings simultaneously attacking multiple networks from anonymous sites in cyberspace.

**Phishing**

Phishing is the use of fraudulent email messages disguised as a legitimate or trustworthy source that ‘fishes’ for personal details, typically by asking for email passwords or by inviting the recipient to reply to the email or to click onto a web link and provide PINs, passwords or account information. Phishing or ‘carding’ scams are a pure example of a type of financial fraud that is only possible through the new information technologies. With the increase in online banking, financial websites will be particularly vulnerable to such attacks. Phishing attacks are also expected to expand as more individuals use e-commerce websites (for shopping, insurance, travel, online brokerage, and other day-to-day activities). As Ollmann observes: ‘While Spam was (and continues to be) annoying, distracting and burdensome to its recipients, Phishing has already shown the potential to inflict serious losses of data and direct losses due to fraudulent currency transfers’ (2008: 4). In 2007–2008 it is estimated that £45–50 billion was spent in online shopping. We might anticipate an increasing level of consumer uncertainty, loss of trust and delegitimising of e-commerce as the extent and range of phishing scams enters the public domain.

**Digital scams**

Sales, advance fee, charity, pyramid selling and lottery scams have followed the creative design expertise of phishers in creating Web information that mimics official documentation, brand insignia and logos and targeting users who are thought to be more vulnerable to deception. ‘Get-rich-quick’ fraudsters ‘profile’ populations that are most receptive to scamming and repeatedly mail (including email) this demographic. In essence the digital fraudster engineers a persuasive ‘imagined community’ – typically woven around believable virtual promises – designed to entrap the unwary into parting with their cash. Thus sweepstakes or lottery scams operate where the potential victim receives the ‘good news’ of a major win and is asked to provide a release fee to access the winnings. Charity fraud solicits contributions to non-existent charities. Job scam frauds ask for up-front fees to facilitate job interviews and employment.

**Facebook predation**

With the spread of Web 2.0 social websites like Bebo, MySpace and Facebook we increase not only the possibility of stealing electronic identities but also of creating new forms of harassment, predation and stalking. The expansion of ‘Facebook’ type websites has seen a massive increase in the illicit use of private and personal information. Web 2.0 websites and Facebook blog culture thus enhances not only identity theft but password harvesting and more technically sophisticated forms of intimidation, solicitation and cyberstalking.
On the globalisation of crime: the Internet and new criminality

**Cookie surveillance**

Another well-documented surveillance strategy is the use of ‘cookies’ or bits of software that monitor, track and archive a user’s online activities. Cookie surveillance belongs with the generic group of electronic tracking devices that automatically monitor Web usage. Electronic surveillance of users’ keystrokes, mouse clicks and website journeys have notoriously been used by some major Web providers and software companies as the basis for ‘data mining’ of user preferences. Cookie surveillance is thus only a harbinger of a growing industry of commercial personal profiling and data mining.

**Spyware**

Spyware refers to a range of digital devices and viruses (botnets, Trojan horses, etc.) that monitor computer activities. Cookies that track online traffic are also useful to those who wish to use confidential information for fraudulent purposes. Commentators argue that the increasing organisation and internationalisation of such illicit markets in stolen identity data promises to make this a major concern for the global policing of the Web. Many of these emerging types of identity theft have come to be covered by the portmanteau term ‘spyware’ as some of the most sophisticated involve the seeding of malicious software viruses and worms in computer systems with the express purpose of automatically monitoring, controlling and exploiting network identities and activities. Given the economic incentives of Web servers to collect such online data to create market profiles we might anticipate that ‘secondary’ forms of identity fraud will increase as fraudsters see profit in selling on electronic information to other criminal groups.9

4.2 Digital piracy

Piracy is another example of transgressive ‘border crossing’ for illicit purposes. Digital piracy primarily involves the theft of intellectual property for profit:

> A pirate is essentially anyone who broadcasts or copies someone else’s creative property without paying for it or obtaining permission. (Mason 2008: 36)

Digital piracy includes the unauthorised downloading, copying, and sharing of copyrighted material, counterfeiting, and forgery. Pirates tend to view information assets as free goods or common wealth to be downloaded and copied without let or hindrance. When carried out on an international scale we have the phenomenon of the global virtualisation, distribution and appropriation of ‘information property’. For the pirate everything found on websites can be downloaded unless blocked by encryption devices, punitive copyright legislation and corporate sanctions. File sharing of music, images and software is usually seen as the most prevalent form of digital piracy. Over the past two decades digital sampling – innocently framed as downloading – has become something like a way of life for millions of Internet users (illustrating the thesis that the very pervasiveness of downloadable content deconstructs conventional rules regarding intellectual property and facilitates the emergence of new definitions and models of ‘ubiquitous criminality’).
The Internet provides the perfect environment for digital piracy. Online auction sites such as eBay and Bidlet provide a perfect environment for new forms of criminality. Individuals trading on eBay, for example, have no knowledge of the artefacts being sold, of the sales process or, in many cases, legal redress (there are global initiatives to introduce compensation systems for fake commerce on such auction sites). Fraud on such auction sites is considered to be the most prevalent type of e-commerce crime in the United States. Another form of copyright violation is commercial counterfeiting. The spread of counterfeit goods, especially counterfeiting of luxury items, suggests that counterfeiting and commodity fraud is being carried out as a new form of illicit industrialisation (especially in the so-called ‘Tiger’ economies where faking high-profile branded goods and counterfeit culture has become a major source of revenue for the black economy).

Taken together these forms of copyright violation create a scenario where the computer game ‘Grand Theft Auto’ becomes a realistic model for the economics of virtual and real commodification. Where pre-digital economic life created recognisable forms of cowboy culture we now move into an era of global counterfeit economics where the counter-economy of copied goods and reverse-engineered products is becoming as extensive as the circulation of commodities in the legitimate economy.

Digital counterfeiting (including digitally facilitated forgery) is a specific example of the more general attack upon the authorial signature, property and authentication that graphically reveals the threatened status of intellectual property in an age of ubiquitous access (Bettig 1996; Blyth and Kovacich 2001; Rifkin 2001).

Where the owners of copyrighted material see downloading, text-sharing and sampling as criminal plundering, the user’s perspective frames digital criminality in the legitimising rhetoric of do-it-yourself creativity, innovation and cultural subversion. File sharing enables every user of the Internet to adopt a situationist attitude towards cyberspace. What was once an exceptional activity of ‘underground’ counterculture now becomes a global norm of mainstream culture. Mixing and mashing in multimedia formats presents itself as alternative, distributed anti-art (even where we recognise that ‘[the] Situationist notion of making art indistinguishable from everyday life is now known as branding’ (Mason 2008: 21)).

Where the legal system views counterfeiting as copyright infringement, file sharers see their activities as new forms of cultural morphing (mixing, mashing, fusion and hybridising). The new digital systems create radical technologies that promise self-transformation. Here ‘piracy’ blurs into the cultural phenomenon of DIY mashing and morphing. Thus for ‘many artists and musicians, the digital bank is there to be plundered’ (Murphie and Potts 2003: 69):

… the Internet is more like a social space than a thing … the magic of the Internet is that it is a technology that puts cultural acts, symbolisations in all forms, in the hands of all participants; it radically decentralises the positions of speech, publishing, filmmaking, and radio and television broadcasting, in short the apparatuses of cultural production … Internet
communities function as places of difference from and resistance to modern society ... They are places ... of the inscription of new assemblages of self-constitution. (Poster 2001: 176, 184, 187)\textsuperscript{10}

The establishment response to free file sharing is predictable. We move from the analogue language of ‘property and its protection’ to the digital realm of global digital protection. Where lawsuits and criminal procedures fail or prove expensive major firms and corporations adopt compromise solutions. After strenuous attempts at criminalising downloading, they turn to more benign forms of regulation; and, finally, corporate media businesses (Apple’s music store iTunes is an example) adopt policies of actively supplying media at a cheap rate and thus quasi-legalising what would otherwise be viewed as piracy. In this way ‘the music industry has accommodated sampling by making it legal – for a fee’ (Murphie and Potts 2003: 70). Another technique of incorporation is to employ hackers as a source of innovation: ‘smart companies, instead of criminalizing hackers, will encourage these user-innovators and solicit their feedback to design better products’ (Pescovitz 2008: 323).\textsuperscript{11}

4.3 From corporate criminality to punk capitalism

The growth of automated electronic scams, of organised phishing gangs and transnational lottery scams is symptomatic of the global reach of cybercrime and suggests that we require a political economy of digital crime to explore the new interlocking systems of electronic banking (e-commerce), telemarketing, global finance capitalism and the dynamic flows of circulation, exchange and appropriation. Such a framework would also need to explore the subcultures of blurred criminality, the global spread of the black economy and the processes of capital redistribution and money laundering by organised criminal syndicates. It is thus no exaggeration to speak of such emergent economies – from underground or black economies to organised money laundering and piracy – as the new economy of punk capitalism (Mason 2008; cf. Featherstone and Burrows 1995). The proliferation of heterodox commercial transactions, illegal trading, and ‘fast business’ enterprises has come to characterise the world of punk capitalism.

These transformations of e-commerce suggest that we require a theorisation of the new criminality as a force of planetary sociocultural change. Future research needs to explore the blurring of the continuum from organised mass-mailing scams and peer-to-peer file sharing networks to the construction of black economies linked to online gambling operations, organised crime and terrorism (McChesney 1997; McChesney et al. 1998; Schiller 1999; Soja 1989).

Consider for example the controversies associated with global patents and the corporate monopoly on such ‘objects’ as genes, seeds and prescription drugs. Is the restrictive pricing of important drugs by the pharmaceutical industry simply an instance of normal monopoly practices (protecting a commercial asset) or a more problematic example of global criminality in the face of a worldwide need for these commodities? As Mason observes in relation to the restrictive practices of drug companies: ‘Never before has an industry needed piracy so badly’ (2008: 62).
Botnets and other forms of malware

While ‘spyware’ is the generic name for ‘viruses’ that fraudulently access computer systems, botnets or robot networks are malicious programs; ‘zombies’, or ‘malware’ that are seeded on a computer for fraudulent purposes. As a form of spyware, botnets enable the hostile downloader to function in the place of the legitimate online user. Like some of the earliest forms of hacking, botnets are frequently used to close a computer system – in so-called ‘denial-of-service’ attacks, the seeding of ‘ransomware’ and ‘logic bomb’ threats. Unlike earlier viruses botnet zombies operate through automated programs that can rapidly ‘scan’ databases in order to extract relevant information patterns. Recent cases of botnet keylogging and data harvesting have seen these technologies linked to blackmailing and extortion crime:

Botnets can also be used to launch coordinated attacks on a particular Internet endpoint. For example, a criminal can attack an Internet gambling Web site and then extort payment to make the attacks stop. The going rate for a botnet to launch such an attack is reputed to be about $50,000 per day. Virus makers compete against each other to compromise PCs exclusively, some even using their access to install hacked versions of antivirus software on victim computers so that they cannot be poached away by other viruses. The growth of virtual worlds and massively multiplayer online games provides another economic incentive for virus creators. As more and more users log in, create value, and buy and sell virtual goods, some are figuring out ways to turn such virtual goods into real-world dollars. Viruses and phishing e-mails target the acquisition of gaming passwords, leading to virtual theft measured in real money. (Zittrain 2008: 46–7)

The unintended impact of ‘smart’ devices like botnets is illustrated by the increase in encryption/decryption competition, the emergence of new forms of global risk management and international governance and the prospect of a globally patrolled and regulated cyberspace. As a response to notorious cases of hacking and botnet scams we see the creation of new forms of policing, criminal legislation, international internet legislation, and state sponsored disciplinary programmes. The past decade has seen the creation of ‘meta-organisations’ specialising in information security, advisory functions relating to digital assurance for the private sector and public bodies concerned with the national threat of cybercrime. We have also witnessed a massive explosion in national and international legislation concerning transnational digital security, intellectual property rights, the governance of electronic commerce and international standards. Given these developments it is likely that IT security organisations as a form of meta-monitoring of corporate and governmental organisations is set to become one of the fastest-growing sectors of economic activity in the industrialised world (see Blyth and Kovacich 2001; Ollmann 2008).
4.4 Cyber-terrorism

The last years of the twentieth century and the first decade of the twenty-first century appear to many as an era of global insecurity. These anxieties are epitomised by the phenomenon of global terrorism and, more particularly, by terrorism based upon information warfare (cyber-terrorism or electronic attacks on IT and communications systems). We might say that global terrorist acts such as those of 9/11 in the US and the London tube bombings in July 2005 represent a conflation or ‘compression’ of every other form of digital malfeasance: configuring money laundering and corporate investment, digital piracy, identity theft, the creation of illicit cells and networks and the strategic manipulation of cyberphobia for terrorist ends. The extent of this compression can be illustrated by the dependence of terrorist networks upon the latest technologies of multimedia platforms and cellular phone telecommunications.

State responses to recent forms of terrorism reveal a consistent pattern: first, a high-profiled awareness of the global character of the new terrorism; second, the view that the present network of terrorists is fundamentally dependent upon ICTs such as mobile phone links and email; and third, that the ‘war on terrorism’ necessitates a political order sensitised to the idea of permanent emergency. Events like the destruction of the Twin Towers in America and the continued threat of terrorist plots against the Western powers is used to create a political environment of increasing legislation against terrorist activity, an increase in CCTV technology and erosion of civil liberties, and further steps towards a surveillance society of total monitoring and control. In this way real and imagined cybercriminality play into the hands of centralising powers and technocratic organisations that reframe society’s problems in terms of total regulation and surveillance: the enemy is both within and without.

The unintended consequences theorem operates here: in striving to ‘protect the public’ from global terrorism governments actually undermine freedoms and civil liberties by introducing draconian security measures (from the rigours of airport and transport security systems to the spread of CCTV cameras across private and public space and the introduction of identity cards and related biometric methods of identification such as voice recognition and retinal imaging). Here the unintended dynamics of global criminality has profound consequences for the restructuring of national and international governmental priorities, policy legislation and their impact upon the conduct of everyday life. Even if a society was not chronically prone to risk prior to these monitoring innovations, the society that is produced by surveillance becomes in a self-defining way a global ‘risk society’ (Beck 1992, 1999). In this way the sociology of global terrorism illustrates the dialectical relationship between cyber-trespass, surveillance and governance.

We have seen that cybercrime – like globalisation more generally – blurs the boundaries between local, regional, national and international activities. Where old style terrorism is targeted at regional and national level, new style cyber-terrorism is explicitly international in its ideology and targets. The new-style terrorism, exemplified by al-Qaeda, becomes a major player in a range of societal transformations that directly affect the power structure and political
economy of whole societies. Here the deterritorialisation of cybercrime assumes the form of an attack upon governments and nation states that has the effect of restructuring citizenship and the quality of life for the population. In other words, like other forms of e-criminality, these border-dissolving phenomena play a powerful role in shaping social and cultural change in the advanced industrial societies.

We find a number of recurrent characteristics:

First, terrorism based upon digital technologies is itself a social form of delocalised cosmopolitan interaction made possible by globalisation.

Second, cyber-terrorism is a product of new circuits and networks of criminal ‘capitalism’ (what might be called ‘asocial capital’). The circuitry of capital today includes the creation of underground markets based upon the flow of criminal transactions and the haemorrhaging of capital in various types of money laundering activity. We thus find interlocking networks that produce the new ‘junk economies’ of global crime (involving people trafficking, drug smuggling, global prostitution and the sex trade, money laundering, organised gambling rackets, and so on). Here the intersection of local and global criminality justifies the use of the concept of ‘glocalised crime’.

Third, the threat of ‘global terror’ is represented as the most universal form of ‘alterity threat’ that legitimises the reconstruction of civil society, governance and military preparedness to create a permanent state of emergency (the ‘war on terror’, the generic threat of jihadist websites, and the Russian ‘raid’ on the information infrastructure of Estonia in May 2007 are recent examples of this phenomenon).

Fourth, responses to this ‘threatening Other’ range from the geopolitical ‘war on terror’ against ‘rogue’ states such as Iraq and Iran to an intense concern with public and private boundary regulation, from physical surveillance (CCTV) to biometric identification, automatic Internet monitoring, and government-sponsored data mining (for example the National Management Information System (NMIS) in the UK).12

The threat of universal terrorism (cyber-jihadism) conjoined with cyber-terrorism presents a massive political incentive to militarise everyday life in the advanced societies under the surface forms of protection and depoliticisation, a process that seamlessly integrates movements towards accelerated geopolitics, global data surveillance and biopolitics. An individual state’s investment in surveillance and monitoring activities has a ‘multiplier effect’ in creating a culture of fear focusing upon ubiquitous, invisible, and uncontrollable viral intrusions. This involvement is escalated when whole political regions are involved – such as NATO’s response to the Estonian cyber-attack. By invoking apocalyptic threats to ‘law and order’, governments are forced to reorganise their priorities and promote panic rhetorics and agendas to protect the body politic from invasive forces.13

5. Conclusion: future research directions

Researchers in the field of cybercrime repeatedly point to three major methodological issues: empirical under-determination, access, and multi-
disciplinarity. ‘Empirical under-determination’ refers to the lack of reliable and comprehensive empirical studies of the different forms and dynamics of e-crime. ‘Access’ refers to the difficulties of defining and researching cybercrime on a transnational and comparative basis and of critically evaluating different studies and findings. ‘Multidisciplinarity’ indexes the importance of developing cybercrime research paradigms with a comprehensive transnational approach to the global reach of cybercrime. Bearing these issues in mind we will briefly sketch some of the ideas and paths that might be pursued in further research in the field of e-criminality.\textsuperscript{14}

**Theoretical frameworks**

Phenomena like rogue trading, corporate corruption, and global terrorism carried out through telecommunications systems exemplify some of the central concerns of so-called ‘risk society’ theory (Beck 1992; Giddens 1990, 1991, 1992, 1998). As social systems become more complex and reflexive they generate unanticipated and chaotic consequences. In the case of the present global financial meltdown this susceptibility to chaotic behaviour is exacerbated through processes of deregulation and privatisation. Beck’s original ideas about the universalisation of risk in late modern societies have been expanded to create a range of global sociological and philosophical frameworks directed towards forms of deep connectivity that transcend the typically ‘nation-based’ explanatory frameworks and their associated public policy formation and regulatory regimes. Some of the more innovative paradigms have built on these beginnings to create new research programmes that integrate the specific study of global crimsapes within more generic social theories of the Internet and cyberculture.\textsuperscript{15}

We might briefly mention the following.

**Risk theory paradigms: from risk society to alterity studies**

Critical research on digital mobilities, border-crossing, and global alterities requires a radical rethinking of some basic philosophical assumptions about identity and sociality in risk-prone environments, complex emergence, risk management, the interaction of private and public space and the like (Hamelink 1996; Massumi 2002). Risk and chaos paradigms need to be developed to provide a more integrated understanding of interlocking systems and networks. Thus the analysis of convergent ‘mobile’ technologies and global communication systems as these impact upon and reconfigure material culture, everyday life and everyday practices requires a much more global approach to everyday life in the new information societies (McCullough 2004). Where these networks are themselves ‘reflexive’ we need to move beyond classical modernisation frameworks to self-reflexive models of socio-economic, political and cultural systems. The philosophical background to the sociology of alterity can be found in the diverse writings of Michel Foucault, Paul Virilio, Jean Baudrillard, Jacques Derrida, Gilles Deleuze, Felix Guattari and Slavoj Zizek (among others).

**Teratological paradigms**

The idea of globalised threats and transgressive behaviours has led to discourses
new social theories of technology

The global impact of ICTs and the development of convergent electronic technologies has refocused scholarship on the creative and unpredictable social uses and applications of digital technology and encouraged the development of explicitly cultural theories of technology that move beyond standard ‘Actor network’ theorising to develop more complex, reflexive and politically engaged accounts of techno-scientific processes. Recent work has stressed such factors as contextuality, the constitutive role of users’ interests, the creative appropriation and transformation of technologies as they are used, recombined and modified for non-standard applications and the fundamental role of socio-economic and political relations in defining the phenomenology of human/non-human systems.

1. Social Informatics and critical cyberculture studies

If we take the idea of cyberspace literally it suggests the construction of new kinds of ‘social space’ and new forms of social relations embedded in those ‘spaces’. Once these ‘virtual worlds’ become institutionalised we create emergent electronic sites of cultural activities and practices made possible by digitisation. It is not simply a case of ‘real’ public spaces being augmented by new virtualities; rather, what has previously been regarded as ‘social space’ (itself symbolically constituted) is in the process of being radically transformed by the new informatic technologies. We could speak of the practices and environments of everyday life being colonised and transformed by digitisation. Not surprisingly, cyberculture as a pervasive ‘postmodern’ phenomenon has become the central theme of such innovative interdisciplinary research programmes as Social Informatics and cyber-demographics (Burrows and Ellison 2004), new forms of geopolitical theory (Soja 1989, 1996), reflexive economic theory (Soros 1998, 2008), the study of power configurations in cyberspace (Jordan 1998; Terranova, 2004), and the sociocultural investigation of electronically situated identities and identification processes.

2. Globalised surveillance perspectives

The confluence of ICTs, accelerated globalisation and risk culture converges upon societal surveillance (one symptom of this is the UK government’s publication of a ‘National Risk Register’ in 2008 which ranks cyber-terrorism as the second most likely form of terrorist attack after an attack on the transport system and before an attack upon a public target). We have seen that cyberspace transforms and elevates the universe of digital access and planetary connectivity into the basic principle of the new world economy. It also produces a world of reflexive social relations based around informatic
principles of categorisation and social sorting. The new technologies thus facilitate the monitoring of everyday life on a continuous basis (the coming of real-time ‘Google Earth’ being indicative of the surveillance possibilities of the new media). Many fear that Foucault’s generalised ‘panopticon’ has been morphed into the global electronic panopticon (Foucault 1977). Private life is threatened by ubiquitous surveillance technologies that increasingly form an integral part of the fabric of everyday life (Davies 1996; Staples 1997). These changes have motivated the development of critical studies of globalised surveillance (Haggerty and Ericson 2006; Lyon 2001, 2003, 2006, 2007; Marx 2004).

3. Cyberphobia and the politics of fear

From the perspective of Web security experts the expansion of the Internet transforms everyone with access to digital media into a potential criminal. This is reinforced by mass media images of e-criminality. Thus popular media in the UK is rife with images of cyber ‘folk devils’ and associated moral panics. Recent debate and legislation relating to cyberspace – fuelled in particular by media concern with online grooming, paedophilia and pornography (especially child pornography) – suggests that we are moving from an age of anxiety to an era of permanent fear and global insecurity. Any critical discussion of cyberphobia has to begin with media representations of Internet ‘threats’ and the debate on censorship, regulation and civil liberties that these images have initiated. In a broader context it is important to understand the sociology and politics of fear as these relate to the transformation of everyday life and social identities in a globalised society.19

4. Prevention, regulation and policing

There are three recurrent themes in the literature on cyber-regulation. Firstly, there is the increasing internationalisation of law and policing relating to cyber-crime. Jurisdictional procedures, legal frameworks and policing models that had evolved within a national framework must be radically reformulated in order to deal with cross-border criminality. Against a general background of the failure of policing models in the 1980s and 1990s we have seen major transformations of cyberspace law, regulation and policing strategies. This new concern for complex risk management has motivated the creation of specialised high-tech police e-crime units and digital law enforcement agencies such as the UK’s Serious Organised Crime Agency, the National Hi-Tech Crime Unit (NHTCU), the Metropolitan Police’s Computer Crime Unit, the Internet Crime Forum and equivalent organisations in the United States such as the National Cybercrime Training Partnership (NCTP), the National White Collar Crime Center, and the National Infrastructure Advisory Council. The other major innovation is the introduction of transnational government regulations that apply to every part of cyberspace. This has encouraged international collaboration in creating global cyberspace protocols. One notable landmark here is the European Council’s joint Convention on Cybercrime.20

A second theme in the emerging discourse of ‘internet governance’ is the expansion of private security companies. The regulation of digitalised public and personal space has created a growing cyber-security industry specialising
in securing computer networks, systems and digital vaults. Infrastructure regulation has led to highly technical innovations in encryption and filtering technologies. The technical literature from the growing security industry reads like a cryptographic arms race of encryption and decryption code struggles (the language of ‘attack vectors’ and ‘counter-attacks’ is now commonplace). Regulatory concerns have also produced new techniques such as digital forensics and the reverse engineering of computer hard drives, Web surfing histories and email tapping (collectively referred to as ‘computer forensics’). Today almost every advanced country has data protection legislation and private security organisations offering specialist protection services. Indeed the ‘leapfrog’ effect of phishing sophistication and counter-security measures has itself become a major source of innovation in addressing online criminality. This creates further layers of reflexive complexity in the detection and policing of online fraud (see for example the Phishtank.com site and the literature produced by the Anti Phishing Working Group (APWG)). In 1996 the UK government set up an Internet Watch Foundation (IWF) that serves as a ‘hotline’ to report illegal Internet content (there is a similar agency that operates on a Europe-wide basis).

Finally, there is the insistent theme of prevention through education, self-protection and self-policing. To counter cybercrime the first stage is to encourage users of cyberspace to become security conscious and apply anti-virus programs and firewalls that obstruct e-criminality and filter unwanted content. Companies and organisations are thus investing in major training programmes for their employees. Education also needs to instruct online users about the differences between licit and fraudulent emails. Banks, online shopping and auction sites have thus begun to invest in policies and security measures that provide advice to protect users. Countering transnational cybercrime is expected to become one of the major public education issues over the next decade.

Notes

2 This approach links social categorisation to the institutional and informational orders of societal control and compliance. For more detail of these connections see Sandywell (2006). On the general problem of sociocultural classifications that reflexively constitute the practices of social life see Bowker and Star (1999) and Lyon (2003).
3 According to George Soros the deregulation of global financial transactions directly served ‘the interests of the managers of financial capital; and the freedom to innovate enhanced the profitability of financial enterprises. The financial industry grew to a point where it represented 25 per cent of the stock market capitalisation in the United States and an even higher percentage in some other countries’ (2008). The subprime crisis of overlending and toxic debts in the US housing market is thus merely an indicator of a more global ‘super-bubble’ that is currently (October 2008) reconfiguring the world economy.
4 While ‘globalisation’ and ‘globalised modernity’ are not synonymous with ‘network society’ or ‘information society’ we can, for present purposes, treat these terms
as conceptual equivalents. For globalisation as a complex and overdetermined economic, political, and cultural process see Bauman 1998; Castells 1996, 1997; Cohen and Kennedy, 2000; Featherstone 1990; Held 2000; Hirst and Thompson 1996; Robertson 1992; Scholte 2000; and Waters 1995. The concept of ‘reflexive globalisation’ designates the phenomenon of self-organising, self-monitoring, self-regulating and self-producing processes as these are emergent within social systems at critical levels of qualitative and quantitative complexity (see Soros 1998). The emergence of global cybercriminality might be compared to the chaotic behaviour of reflexive financial systems where ‘the sheer existence of an unregulated market of this size has been a major factor in increasing risk throughout the entire financial system’ (Soros 2008). In what follows we adhere to Wall’s conclusion that ‘transformations in networking, informational transfer and globalisation have contributed to radical changes in the organisation of crime and the division of criminal labour, and to changes in the scope of criminal opportunity’ (2007: 39).

5 For further analysis of the theoretical background and perspectives that inform this perspective see Sandywell 2006. For the most detailed and comprehensive analysis of the ‘transformation of crime in the information age’ see Wall 2007; also Wall 2001a, 2003 and Balkin et al. 2007. For general sociological introductions to cybercrime see Grabosky and Smith 1998 and Yar 2005, 2006. For links between electronic technology and the surveillance society see Davies 1996; Dawson and Foster 1998; Lyon 1994, 2003.

6 The history of the Internet has been described by its inventor in Berners-Lee and Fiscetti (1999). Its history can be found in Abbate (2000). For an early utopian take on the Internet and cyberspace see Rheingold (1994). An up-to-date survey of Internet and Cyberculture studies can be found in Silver and Massanari (2006). Indispensable resources for the specific topic of cybercrime can be found in Wall 2001a, 2001b, 2003a, 2003b and 2007. For sceptical responses to e-topian rhetorics see Hand and Sandywell (2002).


8 See Wall 2001: 3, 168.

9 For the complex issue of how identities and identifications are constructed through digital media see Turkle 1984 and 1995 and the contributions to Jones (ed.) 1997 on the question of the construction of virtual identity. For technical analysis of phishing scams and security implications see Ollmann 2008.

10 For the theme of ‘mashing’ and ‘morphing’ through such devices as MP3, Napster, and music sharing on Web 2.0 sites see Sandywell and Beer 2005 and Beer 2002.

11 Crackers and hackers are often contrasted as malign (unethical) and benign (ethical) violators of computer security systems (for ‘hacking’ and ‘cracking’ see Taylor 1999; Walch 1999; Wall 2007: ch. 4; and Wark 2004). On the ‘hacker ethic’ see Himanen 2002. For a defence of digital piracy as a force for creativity and social change see Mason 2008: ‘The pirate mentality is a way to mobilise communities, drive innovation, and create social change’ (2008: 67). See also Levy 1984 and Sterling 1994.

12 For further analysis of the implications of these de-democratising forces of global surveillance see Hand and Sandywell 2002.


For background see Landow 1997; Poster 2001; Robins and Webster 1999.


An instructive empirical case study of the dialectic of technology, policing culture, and criminalisation practices can be found in Janet Kahn’s ‘The Technology Game’ (2003: 513–33).


For the ideological functions of fear in society see Furedi 2002, 2005, 2007. For cyberphobia see Sandywell 2006; also J. Dibbell, ‘A Rape in Cyberspace’ (1996). For recent work on cyber-identity and cyber-subjectivities and, more especially, the phenomenology or subjective experience of cyberspace and cybertimes see Lovink 2001, 2002; Massumi 2002; Porter 1996; Poster 2001; Stone 1996; Tomas 1998; for explorations of virtual ‘commonality and ‘communality’ see Rheingold 1994, 2002 and Holmes 1997; for post-human speculations see the work of Donna Haraway, Katherine Hayles, and others; for the transformation of politics in the digital age see Terranova 2004.

The Council of Europe, Convention on Cybercrime, Budapest, 23 November 2001. The ‘Preamble’ states its main objective as ‘the protection of society against cybercrime ... by adopting appropriate legislation and fostering international co-operation’ (Convention, p. 1). The text of the Convention is available online (http:conventions.coe.int/Treaty/EN/Treaties/Html/185.htm). Signatories apart from EU countries include the United States, Canada and Japan, but notably not Russia.

For an account of ‘computer forensics’ see Sommer (2003).

David Wall usefully distinguishes between five levels of Internet regulation: policing by Internet users themselves; the Internet service providers; corporate security organisations; state-funded non-public police organisations; and state-funded public police organisations (2001: 171). For a general introduction to the challenges that cybercrime poses to public regulation and policing see Wall 2001a, 2001b, 2003a, 2003b and 2007, chapters 8 and 9 and Grabosky and Smith 1998; for general background see Barrett 1996, 1997; Blyth and Kovacich 2001; Ellison 2001; Fuchs 2007; Steffik 1999; Thomas and Loader 2000; Terranova 2004; Webster 2006.

Further reading

On the interconnections between globalisation and new communication technologies see Manuel Castells’ influential The Rise of the Network Society (1996), and on the transformation of social, political and economic life by the Internet see his book The Internet Galaxy (2002). On the globalisation of crime, an excellent overview is provided by Katja Franko Aas in Globalization and Crime (2007). On the globalisation

**References**


On the globalisation of crime: the Internet and new criminality


On the globalisation of crime: the Internet and new criminality


