The internet and its opportunities for cybercrime

Koops, E.J.

Published in:
Transnational Criminology Manual

Publication date:
2010

Document Version
Peer reviewed version

The Internet and its Opportunities for Cybercrime

Prof. Bert-Jaap Koops, TILT – Tilburg University

in: M. Herzog-Evans (ed.), Transnational Criminology Manual, Vol. 1, Nijmegen: WLP, p. 735-754

Abstract
The Internet deserves special attention in criminology as well as criminal law and policy, because of several characteristics: it is global, instantaneous, intrinsically transborder, digital, and enables automated information processing. Because of these characteristics, the Internet provides special opportunities to commit cybercrimes: crimes in which computer networks are the target or a substantial tool. This chapter provides a concise review of literature that has investigated how and why the Internet provides special opportunities to commit crime, and what this implies for the governance of (cyber)crime. It sketches some typologies of cybercrime, and lists 12 risk factors of the Internet that in combination provide a unique opportunity structure for crime. Next, the chapter discusses what little is known of cybercriminals, organised cybercrime, and cybervictims, and briefly discusses the challenges and limitations of law enforcement and other countermeasures. Although empirical research on cybercrime is scarce, the theoretical insights and hypotheses advanced in the literature warrant the conclusion that the Internet is transforming crime. It is suggested that cybercrime is becoming organised, large-scale, diversified with increasing division of labour, and is expected to develop increasing ties with offline organised crime. Moreover, offline and online victimisation seem to show significant overlap for some crimes. Now that Internet use has become a routine activity in everyday life, criminology as well as criminal law and policy should also incorporate the Internet and cybercrime in their own routine activities, while paying attention to the peculiarities and complexities of the unique phenomenon that is the Internet.

1 Introduction

The Internet was created in the 1960s, but it only caught the attention of governments and criminologists in the mid-1990s when it became a large-scale medium for the general public. Before, the focus had been on *computer*-related crime. Now, the buzzword was *cyber*crime, stressing the fact that computer networks – 'cyberspace' – raised new questions for criminal law and policy. Perhaps the Internet even changes the nature of crime itself, as witnessed by the title of a seminal work by David Wall (2007), *Cybercrime – The Transformation of Crime in the Information Age*.

The Internet deserves special attention because of several characteristics. It is global and allows for real-time connections between people regardless of their location. Therefore, time, distance, and national borders are much less important than in traditional crime. The Internet, being a digital network, allows for processing data and information in automated ways, almost at the speed of light, and on an unprecedented scale.

Because of these characteristics, the Internet provides special opportunities to commit crimes, which are usually called cybercrimes. Cybercrime can be defined as crime in which computer networks are the target or a substantial tool. Cybercrime deserves specific attention from a criminological perspective, because of the unique character of the Internet. 'Routine activity theory (and, indeed, other ecologically oriented theories of crime causation) thus appears of limited utility in an environment that defies many of our taken-for-granted assumptions about how the socio-interactional setting of routine activities is configured' (Yar, 2005, p. 425).

This chapter investigates how and why the Internet provides special opportunities to commit crime, and what this implies for (cyber)crime control and Internet governance. I will sketch the types and characteristics of cybercrime (section 2), cybercriminals (section 3), and cybervictims (section 4). I will then briefly discuss counterstrategies (section 5), and conclude with a reflection

on the Internet's crime opportunity structure in relation to crime and Internet governance (section 6).
Some limitations apply. There is a scarcity of empirical research on cybercrime: little is known of cybercriminals, and hardly anything of cybervictims, in practice. The chapter can therefore only sketch theoretical insights and hypotheses advanced in the literature. Moreover, the length constraints of this chapter only allow for a bird's eye view. I will not discuss cyberpiracy, which is in many respects a different and contentious form of cybercrime, nor cybersex crimes, which is treated elsewhere in this volume (Cuijpers & Van der Knaap, 2010). Also omitted are cyberterrorism and cyberwarfare (Denning, 2001; Stohl, 2007; Brenner, 2009) , which are forms of cyberattacks with elements of crime, but which have a different context than the classic crime perspective taken in this chapter.

2 Cybercrime

2.1 Prevalence and perceptions of cybercrime

The exact prevalence of cybercrime is unknown. Convictions for cybercrimes are still relatively rare (compared to other crimes), although that does not mean cybercrime is not prevalent (Smith et al., 2004, pp. 25-29). There is supposed to be a high 'dark number' of undetected, unreported, uninvestigated, or unresolved cybercrimes, due to the invisibility and complexity of digital traces and a general reluctance of business victims to report for fear of reputation damage. Crime victim surveys have only recently begun to include questions on Internet crime, often limited to fraud and illegal or offensive content; they tend to exclude malware and other 'core' cybercrimes since these are difficult to recognise for average computer users. Many statistics are published of computer-security incidents, notably of viruses and other malware and phishing attempts. However, these often come from security companies with an interest of selling, e.g., anti-virus software, and should therefore be taken with a (large) pinch of salt. Another complicating factor is the 'mythology' of cybercrime fed by popular images in movies and novels, with a stereotypical hacker as the archetypical cybercriminal (Wall, 2008a; Wall, 2008b; cf. Jewkes & Yar, 2010, pp. 104-166). Such popular perceptions can be far removed from reality. Nevertheless, the overall trend in the literature is to suppose that (many) more cybercrimes must occur than is empirically established, even if research efforts fail to shed light on the 'dark number'. David Wall (2007, p. 28) warns against the conundrum of our beliefs about cybercrime's prevalence: 'we are shocked by cybercrime, but also expect to be shocked by it because we expect it to be there, but – confusingly – we appear to be shocked if we are not shocked (if we don't find it!).'

2.2 Typologies of cybercrime

To understand cybercrime, it is useful to make some distinctions, since the motivations and modi operandi of perpetrators may differ for various types of cybercrime. The most common distinction is between the Internet as a tool or as a target. The European Commission (2007, emphasis added) defines cybercrime as 'criminal acts committed *using* electronic communications networks and information systems or *against* such networks and systems'. Besides computer networks as instrument or object of crime, Donn Parker (1973) already pointed out a third type where computers are the *environment* of crime, in the sense of a more or less neutral background for a crime.
The typology of the Internet as object, instrument, or environment is mirrored in what is probably the most useful categorisation of cybercrime to use today: the list of substantive crimes in the Council of Europe's Cybercrime Convention (see *infra*, section 5.1). The Convention criminalises:
1. offences against the confidentiality, integrity and availability of computer data and systems; these include illegal access (hacking), illegal interception, data interference (e.g. viruses), system interference (e.g., denial-of-service attacks), and misuse of devices (e.g., possessing hacker software);
2. computer-related offences; these include forgery and fraud;
3. content-related offences and copyright offences; the former covers child pornography (racism is included in a separate Protocol to the Convention).

A different, more chronological, typology is offered by Wall (2007, pp. 44-48), focusing on the evolving opportunity structure of cybercrime. The first generation of cybercrimes consists of traditional crimes where (stand-alone) computers are merely a tool; these are 'low end' cybercrimes. The second generation, from the 1970s onwards, consists of crimes facilitated by local or global computer networks; these are still largely traditional crimes, but they give rise to new globalised opportunities and jurisdictional problems. The third generation are 'true crimes wholly mediated by technology', constituting a 'step-change in the transformation of cybercrime' (Wall, 2007, p. 47). These are 'high end' and *sui generis* cybercrimes that would not exist without the Internet. The focus of this typology is not so much the role of the Internet as tool or target, but the way in which crime itself is being transformed by the Internet, evolving into new forms with different patterns of offender organisation and offender-victim relations.
In this respect, the question arises whether a fourth generation is emerging, where cybercrime occurs not only through or on the Internet, but in completely virtual spaces, such as massive multi-player online role-playing games (e.g., World of Warcraft) and virtual worlds (e.g., Second Life). Should abuse committed in these virtual spaces, such as stealing virtual swords, having sex with a young-looking avatar, or abusing an avatar, be treated as a new, *sui generis* type of crime – a fourth generation of 'virtual crime' –, or as just a new way of committing traditional crimes (second generation), or not as crime at all since it is just 'virtual' and not 'real' or because different social norms apply in virtual communities? Current literature seems to incline towards the latter approaches: *if* there is some form of real (i.e., non-virtual) harm – which is not evident with 'virtual crime' –, the behaviour can be treated as a traditional offence (Lastowka & Hunter, 2005; Kerr, 2008; Brenner, 2008; Clough, 2010, pp. 16-21).
Another relevant classification is based on different motivations. Thomas and Loader (2000) distinguish between hackers and phreaks (motivated by curiosity), information merchants and mercenaries (motivated by financial gain), and terrorists, extremists, and deviants (motivated by political or social activity). For some other classifications, see Walden (2008, pp. 21-23).

2.3 Risk factors of cybercrime

The Internet has several characteristics that are particularly relevant to explain the opportunity structure for cybercrime. It is a global network, provides for instantaneous connections, in a networked structure that is decentralised, and it is based on digital representation of information. These features of the Internet form the basis of 12 specific, interrelated, risk factors that facilitate cybercrime. The Internet:
1. has a *global reach*, enabling perpetrators to look for the most vulnerable computers and victims anywhere in the world without having to leave home or the next-door Internet café (Yar, 2005, p. 421);
2. related to this, leads to *deterritorialisation*, which implies that cybercrime is almost by definition international, with consequent legal challenges of jurisdiction and cross-border co-operation;
3. allows for decentralised, *flexible networks* in which perpetrators can (loosely) organise themselves to divide labour or to share skills, knowledge, and tools (cf. *infra*, section 3.3);
4. facilitates *anonymity*, at least for perpetrators who have the knowledge and take some effort of using anonymisation tools such as remailers and torrent networks; however, also less tech-savvy perpetrators are (or feel) relatively anonymous when they operate at a (large) distance from behind an IP number, email address, or scam Facebook profile that is often not easy to trace to a specific individual (Sandywell, 2010, p. 44);
5. enables *distant interaction* with victims, removing potential social barriers that perpetrators face in physical, person-to-person interaction; cybercrime thus involves 'anonymous, networked and rhyzomatic relations between perpetrators and victims' (Sandywell, 2010, p. 44);
6. facilitates *manipulability* of data and software with minimal cost (Sandywell, 2010, p. 44), because it is based on digital representation (allowing for copying without loss of quality, and altering without visible traces) and because the Internet was built as an open infrastructure with intelligence at the end points to foster innovation by end-users;
7. allows for *automation* of criminal processes, where one piece of software launched on the Internet can replicate and attack millions of computers at the same time – but also over longer periods of time – and where basic software such as a sample virus can be easily customised by so-called 'script kiddies' to create a new virus (Wall, 2007);

8. can blow up the *scale* of a crime from a minor nuisance to major harm, for example when a virus has far graver consequences than a curious script kiddie imagined, or when a remark or (sex) photograph posted online acquires a global and permanent reach; for example, 'harassment writ large in cyberspace – expanded so drastically in target, scope, and reach – has far greater impact than any schoolyard attack' (Franks, 2010);
9. allows for *aggregation* of a large number of insubstantial gains, for example, through salami techniques (stealing 0.5 cent from ten thousand bank accounts a thousand times); more in general, cybercrime often has many victims with relatively small damage each; this *de minimis* problem may be one of the biggest challenges of cybercrime since it reduces incentives to report, investigate, and prosecute the crime (Wall, 2007);
10. facilitates an *information economy* where information has become a valuable asset , both in the legal market (e.g., music, movies, software, books) and in the black market, where credit-card numbers, personal information, and passwords are traded to facilitate fraud and theft (Wall, 2007, p. 32);
11. has structural *limitations to capable guardianship* that can serve as a social or technical obstacle to commit crime (Yar, 2005, p. 423);
12. has *rapid innovation cycles*, allowing for new techniques and tools to be developed in short periods for committing crime and for circumventing existing countermeasures.
Although authors tend to point out different subsets of these characteristics or risk factors as the major factors to take into account, they generally agree that it is the *combination* of such factors that makes cybercrime a special challenge and that imply that the Internet effects changes in crime. For example, Balkin and Kozlovski (2007, p. 2) summarise: 'Digitization, anonymity, interconnectivity, decentralization, and interdependence structure the online world as we currently know it. Hence they structure the opportunities for crime and the ways that people commit crimes and breach network security.' Sandywell (2010, pp. 44-45) concludes that '[w]hen combined these features create ubiquitous digital platforms that facilitate information-based borderless crime on a planetary scale and hence prefigure the emergence of a situation of permanent information warfare.'

3 Cybercriminals

3.1 Hackers and their hats

It is customary, at least in sociological and technical literature, to distinguish between two basic types of hackers: good guys, called 'ethical hackers' or 'white hat hackers', and bad guys, called 'crackers' or 'black hat hackers'. For many, the term 'hacker' retains the aura from the 1980s and early 1990s where hackers wearing white hats played a crucial role in the development of the Internet by testing systems (Wall, 2007, p. 55; Sterling, 1994). This generation shared a code of norms, a 'hacker ethic' (Himanen, 2000), to enhance information security, freedom of information, and access to technology, and ultimately aiming at improving the Internet and the world at large. Subcultures within the hacker community, however, differed in background, some being simply curious wizzkids, some being 'utopians', and others being fiercely anti-establishment 'cyberpunks'. The latter groups did (and do) not mind doing harm to information systems if they think it contributes to their goal, and hence, tend to be disruptive in a society dependent on information systems (Wall, 2007, pp. 55-56). Moreover, with the Internet reaching mass public in the 1990s, other groups started to use hacking driven by other motivations, such as financial gain, terrorism and other types of 'hacktivism'. Deviating from the 'hacker ethic', such perpetrators were termed 'crackers' by the self-righteous 'ethical hacker' community. But in fact, it has become difficult over time to distinguish between clear shades of white and black in the hats of hackers: 'hacking has developed far beyond the original first generation system hacks to reveal a broad array of activities and motivations. Under close scrutiny this range of behaviours are found to represent a spectrum of qualitatively different types of trespass, from intellectually motivated acts at one end to politically or criminally motivated trespass at the other' (Wall, 2007, p. 54).
The dominant discourse of law and policy actually does not distinguish substantially between the various motivations of hackers: regardless of the colour of the hat, hacking – unless with explicit consent when a company orders a hacker to test their system – is generally considered a criminal

act. There is justification for this, since for a victim of illegal computer access it is difficult to determine what the hacker has done and why, and the integrity of the computer system is corrupted (Furnell, 2010, pp. 176-177). It is also the result of the 'established institutions of cyberspace [having] enlisted the power of conceptual schema in their quest for order and control' that nowadays, hacking is 'imbued with a normative meaning whose core refers to harmful and menacing acts, and as a result it is virtually impossible to speak of, let alone identify, the hackers that engage in activities of significant social value' (Nissenbaum, 2004, p. 213).

3.2 Types and characteristics of offenders

Even though hackers are now generally seen to wear grey to black-coloured hats, there are still distinct differences between subgroups of hackers, and moreover, the stereotypical hacker is far from the only cybercriminal on the block. Some characteristics can be given of cybercrime offenders, although it should be stressed from the start that, similar to prevalence data, little empirical knowledge is available of offenders (with the exception of a few special types, such as cyberstalkers and child pornographers) (Van der Hulst & Neve, 2008). Nevertheless, based on literature study and theory, some tentative insights can be provided.

On average, cybercriminals tend to be male, white, and young, but the variation in offender groups is rising. Cybercriminals are, again generally speaking, also expected to be to some extent technical savvy, have a disregard for the law or a feeling of being above or beyond the law, have an active fantasy life, be a control freak or risk-taking, and have strong – if differing – motivations (Cross, 2008, pp. 88, 93-94).

But types of cybercriminals differ, depending on their aims, methods, or skills. Hackers are for example characterised according to their skill as 'gurus', 'wizards', or 'samurai' (whitish hats with great skills) or, conversely, as newbies, 'cluebies', or 'script kiddies' (whitish to blackish hats with no or low expertise) (Wall, 2007, pp. 55-56, 65-66). The most extensive and most interesting typology is the 'hacker circumplex', in which Rogers (2006) distributes nine hacker types in a circle consisting of four quadrants of different motives:

1. revenge (against persons, organisations, countries, or continents);
2. financial gain;
3. curiosity (knowledge, sensation, intellectual challenge);
4. fame (media attention, boasting, popular hero).

As Van der Hulst and Neve (2008, p. 112) note, however, this model is still an hypothesis needing to be empirically tested. Moreover, some other types of motivations may also play a role, such as 'for fun', sexual drive, or political motives (Cross, 2008, p. 94; Wall, 2007, pp. 62-63).

Van der Hulst and Neve (2008, pp. 106-107), based on a literature review, distinguish between three basic offender types associated with the different motivations:

1. young male criminals, who hack for fun, curiosity, or peer respect;
2. ideological hackers, who are intelligent and eager to learn, some of whom are obsessive, anti-social, or have a minority complex;
3. financially-motivated hackers, from various backgrounds.

The FBI (Icove et al., 1995) has developed a 'Computer Crime Adversarial Matrix' – which may be outdated since it is over 15 years old – that distinguishes between 'group' and 'individualist' (black-hat) hackers. Group hackers function in peer groups, with a distinct (anti-)subculture and maintaining international contacts; they belong to the above type 1 or type 2. Individualist hackers are loners who share expert information with other hackers and keep records; they belong to the above type 2 or type 3. The FBI's Matrix also comprises of espionage perpetrators from foreign intelligence services, and fraudsters.

The latter group has been studied by Leukfeldt (2010), who investigated whether online fraud perpetrators differ from offline fraudsters. He concludes that there are more similarities between the two than would be expected on the basis of the Internet's opportunity structure; many personal and socio-economic characteristics are the same. However, e-fraudsters do start committing online fraud earlier in their criminal careers, and they have less records for drugs. These differences might be explained by the fact that offline scams, unlike e-fraud, require social skills usually acquired later in life, and perhaps drug addicts who need money fast stick to direct-yielding offline scams. The most important conclusion for the purposes of this chapter, nevertheless, is that the '(perceived benefits of the) Internet does not ensure that a new group of people commits fraud offences' (Leukfeldt, 2010, p. 63).

A category that merits special attention are insiders, since a substantial proportion of cybercrime is committed by people within an organisation. Individuals who threaten vital infrastructures (motivated by revenge, financial gain, or espionage) tend to be introverted, computer-dependent, socially isolated, vulnerable to ethical 'flexibility', have a sense of entitlement and anger at authority, reduced loyalty to employers, and lack empathy (Shaw et al., 1998). Insider cybercriminals can be distinguished according to their different activities: espionage (generally by 'spies' high in the management hierarchy), sabotage (usually motivated by personal revenge), theft (often committed by younger persons lower in the hierarchy), and abuse (minor forms of misuse by employees, which cumulatively cause damage to the company) (Nykodym et al., 2005). It is hypothesised that computer addiction (possibly in the form of Internet Addiction Disorder or Pathological Computer Use) is a risk factor for insider cybercrime (Nykodym et al., 2008).

3.3 Are cybercriminals organised?

Important questions in the literature are to what extent cybercriminals are organised – a counterintuitive proposition for those who hold the stereotypical view of the loner hacker nerd – and whether traditional organised crime is transferring to the Internet. Again, too few data are available to say anything definitive about these questions; indeed, '[a]ssertions without cited supportive evidence are quickly transformed into hearsay and anecdote which are in turn recycled within other authors' assertions concerning cybercriminal activity' (McCusker, 2006, p. 268; cf. Van der Hulst & Neve, 2008, p. 127).

Nevertheless, the literature does offer hypotheses based on anecdotal evidence. There seems a trend towards increasing diversification and specialisation of tasks, in which hackers, virus writers, and spammers focus on their own special expertise, while collaborating to commit a wider range of cybercrimes (Van der Hulst & Neve, 2008, p. 80). Wall (2007, pp. 41, 43) observes a specialised division of labour with 'deskilling' and 'reskilling' of tasks in automated attacks, and he asserts (2007, p. 155) that 'the new generation of cybercrime is becoming much more organized at a higher level than its predecessors'. A distinct 'underground' criminal subculture is emerging, in which cybercrime tools and knowledge are shared and traded, and task-specific expertise is rented and hired for one-off operations. This may also include hiring students or expert ICT personnel from regular businesses; Van der Hulst and Neve (2008, pp. 126, 148) assert that 'in some cases Dutchmen are also members of organised (Eastern European) criminal networks acting as service performers'. The high unemployment of cryptologists and ICT experts in Eastern Europe is hypothesised to be a risk factor for organised cyberfraud (Bekkers et al, 2005, p. 109).

Whether the organisation of cybercriminals is similar to traditional organised crime, is debatable. Brenner (2002) argues, based on the characteristics of offline organised crime and the online environment, that cybercrime will not develop the organised-crime models of the gang or the Mafia, but instead 'will almost certainly emphasize lateral relationships, networks instead of hierarchies' in a fluid, 'swarming' model 'in which individuals coalesce for a limited period of time in order to conduct a specifically defined task or set of tasks' (Brenner, 2002, p. 50). As McCusker (2006, p. 265) points out, however, offline organised crime nowadays also comprises horizontal networks of cell-like crews, so that the difference between offline and online organised crime may be less poignant than Brenner suggests.

McCusker (2006) investigated whether current forms of organised cybercrime derive from cybercrime that has organised itself, or from organised crime that has moved online. He concludes overall that cybercrime is perpetrated by 'criminal individuals and/or groups online who are organised rather than traditional organised crime groups who are online' (p. 273). However, he also observes that both underground communities can benefit from combining efforts, because of an overlap in skills and motivation (p. 266). In any case, organised crime groups will be willing to pay cybercriminals for information to facilitate their (offline) activities, and they will also employ the Internet's opportunities to launder money or hide their traces. Whether organised crime will eventually mutate into full-fledge organised cybercrime depends ultimately on the opportunity structure of offline crime as compared to the opportunities of online crime (McCusker, 2006, p. 273).

4 Cybervictims

Even more so than with cybercriminals, cybervictims are an unknown group. Victimisation surveys do yield some data on prevalence, but hardly any data are available on risk factors for specific groups of victims.

Surveys among organisations suggest that businesses and public agencies suffer significantly from cybercrime. Figures differ greatly, however. In a 2002 US survey from the Computer Security Institute and the FBI, 90% of organisations reported a computer-security breach in the past year, and 80% reported financial loss as a result; a 2000 global survey in 12 countries by KPMG yielded only 9% of organisations reporting a security breach in the past year. The difference seems too large to be explained by national differences or the two-year measurement difference. Several other surveys report incidences of 10% to 40% of organisational victimisation (see Smith et al., 2004, pp. 14-16, for these surveys).

Individual victimisation studies remain scarce. Based on consumer complaints, data are available about credit-card fraud and identity theft in the US, which show a steady and substantial increase from 2000 onwards for fraud, and a similar increase for identity theft until 2008 after which the number declines or stabilises (FTC, 2010); a similar development is visible, although with significantly lower numbers, in other countries (Van der Meulen, 2010).

Victim surveys tentatively suggest that the overall number of victims of cybercrime is low. The largest survey, the International Crime Victim Survey of 2004/05 conducted in 38 countries, showed that 1% of respondents had been victim of Internet-related fraud in the past year (the highest prevalence was the US with 3.3%, followed by Poland, Germany, Bulgaria, and the UK). Internet fraud occurred ten times less than offline fraud, which had 9% victimhood. Taking into account Internet use data, only 2% of Internet users were victim of Internet fraud. The survey did not find a correlation between Internet use by national population and prevalence of Internet fraud (Van Dijk et al., 2007, pp. 14-15, 86). A 2000 Canadian victim survey found that 5% of Internet users had experienced computer security problems in the past year, including viruses, hacking, personal information being made public, or receiving threatening email (Kowalski, 2002, quoted in Smith et al., 2004, p. 20).

Being threatened online has recently been studied in a large-scale Dutch victim survey by Van Wilsem (2010), who found 2% having experienced threatening email, sms, or chat, while 6% had experienced offline (face-to-face or letter) threats. Of the 2% online victims, a majority had also experienced offline threats, suggesting an interweaving of offline and online risk factors. Online threat victimisation was experienced almost exclusively by young people, up to 25 years of age. Other risk factors for cybervictimisation were out-house activities, computer activities such as buying online, using a webcam, or maintaining a Social Networking Site profile, and being impulsive. Interestingly, computer activity also seemed to be a risk factor for offline threats, suggesting that questions concerning computer and Internet use may be relevant to include in victim surveys of any type of crime (Van Wilsem, 2010).

Indeed, our notions of victimisation and studying victimhood may have to be adapted due to the transformation of crime in the Internet age. As Wall (2007, p. 19) has argued, '[i]f cybercrimes are indeed, minor in nature but large in aggregate, this may affect the way that we construct victim profiles.'

5 Counterstrategies

To reduce the opportunities provided by the Internet for committing cybercrime, various strategies can be considered. Obviously, substantive and procedural criminal law and mutual assistance in criminal matters are important, but these must be complemented with various other strategies. The scope of this chapter does not allow discussion of all counterstrategies. I will limit myself to indicate the Cybercrime Convention and a few other types of strategies, including some limitations of these counterstrategies.

5.1 The Cybercrime Convention and challenges for law enforcement

The 2001 Convention on Cybercrime ('Cybercrime Convention') of the Council of Europe is the most comprehensive international legislative effort to combat cybercrime to date.[1] By July 2010, it was ratified by 29 European countries and the US. The Convention harmonises (or approximates) substantive criminal law by criminalising computer-targeted, computer-assisted, and content and copyright offences, as well as procedural criminal law by requiring states to establish basic digital investigation powers, including computer search and seizure, network search, expedited preservation of data, and telecommunications investigation. With this common legislative framework and through additional provisions on mutual assistance in criminal matters and a 24/7 network of national contact points, the Convention facilitates investigating and prosecuting cross-border cybercrime.

Many countries, also those that have not ratified the Convention, have legislation in place to criminalise and investigate cybercrimes. Although gaps exist and legislation may lag behind technical developments, the basic forms of cybercrime are by now criminalised in most countries around the world. Law in the books, however, is far from sufficient: combating cybercrime requires law in action as well. The bottleneck of law as a countermeasure for cybercrime lies here rather than in legislation itself. Significant challenges for law enforcement include international cooperation as well as allocating resources, giving priority, and providing training to combat cybercrime (European Commission, 2007). Also digital evidence presents difficulties, such as preserving volatile traces, connecting computer traces to individual suspects, and explaining digital evidence in court (Walden, 2007, pp. 353-389). A large amount of cases (75%) referred for prosecution to US federal authorities have been declined, primarily for lack of evidence (Smith et al., 2004, pp. 38, 155), which underlines the complexity of digital investigation and proof. Still, since a similarly high proportion of offenders appear to plead guilty in cybercrime cases as in traditional crime (Smith et al., 2004, p. 150), evidence problems need not be exaggerated.

On a more fundamental level, the Cybercrime Convention has received criticism in its continuation of the 'localized, decentralized system of law enforcement we have had for centuries', which ignores the intrinsic boundary-transcending nature of the Internet (Brenner, 2007, p. 218). This is a valid critique, although it is hard to see realistic alternatives to (cooperation between) local law enforcement in light of the prevailing national sovereignty that still lies at the heart of criminal law (Koops & Brenner, 2006). Another fundamental and underestimated problem is to organise security governance in such a way that cross-border cyberattacks, such as massive denial-of-service attacks on government computers, are promptly relegated to the right authority for an appropriate response, while the attack itself provides no clue whether it is cybercrime (for police), cyberterrorism (for security agencies), or cyberwarfare (for military) (Brenner, 2009).

5.2 First, second, and third party strategies

Convicting offenders is only one example of what Neal Kumar Katyal (2001) calls first-party strategies to combat cybercrime: those targeted at offenders. Katyal points out that many other strategies exist to raise perpetration costs, including those based on social norms and Internet architecture. Moreover, second-party strategies focusing on victim precaution can also reduce opportunities for crime; this includes not only awareness-raising or stimulating use of firewalls, but also changing our perceptions of victimhood when networks (rather than people) are being attacked or in light of the 'de minimis' (*supra*, section 2.3) problem of cybercrime. Finally, third-party strategies engage third parties, such as Internet Service Providers, financial service providers, software and hardware manufacturers, and other possible 'capable guardians' as an opportunity-reducing strategy.

Katyal's (2001) specific suggestions for implementing concrete countermeasures may not be particularly convincing; nor are some other measures proposed in the literature, such as the radical second-party strategy to impose criminal liability on computer users for negligent computer security (Brenner & Clarke, 2006). Indeed, second-party strategies should generally be used with great caution lest, as a side-effect, liability is shifted to consumers who have little

[1] See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG for the text and explanatory memorandum of the Convention, and a list of signatures and ratifications.

capacity to prevent falling victim to cybercrime anyway (Van der Meulen, 2010). Regardless of concrete proposals, however, Katyal's notion of first-, second-, and third-party strategies provides a useful conceptual tool for discussing and devising a broad, comprehensive array of opportunity-reducing measures. Particularly the use of digital architecture as a regulatory tool to combat cybercrime deserves more attention from governments than it does (Katyal, 2003), although there are also challenges and downsides to technical solutions that need to be factored into the equation (see, e.g., Reidenberg, 2003; Starr, 2004; Koops, 2008).

6 Conclusion

The Internet provides opportunities for committing crime through a combination of characteristics, many of which make the Internet what it is famous for: a massive, global, open network allowing for instant communications, that has transformed social and economic processes. Given its impact in the information age, it can also be expected to transform crime. A dozen risk factors are pointed out in the literature which create a unique opportunity structure for cybercrime: global reach, deterritorialisation, flexible network structure, anonymity, distant offender-victim interaction, manipulability of data, automation of crime, massive scale, aggregation of negligible damages, information as commodity, limitations to capable guardianship, and rapid innovation cycles.

Majid Yar (2005) has applied Routine Activity Theory to determine whether cybercrime is or is not qualitatively different from offline crime. He concludes that 'although some of the theory's core concepts can indeed be applied to cybercrime, there remain important differences between "virtual" and "terrestrial" worlds that limit the theory's usefulness. These differences, it is claimed, give qualified support to the suggestion that "cybercrime" does indeed represent the emergence of a new and distinctive form of crime' (Yar, 2005, p. 407). Even if cybercrime to some extent represents 'old wine in new bottles' (Grabosky, 2001), its scale and variety imply that 'we are dealing with *an awful lot of wine* in very many, differently shaped and capacious bottles' (Jewkes & Yar, 2010b, p. 3).

Although yet little is known empirically of cybercriminals and their organisation types and levels, theory and anecdotal evidence suggest that cybercrime is becoming organised, large-scale, diversified with increasing division of labour, and it is expected to develop increasing ties with offline organised crime. Moreover, although empirical knowledge of cybervictims is even more scarce, some studies suggest that offline and online victimisation show significant overlap, tentatively finding that in some contexts, offline behaviour is a risk factor for online victimisation, or that computer or Internet use may be a risk factor for offline victimisation.

These findings and suggestions, which need to be tested and developed in future research, provide good reason to integrate the Internet and cybercrime in mainstream criminological research as well as in general criminal law and policy. The Internet has become part and parcel of everyday life, and Internet use is routine activity today (at least for most people in developed countries). Criminology should therefore incorporate the Internet and cybercrime in its own routine activities, without, however, losing sight of the peculiarities of the Internet, the many differences between offline and online crime, and – despite the global character of the Internet – significant national differences in opportunity structures for specific cybercrimes (cf. Van der Meulen, 2010).

At the same time, the Internet's opportunity structure for (cyber)crime also challenges research and policy in the field of Internet governance. The future of the Internet is already fraught with challenges for multi-level and polycentric governance without seeing potential cybercriminals behind every IP address (Goldsmith & Wu, 2006; Zittrain, 2008), but Internet governance cannot afford to disregard the Internet's many opportunities for crime and the risks for victimisation. Criminologists and Internet scholars should join forces to attempt devising comprehensive approaches to regulating the Internet that reduce opportunities for crime while preserving as much as possible of its unique character.

Before such comprehensive approaches to Internet governance can even be considered, much more theoretical and empirical research will be required, however. As most scholars observe, we are just starting to research cybercrime. A good starting place is the agenda for research presented by Sandywell (2010, pp. 42-43), challenging us:

1. to theoretically describe the differences between pre-digital and digital crime;
2. to explain the continuities between analogue and digital crime;

3. to analyse (non-deterministically) the role of the Internet in transforming the global culture of crime;
4. to model emergent forms and characteristics of cybercrime;
5. to explain societal, cultural, and governmental responses to cybercrime and their consequences in different national and geographical contexts;
6. to investigate whether and how cybercrime affects new attitudes to security, surveillance, transnational regulation, and policing.

Bibliography

Balkin, J.M. & Kozlovski, N., 2007. Introduction. In: Balkin et al. eds., 2007. Cybercrime. Digital Cops in a Networked Environment. New York/London: New York UP, pp. 1-10.

Balkin, J.M. et al. eds., 2007. Cybercrime. Digital Cops in a Networked Environment. New York/London: New York UP.

Bekkers, R., Bongers, F., Segers, J. & Schellekens, M., 2005. Hoe fraudeurs de draad kwijtraken. Een juridisch perspectief op nieuwe fraudevormen bij mobiel betalen. Utrecht: Dialogic / Tilburg: TILT.

Brenner, S.W. & Clarke, L.L., 2006. Distributed Security: A New Model of Law Enforcement. John Marshall Journal of Computer & Information Law, 23, pp. 659ff.

Brenner, S.W., 2002. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. North Carolina Journal of Law & Technology, 4, pp. 1-50.

Brenner, S.W., 2007. The Council of Europe's Convention on Cybercrime. In: Balkin et al. eds., 2007, Cybercrime. Digital Cops in a Networked Environment. New York/London: New York UP, pp. 207-20.

Brenner, S.W., 2008. Fantasy Crime: The Role of Criminal Law in Virtual Worlds, in The Vanderbilt Journal of Entertainment and Technology Law, 11(1), pp. 1-97.

Brenner, S.W., 2009. Cyberthreats. The Emerging Fault Lines of the Nation State. Oxford: Oxford UP.

Clough, J., 2010. Principles of Cybercrime. Cambridge (UK): Cambridge UP.

Cross, Michael. 2008. Scene of the Cybercrime. 2nd ed. Syngress.

Cuijpers, C. & Van der Knaap, L., 2010. Cyberpaedophilia. In: M. Evans, ed. 2010. Encyclopaedia of Criminology. Nijmegen: WLP.

Denning, Dorothy E., 2001. Activism, hacktivism, and cyber terrorism: The internet as a tool for influencing foreign policy. In: J. Arquilla & D. Ronfeldt, eds. Networks and Netwar: The Future of Terror, Crime and Militancy. RAND.

European Commission, 2007. Towards a general policy on the fight against cyber crime. COM(2007) 267 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

Franks, M.A., 2010. The Banality of Cyber Discrimination, or, the Eternal Recurrence of September. Denver Law Review Online, 87, pp. 1-6.

FTC (Federal Trade Commission), 2010. Consumer Sentinel Network Data Book for January – December, 2009. Washington, D.C: FTC, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.

Furnell, S., 2010. Hackers, viruses and malicious software. In: Y. Jewkes & M. Yar, 2010. Handbook of Internet Crime. Cullompton: Willan Publishing, pp. 173-93.

Goldsmith, J. & Wu, T., 2006. Who Controls the Internet? Illusions of a Borderless World. New York (NY): Oxford UP.

Grabosky, P., 2001. Virtual Criminality: Old Wine in New Bottles?. Social & Legal Studies, 11, pp. 243-49.

Himanen, P., 2000. The Hacker Ethic and the Spirit of the Information Age. New York (NY): Random House.

Icove, D., Seger, K., & Von Storch, W., 1995. Computer Crime, A Crimefighter's Handbook. Sebastopol (CA): O'Reilly & Associates.

Jewkes, Y. & Yar, M., eds. 2010a. Handbook of Internet Crime. Cullompton: Willan Publishing.

Jewkes, Y. & Yar, M., 2010b. Introduction: the Internet, cybercrime, and the challenges of the 21st century. In: Y. Jewkes & M. Yar, 2010. Handbook of Internet Crime. Cullompton: Willan Publishing, pp. 1-8.

Katyal, Neal Kumar, 2001. Criminal Law in Cyberspace. University of Pennsylvania Law Review, 149, pp. 1003-1114.
Katyal, Neal Kumar, 2003. Digital Architecture as Crime Control. The Yale Law Journal, 112, pp. 2261-89.
Kerr, O., 2008. Criminal Law in Virtual Worlds. University of Chicago Legal Forum, pp. 415ff.
Koops, B.J. & Brenner, S.W., eds. 2006. Cybercrime and Jurisdiction: A Global Survey. The Hague: T.M.C. Asser Press.
Koops, B.J., 2008. Criteria for Normative Technology. An essay on the acceptability of "code as law" in light of democratic and constitutional values. In: R. Brownsword & K. Yeung, eds. 2008. Regulating Technologies. Oxford: Hart Publishing, pp. 157-174.
Kowalski, M., 2002. Cyber Crime: Issues, Data Sources and Feasibility of Collecting Police-Reported Statistics. Ottawa: Canadian Centre for Justice Statistics.
Lastowka, F.G. & Hunter, D., 2005. Virtual Crimes. New York Law School Law Review, 49, pp. 293-316.
Leukfeldt, R., 2010. The e-fraudster: a criminological perspective. MSc. Leicester: University of Leicester.
McCusker, R., 2006. Transnational organised cyber crime: distinguishing threat from reality. Crime Law and Social Change, 46, pp. 257-73.
Nissenbaum, H., 2004. Hackers and the Contested Ontology of Cyberspace. New Media & Society, 6, pp. 195-217.
Nykodym, N., Ariss, S. & Kurtz, K., 2008. Computer Addiction and Cyber Crime. Journal of Leadership, Accountability and Ethics, (Fall), pp. 78-85.
Nykodym, N., Taylor, R. & Vilela, J., 2005. Criminal profiling and insider cyber crime. Computer Law & Security Report, pp. 408-414.
Parker, D.B., 1973. Computer Abuse. Palo Alto.
Reidenberg, J., 2003. States and Internet Enforcement. University of Ottawa Law and Technology Journal, 1, pp. 213-230.
Rogers, M., 2006. A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation, (3), pp. 97-102.
Sandywell, B., 2010. On the globalisation of crime: the Internet and new criminality. In: Y. Jewkes & M. Yar. eds. 2010, Cullompton: Willan Publishing, pp. 38-66.
Shaw, E., Ruby, K.G. & Post, J.M., 1998. The Insider Threat to Information Systems. The Psychology of the Dangerous Insider. Security Awareness Bulletin, (2), http://www.pol-psych.com/sab.pdf.
Smith, R.G., Grabosky, P. & Urbas, G., 2004. Cyber Criminals on Trial. Cambridge (UK): Cambridge UP.
Starr, S., 2004. Can Technology Can Spam?. Spiked (May), pp. 1-5.
Sterling, B., 1994. The Hacker Crackdown. Law and Disorder on the Electronic Frontier. London: Penguin.
Stohl, M., 2007. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. Crime, Law and Social Change, 46, pp. 223-38.
Thomas, D. & Loader, B., 2000. Cybercrime in the information age. In: D. Thomas and B. Loader, eds. 2000. Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Routledge, pp. 6-7.
Van der Hulst, R.C. & Neve, R.J.M., 2008. High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie. The Hague: WODC.
Van der Meulen, N., 2010. Fertile Grounds. The Facilitation of Financial Identity Theft in the United States and the Netherlands. (in press)
Van Dijk, J., Van Kesteren, J. & Smit, P., 2007. Criminal Victimisation in International Perspective. Key findings from the, 2004-2005 ICVS and EU ICS. The Hague: WODC / Meppel: Boom Juridische uitgevers.
Walden, I., 2007. Computer Crimes and Digital Investigations. Oxford: Oxford UP.
Wall, David S., 2007. Cybercrime. The Transformation of Crime in the Information Age. Cambridge (UK): Polity Press.
Wall, David S., 2008a. Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. International Review of Law, Computers and Technology, 22(1-2), pp. 45-63.

Wall, David S., 2008b. Cybercrime and the Culture of Fear: Social Science fiction and the production of knowledge about cybercrime. Information Communication and Society, 11(6).
Yar, M., 2005, The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2, pp. 407-27.
Zittrain, J., 2008. The Future of the Internet. And How to Stop It. New Haven & London: Yale UP.