In addition to 'computer assisted' crimes we have those which are 'computer oriented'. This category of offence takes as its target the electronic infrastructure (both hardware and software) that comprises the 'fabric' of the Internet itself. Examples include various forms of 'malicious software' (viruses, worms, Trojans) that corrupt files and hard drives; 'denial of service attacks' that overload server capacity and effectively 'crash' websites; and various forms of 'defacement' through which web content is manipulated, changed and/or deleted without permission or authorization. Again, to take the example of China, it was the emergence of a hitherto unknown phenomenon, a computer virus in the form of a malware program known as 'Ping Pong' that first drew cybercrime to the attention of the Chinese public. According to a Symantec report at the end of 2006, Beijing is now home to the world's largest collection of malware-infected computers (nearly 5 per cent of the world's total) and research by the security company Sophos showed that China has overtaken the US in hosting Web pages that secretly install malicious programs on computers to steal private information or send spam e-mails (http://www.msnbc.msn.com/id/19789995/).

Cyber-warfare and cyber-terrorism

The decision by Google to pull out of China is said to have followed a cyber-attack it believes was aimed at gathering information on Chinese human rights activists. Most recently attention has been directed, in the post-September 11 context of the 'War on Terror', toward the possibility of attacks upon computer infrastructure by terrorist groups (so-called '*cyber-terrorism*'). For example, Dorothy Denning (2010) has outlined six areas of terrorist practice that have been substantially altered or enhanced by the Internet and the Web: media operations, attacks, recruitment, learning, finance, and security. However, while most commentators have focused on the specific threats from named terrorist cells and networks such as al Qaeda, state-authorized and government-sponsored attacks also appear to be on the rise and, again, China has suddenly appeared alongside nations that are more usually identified as posing a threat. *The Military Balance 2010* is an annual study published by the International Institute for Strategic Studies (IISS) and is an assessment of global military capabilities which now includes analysis of cyber-terrorism and *cyber-warfare* (http://www.iiss.org/publications/military-balance/). A news report about *The Military Balance* illustrates the complexity of understanding where the battle lines are drawn in a cyber-society:

> In December the South Korean government reported an attack in which it said North Korean hackers may have stolen secret defence plans outlining the South Korean and US strategy in the event of war on the Korean peninsula. Last July,

> espionage protection agents in Germany said the country faced extremely sophisticated Chinese and Russian internet spying operations targeting industrial secrets and critical infrastructure such as Germany's power grid.
>
> One of the most notorious cyber-warfare offensives to date took place in Estonia in 2007 when more than 1 million computers were used to jam government, business and media websites. The attacks, widely believed to have originated in Russia, coincided with a period of heightened bilateral political tension. They inflicted damage estimated in the tens of millions of euros. China last week accused the Obama administration of waging 'online warfare' against Iran by recruiting a 'hacker brigade' and manipulating social media such as Twitter and YouTube to stir up anti-government agitation. (www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat)

According to IISS terrorism and warfare in ***cyberspace*** may be used to disable a country's infrastructure, meddle with the integrity of another country's internal military data, confuse its financial transactions or to accomplish any number of other possibly crippling aims (ibid.). In June 2009 the Pentagon created US Cyber Command and in Britain it was announced that a cyber-security operations centre would be established at GCHQ in Cheltenham. Yet governments and national defence establishments at present have only limited ability to tell when they were under attack, by whom, and how they might respond (ibid.).

While these measures might give cause for alarm and seem to be in response to threats that might come from a Hollywood movie (almost certainly starring Bruce Willis) we should not overstate the threat of cybercrime, cyber-terrorism or cyber-warfare. Further, it has not been my intention here to paint China as a particular problem; rather, it has been presented as a fascinating case study illustrating the speed and scope of Internet penetration and the consequent shifts in local and global power that occur. However, we must retain a healthy scepticism about claims made in the West regarding the threats posed by rapidly developing nations such as China. Put bluntly, media commentators, politicians, criminal justice actors and security professionals in countries like the UK and US may have strong vested interests in overplaying the risks presented. As Majid Yar (2010) has intimated, much of the debate about Internet regulation and censorship appears to be based on speculative notions of the anti-social and harmful impacts it may have at some point in the future rather than actual, current levels of victimization. Some of the concern expressed by authorities in the West about China as a source of cybercrime, cyber-terror and cyber-warfare therefore might reasonably be said to emanate from economic and political fears about Chinese growth and dominance in arenas and markets that other countries (particularly the US) have owned for many decades. Maggie Wykes (with Daniel Harcus, 2010) concurs, and suggests that the media has been instrumental in heightening public fears about the possibility of terrorist attack. It is her view that since

9/11 the media have consistently reported that terrorist groups use Internet technologies to organize and plan both terrestrial and cyber-attacks, and that these accounts have supported the concept of an ever-present global threat and underwritten policy from the US and its allies regarding the 'War on Terror'. Wykes suggests that the meaning of terrorism in the 21st century has been reconstructed and allied to the Internet through hyper-realistic criminalizing practices and fear-inducing discourses which have legitimated policies, alliances, laws, actions and – as we saw in Chapter 8 – invasive surveillance methods, with profound implications for netizens, citizens and the exercise of power (Wykes with Harcus, 2010).

Although global acts of cyber-facilitated warfare and terrorism are certainly possible, and their consequences terrifying to contemplate, it is the more mundane, 'ordinary' cybercrimes that affect millions of people worldwide that are of most concern to most of us, so let us take a brief overview of some of the offences that come under the heading of 'cybercrime'.

'Ordinary' cybercrimes

Electronic theft and abuse of intellectual property rights

One of the most obvious consequences of the new information and communications revolution is its creation and distribution of unimaginably more information-based products which force us to re-evaluate traditionally held ideas about crime and criminality. For example, theft has commonly involved one person taking something belonging to another person without his or her permission – the result being that the first party no longer has possession of the property taken. Investigation of this type of offence is usually relatively straightforward in so far as it involves property that is tangible, visible and atom based (Goodman, 1997). But in a virtual context, it is quite possible for one person to take something that belongs to another person without permission and, in some cases, make a perfect copy of the item, the result being that the original owner still has the property even though the thief now has a version as well. Intellectual property can take a number of recognized forms – patents, trademarks, trade secrets, industrial designs and copyright. Such acts challenge conventional and legal definitions of offences and render traditional copyright laws irrelevant (Wall and Yar, 2010).

Electronic reproduction of data can take many forms. One of the most common is 'peer-to-peer' (or P2P) file-sharing, which has arguably returned to the Internet a sense of the liberal, collective ethos and benign anarchy that characterized its early days in the 1960s and 1970s. But for the film and music

industries who are losing millions of dollars in lost sales, this form of 'digital piracy' taking place in teenagers' bedrooms the world over is every bit as unlawful as the knowing and criminal use of the Internet to market or distribute copyrighted software (Yar, 2006). Moreover, it is not just young people who believe that it is morally acceptable to illegally download movies, music and software: in the US a survey found that only 26 per cent of professionals oppose piracy (Yar, 2010). The industry has been slow to respond to the problem of file-sharing, and broadband technology has made it even quicker and easier to download music and movies illegally. However, some CDs are now being manufactured in such a way as to make it impossible to play them (and copy them) on a PC. Meanwhile, the Record Industry Association of America (RIAA) is taking legal action against individuals it alleges offer file-swapping services on university campuses, and the Movie Picture Association of America is attempting to close down sites that distribute films online. But many believe that big corporations are being forced into playing cat-and-mouse games they can't possibly hope to win because – as the RIAA's infamous closure of Napster demonstrated – when the illegal business of one outfit is terminated, numerous others will appear in its wake. Most recently, legal controversy has arisen around the Sweden-based website 'Pirate Bay', which directs searchers to media files available across the Internet, but does not store or offer any content itself, as a way of circumventing anti-piracy laws. While copyright-holders claim it is a major source for piracy, its operators claim they are acting within the law, and the case remains ongoing.

Hate crime

Hate crime may be racist, religiously motivated, homophobic, gendered, disablist (Chakraborti and Garland, 2009) or, as we shall see, simply a violent reaction to a particular offender who has been in the news. The promotion of hatred is widespread and the Internet is a relatively cheap and accessible means of connecting similarly minded people across the world and coalescing their belief systems. The Net is also a sophisticated tool for recruitment and unification, providing links between hate movements that were previously diverse and fractured, and facilitating the creation of a collective identity and empowering sense of community (Perry, 2001). In fact, while the potential of the Internet as a weapon of warfare has already been discussed, it must also be remembered that the Internet has increased the global reach of terrorist groups, such as al Qaeda, who can use computer and telecommunication links, email, cellular and radio networks to conduct operations over long distances while dispensing with the need for fixed physical presence. Coleman and McCahill (2010) note that a former radical Muslim claimed that more than half of young Saudis who had embraced a radical ideology were recruited through the Internet. In Europe

various groups on the political far right – neo-Nazis, skinheads and groups with ties to the Ku Klux Klan – use the Net to target a youthful and impressionable audience with racist, anti-semitic and homophobic propaganda with little fear of the kind of legal sanction that might accompany the circulation of such material in more 'traditional' forms. Although Germany and many other European countries have criminalized the publication and distribution of hate propaganda, the Internet remains largely unregulated and there is little the police can do unless a specific crime is reported. Moreover, the constitutional protection afforded to 'free speech' in the USA makes it difficult to challenge the global dissemination of messages of hate.

Although often targeted at broad demographic groups, religions and so on, hate crime is increasingly taking the form of vigilantism against individuals. Two examples from recent years demonstrate how unregulatable the Internet can be and how linked technologies can create 'viral' chains of communication in a very short space of time. In November 2008 the case of 'Baby P' or 'Baby Peter', a two-year-old tortured and killed by his mother's boyfriend, shocked the British public. Breaching two separate legal orders, several Internet sites revealed the child's identity and posted photographs of his mother and stepfather along with their names, address, and other personal details. Several social networking sites had to take swift action to remove pages with the mother's profile on after online vigilantes began a campaign calling for violent retribution against them, and the court trial itself had to be postponed for several months (with the cause of the delay being cited as 'legal reasons'). In March 2010, following the recall to prison of Jon Venables on suspected child pornography offences, an entirely different individual, David Calvert, was mistakenly identified as the man who, as a child, had murdered James Bulger. Within a few days more than 2,370 people had joined a group on the site asking whether Calvert was in fact Venables (this despite the fact that Venables was in prison and Calvert was at home). The group was removed after complaints to Facebook, but the rumours persist on other sites such as Yahoo Answers, with people claiming to have learned his identity via text messages. Calvert is said to have endured a torrent of abuse and had to produce family photo albums to prove his identity to doubters. So severe was the reaction against him by some parts of the community that a panic button was installed at his home (*Guardian*, 9 March 2010).

It was in fact Jon Venables and his co-accused Robert Thompson who led to a change in the law governing blame attributable to Internet Service Providers (ISPs). In July 2001 ISP Demon won a change to the injunction protecting the two boys when they were released from custody and given new identities. The original form of the injunction, designed to prevent the mainstream media from publishing or broadcasting details of the offenders or their whereabouts, was deemed 'inappropriate' for the Internet because of the risks of a service provider inadvertently providing access to material about the pair

and consequently being found in contempt of court. ISPs are now compelled to take all reasonable measures to prevent this from happening. A similar order was imposed on behalf of Maxine Carr following her release from prison in 2005 (the first time a lifetime injunction to protect identity has been awarded to someone not convicted of murder). Her QC made the case for his client's anonymity on the basis of serious threats and allegations made in Internet chat rooms and their linking to unfounded press reports about her (*Guardian*, 25 February 2005).

More legally ambiguous are 'hate' behaviours that might be termed 'cyber-bullying' or 'trolling'. As we shall see later in this chapter, some bullying among children and young people is linked to sexual behaviour but, much like traditional bullying it may range from name-calling to serious threats of assault and blackmail. Like its 'real-life' equivalent, cyber-bullying behaviours may be covered by legislation (such as the 1997 Harassment Act) but much of it consists of low-level abuse, gossip and rumour which, while potentially very upsetting to the recipient, is not usually a criminal offence. 'Trolling' on the other hand is usually associated with more serious behaviour. Formerly known as 'flaming', trolling has become associated with the worst displays of hatred, misogyny, racism and homophobia, usually on public Internet forums and has, in several cases, resulted in the victim taking their own life. Trolls can be prosecuted in the UK under the Malicious Communications Act, introduced in 1988 and updated in 2003 to make it an offence to make improper use of a public electronic communications network such as grossly offensive, indecent, obscene, menacing or annoying phone calls and emails. There have been numerous reported cases involving celebrity victims; for example, a young man who used Twitter to send Olympic diver Tom Daley offensive tweets during the London 2012 Games was arrested and issued a formal harassment warning. Several offenders have been sentenced to prison sentences for trolling.

Invasion of privacy, defamation and identity theft

The entitlement to security of person is regarded as a fundamental human right, yet the scope and pervasiveness of digital technologies open up new areas of social vulnerability. Invasion of privacy takes many forms from 'spamming' to online defamation, stalking and violence. Spamming has thus far been considered little more than an extension of conventional junk mail, although it is increasingly being recognized as an insidious and frequently illegal activity. It can encompass electronic chain letters, links to pornographic sites, scams claiming that there are extensive funds – for example, from over-invoiced business contracts or a deceased relative's will – available for immediate transfer into the target's bank account, fraudulent pyramid investment schemes, phoney cancer cures and bogus test kits for anthrax.