1 The digital revolution and criminal law: backgrounds

This first introductory chapter comprises some background sketches for the chapters that follow. The internet is centre stage in this book. For this reason, this chapter begins with a brief outline of its origins, first along traditional lines (Section 1.1) and then from a sociological perspective (Section 1.2). This is followed by a general legal-sociological introduction to the subject of 'criminal justice on the internet' based on the notion of social control (Section 1.3). This chapter goes on to outline some general changes in crime that may (possibly) coincide with the digital revolution as an introduction to the various types of cybercrime that are discussed further on in this book (Section 1.4). Finally, this chapter outlines a few broader social trends as a social backdrop to the theme of this book (Section 1.5). Definitions of the concepts are dealt with in Chapter 2.

1.1 The internet: a short history of its origins (1962-2000)

Today's internet is a worldwide network of connected computers that originated in the 1960s during the Cold War. In 1957, the Soviet Union successfully launched its Sputnik satellite into an orbit around the earth. The United States was shocked into action by this technological achievement and in 1958 it founded the Advanced Research Project Agency (ARPA)[1] with the objective of 'keeping the United States out front when it comes to cultivating breakthrough technologies for national security rather than in a position of catching up to strategically important innovations and achievements of others'.[2] In 1962, Joseph Licklider, a psychologist and computer scientist working at ARPA, presented a dream about worldwide social interaction via a galactic network. In the years that fol-

1 These days ARPA is called 'Defense Advanced Research Projects Agency' (DARPA; www.darpa.mil).

2 Retrieved 30 March 2017 from www.darpa.mil.

lowed, American technicians collaborated on the linking of computers, with ARPA in the leading role.

Although this linking of computers served a military purpose, the developers claimed that they primarily had scientific objectives in mind (Cohen-Almagor, 2011). By the end of 1969, they had linked four[3] computers in a network via lines that they had leased from a telecoms company. This so-called ARPANET is universally considered to be the primaeval version of our modern-day internet (Leiner et al., 2009; Glowniak, 1998; Cohen-Almagor, 2011; Van Eekelen & Vranken, 2012). The first e-mail application was installed on the ARPANET in 1972, and in 1973 the first personal messages were sent over the net (Leiner et al., 2009; Cohen-Almagor, 2011).

ARPANET's technical design catered for efficient and secure exchange of information and ensured that the internet stayed up even if part of it goes down. The internet does not have a vulnerable central point in its hierarchy of computers. Instead it is a horizontal network of routes along which data traffic in principle always finds its way. Technical measures safeguard the efficient use of the network's capacity and ensure that messages are transmitted without any corruption.[4] Another important principle of ARPANET is its 'open architecture', which means that the technical specifications are open to everyone. Because of this, designers of other systems can interface and link up with it. ARPANET is not one system run by one software program; instead it is an infrastructure that is accessible to a wide range of programs – those that still had to be developed. Key here is an open dialogue in which information is freely shared with a view to developing new technology together. A limitation of the ARPANET when it was first created, however, was that – outside the military – it was only accessible to a group of scientists (Leiner et al., 2009; Glowniak, 1998; Cohen-Almagor, 2011).

The ARPANET was not only expanded because more computers were connected to the network, but especially because other computer *networks* were being developed and connected to ARPANET, such as the British Joint Academic Network (JANET) in 1984 and the American National Science Foundation Network (NSFNET) in 1985 (Leiner et al., 2009; Glowniak, 1998). From the very beginning, these two networks from the academic world considered all scientists

3 These four connected computers are located in Los Angeles, Santa Barbara (both at the University of California), Menlo Park (Stanford Research Institute) and Utah (University of Utah).

4 Van Eekelen and Vranken (2012) give an explanation of technical aspects that relate to the efficiency and robustness of data communication on the internet, such as packet switching, routing and TCP/IP.

to be their target audience. A few years later, NSFNET also started targeting the corporate sector. So ARPANET ceased to be *the* network; instead it was part of the larger whole consisting of several interlinked networks called 'the internet' (a contraction of 'interconnected networks'). The academic National Science Foundation (NSF) took over ARPA's pioneering role.

In the eighties and nineties, the internet grew from having 213 connected computers in 1981 to 2.2 million in 1994 (Leiner et al., 2009; Glowniak, 1998). The original ARPANET was dismantled in 1990, and ARPA handed its management responsibilities over to NSF. Those days the internet was already running on the basis of a larger set of computer networks and widely accepted communication protocols[5] (Leiner et al., 2009). From 1988 onwards, more and more countries hooked up their top-level domains (TLDs)[6] to NSFNET (Cohen-Almagor, 2011).[7] The National Research Institute for Mathematics and Computer Science in the Netherlands (CWI) was the first to produce an internet connection in Europe on 17 November 1988.[8] Other countries soon followed suit. The internet expanded, not only in terms of its size but also in terms of new applications. As an example, Philip Zimmerman made his free encryption software Pretty Good Privacy (PGP) available online in 1991 (Cohen-Almagor, 2011).

This rapid expansion brought problems in its wake. The internet backbone (the internet's principle data routes along main connections) was having to process more and more data traffic and so the backbone's telecommunication lines needed an ever-increasing capacity. Organisational issues also raised their heads. The management and consultation structures surrounding the new internet steadily become more complex (Leiner et al., 2009). In 1991, some internet pioneers launched the international non-profit Internet Society (ISOC) to support forums involved in the evolution of the internet (Cerf, Kahn & Chapin, 1992; Cohen-Almagor, 2011).[9]

5 From 1974 onwards, the transmission control protocol (TCP) and the internet protocol (IP), in particular, set the stage for standardisation for setting up connections and for data exchange (Cohen-Almagor, 2011).

6 TLDs are names that divide the internet domain at the highest level. Besides domain names for countries (such as '.nl'), there are also TLDs for various social functions, like .gov, .com, and so on. The Internet Corporation for Assigned Names and Numbers (ICANN) manages domain names.

7 Leiner et al. base their work on www.zakon.org/robert/internet/timeline/ (Retrieved 30 March 2017).

8 Retrieved 30 March 2017 from www.cwi.nl/nieuws/2013/cwi-viert-25-jaar-open-internet-in-europa-in-november.

9 These days, its mission is 'to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world'. (Retrieved 30 March 2017 from www.internetsociety.org).

A breakthrough came in the nineties when internet service providers (ISPs) began offering private individuals internet access via modems and fixed landlines. In the Netherlands, 1993 is generally considered to be the year in which ISPs were in a position to connect private individuals to the internet.[10] That said, the Hobby Computer Club website claims that its members went online in 1991.[11]

The number of connected computers rose from around 2.2 million in 1994 to virtually 30 million in 1998 (Glowniak, 1998). In 1989, Tim Berners-Lee designed the principle of the *world wide web* using web pages based on HTTP and HTML technology. He also produced the *WorldWideWeb* web browser, but it was not a success. The popular web browser, Mosaic, was launched in 1993. It ran until 1997. Then in 1994 the Netscape web browser (1994-2008) and in 1995 the Internet Explorer (1995 to date) followed. In that same period, shops appeared on the internet and First Virtual was the first cyberbank with an online payment system. Yahoo! entered the scene in 1994 and Google followed in 1996. NSF privatised its management tasks in 1995 and shut down NSFNET. With that, the backbone was effectively transferred into private hands (Cohen-Almagor, 2011).

By the end of the nineties, the backbone in the United States consisted of networks that were the property of telecoms companies. The networks are interconnected to interfaces where data traffic goes from one network to another, thus creating a single entity. These telecoms companies are effectively *network* service providers (NSPs). Some smaller NSPs lease network capacity from the larger ones. The *internet* service providers (ISPs) provide network connectivity between a network and an NSP in a limited geographic area (*local* area network (LAN)). Small ISPs can connect their LAN to a large ISP, which in turn connects to an NSP. This expansion of the network places the management responsibilities with various parties at various levels (Glowniak, 1998). So, unlike it was in the beginning with ARPA and NSF, it is no longer the case that one party has control of the entire network. The ultimate responsibility for the issuance of domain names and IP addresses,[12] however, was put into the hands of one organisation. The Internet Corporation for Assigned Names and Numbers (ICANN) was established for that purpose in 1998 (Cohen-Almagor, 2011; www.icann.org).

10 For instance: 'The American government opened the internet to businesses and private individuals in 1993. Until that time, it had been reserved for the government and education.' (Retrieved 15 November 2013 from http://nl.wikipedia.org/wiki/Internet).

11 Retrieved 17 December 2014 from http://groepen.hcc.nl/nieuws/hcc-nieuws/1120-hcchob-bynet-is-de-eerste-nederlandse-ispvoor-prive-gebruik.html. Retrieved 30 March 2017 from https://nl.wikipedia.org/wiki/Geschiedenis_van_het_internet_in_Nederland.

12 IP stands for internet protocol. Every device that is connected to the internet has a fixed or temporary IP address.

By the end of the nineties, there was indeed a 'worldwide network' but it was not distributed evenly across the planet. For instance, by 1998 there were about 150 million internet users in more than 60 countries, but nearly 90% of that population lives in 15 highly industrialised countries, the United States taking the lead. 'In 2000, the USA produced almost two-thirds of the top thousand most visited websites. It accounted for 83% of the total page views of Netusers. Less than 10% of the world speaks English as their first language (...). In the late 1990s, an estimated 85% of the web was written in English (Curran & Seaton, 2009)' (Cohen-Almagor, 2011, p. 56). While the gap between rich and poor countries expressed in the percentage of inhabitants with internet access did start to close after 2000, it is still significant (Cohen-Almagor, 2011). This is not entirely as it should be from the perspective of equality. But at the same time, it is clear that the ARPA initiative, as intended, has certainly led to technological advantages, particularly in highly industrialised countries.

That concludes this brief history of the internet up until 2000. The other chapters discuss specific recent developments and internet applications, for instance, the development of criminal legislation for cybercrime is discussed in Chapter 3, and the police and the internet in Chapter 5. Regarding more recent developments, suffice it to say that the Netherlands is one of the countries with high internet density. 'The Netherlands has been at the top of the European ranking for many years with the largest proportion of households that have access to the internet.'[13] In 2016, 94% of the population in the Netherlands aged 12 years or older had access to the internet, and 93% had a broadband connection. Statistics Netherlands research on ICT usage among people aged 12 to 75 shows that internet usage is age related. In 2016, 99% of 12 to 25-year-olds had access to the internet; that percentage is 78 for those aged 65 or older (statline.cbs.nl). The turnover from online shopping in the Netherlands amounted to 20.1 billion euro in 2016.[14] According to a press release, the AMS-IX in Amsterdam is the largest internet exchange in the world (Box 1.1)[15]

13 Retrieved 30 March 2017 from www.cbs.nl/nl-NL/menu/themas/bedrijven/publicaties/digitale-economie/artikelen/2012-3636-wm.htm.

14 Retrieved 30 March 2017 from www.thuiswinkel.org.

15 AMS-IX stands for Amsterdam internet exchange (AMS is also the abbreviation for Amsterdam in international air traffic).

Box 1.1 The *AMS-IX*

'A greyish warehouse on a typical Dutch industrial site. (...) There is nothing special about it on the outside, but Amsterdam is a busy traffic plaza in a worldwide web of data connections. Several transatlantic submarine cables come ashore in the Netherlands and then make their way to the capital. Each second, vast quantities of information flow through data cabinets located in South-East Amsterdam and in Sloterdijk. Together they constitute AMS-IX, the largest internet exchange on the planet.

Hundreds of internet companies, such as internet service providers and Google, Facebook and Twitter, too, connect with each other via this platform in Amsterdam. (...) The value is huge. According to Deloitte, Amsterdam as an internet city put more economic weight in scale in 2014 than the Port of Rotterdam or Schiphol Airport. And that is mainly down to the size and growth of AMS-IX. Last year the exchange grew by 30 per cent.'

Source: De Volkskrant, 7 February 2015, p. 4

The internet is evolving rapidly, not only in terms of software programs and applications that users come up with, but the penetration rate is also still increasing. The internet was initially linked to traditional computers, i.e. devices with a calculation capacity and a monitor plus keyboard intended to run a range of programs. At the moment, the internet is rapidly becoming mobile through small, mobile computers like smartphones and tablets and through built-in internet screens that come standard in vehicle dashboards. The internet is increasingly connecting devices that no are longer like computers in the traditional sense of the word, but are made for a specific purpose, for instance, industrial devices that can be remotely controlled via the internet, measuring devices that transmit signals via the internet, or domestic appliances that people can switch on or off via the internet. These kinds of applications are referred to as 'the internet of things' (IoT). The term 'the internet of everything' (IoE) has since emerged, too. It refers to a world in which every object and every person is connected to the internet.

This development began with connecting a few computers and thereby creating a computer communications network. Slowly but surely it has evolved into something more all-encompassing. It is no longer the case that there is a

computer network out there 'somewhere'; instead there are digital devices all around us that are connected to a worldwide computer network, and thus with one another. 'Computerised devices and systems' (Section 2.1) have increasingly become a factor in daily life in more and more places and in various ways. We call this development the 'digitisation of society'.

1.2 The internet explained from a sociological perspective[16]

Section 1.1 outlines the origins of the internet along relatively traditional lines: the Cold War, ARPANET as the answer to Sputnik, and the expansion of the internet. But another approach is possible: a sociological explanation for the emergence of the web. Of all the conceivable options, why exactly was a galactic network deemed to be the answer to Sputnik? Why did the network grow so rapidly, and why was the internet not restricted to military use?

For almost a lifetime, we as people thought that we had pretty much mapped the entire world. After we finally managed to reach the North Pole, after many failed attempts, and then the South Pole at the start of the twentieth century, it did not seem like there was that much undiscovered terrain left on earth, at most maybe some secluded places in the vast primaeval forests of the southern hemisphere, or perhaps one or two deep troughs in the ocean, but there were no Major Missions left, no unknown worlds that captured everyone's imagination. Prior to the discovery of the North Pole, emotional as well as scientific discussions raged about what its wastelands would be harbouring. An open polar sea? A route to the centre of the earth where new populations sat waiting to be discovered? It eventually turned out to be a desolate icy expanse without any land (Fleming, 2001).

The Norwegian Roald Amundsen claimed the last major trophy: the South Pole. Explorers looking to discover new worlds lurking behind known horizons had to turn more and more to the space between the planets and the stars in their quest for new discoveries. People had to travel further and look closer to discover new worlds. It was an endeavour reserved for a very small elite: a few predominantly Western scientists using prohibitively expensive equipment and a handful of astronauts. Mankind as a whole sat physically and spiritually captured, as it were, within the boundaries of the world around it. But behold, because of this predicament, through its urge to expand and its creativity, *homo technologicus* created a new world within the existing space: cyberspace. Once

16 This section is an adaptation of an earlier work (Stol, 2010).

again there was light and space, space to see opportunities, space to follow new paths, space for hope and optimism, space for inspiration and discoveries, space for creativity, entrepreneurship and freedom. Space, not only for a few scientists, but for many. As an example, here is a quote about new developments in Kenya:

> 'As opposed to the older hippo generation, that still complains about colonialism and imperialism, the cheetahs are taking charge. They are connected to the web, are joining online networks and are urging others to join in. (...) The internet has given them the key to drag Africa out of the gutter. Or, as Tonee Ndungu puts it, "We lived on a glimmer of hope. Finally, finally we can reach it and grasp it." Ndungu, too, is a real cheetah.'[17]

This brief analysis of society fits into the tradition of optimistic social scientists, of which American Lewis Mumford is an important exponent. In his *Technics and civilization* (1934), Mumford argues that it is not so much technology that determines the course of history, but rather the mental development of humans or, if one prefers: culture. It is not the serendipitous technological inventions of ingenious or mentally disturbed engineers that determine the course of history, according to Mumford, instead it is the mental state in which a society exists that determines which technologies this society produces. In this analysis of society, it is no accident that the internet arose in a period when people had had no prospect of pioneering in new areas for decades – the fact that most people do not in fact wander the earth does not detract from this. It is about the absence of prospects, the lack of space to explore.

Global cyberspace is not necessarily due solely to a couple of technicians hooking up a few computers. That explanation is too simple. Cyberspace is the result of the fact that humankind found itself in a state of mental imprisonment in its everyday environment due to the lack of space to explore. Cyberspace was the answer to the lack of opportunities to pioneer and find new paths. Cyberspace was the new world to be discovered and conquered – the new frontier. It is no coincidence that the terms 'cyberspace' and 'Wild West' are often heard in conjunction. The first search results that Google produces after entering both terms is entitled 'Why the Internet is Like the Wild West'.[18] The sociological perspective (the exploring man) is better at explaining why there is tension between the internet and law enforcement than a rational-technological point of view (how engineers built a network) is. After all, the exploring man seeks

17 De Volkskrant, 25 March 2010.

18 The search key "internet" AND "wild west" elicited 814,000 search results on Google (30 March 2017).

space and freedom for creativity, and that does not always equate to uniform rules of conduct and enforcing these rules.

1.3 Social control on the internet[19]

1.3.1 Social control: three points of view

Criminal justice requires the regulation of behaviour. There are several mechanisms for regulating behaviour, such as physical containment (e.g. fences, thresholds, internet filters), chemical control (e.g. medicines), psychotherapy (e.g. cognitive behavioural therapy) and social control (e.g. education, upbringing, supervision, reward, and punishment).[20] This section deals with social control as a mechanism for regulating behaviour in cyberspace.

Social control is when people use sanctions (positive or negative)[21] to keep or bring the conduct of others in line with the standards advocated within the group (Stol, 1996). The focus on a *group* standard is what distinguishes social control from pursuing personal goals. The existence of a standard or generally applicable rule of conduct is what distinguishes social control from arbitrary behavioural influence.

There are two basic types of social control. Informal social control is given shape and substance through the everyday activities of normal people in their everyday environment. In this setting, people are not actively occupied with social control; instead they bring up their children, take care of one another, keep an eye on one another, gossip about one another, respect and correct one another, all as a matter of course. Formal social control is exercised by people whose special task is to exercise this control based on rules and regulations, including through criminal justice proceedings. This control is mandatory as it were, and those with this controlling function, the mandate holders, mainly act on behalf of others. Police work is a prime example of formal social control (Cachet, 1990; Stol, 1996). Law and order in our society are basically effected by informal social control and thus the population's everyday activities. If they have problems that they cannot solve, they can appeal to persons who exercise

19 Parts of this section are based on earlier works (Stol, 1996, Section 1.3; Stol, 2010).

20 A slightly different perspective is regulating conduct through system designers to ensure that safe systems are designed ('security by design'). We will not go into that aspect here.

21 Positive sanctions are those in which the other person's conduct elicits an affirmative response (appreciation, reward); negative sanctions are those involving an opposite response (disapproval, punishment).

social control as a special task, such as police officers. It is not possible to draw a clear line between formal and informal social control; rather, it concerns what Weber calls 'pure ideal types' (1922, p. 10), i.e. hypothetical constructs that do not occur as such in social reality, but which help when it comes to studying reality.

In line with the two basic types of social control, in 2000 Atchison observed two control systems on the internet: an informal system in which internet users monitor one another, and a formal system of government control. 'Informal control on the Internet operates at the individual and/or group and the organizational level. At the individual level, the most effective control is through self-regulation. If this does not work, netizens have devised a series of direct and indirect informal mechanisms to prevent future violations of netiquette. (...) Formal systems of control rely on the use of legal sanctions and government bodies to assure compliance' (2000, p. 94). Perhaps it was possible to describe social reality in cyberspace in this way in 2000, but such a dichotomy does not adequately reflect the situation as it stands now. It is as though an intermediate level has emerged between formal and informal social control.

For instance, De Pauw (2010) recognises three types of social control in the world of online games: informal, semi-informal and formal social control. The intermediate level between formal and informal control consists of the control that the owner of a game, a virtual community or a sector (for instance, the video game industry) exercises by a moderator or monitoring department which may, for instance, set rules and respond to complaints. This semi-informal control is a kind of supervision that members of a community or sector have organised among themselves. Like De Pauw, Wall (2008) also recognises a level of control between formal and informal. He talks about a stratum of security managers and he seems to assign them more of a unique, individual character than De Pauw does. 'Internet users and user groups, for example, maintain online behaviour through the application of moral censure. Virtual environment security managers are collectively emerging as *a new strata [sic] of behaviour governors*. They "police" the behaviour of the online community according to its particular norms and can apply a range of sanctions from censure, to temporary or permanent withdrawal of access rights.' (Wall, 2008, pp. 57-58, emphasis added).

Rather than basing the argument on the dichotomy mentioned earlier, it would be better to study social control from three perspectives: (1) social control by the public in their everyday environment (informal social control); (2) social control by the public who are organised based on ideological or commercial intentions (interest groups, companies); and (3) social control by the government

with the police in a special position because of their investigative duties and powers (formal social control). In their contribution on social control on the internet, Huey, Nhan and Broll (2012) mention the same players, even though they group them slightly differently. 'These groups of actors are loosely categorized as: government (including federal, state/territorial/county and local bodies and their delegates); law enforcement (the patchwork of international, national, state/territorial and local policing agencies); private industry (encompassing the variety of private enterprises) and the general public (referring to everyday citizens, either as individuals or as members of online groups).' The police and formal social control are discussed in greater detail in Chapter 5. Below we will look at the first two points of view as a general background to that chapter.

1.3.2 Informal social control on the internet

Throughout society there are everyday rules of behaviour and informal social control, and the same applies to cyberspace. To start with, presumably when you go online you feel that you have to behave properly. You do not go berserk the minute you enter cyberspace. What stops you? It is those internalised norms from your upbringing and schooling that you take into account in cyberspace, and which you abide by as a matter of course. In this regard, the German sociologist Elias (1939) talks about 'self-monitoring'. The French philosopher Foucault (1975) talks about 'self-constraint'. The American criminologists, Gottfredson and Hirschi (1990), mention 'self-control'. These are various perspectives of the same phenomenon: self-regulation. More on the subject in Section 1.3.5.

When you enter a new environment, like cyberspace or a particular community within cyberspace, it is always a matter of getting a feel for what the applicable rules are. To simplify this, codes of conduct are often deliberately laid down, for instance, in a 'netiquette', a security page or a list of *frequently asked questions* (FAQ). In the online game, Habbo, for instance, the general terms and conditions stipulate that violations of privacy, posting insulting texts, spreading viruses and using fake identities is not permitted.[22] But even when codes of conduct are not explicitly laid down, you will certainly come across them if you pay attention. For instance, in their research into codes of conduct within online student communities, Svensson and Van Wijk (2004) conclude, 'In both networks, copying copyrighted work is viewed as positive, sharing pornography as not positive and not negative, and spreading child pornography is strongly

22 Retrieved 18 March 2016 from https://help.habbo.nl/entries/20213383-Algemene-voorwaarden-Habbo-nl.