3 Types of cybercrime and their criminalisation

Jan-Jaap Oerlemans & Wytske van der Wagen*

3.1 Introduction

As shown in Chapters 1 and 2, cybercrime involves many different offences. In this chapter, we examine the most prominent types of cybercrime. In doing so, we will also mention the most important criminalisations of cybercrime, for which we rely heavily on a UN study on cybercrime and the Convention on Cybercrime. An overview of the relevant provisions in the Convention on Cybercrime can be found in the appendix at the end of this chapter.

The chapter is structured as follows. Section 3.2 offers an overview of the types and criminalisation of cyber-dependent crime. Section 3.3 describes the types and criminalisation of cyber-enabled crime. Section 3.4 offers a perspective on future developments. Section 3.5 summarises the chapter. Finally, Section 3.6 lists a number of discussion questions and Section 3.7 presents the key concepts relating to the types of cybercrime and criminalisation.

3.2 Cyber-dependent crime

Cyber-dependent crime, as explained in Chapter 1, involves criminal behaviour whereby computers and networks are both the target and the means of crime. This concerns behaviour that can affect the integrity, availability and exclusivity of data in computers (see, for example, Franken Committee, 1987). Availability refers to the storage, processing and transfer of data. For example, a ddos attack (see Section 3.2.4) affects the availability of data. Data integrity refers to the accuracy and correctness of data and

* Prof. dr. J.J. Oerlemans is an endowed professor of intelligence and law at the Willem Pompe Institute for Criminal Law and the Montaigne Centre for the Rule of Law and Justice of Utrecht University. Dr. W. van der Wagen is assistant professor in criminology at the Erasmus School of Law (Erasmus University Rotterdam).

programs. For example, if a computer is hacked and account information in a document is altered, this alters the integrity of data on a computer system. Data exclusivity refers to the aspect that unauthorised persons cannot become acquainted with confidential data. This can also include computer hacking and copying confidential data. The best-known types of cyber-dependent crimes are discussed in the following text, namely: computer hacking (Section 3.2.1), malware (Section 3.2.2), botnets (Section 3.2.3) and ddos attacks (Section 3.2.4).

As stated earlier, we refer to the Convention on Cybercrime as a reference point to discuss the criminalisation of cyber-dependent crimes, as it is the oldest most influential treaty in the field of cybercrime. The treaty can be traced back to 1989 in the Council of Europe's Recommendations on cybercrime (Weber, 2003).[1]

The Convention on Cybercrime has three important functions:

1. it harmonises criminal substantive law in relation to cyber-dependent and certain cyber-enabled crimes;
2. it harmonises criminal procedural powers to collect digital evidence; and
3. it facilitates legal assistance with regard to digital evidence (by establishing a 24/7 contact point for legal assistance) and extradition (Oerlemans, 2021).

The Treaty was established in 2001 in Budapest after four years of drafting it. It is considered very successful, especially compared to other international treaties of the Council of Europe, because it has a large number of ratifications (66 in 2021). States that are not part of the Council of Europe can also sign and ratify the treaty. Most notably, the influential United States ratified the Convention on Cybercrime. This was not surprising because it played a major role in the negotiations of both the plenary sessions and drafting of the treaty (Weber, 2003). Most states in the European Union, and countries such as Japan, the Philippines, Australia, New Zealand, Ghana, Morocco, South Africa, Argentina, Peru and Costa Rica ratified the Convention on Cybercrime.

[1] That is, the Committee of Ministers Recommendation no. 89 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation no. 95 concerning problems of criminal procedural law connected with information technology.

Remarkably, large countries such as the Russian Federation, India, and China did not ratify the Convention on Cybercrime. As a result, divergences exist in the criminalisation of cybercrime, which hamper legal assistance. For example, in order to protect persons within its own jurisdiction, states are unlikely to extradite suspects where the conduct is not also criminalised in its own country. This principle of 'dual criminality' is central to many forms of international cooperation. It can be found, for example, in multilateral and bilateral extradition treaties, as well as in national laws. The principle of dual criminality also plays a role in legal assistance, such as requests for the interviewing of witnesses, or the collection of evidence. Especially for coercive or intrusive measures, such as search and seizure, or freezing of property, states ensure that the agreements for cooperation are subject to dual criminality (UNODC, 2013, p. 59) (see further Chapter 8).

Besides the Convention on Cybercrime, there are many other international instruments which aim to harmonise the criminalisation of cybercrime.[2] Many of these treaties have provisions of criminal substantive law that are similar and inspired by the provisions in the Convention on Cybercrime. Generally, harmonisation of the legal framework relating to cybercrime tends to be higher in Europe and the Americas, compared to Africa, Asia and Oceania (UNODC, 2013, p. 58).

3.2.1 Hacking

3.2.1.1 Computer hacking

The offence of computer hacking (also called: 'cyber trespassing') is one of the cybercrimes that is committed relatively often. Hacking is about the deliberate and unlawful intrusion into a computerised work. This can be done in many different ways (see Bernaards, Monsma, & Zinn, 2012), such as:

1. providing access to a computer or network by means of a clever ruse;
2. the use of account log-in data offered on the internet;
3. using computer power (e.g. by using a so-called 'brute force attack')[3] to crack a password; and
4. by exploiting vulnerabilities in software on computers.

[2] See for an overview UNODC, 2013, pp. 63-72.

[3] A brute force attack refers to a method by which a program, backed by powerful computing power, is used to automatically crack passwords by trying numerous combinations of characters. Generally, the more complicated and longer the password, the longer it takes to crack it.

It is important to note, however, that hacking as a term also has a broader meaning that is not necessarily connected to crime. Its non-criminal meaning can be traced back to the origin of hacking (as described in Chapter 2) and the development of the hacker phenomenon. For example, hacking may also refer to tinkering with a device or machine to function as not originally intended or designed for and solving technical problems or obstacles (Blankwater, 2011; Steinmetz, 2015a). Such definitions of hacking are still used, for example, in so-called "hackerspaces", physical meeting places where hackers (in the broad sense of the word) meet to tinker with hardware, electronics and software. These (original) meanings of hacking, which can be traced back to the 1960s and 1970s, focus mainly on the creative and innovative use of technology (Nissenbaum, 2004), an aspect that is also (still) part of the hacker culture (Blankwater, 2011; Jelsma, 2017). In other words, non-criminal variants of hacking also exist; the hacker community is a heterogeneous group (see for example Althoff et al., 2020; Steinmetz, 2015a). As mentioned earlier, the focus of this book is on criminal forms of hacking.[4]

Criminalisation

Computer hacking is, generally speaking, criminalised as the intentional and unlawful intrusion into the whole or any part of a computer system without right (Art. 2 Convention on Cybercrime).[5] Intentional means, in simple terms, that a person performs an act 'knowingly'. 'Without right' means "in violation of the law". In the context of computer hacking, for example, it is a matter of a person not having received permission from the owner of a device to hack into it. There are, however, also persons who hack *with* permission. They are hired by companies, for example, to 'hack into' computers and provide the company or institution with security advice. They are also called 'ethical hackers' (see Section 3.2.1.2). People who work for a company and carry out such tests are also called 'penetration testers' or 'pen testers'. The hacking then takes place with (formal) consent of the client and is therefore not punishable.[6] We emphasise that this book focuses merely on computer hacking in the criminal sense. This entails that we focus on hacks and hacking in which actual illegal *intrusion* takes place. Computer intrusions may

[4] The older studies on the hacker phenomenon pay much attention to the hacker culture as well as to the changing definition of hacking (see for example Levy, 1984; Taylor, 1999).

[5] A computer system is defined in Art. 1(a) of the Convention on Cybercrime as: 'Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'.

[6] The 'unlawfulness' of the conduct ceases due to the permission to hack as stated in the agreement. The hacking is then not punishable.

be done by using technical means, such as software, which may in turn make use of a vulnerability in a computer program, which enables it to install on a computer and provide the offender unauthorised access to a computer system.

Illegal access to a computer system threatens the integrity of computer systems. The legal interest is infringed not only when a person without authorisation alters or 'steals' data in a computer system belonging to another, but also when an offender merely 'looks around' in the computer system (UNODC, 2013, p. 82). The criminalisation of illegal access to computers represents a deterrent to many other subsequent acts against the confidentiality, integrity and availability of computer systems or data, and other cyber-enabled crimes, such as identity theft and computer-related fraud or forgery.[7]

Many states amended their criminal substantive law in order to criminalise hacking. The reasons behind this is that criminal substantive law is traditionally focused on protecting physical objects, instead of intangible object, such as data or information. For example, the criminalisation of 'theft' often applies to physical objects. A 'theft' of computer data, for instance may not fall within the scope of the constituent elements of traditional theft. The data would still remain in the possession of the original bearer, thus (depending upon national law approaches) possibly not meeting required legal elements, such as the 'taking' of the object (UNODC, 2013, p. 52).

Some states also implemented certain provisions that function as 'aggravating circumstances' for hacking. For example, most EU states are obliged to incorporate the following aggravating circumstances for hacking following Directive 2013/40/EU on Attacks against Information Systems.[8] Article 9(4) of Directive 2013/40/EU states that for the crimes of 'illegal system interference' and 'illegal data interference' (see para. 3.2.2) the crimes must be punishable by a maximum term of imprisonment of at least five years where:

a. they are committed within the framework of a criminal organisation (...);
b. they cause serious damage; or
c. they are committed against a critical infrastructure information system.

[7] See Council of Europe, 2001, Explanatory Report to Council of Europe Cybercrime Convention, ETS No. 185, para. 44.

[8] After the Treaty of Lisbon, the EU now has a mandate for cybercrime legislation. Art. 83(1) of the Treaty on the Functioning of the European Union lists 'computer crime' as a 'serious crime with a cross-border dimension'.

3.2.1.2 Ethical hacking

As indicated earlier, there are also hackers who test computer and network systems for their security. This may be done without the owner's consent, but not with the aim of committing criminal offences. The objective here is not to take over data and publish it, but to show security vulnerabilities. These 'ethical hackers' serve a higher purpose, namely the public interest. They want to offer society 'a helping hand' (see also van 't Hof, 2015).

When there is no consent given to gain access to a computer system, the decision may be made to prosecute for hacking. However, we believe that this kind of access to a computer system should not automatically lead to prosecution, because there is public interest in finding (and solving) vulnerabilities in computer systems. For now, a small number of states created guidelines for 'Coordinated Vulnerability Disclosure' (CVD, also called 'Responsible Disclosure') of these vulnerabilities and how companies and governmental authorities should deal with ethical hackers. Let us now take a look at the example of the Netherlands, which is relatively far in developing a set of guidelines for the disclosure of vulnerabilities.

(Dutch) Coordinated vulnerability disclosure-guideline

The Dutch National Cyber Security Centre drew up the guideline 'Coordinated Vulnerability Disclosure' (NCSC, 2013, 2018). The aim of the guideline is to contribute to the security of ICT systems by sharing the knowledge of vulnerabilities by ethical hackers with the owners of ICT systems, so that they can fix the vulnerabilities before they are actively abused by third parties.

The guideline states that the organisation and the reporter can agree not to report the incident (primarily of computer hacking), as long as the reporter operates within the preconditions of the policy of the company or institution. The Dutch Public Prosecutor's Office will take into account whether the Coordinated Vulnerability Disclosure policy has been complied with in its decision to prosecute.

When it comes to prosecution, judges may nevertheless take into account the social interest. In that case, courts will assess whether the conduct met the proportionality principle (no more computer hacking has taken place and no more data have been acquired than is necessary to achieve the objective) and subsidiarity principle (were there less far-reaching ways available to achieve the same objective).

From an international legal perspective, it is problematic that there is no *international* responsible disclosure guideline. Hackers must realise that they may hack a computer system on a territory of a state, that does not take the 'social interest' in ethical hacking into consideration like other states. As a result, they may be prosecuted for computer hacking by foreign law enforcement authorities (Falot & Schermer, 2016).

From a rational choice perspective (see also Chapters 7 and 9), it is relevant to emphasise that this policy is still under development and that there are significant advantages and disadvantages in reporting ICT vulnerabilities (Weulen Kranenbarg, Holt, & van der Ham, 2018). For example, it appears that young ethical hackers, out of fear of prosecution or frustrated with communication with ICT owners, do not always report the vulnerabilities they find (Spronk & Weulen Kranenbarg, 2020; van der Wagen et al., 2019).

3.2.2 Malware

Malware is a collective term for various types of malicious software. This includes types of malware such as viruses, worms, and Trojan horses. A 'virus' refers to malicious software that infects computer systems. Typically (unlike a worm) it requires an action from the computer user, such as opening an attachment in an email containing the malware. A 'worm' is malicious software with the functionality to spread *itself* within a network of computers. A 'Trojan horse' (the name has its origins in Greek mythology) is an innocent-looking programme that actually contains malware, such as an attachment to a Word document with an innocent-looking file name such as an invoice. Once this file is opened, the system becomes infected (Holt, Bossler, & Seigfried-Spellar, 2015).

In the past, a strict distinction was made between viruses, worms and Trojan horses, but nowadays malicious software often has characteristics of all these types: the malicious software (a virus) can spread itself to other computers (characteristic of worms) and often pretends to be an innocent-looking programme (i.e. a Trojan horse). For this reason, the collective term 'malicious software' is usually used nowadays. Malware often contains many functionalities that can be of use to a cyberoffender. Examples include the functionality of a backdoor to gain access to a computer and remotely take screenshots, switch on a microphone or camera, take over data or change data (Bernaards et al., 2012). By registering keystrokes, hackers can, for example, capture passwords and use these to break through login and password security later on.

Sometimes the malware is a conduit for other malicious software to be downloaded onto the computer. This is sometimes the case with botnets, which Section 3.2.3 discusses in more detail. If (bot) malware has already been installed on the computer and the computer is therefore part of the botnet, this malware can bring in other malware (e.g. van der Wagen & Pieters, 2015, p. 2020). Ransomware is also a possibility. As this is a recent and persistent phenomenon, this manifestation deserves further attention.

3.2.2.1 Ransomware

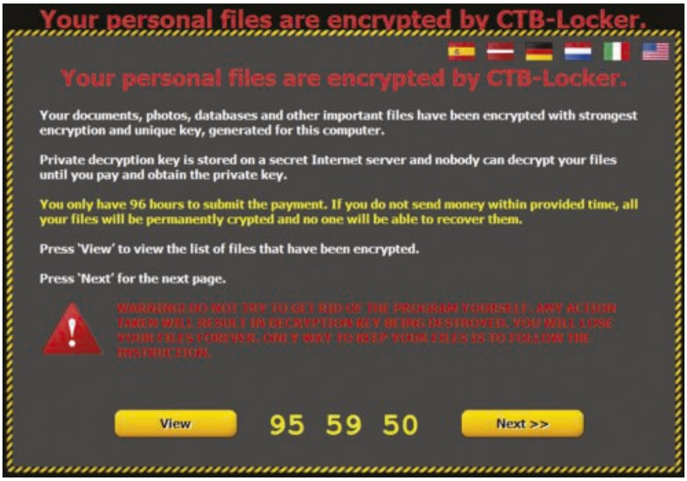
According to Europol, ransomware is the most popular type of malware among cybercriminals for several years now (iOCTA, 2017). Ransomware is software that blocks access to someone's computer system or files on the system and subsequently demands a ransom to be paid for unlocking the computer or files. Cryptoware is a specific type of ransomware, which encrypts files on computer systems (Custers, Oerlemans, & Pool, 2020).

The 'success' of ransomware can be explained by the fact that individuals and organisations are readily prepared to pay for data that is no longer accessible. This could be family photos or holiday snaps located on the encrypted computers of private individuals, but also the financial administration of a company or multinational. Cybercriminals attack systems where there is a high chance that the victim will pay the ransom. Today, ransomware can be very advanced malware, in which the files cannot be decrypted by means of digital forensics or brute forcing, but this was not yet the case with the first ransomware.

The first ransomware attempted to get people to transfer money by means of social engineering through 'screen lockers'. An example of this is the so-called 'police virus' (2012), where a message appeared stating that the user had child pornography or illegal copyrighted files on the computer and risked arrest. It was not easy to click away the extra screen with the fake warning, as it kept reappearing. If one paid with a prepaid card, the 'blockage' on the computer would be lifted (van der Wagen & Pieters, 2020).[9]

[9] Often the extra browser window disappeared when the computer was restarted.

Soon cybercriminals developed the more sophisticated type of ransomware called ‘cryptoware’, which encrypts files and makes them inaccessible. This ransomware cannot be removed by booting up the computer or using anti-virus software, unlike the first screen lockers. Figure 3.1 provides an example of cryptoware. CTB-Locker was a successful type of ransomware in 2015.[10]



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press ‘View’ to view the list of files that have been encrypted.

Press ‘Next’ for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

Figure 3.1 Example of ransomware (‘CTB-Locker’).

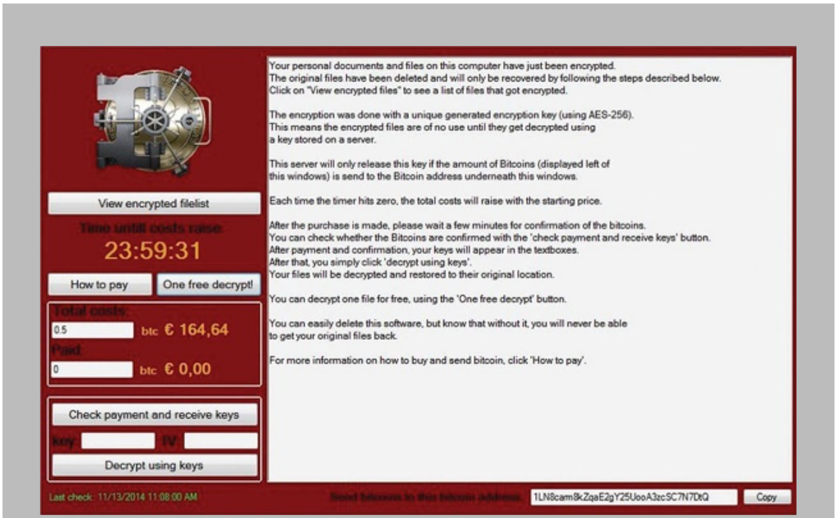
After infection, access to the files can only be regained after payment, usually in the cryptocurrency Bitcoin, by decrypting the files with a key transmitted by the offender to the victim (Oerlemans et al., 2016).

Case study: CoinVault

In the CoinVault case, two young Dutch men were convicted of extortion using ransomware.[11] Figure 3.2 shows the ransomware ‘hostage note’ that is presented when a computer is infected.

[10] Computer Incident Response Center Luxembourg, ‘A new wave of crypto ransomware targeting Luxembourg’, 5 February 2015.

[11] Court of Rotterdam 26 July 2018, ECLI:NL:RBROT:2018:6153, *Computerrecht* 2018/210, pp. 281-291, with annotation by J.J. Oerlemans (*CoinVault case*).



Time untill costs raise:
23:59:31

Total costs:
0.5 btc € 164,64
Paid:
0 btc € 0,00

key: IV:

Last check: 11/13/2014 11:08:00 AM

Your personal documents and files on this computer have just been encrypted.
The original files have been deleted and will only be recovered by following the steps described below.
Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-256).
This means the encrypted files are of no use until they get decrypted using
a key stored on a server.

This server will only release this key if the amount of Bitcoins (displayed left of
this windows) is send to the Bitcoin address underneath this windows.

Each time the timer hits zero, the total costs will raise with the starting price.

After the purchase is made, please wait a few minutes for confirmation of the bitcoins.
You can check whether the Bitcoins are confirmed with the 'check payment and receive keys' button.
After payment and confirmation, your keys will appear in the textboxes.
After that, you simply click 'decrypt using keys'.
Your files will be decrypted and restored to their original location.

You can decrypt one file for free, using the 'One free decrypt' button.

You can easily delete this software, but know that without it, you will never be able
to get your original files back.

For more information on how to buy and send bitcoin, click 'How to pay'.

Send bitcoins to this bitcoin address: 1LN8cam8kZqaE2gY25UooA3zcSC7N7DtQ

Figure 3.2 Screenshot of CoinVault ransomware.

As with many other ransomware, a message is displayed stating that the victim's computer files have been encrypted. The files can only be decrypted if a sum in bitcoins is transferred to the offenders. With the key, victims can decrypt the files on a computer. A timer runs down to show how much time the victims had to pay the sum of half a bitcoin (at the time, (only) 164.64 euros). CoinVault also offered the option of testing one file for decryption and included a button with more information on how to pay with bitcoin. In this way, the victim could see that payment would actually lead to decryption. For the offender, this is a strategy to encourage victims to pay, thus making the 'business model' more likely to succeed.

In this case, the young men were given 240 hours of community service. Even for Dutch standards, this is a relatively mild punishment considering the seriousness of the behaviours, the damage that occurred, and the maximum prison sentence being nine years for the offence of extortion.

Europol notes that ransomware attacks have recently become more targeted, profitable and damaging (iOCTA, 2019). Illustrative is the ransomware attack on money transfer company 'Travelex'. In January 2020, Travelex was the victim of infection by ransomware of the 'Sodinokibi'-family. Cybercriminals encrypted all computers and backups of the company and even exfiltrated 5 Gb of sensitive data, including social security numbers, date of birth and payment information. This data was used to put further pressure on Travelex. The company paid U.S. $2.3 million in ransom (iOCTA, 2020). Ransomware even brings entire municipalities to a standstill. For example, the municipal computers of major cities such as Atlanta and Johannesburg have already been held hostage for the payment of ransoms in Bitcoin in 2018.[12]

The ransomware attack on the container company Maersk in 2017 and an important oil pipeline in the United States of the company Colonial Pipeline in 2021, show that critical infrastructures can also be affected by ransomware.[13] Maersk suffered around EUR 300 million in damage and had to reinstall around 45,000 computers. As a result of the attack, a (fully automated) container shipment area in the harbour of the Dutch city of Rotterdam was shut down for a week.[14] The European cybersecurity institute ENISA reported in 2018 that more and more attacks also target hospitals or medical devices, which are vulnerable (ENISA, 2018). We might expect, for example, the first ransomware attack on a Tesla or other 'smart car' in the near future. For now, ransomware is still mostly targeting companies and these attacks get more sophisticated (see for example the recent attacks on Kaseya, allegedly committed by the Russian cybercriminal group called "REvil").[15]

Criminalisation

In the Convention on Cybercrime, the use of malware is specifically criminalised in Article 4. Article 4 states that each party of the convention must criminalise the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right.

In addition, Article 6 obliges convention states to criminalise the production, sale, procurement for use, import, distribution or otherwise making available of malware and password or other computer codes that are used to access

[12] See e.g. 'Atlanta City computer network remains hobbled by cyberattack', *The New York Times*, 23 March 2018.

[13] See A. Greenberg, 'The untold story of NotPetya, the most devastating cyberattack in history', *Wired*, 22 August 2018. See also J. Ainsley & K. Collier, 'Colonial Pipeline paid ransomware hackers $5 million, U.S. official says', *NBC News*, 13 May 2021.

[14] D. Bremmer & L. van Heel, 'Wereldwijde hack legt bedrijven en Rotterdamse terminal plat' ['Worldwide hack cripples companies and the harbour of Rotterdam'], *AD.nl*, 27 June 2017.

[15] See for example D. Sason, 'REvil ransomware attack on Kaseya VSA. What you need to know', *Varonis.com*, 29 July 2021.

computer systems. The goal is to discourage the possession and distribution of malware and passwords. This provision is understandable since there is a lively trade in malware and other tools to commit cybercrime on online markets (UNODC, 2013, p. 92). The Convention on Cybercrime does require *intent* that it be used for the purpose of committing offences like computer hacking. This prevents the overcriminalisation of unknowing possession, or possession with legitimate intent, such as the possession of malware by a white hacker of computer security company who uses it for 'penetration testing' of a client's IT infrastructure.

However, in case of ransomware, many states will be able (or prefer) to prosecute for more 'traditional crimes', such as extortion; a crime that may also have a higher maximum prison sentence. In that case it is important, of course, that the exact behaviour is criminalised, more particularly that people or organisations are extorted not by the use of 'violence' in a physical sense, but by the threat of the hindrance or alteration of data.

As mentioned before, some states implemented international legislation which prescribes a higher prison sentence when aggravating circumstances apply. For example, when thousands of computers or a large organisation is the victim of ransomware, a higher prison sentence may apply because the threshold of 'serious damage' is met.[16]

Finally, it is also conceivable that the offence of fraud is involved, as victims are induced to transfer money to the extortionists by means of a cunning trick (social engineering). It is noteworthy that banking malware is both a cyber-dependent crime (by infecting computers with malware and hacking) and a cyber-enabled crime (by committing fraud). The Convention on Cybercrime specifically criminalises 'computer-related fraud' in Article 8. It obliges member states of the convention to adopt legislation or other measures to establish as criminal offences under its domestic law, when committed intentionally and without right, causing a loss of property to another person by (a) any input, alteration, deletion or suppression of computer data, or (b) any interference with the functioning of a computer system, with "fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person". Sometimes, domestic legislation already covers this criminal behaviour, but oftentimes, states must amend their articles related to fraud to specifically incorporate the elements of (a) and (b) mentioned earlier.

[16] See Art. 9(4) of the directive 2013/40/EU on Attacks against Information Systems.

3.2.3 *Botnets*

A botnet is a network of infected computers with malware that is controlled by one or more administrators (also called a 'botherder' or 'botmaster') (Bernaards et al., 2012, p. 45). Figure 3.3 depicts a simple (centrally controlled) botnet.

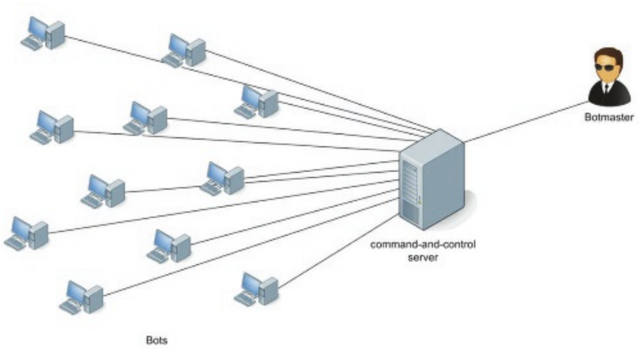


Figure 3.3 Simple model of a botnet (Plohmann, Gerhards-Padilla & Leder, 2011).

The botmaster controls the infected computers via a server called a 'command-and-control' server. These computers are also called 'zombie computers', because they are under the control of a third party. There are also botnets that are not so much centrally controlled from a central command- and control server, but have a so-called 'peer-to-peer' infrastructure. In that case, the bots give commands to each other after one of them gets an instruction from the third party (a so-called principle of self-propagation of commands). These botnets have a more complex infrastructure and are therefore more difficult to detect. There are also botnets that are built both centrally and peer-to-peer, also known as a hybrid infrastructure (Plohmann et al., 2011; Wagenaar, 2012).

Case study: ZeuS

The evolution of ZeuS malware is illustrative of the development and sophistication of malware and its botnet infrastructure. ZeuS malware was first identified in July 2007 when it was used to steal information from the U.S. Department of Transportation.[17] ZeuS developed into so-called banking malware, aimed at frequently acquiring and transferring money from one back account to another. The malware recognises the name of the bank or the URL the victim is searching for and guides the victim to the fake website that the cyber offender has created (Bernaards et al., 2012, p. 43). The fake websites may be very hard to distinguish from the real websites for online banking. When the victim wants to transfer money to another account, behind the screens the amount and the beneficiary are modified. This type of attack is also referred to as a *man-in-the-browser-attack* (Custers, Pool, & Cornelisse, 2019). Later on, banks used a two-factor identification system that requires an authentication code. Cybercriminals came up with schemes to acquire the code, for instance through a chat screen or another type of pop-up screen, or by calling them, pretending to be a bank employee) (Sandee, 2015, pp. 17-18).

The botnet infrastructure of Zeus developed from a more regular botnet with centralised command-and-control servers to a peer-to-peer botnet. The Zeus P2P network served two main purposes. Bots exchanged configuration updates with each other and bots exchange lists of proxy bots, which were designated bots where stolen data was dropped and commands were retrieved. As a backup channel, P2P Zeus also automatically generated domain names to quickly contact a web server when a network connection was lost (Andriesse et al., 2013).

Ultimately, ZeuS malware and its botnet evolved to something more than banking malware. The new 'GameOver ZeuS' malware was also used for ddos attacks, Bitcoin theft, Skype credentials, and even collecting confidential information like email addresses belonging to Georgian intelligence officers and classified Ukrainian secrets. Security researchers estimate the criminal organisation behind GameOver ZeuS consisted of dozens of individuals and made between 70 and 100 million dollars in total. The original creator of ZeuS was not arrested and is suspected to reside somewhere in the Russian Federation.[18]

[17] J. Finkle, 'Hackers steal U.S. government, corporate data from PCs', *Reuters,* 17 July 2007.

[18] G.M. Graff, 'Inside the hunt for Russia's most notorious hacker', *Wired,* 21 March 2017.

Botnets are also referred to as the 'workhorses of cybercriminals' (Oerlemans et al., 2016) or the 'Swiss army knife of cybercrime' (Bernaards et al., 2012). This is because botnets can be used in many different ways to make (criminal) money. Examples of this are collecting personal data (see above), managing infected computers with ransomware (administration), sending spam with the (email) box of the infected computer and managing virtual money that is created by infected computers by, for example, 'mining bitcoins' via 'mining malware' (Wagenaar, 2012). Mining malware uses the processing power of computers to create new virtual money through calculations (see Section 3.3.3 on virtual currencies).

Criminalisation

For a botnet to work, whether it is a centrally controlled or peer-to-peer botnet, computer hacking must take place. Therefore, when botnets are created the offence of illegal access to computer systems (hacking) also takes place (Art. 2 Convention on Cybercrime). In addition, the use of malware which amounts to the offence of intentional damaging, deletion, deterioration, alteration or suppression of computer data without right, is applicable (Art. 4 Convention on Cybercrime). The Convention on Cybercrime did not specifically criminalise the use or creation of botnets, probably because botnets were not yet a well-known phenomenon relating to cybercrime.

In the EU Directive on attacks against information systems (2014), the use of botnets is considered as an aggravating circumstance because many computers are hacked to create it. Member States must criminalise this as an offence with up to three years in prison.[19] Botnets are also used to carry out ddos attacks, a form of cybercrime dealt with in more detail in the following section.

3.2.4 Ddos attacks

During a ddos attack, multiple computers simultaneously visit another computer, such as a website server, and overload the website server with network traffic. Ddos attacks are popular with teenagers who do not want to

[19] See Art. 9(3) of Directive 2013/40/EU: "Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose."

take an exam on a computer on a certain date and teenagers who want to make it difficult for their opponents in computer games, but are also launched by seasoned cybercriminals. This is a type of cybercrime that has become increasingly common in recent years. Ddos attacks have been in existence now for more than 20 years (with the first attack in 1999). On 22 July 1999, a computer at the University of Minnesota suddenly came under attack from a network of 114 other computers infected with malicious malware called 'Trinoo'. The malware enabled the infected computers to send superfluous data packets to a computer server of the university, overwhelming its computer and preventing it from handling legitimate requests. In the following months, other websites became victims, including Yahoo, Amazon, and CNN.[20]

Nowadays, ddos attacks are prevalent and offenders can purchase pre-existing automated tools and deploy them for their own purpose, which makes conducting a ddos attack a relatively cheap and easy way of carrying out an attack for threat actors who may have limited skills or experience in engaging in cybercrime. Cyber offenders who are looking for financial gain make use of it as a form of extortion for web shops or online gambling websites, for example. These kinds of websites need to stay online for their income and are often prepared to pay money to prevent this. The hacktivists, as discussed earlier, bring certain websites down for ideological or political reasons. Moreover, criminals can use ddos attack as a decoy or smokescreen, while offenders hack the computer systems of the target in the meantime (iOCTA, 2020, p. 32).

Ddos attacks can have major consequences. For example, when a cyberoffender attacks a telecommunication provider, it may lead to unavailable internet connections of clients of these providers. With this form of cybercrime, the force multiplier principle discussed in Chapter 2 is very clear: a single perpetrator can generate a lot of impact with just a few mouse clicks.

[20] See 'The first DDoS attack was 20 years ago. This is what we've learned since', *Technology Review,* 18 April 2019.

Case study: Webstresser.org

In April 2018 the popular ‘ddos service’ on the internet ‘Webstresser.org’ was taken offline in an international police operation.[21] Through this service, which advertised as ‘testing’ the capacity for handling network traffic, people actually rented a botnet for as little as 15 euros to carry out a ddos attack. Figure 3.4 is a screenshot of Webstresser.org, after it was made inaccessible by law enforcement authorities.

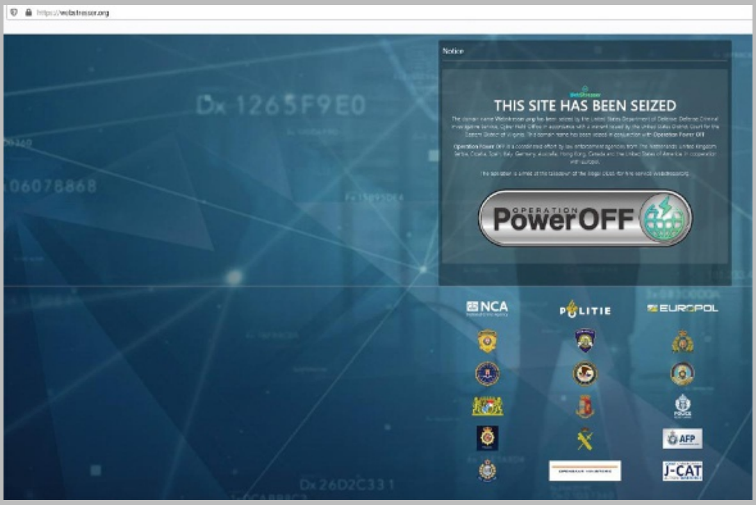


Figure 3.4 Screenshot of the website webstresser.org.

The operation allowed the police to obtain data on more than 151,000 users of this website. The low-threshold to conduct a ddos attack with webstresser.org led to the disruption of computer exams at schools, for example.[22] So far, no convictions have been published in the Netherlands as a result of the operation. The police report that officers had a ‘knock-and-talk’ intervention with the (often young) clients of Websstresser.org about their criminal behaviour. The aim is for these

[21] ‘Nederlandse Politie haalt ddos dienst webstresser.org offline’ [‘Dutch police take ddos service webstresser.org offline’], *Tweakers.net*, 25 April 2018.

[22] N. Klaassen, ‘Pssst, wil je een cyberaanval uitvoeren? Dat kost 15 euro’ [‘Pssst, would you like to launch a ddos attack? That will cost 15 euros’], *AD.nl*, 31 January 2019.

people to realise that they are not as anonymous as they may have thought they were (see also Chapter 9).[23]

Criminalisation

Ddos attacks are criminalised in Article 5 Convention on Cybercrime. Member states must adopt legislative and other measures to establish as criminal offences under its domestic law to criminalise ddos attacks, formulated as the intentional “serious hindering (without right) of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data”.[24]

The EU Directive 2013/40/EU formulated aggrevated circumstances for ddos attacks, providing a maximum prison sentence of no less than five years when the attack involves ‘considerable damage’ or is aimed at a ‘vital infrastructure’. In case a botnet is used to carry out the ddos attack, the Directive stipulates a maximum prison sentence of no less than three years.

3.3 Cyber-enabled crime

Cyber-enabled crime refers to crime in which computers and the internet are used as tools to commit traditional crime (Tollenaar et al., 2019; Wall, 2014; see also Chapter 1). This section takes a closer look at various types of cyber-enabled crime. In succession, these are: cyber-enabled fraud, online drug trafficking, money laundering with virtual currency, and online sex offences.

3.3.1 Cyber-enabled fraud

Cyber-enabled fraud is a common form of digitalised crime (Clough, 2015, see also Chapter 6). In cyber-enabled fraud cases, the victim is often persuaded to transfer money to someone who pretends to be a family member in need of money or to comply with other ‘fake payment requests’ (Rooyakkers & Weulen Kranenbarg, 2020), to send a bank card (with PIN number) after a

[23] ‘Politie en justitie gaan wereldwijd achter de gebruikers van ‘DDoS-for-hire websites’ aan’ [‘Police and judiciary go after users of “DDoS-for-hire websites” worldwide’], *Politie.nl*, 28 January 2019.

[24] In addition, Art. 4 of the Convention on Cybercrime about ‘data interference’ may apply, since it criminalises the ‘suppression of data’ without right.

message has supposedly been sent by the bank, or to transfer money via a fake website after receiving a fake invoice (Jansen & Leukfeldt, 2016).

When we talk about internet scams, the term ‘phishing’ is often used, which refers to stealing personal data such as user names, passwords, IP addresses and bank details (e.g. van der Wagen & Bernaards, 2020). Phishing usually takes place via digital means of communication, such as emails, but nowadays also via other mediums such as WhatsApp and Snapchat. In this respect, three methods can be roughly distinguished:

1. Sending a phishing email with a trick to get people to give up personal data;
2. Sending a phishing email with an attachment; when the attachment is opened, malware is installed on a computer; and
3. Sending a phishing email with a link to a ‘fake’ website.[25]

When visiting the fake website, malware is installed on the computer. Because of the malware component, phishing actually falls under the heading of cyber-dependent as well as cyber-enabled crime. In order to create phishing messages, real messages are often ‘cloned’ or partially forged. Of course, it is important to make them as credible as possible so that victims click on the link or visit the relevant website. Offenders therefore often use the same company colours, logos and jargon of the companies on whose behalf they are supposedly operating (van der Wagen & Bernaards, 2020). The aim is always to get people to hand over something (information) that will later be abused.

In phishing scams, the tasks of making money with someone else’s data are often divided up between different people (as discussed in Chapter 2 and later in Chapter 5 with regard to ‘crime-as-a-service’). One can think of roles such as ‘web designer’, ‘hacker’, ‘malware distributor’, ‘botnet herder’ and ‘money mule’ (see also Faber et al., 2010). Specialised ‘spammers’ are also often involved in phishing because they often have a botnet or can hire one. In this case they send phishing messages or rent out the computers that are part of the botnet (van der Wagen & Bernaards, 2020). The skills of the people involved vary widely and are both ‘low tech’ and ‘high tech’ (Leukfeldt, Kleemans, & Stol, 2016). This often involves a planned approach, intensive cooperation and clear coordination between the people involved.

[25] N. Vloeimans, ‘Snapchat populair bij fraudeurs dit jaar’ [‘Snapchat popular with scammers since this year’], *RTV Noord*, 4 March 2020.

A special form of phishing is 'CEO fraud'. The identity of a company's Chief Executive Officer (CEO) is in that case misused to instruct an employee in (most often) the finance department to make a payment – usually by email (iOCTA, 2016, 2018). In reality, the undue payment is transferred to someone else (usually a money mule).

Case study: CEO fraud

For example, in 2018, two directors of Pathé Cinemas in Amsterdam (the Netherlands) had been defrauded via a phishing mail of a total of 19 million euros. The offenders instructed the director to transfer the large sum of money as an investment project. The directors complied with the instruction without checking the authenticity of the email. In order to make the payments, they borrowed money from Pathé headquarters in Paris, which led to questions. After the fraud scheme was discovered, the directors lost their jobs.[26] In order for such a ruse to be convincing, cybercriminals often carry out a lot of reconnaissance work before sending a carefully designed targeted phishing mail ('spear phishing mail').

Criminalisation

Like other cyber-enabled crimes, cyber-enabled fraud is often criminalised using a general offence for fraud (UNODC, 2013, p. 77). The diversity in criminalising cyber-enabled fraud derives in part from differences between national legal systems in the extent to which 'traditional' offences can be applied in a 'cyber' environment. Traditional fraud offences, for example, often require the direct deception of a *person* and may suffer challenges in their extension to acts committed through the manipulation of a computer system or computer data. In order to address such legal challenges, national cyber-specific provisions for fraud often focus on the manipulation of *computer data or systems* with dishonest or fraudulent intent, rather than on the element of deception of an individual (UNODC, 2013, pp. 97-98).

Article 8 of the Convention on Cybercrime requires each party state to adopt legislative or other measures to criminalise, when committed intentionally and without right, the following acts: the causing of a loss of property to

[26] See the court decision of the Court of Amsterdam (31 October 2018, ECLI:NL:RBAMS:2018:7881).

another person by (a) any input, alteration, deletion or suppression of computer data, (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. When malware is installed on victims' computers, the offence of computer hacking and data interference may also be applicable.

National provisions on cyber-enabled forgery typically require two necessary elements: (i) the alteration or manipulation of computer data, and (ii) a specific intent to use the data as if they were authentic (UNODC, 2013, p. 98). The Convention on Cybercrime also obliges party states to criminalise 'computer-related forgery' (Art. 7), referring to the input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.

Finally, the UNODC study found that some states specifically criminalise cyber-enabled identity-theft, but many states refer to existing criminalisation for identity-theft (UNODC, 2013, p. 99).

3.3.2 Online drug trafficking

Over time, the internet has become an increasingly important platform for the sale of various types of drugs. For example, back in 2008, an entrepreneur from The Hague saw a gap in the drugs market: online coffee shops.[27] As you may be aware, in the Netherlands the selling of soft drugs is in part legalised and sold in 'coffee shops'. Whereas a physical coffee shop can only serve customers in the region, the internet has the potential to reach worldwide. This is how the website 'Wolkenwietje.nl' (which can be translated as: 'cloudy weed') was born, probably the first online coffee shop that operated from the Netherlands. Soon, the website was taken offline at the request of the police. Till date, coffee shops in the Netherlands are not permitted to receive a licence from municipalities to do business online. One of the reasons is that online coffee shops cannot practically meet all the legal criteria, such as checking the age and nationality of the buyers. Of course, this does not mean that Dutch online drug shops do not exist in practice (Oerlemans & van Wegberg, 2019). For example, the website 'Groentethuisbezorgd.com' advertises with:

[27] 'Politie sluit digitale coffee shop' ['Police closes digital coffee shop'], *Telegraaf.nl*, 19 March 2008.

> Buy weed online and order weed easily through groentethuisbezorgd.com! Buying weed online is safe and reliable. Order your weed online and get it delivered the next day. Instead of visiting the coffeeshop, you can now buy weed online.[28]

Case study: Silk Road

The online sale of drugs has become considerably more professional over the years. 'Silk Road' was one of the largest online drug markets from 2011 to 2013. Websites that act as marketplaces for drugs, among other things, are called *darknet markets* (Martin, 2014). Darknet markets that specialise in drugs are characterised by the following: (1) accessibility through the anonymisation network Tor (see further Chapter 5); (2) payment in cryptocurrency (see Section 3.3.3); and (3) the delivery of drugs through (postal) mail (Verburgh et al., 2018).

The economic model in these modern online drug markets is usually as follows. For each transaction between a buyer and seller, the administrator of the 'web shop' receives a small percentage in cryptocurrency. In the case of Silk Road, at the time of the arrest, the Silk Road administrator had $28 million stored in his digital wallet after two years of work.[29] The bitcoins were eventually sold (after confiscation by the U.S. Secret Service) by auction and Ross Ulbricht was sentenced to life imprisonment.[30]

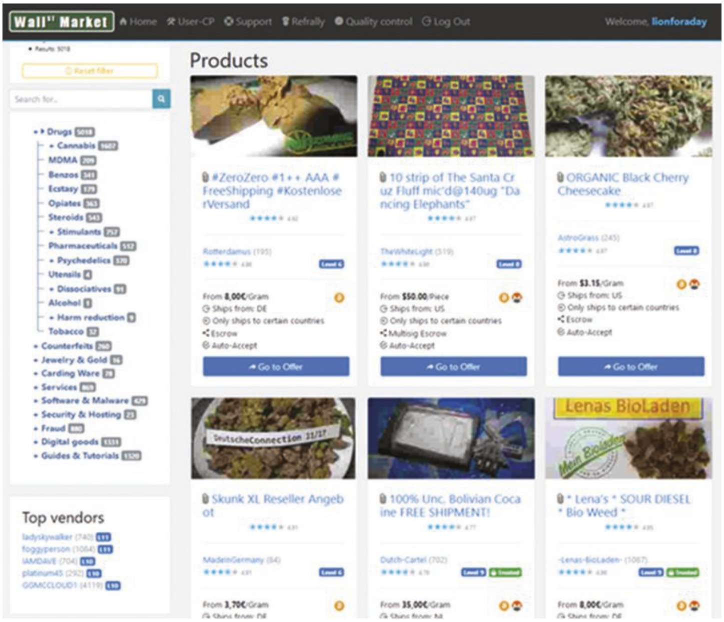
There is often a strict hierarchy on darknet markets and forums (see also Chapter 5). With various tasks and responsibilities, an attempt is made to maintain order and remove undesirable members or troublemakers. 'Administrators' determine the rules, purpose and direction of the forum or marketplace. 'Moderators' often oversee the forum and change or modify the content on the website. They are often persons trusted by the administrator

[28] Translated from Dutch. 'Groente thuisbezorgd' can be translated as 'vegetables delivered at home'.

[29] See extensively J. Bearman, 'The rise and fall of Silk Road', *Wired Magazine,* 23 May 2015.

[30] S. Thielman, 'Silk Road operator Ross Ulbricht sentenced to life in prison', *The Guardian*, 29 May 2015. The 144,336 bitcoins were worth more than $28 million at the time. See also press release 'Manhattan U.S. Attorney Announces Forfeiture of $28 Million Worth of Bitcoins Belonging to Silk Road', 16 January 2014, U.S. Department of Justice.

and experts in a particular field. 'Vendors' can often achieve a certain status through good reviews from customers. The quality of their products and the delivery process is thereby constantly assessed (Holt, 2013a, 2013b). The Europol report (iOCTA, 2014) on organised cybercrime stated that reputation and the associated nickname are particularly important for these cybercriminals. It is one of the most important factors in creating trust and for customers to decide whether they want to use the services offered. Figure 3.5 is an example of a darknet market ('Wall Street Market'). It illustrates how drugs is offered with payment in different virtual currencies (see Section 3.3.3 about money laundering and virtual currency).



Top vendors
ladyskywalker (740)
foggyperson (1064)
IAMDAVE (704)
platinum45 (292)
GGMCCLOUD1 (4119)

#ZeroZero #1++ AAA #FreeShipping #KostenloserVersand
Rotterdamus (195)
From 8,00€/Gram
Ships from: DE
Only ships to certain countries
Escrow
Auto-Accept

10 strip of The Santa Cruz Fluff mic'd@140ug "Dancing Elephants"
TheWhiteLight (519)
From $50.00/Piece
Ships from: US
Only ships to certain countries
Multisig Escrow
Auto-Accept

ORGANIC Black Cherry Cheesecake
AstroGrass (245)
From $3.15/Gram
Ships from: US
Only ships to certain countries
Escrow
Auto-Accept

Skunk XL Reseller Angebot
MadeInGermany (84)
From 3,70€/Gram

100% Unc. Bolivian Cocaine FREE SHIPMENT!
Dutch-Cartel (702)
From 35,00€/Gram

* Lena's * SOUR DIESEL * Bio Weed *
-Lenas-BioLaden- (1067)
From 8,00€/Gram

Figure 3.5 Screenshot of 'Wall Street Market' (archive of J.J. Oerlemans).

In addition to drugs, many other illegal goods and services are offered on darknet markets, such as stolen personal data, malware, medicines and weapons (see e.g. Holt & Lampke, 2010; Leukfeldt, Kleemans, & Stol, 2017b; Soudijn & Zegers, 2012, see also Chapter 5). In 2016, research conducted by the firm RAND, commissioned by the WODC, estimated that between 15-25 million US dollars worth of drugs are traded on darknet markets every month.

We expect a shift from drug trading on online (darknet) market places to apps, such as 'Telegram'. For example, it is known that price lists containing drugs are circulated via communication services such as WhatsApp and Telegram, and the drugs are delivered to the home by a courier on request (Oerlemans & van Wegberg, 2019). This means that the evidence of a transaction can be found on these smartphones and that the investigation process must change to find relevant evidence (see further Chapter 8).

Criminalisation

As far as criminalisation is concerned, there is little that is new under the sun. Trading in illegal goods, such as drugs and firearms is almost always criminalised. It does not matter whether the trade takes place on a darknet market, in a channel on Telegram or on the streets. Since there are no specific provisions specifically addressing *online* drug trafficking in the Convention on Cybercrime (or other treaties), we will not go into further detail.

3.3.3 Money laundering and virtual currency

Cryptocurrencies, such as Bitcoin and Monero, are used to buy illegal goods and services and they can also be used to launder money. Cryptocurrency is virtual money based on cryptographic software, with no central authority to oversee the management of the money (e.g. Oerlemans et al., 2016). Cryptocurrencies are not regarded by the government as official 'real money' (fiat money); they are merely bits and bytes ('virtual money').

With the cryptocurrency Bitcoin, a network of Bitcoin users verify whether a transaction is legitimate or not. The network acts as a kind of registry and this registry is called the blockchain. Bitcoins are sent to a Bitcoin address, such as '1X6GYUigC9tYGqdNPJyL2769U9jd8P3vT'. Bitcoins can be sent, for example, via a website or via apps connected to the blockchain. All transactions in the blockchain are public and anyone who wants to can follow the transactions. Bitcoins are therefore not anonymous, but it is sometimes difficult to identify the people behind a bitcoin address. If a user's identity becomes known, for example if the user divulges it on the internet, their entire transaction history can be traced. Bitcoins are stored on a computer in a file called a 'bitcoin wallet'. This virtual wallet can be accessed via an internet user account or, for example, on a USB flash drive.

Case study: money laundering of bitcoins from Agora and Evolution Market

On 10 March 2017, the Court of North Holland sentenced a suspect for online drug trafficking and money laundering.[31] The suspect traded mainly in XTC pills and LSD through the – at the time popular – darknet markets 'Agora' and 'Evolution'. The offender specialised in supplying so-called 'resellers' and belonged to the higher segment of drug trafficking. The evidence was based on, among other things, reviews of the drug trafficker's customers on the darknet markets.

The case examines in detail the cryptocurrencies used, in this case bitcoins, 'paycoins' and 'opalcoins' (so-called 'altcoins'). Using financial investigation techniques, the investigators checked whether a connection could be made between the bitcoin addresses in the digital wallet on the suspect's laptop and the transactions and bitcoin addresses appearing on Agora and Evolution. For example, in the period from 24 February to 9 March 2015, 889.90 bitcoins had been transferred from the darknet markets with a (at the time) value of 208,125.72 euros. Sixteen (incoming) transactions were found that could be linked to the accused from Evolution or Agora.

In this case, the suspect was convicted of money laundering. The origin of the cryptocurrencies (from the online drug trade) was concealed by exchanging the bitcoins for euros. These sums of money originated from crime. The court classified the purchase of the cars and luxury goods as acts of concealment, as these were purchased with money originating from the narcotics trade. The virtual money that the accused still had in his possession and the luxury goods were confiscated by the court. Despite the relatively young age of the accused when he committed these offences, he was sentenced to a substantial prison term of three years.

Criminalisation

Money laundering involves the concealment of the origin of criminal money from authorities. Research shows that the use of virtual currencies brings with it a high degree of anonymity, thereby facilitating money laundering

[31] Court of Noord-Holland 10 March 2017, ECLI:NL:RBNHO:2017:1940.

through virtual currency transactions. Yet, as with online drug trafficking, it is important to put money laundering using cryptocurrencies such as bitcoin into perspective. The scale of drug trafficking and money laundering over the internet dwarfs compared to the scale of drug trafficking and money laundering in the physical world (Europol, 2015b). At the same time, research shows that bitcoin is a popular means of payment among cybercriminals (Europol, 2016).

In practice, to provide evidence for money laundering, the public prosecution must prove that the (virtual) money originated from crime. In money laundering cases, software such as 'Chainalysis' is often used to prove that the bitcoins originated from online drug marketplaces. So-called 'money laundering typologies' can also be distinguished which can be useful in proving money laundering. These include an unreasonably high commission for converting bitcoins into euros, the provision of absolute anonymity by the offender to customers and the use of 'bitcoin mixers' (Wegberg, Oerlemans & van Deventer, 2018), which conceal the origin of the bitcoins.

Case law shows that bitcoins are often used in money laundering cases, but it is likely that in the future we will also see convictions using other cryptocurrencies. The purchase of illegal goods on darknet markets, for example, is often also possible with Monero (Oerlemans & van Wegberg, 2019).

The Convention on Cybercrime does not specifically address money laundering, as opposed to other conventions and international treaties. Money laundering regulations can be found in other treaties and EU legislation, such as the Fifth European Anti-Money Laundering Directive.[32] Similar to Section 3.3.2 about the criminalisation of online drug trafficking, we will not go into detail of regulations of other conventions. Here, it suffices to say that the Fifth Directive specifically regulates crypto exchange platforms and crypto wallet services to combat money laundering through virtual currencies. Crypto exchange platforms are platforms where you can exchange virtual currency for other virtual currency (for example, from bitcoin to Ethereum or vice versa) or exchange virtual currency for fiat money (for example, from bitcoin to the euro or vice versa). Crypto wallet services are services that, for example, offer online bitcoin wallets.

[32] EU Directive 2018/843 of 30 May 2018 amending Directive 2015/849 on prevention of the use of the financial system for the purpose of money laundering or terrorist financing.

3.3.4 Online sex offences

The internet has made new forms of sex offences possible, but it also plays a role in facilitating and enabling existing sex offences. For example, the internet facilitates the distribution of child pornography images and videos on a large scale (Jenkins, 2001; Taylor & Quayle, 2006). The internet also facilitates direct remote (sexual) contact between people, which makes new crimes (as discussed further in this section). This section discusses a number of sex offences in which computers and the internet specifically enable the crimes.

3.3.4.1 Child pornography

Child pornography is one of the most common forms of cybercrime. Simply stated, child pornography involves the depiction of sexual behaviour by minors.[33]

On a global level, it is clear that the criminalisation of child pornography has a dynamic character due to changing mentality about sex and minors. The sixties, for instance, were a time of unprecedented openness and sexual freedom and expression, in which sexual contact between adults and children was not rejected outright. In those days, some people bought child pornography in sex shops or through mail orders (Taylor & Quayle, 2003). From the 1980s, a change in mentality took place. The women's movement pointed out the harmful effects of pornographic and child sexual abuse materials. In addition, the police and judiciary pointed out that the production of child pornography often goes hand in hand with child abuse (Kool, 1999). In the 1980s, many states started criminalising child pornography specifically, many with an age limit of persons younger than 16. Many states that ratified the Convention on Cybercrime after 2001 revised upward the age limit for child pornography to 18 years.

Large-scale use of the internet in the 1990s also led to an increase in the distribution and, consequently, the possession of child pornography (Prichard, Watters, & Spiranovic, 2011; Wolak, Finkelhor, & Mitchell, 2011). The widespread availability of child pornography can be expressed in the large number of images that suspects have in their possession. There are cases of child pornography in which offenders possess millions of child pornography

[33] The term 'Child Sexual Abuse Materials' (CSAM) is also often used. In this book, we use the term child pornography, because it is also used in the Convention on Cybercrime and is clearer in legal terms.

images.[34] During the period of 1990 to 2000, there was a shift from physical to digital meeting places for child pornography users and distributors. For example, child pornography was distributed on online forums and peer-to-peer networks (Stol et al., 2008). Child pornography can also be distributed both in a commercial circuit with paying customers and exchanged between child pornography users without payment (Stol et al., 2008).

Van der Bruggen & Blokland explain in their work that the next step is the exchange of child abuse materials in professional networks. On child pornography forums accessible via the dark web (mainly Tor), between thousands to hundreds of thousands of individuals are consciously looking for child pornography (van der Bruggen & Blokland, 2020). These forums not only facilitate the exchange of child abuse materials, but also advice to hide from the eye of law enforcement authorities. In contrast to all other online markets, there is no financial motive involved. Rather, there seems to be a kind of exchange (van der Bruggen & Blokand, 2020).

Members communicate with each other through 'forum threads', series of messages centred around a certain theme, such as the type of material ('boys versus girls', 'hardcore versus softcore', 'teen versus pre-teen', etc.), informative sections (e.g. on computer security techniques and technical shielding, or child abuse) and sections related to forum management where administrators welcome members and explain the house rules (van der Bruggen & Blokland, 2020). Sometimes members with a higher status are granted access to hidden sections of the forum if they provide material, which is often associated with a greater degree of prestige and authority (van der Bruggen & Blokland, 2021).

Case study: distributing child pornography on dark web forums

On 3 March 2020, a Dutch suspect was convicted of participating in a criminal organisation, in which he was active on three child pornography forums.[35] The suspect in this case was 'chief administrator' and the host of two chat rooms. He 'promoted' regular

[34] See for example Court of Rotterdam 9 December 2009, ECLI:NL:RBROT:2009:BK6022 ,Court of The Hague 13 March 2013, ECLI:NL:RBDHA:2013:2872 and Court of Rotterdam 31 March 2017, ECLI:NL:RBROT:2017:2445.

[35] See Court of Overijssel 3 March 2020, ECLI:NL:RBOVE:2020:913.

forum 'visitors' to 'moderator' status if they were noticed positively for a long time. The 'staff' of the chat sites had different ranks with their own chat channels. On these channels people could talk more privately and freely, because outsiders could not read along as easily. The members kept notes of meetings, which later contributed to the evidence against the child pornography users.

The court did not go along with the defence that sharing text and links to child pornography of visitors in the chat channels was not distribution of child pornography. The warning on the chat sites that no child pornography was to be distributed was also not convincing to the judges, because it could be deduced from other evidence that child pornography was actually being distributed. The court sentenced the suspect to three years imprisonment and an obligatory treatment for mental health illnesses.

Criminalisation

In most, if not all jurisdictions worldwide, sexual abuse of minors is criminalised (Schermer et al. 2019, p. 9). Some states specially criminalise (a) sexual activities with minors that did not reach the legal age for sexual activities, (b) when offenders engage in sexual activities with a child where abuse is made of a recognised position of trust, authority or influence over the child (such as a school teacher, priest, or a position within a family), and (c) when abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.[36]

More specifically in relation to child abuse materials, Article 9 of the Convention on Cybercrime criminalises producing, offering, distributing, procuring and possessing child pornography. The term 'child pornography' refers to pornographic material that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; (c) realistic images representing a minor engaged in sexually explicit conduct.

Note that Article 9 does not explicitly criminalise 'accessing child pornography' through streaming videos that can be made available on

[36] See most notably, Art. 18 of the Lanzarote Convention. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

websites. It is then possible to watch child pornography movies online by permanently downloading (and possessing) the material. Therefore, states may need to explicitly criminalise the accessing of child pornography (Gercke, 2011, p. 149).

States can decide themselves whether they set an age limit of 18 years or 16 years (although a large majority of states sets it at 18) and states can decline criminalising the behaviours under points b and c which constitute 'virtual child pornography'.[37] In the Explanatory Memorandum to the Convention on Cybercrime virtual child pornography is further described as: images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct. This includes pictures that are altered, such as morphed images of natural persons, or even generated entirely by the computer.[38]

The problem with virtual child pornography is that no physical abuse of a minor takes place during the production of the material. In the past, the rationale for criminalising child pornography was the damage actually inflicted at the time of the creation of the image and the protection against the circulation of this material. The crime descriptions in most criminal law systems deal with real victims as opposed to 'virtual' victims. However, there are several reasons why criminal liability is also extended to virtual child pornography. These include avoiding evidentiary problems and the fact that the materials can be used to corrupt children, as well as the idea that virtual child pornography may act as a 'stepping stone' for consumers of child pornography, prompting them to move to real child pornography or possibly even sexual abuse (Schermer et al., 2016, p. 28; Strikwerda, 2015).

3.3.4.2 Sexting

The word sexting is a contraction of the words 'sex' and 'texting'. It is an umbrella term for sending, receiving or forwarding sexually oriented messages via mobile phones or other (online) media, such as a computer or tablet (van Berlo & Ploem, 2018). Sexting is common among young people and adolescents (Lievens, 2014). The consequences of sexting need not always be negative or harmful (Gorissen et al., 2020).

Criminalisation

Sexting is usually punishable if the image depicts sexual behaviour by a minor (then it concerns the distribution of child pornography as criminalised in

[37] Art. 9 Convention on Cybercrime.

[38] Explanatory report of the Convention on Cybercrime, para. 101.

Article 9 Convention on Cybercrime). Under certain circumstances, the act can be criminalised when adults use it for stalking (when the stalking is systematic and there is an unlawful and intentional infringement of a person's privacy) (Ten Voorde, 2017).

As mentioned before, sexting is not always harmful for the sexual development of people. In the Netherlands, the Public Prosecution Service does not prosecute consensual sexting among young people. It will prosecute, however, when damage is caused to the depicted minor or when the images were created after deception or threats. For that reason, a distinction is made between three categories of sexting:[39]

- Category I: there are (indications of) commercial elements, pressure, coercion, deception, secret recordings, a dependency relationship, a victim younger than 12 years, a more than limited age difference (five years or more) or a possible other sex offence; if the suspect is 23 years or older, this automatically constitutes Category I.
- Category II: there are indications of motives other than those in Category I; these include bullying, defamation, slander or intimidation.
- Category III: The visual material appears to have been created voluntarily, the persons involved are both minors and there are no aggravating circumstances as described in Categories I and II.

In principle, the Dutch Public Prosecution Service states that criminal law is also not intended for offences that fall under Category III, because this is usually not legally possible or not in the interest of the parties involved to prosecute (Gorissen et al., 2020). Cases of Category I sexting are so serious that prosecution will usually be opted for. Category II sexting cases are also eligible for a conditional dismissal. In these cases, the choice is often made for the dismissal of the case of prosecution for libel or defamation.

3.3.4.3 Grooming

'Grooming' is defined as the online encapsulation of a minor with the intention of committing sexual abuse or producing child pornographic images (Lindenberg & van Dijk, 2016). It often takes place via either online chat or a webcam.

Literature distinguishes different phases that groomers and their victims go through (see in particular O'Connell, 2003). In short, a friendly relationship is usually built up with the victim first before the perpetrator proceeds to

[39] See the Dutch 2016 instruction for prosecuting child pornography offences.

communicate about sexuality. In the meantime, the perpetrator often assesses the risk by asking about the location and number of computer users (Gorissen et al., 2020). In the next phase of exclusivity, the feeling of friendship is strengthened and the relationship is characterised by a strong sense of reciprocity whereby, through mutual respect, communication must remain secret from others. Subsequent communication about sexuality establishes an exclusive relationship of trust and provides the perpetrator with the material with which to put pressure on or blackmail the minor (Gorissen et al., 2020).

Criminalisation

In criminal law, online grooming often represents a form of criminalisation of acts preparatory to 'offline' abuse of children (UNODC, 2013, p. 103). It is often criminalised as a proposal, through information and communication technologies, of an adult meeting a child who has not reached the age of 16 with the intention of engaging in sexual activities.[40]

Grooming is not specifically criminalised in the Convention on Cybercrime. However, when during grooming, the victim is engaged in sexual activities or genitalia are exposed via webcam, this may trigger offences such as child pornography. If payment is involved, provisions regarding child prostitution may apply. Finally, if the perpetrator exposes himself or herself, and masturbates or forces or coerces the victim to do or undergo sexual activities, this may constitute corruption of minors or even sexual assault (Schermer et al., 2016, p. 42).

Case study: 'Sweetie'

Sweetie was a virtual Filipino 10-year-old girl who was deployed by Terres des Hommes in 2013 to generate attention for the problem of webcam sex with minors. About 20,000 men from some 71 countries sought contact with Sweetie. The researchers collected personal details and Facebook data that allowed some 1,000 men to be identified in the ten weeks of the project.[41]

[40] See Art. 18(1)(a) and 20(1)(a) of the Lanarote Convention.

[41] F. Huiskamp, 'Eerste veroordeling na chatten met virtuele lokmeisje Sweetie' ['First time that a man is sentenced for chatting with virtual girl Sweetie'], *NRC Handelsblad*, 21 October 2014.

It can be difficult to prosecute a case like Sweetie for two reasons. The first problem is that since Sweetie is not a real person, states must have criminalised virtual child pornography or sexual abuse with not a real, but 'realistic person'. In addition, perhaps offenders can be prosecuted for grooming, but then there must be acts of a proposal to meet a – not necessarily real – child. This kind of criminal case also challenges the criminal investigation itself, as live webcam performances leave few traces and little evidence that law enforcement can use. Further difficulties arise from the fact that webcam sex tourism often has a trans-border character, which causes jurisdictional conflicts and makes it more difficult to obtain evidence or even launch an investigation (see Schermer et al., 2016; see also Chapter 8).

3.3.4.4 Sextortion

'Sextortion' is a contraction of the words 'sex' and 'extortion' and refers to the use of sexually oriented images as a means of blackmail (Hong et al., 2020; Wolak & Finkelhor, 2011). It is a relatively new phenomenon that is also receiving a lot of attention from society and legislators worldwide (Gaarthuis, 2021).

Sextortion often occurs when someone is first enticed to show or send a relatively innocent nude image, and then these images or webcam recordings are used to coerce that person into performing more – and increasingly more – sexual acts in front of the webcam, with the threat that the images will be distributed via the internet. When, prior to the sextortion, the images or videos were copied from the victim's computer, the accused can of course also be charged with computer hacking and installing malicious software. The difference with unwanted sexting and sextortion is that threats are used to force a victim to do something, even if the distribution of the images never takes place (Wolak et al., 2018).

Case study: Aydin Coban

Aydin Coban, also known as the 'webcam extortionist', gained international notoriety as a suspect after the suicide of 15-year-old Canadian Amanda Todd in 2012. The offender's practices had driven her to such desperation that she decided to end her life. Her YouTube video about this became widely known.[42]

Aydin Coban became a suspect in a Dutch criminal case after Facebook's security department forwarded a report to British law enforcement authorities about a possible child abuser. After some time, British law enforcement authorities informed the Dutch authorities. The offender worked in a sophisticated way. He used many aliases on Facebook to seduce 34 underage women and five adult men, to take nude videos or photos and then to extort them to provide him with new material. In doing so, he posed as an underage boy. Aydin Coban also used images to blackmail masturbating men who engaged in webcam sex with – so they thought – an underage boy. In case of non-payment, the suspect would spread the images among friends and family. He hid his IP address with a 'virtual private network' (VPN) connection (see further Chapter 8) and misused other people's passports to register with the online payment service Skrill. He used the Western Union payment service to withdraw the sums (totalling more than 30,000 euros) he had obtained through webcam extortion.[43]

The Amsterdam Court of Appeal finally sentenced Aydin Coban to 10 years and 243 days in prison for the 'sextortion' of his victims. In 2021 he was extradited to Canada, which wants to prosecute him for the death of Amanda Todd.[44]

[42] See CBC, 'The sextortion of Amanda Todd', 15 November 2013 and Zembla, 'De dood van Amanda Todd' ['The Death of Amanda Todd'], 4 December 2014 (documentary).

[43] Court of Amsterdam 16 March 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, with annotation by J.J. Oerlemans (*Aydin C.* case).

[44] A. Judd, 'Amanda Todd's accused cyberbully, Aydin Coban, appears in B.C. Supreme Court', *Globalnews.ca*, 12 February 2021.

Criminalisation

In the Aydin C. case, the behaviour of Aydin C. was classified as (online) sexual assault, and extortion, because the victims often did not have any way to prevent the offender from distributing the images and therefore felt forced to give in to the perpetrator. Most states will criminalise such behaviour as sexual abuse or extortion.

The Convention on Cybercrime does not specifically criminalise sextortion. However, when a minor is involved in sextortion, child pornography is likely an offence. Under Dutch law, for example, sextortion may be considered as a case of (attempted) 'remote sexual assault'. Note that cyber-dependent crimes may also apply when the offender uses malware to hack into the victims computers in order to obtain more material or put victims under further pressure by copying and threatening to disclose private information.

3.3.4.5 Revenge porn

Revenge porn is the online posting of sexual images or videos with the aim of taking revenge on a person. Perpetrators of revenge porn are often ex-partners who received sexually explicit images at the time of the relationship and disseminate these as revenge for the break-up of the relationship in order to publicly shame or humiliate the victim (Gorissen et al., 2020; McGlynn, Rackley, & Houghton, 2017; Stroud, 2014). Note that the offenders are not always (ex-)partners and that the motive is not necessarily revenge; motivations can also include humiliating the victim, strengthening friendships between offenders, regulating each other's sexual behaviour and increasing one's own popularity (Gorissen et al., 2020).

Finally, we would like to point out here a possible emerging form of revenge porn involving 'fictitious pornography' by means of 'deepfakes'. For example, someone's head is then placed on sexual images of a different person, such as on the body of a pornographic film actor or actress, by use of 'face swapping' (see also Section 3.4).

Criminalisation

Revenge porn may already be criminalised as the offence 'libel', where someone's honour or good name is attacked with the apparent aim of making it public. Van der Hof (2016) explains that this may be the case, for example, when a revenge porn photo of an ex is posted online with accompanying texts via chat, on internet forums or on social media. When minors are involved, crimes such as the distribution of child pornography may be applicable or virtual child pornography when they are morphed pictures or so-called deepfakes (deep fakes will be discussed in Section 3.4.3). Revenge porn may include cyber-dependent crimes, such as the hacking into an online storage system or secretly taking images from a webcam using malware.

States can also explicitly criminalise revenge porn due to the harmful effects. The Convention on Cybercrime does not specifically address revenge porn. States can make it punishable to intentionally and unlawfully make an image that is sexual in nature of a person or to have it at one's disposal, while that person knows or should reasonably suspect that it has been obtained by or as a result of an unlawful act. The publication of revenge porn on the internet, coupled with personal data ('exposing'), can be made punishable if it has been obtained through an unlawful act and the suspect knows that the publication could be detrimental to that person.

3.3.5 Content crimes

The increasing use of social media and user-generated content also led to an increase in crimes with respect to defamation, contempt, threats, incitement to hatred, insult to religious feelings, and so on (Williams & Burnap, 2016; Yar, 2012a). The impact and longevity of (hateful) information can be multiplied when placed on the internet and the content is easily accessible to minors (UNODC, 2013, p. 107).

The Convention on Cybercrime addresses content crimes by criminalising child pornography (see Section 3.3.4.1) and offences related to copyright infringements (in Art. 10). The Convention on Cybercrime obliges party states to take legislative or other measures to criminalise copyright infringements. However, party states have the right to not impose criminal liability in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the party's international obligations set forth in other international treaties on copyright.

States respond to cyber-enabled content crimes in different ways. Oftentimes, harmful content crimes are already criminalised under existing criminal laws. It does not matter whether the behaviour occurs in the physical world or online: it is still illegal. Some authoritarian states, such as China, seek to censor information on websites that 'undermine state interests' or protect its citizens from harmful information. States may require websites, hosting providers or even internet access providers to filter out information beforehand. This clearly endangers the freedom of expression, which is a fundamental right in most states.[45]

Content available on the internet is, in principle, subject to the same human rights regime as traditional media, such as printed matter and speech. To protect these fundamental rights, most states require authorisation of a judge, before data must be removed online. Blocking or filtering out internet content clearly endangers the original idea of a 'free and open internet' that is available worldwide. At the same time, states seek ways to uphold the law in their own territories (see e.g. Glasius & Michaelsen, 2018; Roberts, 2020).

Clearly, there are enforcement issues with regard to cyber-enabled content crimes (as well as with other cybercrimes). The biggest challenge is probably jurisdiction. By hosting information in a different state, it may be difficult to take down the information by law enforcement authorities from another state, since it does not have the jurisdiction to enforce (see further Chapter 8).

Case study: The Pirate Bay

The Pirate Bay is a website, more specifically a search engine, which has an index of Torrent-files. These files are often (copyrighted) music or movies. These files can be downloaded and distributed by using specific software. This software facilitates peer-to-peer (P2P) file sharing among users of the BitTorrent protocol. The case of The Pirate Bay is illustrative of how states may seek to remove information from the internet and how difficult this may be to achieve.

[45] For example, in the case of *Yildirim v. Turkey* (18 December 2012, ECLI:CE:ECHR:2012:1218JUD000311110), the European Court of Human Rights decided that the temporary blockage of YouTube by the State of Turkey was deemed disproportionate and infringed the freedom of expression enshrined in Art. 10 of the European Convention on Human Rights.

The Pirate Bay has been active since 2003 and is still online, although the organisation behind The Pirate Bay is often prosecuted and convicted in many states.[46] The founders and organisation behind The Pirate Bay were often prosecuted or indicted by copyright holders for violating copyright law and money laundering. In 2015, the last remaining founder of The Pirate Bay served a prison sentence.[47] Nowadays, access to The Pirate Bay is forbidden in many countries. For instance, in the Netherlands, internet access providers are obligated to block access to The Pirate Bay by filtering out network traffic.[48] After the court orders, the website often switches website addresses and hosting providers in order to continue operating. The website is still available through proxy or VPN-services, which reroute network traffic (see Chapter 8).

3.4 Future developments

The digitalisation of our lives continues and will also have a continuing impact on crime. It is likely that certain forms of cybercrime will become even more sophisticated in the future. It is also conceivable that new actors will appear on the scene and that new types of cybercrime will arise. In this section, we list the most important developments and their influence on crime.

3.4.1 Increased involvement of state actors

Not just criminals commit cybercrime. When states engage in cyberespionage on foreign territory, they may commit crimes such as hacking and installing malware in order to collect intelligence.[49] Europol warned in their report on internet organised crime that foreign states engage in cyber-attacks, disinformation campaigns and disruption of critical services (iOCTA, 2020,

[46] See e.g. the Wikipedia page on The Pirate Bay. See also the case of *Stichting Brein v. Ziggo B.V. & XS4ALL Internet BV* of the European Court of Justice of 14 June 2017, C-610/15, ECLI:EU:C:2017:456.

[47] Ibid.

[48] See e.g. Court of Appeals of Amsterdam 2 June 2020, ECLI:NL:GHAMS:2020:1421.

[49] See, e.g., R. Gallagher, 'The inside story of how British spies hacked Belgium's largest telco', *The Intercept*, 13 December 2014.

p. 13). In the Netherlands, the Dutch National Cyber Security Centre has been warning since 2019 that state actors pose a greater cybersecurity threat than criminals (NCSC, 2018). Foreign state actors mainly carry out economic digital espionage in the Netherlands on Dutch 'top sectors', such as the high-tech sector (such as a chip manufacturer) and the agricultural sector.

In addition, there are now instances in which ransomware endangers the critical infrastructure of states, such as the already mentioned attack on Colonial Pipelines in the United States (see also Section 3.2.2.1). Similar dangers exist when 'wiper malware' or ransomware infects computers of companies in the energy sector, air flight or traffic control, water management, hospitals, municipalities, and so on. In these instances, states may consider these attacks as 'threats to national security' (NCSC, 2020, 2021). As a result, intelligence and security services enter the 'online arena' and may engage with 'threat actors' (such as other intelligence and security services) in order to disable their infrastructure used for cyber attacks or gather intelligence about their activities. We expect a more prominent role of intelligence and security services in combatting cybercrimes that have serious consequences for states.

3.4.2 The 'internet of things'

Another important contemporary development that will undoubtedly play a role in the future is the so-called 'internet of things'. Devices that are part of the 'internet of things', collect data about their environment, exchange this data through a network and make (semi)autonomous decisions that affect the environment (van Berkel et al., 2017). Examples include devices such as internet cameras, smart cars, smart traffic lights (with sensors such as people counters), smart lights, smart plants (which indicate when they need water), et cetera. Using sensors in the devices, things such as temperature and (air) humidity can be measured.

In recent years, it has already become apparent that many objects are insufficiently secured or that people do not change the default settings. These devices can be hacked and then become part of a botnet used to carry out ddos attacks. In 2016, for example, hundreds of thousands of devices that formed part of the 'Mirai botnet' attacked a large hosting provider, rendering popular services for millions of users such as Twitter, Netflix and CNN inaccessible for some time.[50]

More serious consequences can arise when devices connected to the body, such as an insulin pump or pacemaker, are hacked. In 2013, for example, it became known that then US Vice-President Dick Cheney no longer allowed his pacemaker to be connected via a network for fear that it would be hacked.[51] Slowly an 'Internet of People' is emerging. In the future, digital technologies will increasingly integrate with the human body. Ienca (2015) indicates that in theory it is also possible for personal information such as bank details to be stolen or manipulated by hacking into neurological devices that are connected to people's brains. In this context, he speaks of so-called 'neurocriminals and brain hacking', which will bring stories about popular science fiction literature called 'cyberpunk' into reality (see also Gasson & Koops, 2013).

The next step is for all these devices and people to seamlessly connect and work with each other, creating an 'Internet of Everything'. Performing ddos attacks on networks or infecting devices in networks could then have very serious consequences for the economy, but possibly also for people's health, and can endanger the continuity of vital services.

3.4.3 The use of artificial intelligence by cybercriminals

Many forms of cybercrime, as also mentioned in Chapter 2, are partly automated, which implies that many actions in the criminal process can be performed by machines. The use of artificial intelligence (AI) and machine learning (ML) by cybercriminals can be seen as the next step in the automation of crime. Artificial intelligence does not just involve machines taking over tasks, but machines capable of learning and making decisions on their own (Bostrom, 2014). Security experts and scientists alike indicate that it will not be long before the use of AI by cybercriminals is widespread (Brundage et al., 2018; Goodman, 2015; UNICRI/Interpol, 2018). For example, cybercriminals could integrate AI into malware, make social engineering attacks more sophisticated and personalised (Brundage et al., 2018) and train software to go undetected (Bahnsen et al., 2017).

[50] N. Woolf, 'DDoS attack that disrupted internet was largest of its kind in history, experts say', *The Guardian*, 16 October 2016.

[51] L. Vaas, 'Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking', *Naked Security*, 22 October 2013.

Machine learning techniques are also increasingly used in ‘deep fakes’. Deep fake technology enables “to create audio and video of real people saying and doing things they never said or did” (Chesney & Citron, 2019, p. 1753). This type of technology can have some beneficial use (e.g. in education, art and autonomy), but many harmful uses as well, including causing harm to individuals or organisations (through extortion and sabotage) and harm to society (e.g. through manipulation of elections, eroding trust in institutions and exacerbating social divisions). In the cyberdomain deep fake technology is frequently used to create fake pornographic material for harassment, blackmail and sextortion (Hayward & Maas, 2020). We can expect the use of this technology to become more widespread in the future.

3.5 To conclude

This chapter has explained the main types of cyber-dependent and cyber-enabled crime. You should now be able to understand how these crimes are committed and how they are often criminalised. As we have seen, in practice several offences often occur simultaneously. For example, it is possible to commit fraud after the financial personal data has been taken over by computer hacking and installing malware. It is even possible that the computers of multiple victims are controlled via a botnet and that those involved work together in a criminal partnership. The money earned can then be laundered using bitcoins.

With the knowledge gained in this chapter, you will be able to recognise the modus operandi and possible criminal acts.

3.6 Discussion questions

1. Is it possible to make a clear distinction between cyber-dependent crime and cyber-enabled crime?
2. What are the advantages and disadvantages of reporting vulnerabilities in software? Are ethical hackers sufficiently protected in an international context?
3. After reading this chapter, what do you think of the statement: “The law is too far behind in criminalising cybercrime”?
4. What often explains the divergences in the criminalisation of cybercrime between states?

5. Is it desirable to explicitly criminalise the phenomenon of revenge porn?
6. What do you think of the fact that virtual child pornography has been criminalised?
7. Do we miss certain criminalisations of cyber-dependent of cyber-enabled crime?
8. What are your considerations when doing desk research or 'data science' on investigative data, when the case has not yet been decided by a criminal court?
9. Is it right that cryptocurrencies are not 'real' (fiat) money?
10. Should cryptocurrencies be regulated?
11. Should we allow internet filtering to combat copyright infringements?
12. Should the government do more to combat hate speech on the internet?

3.7 Core concepts

- Banking malware
- Bitcoin
- Botnets
- Computer hacking
- Content crimes
- Critical infrastructures
- Darknet market
- Ddos attack
- Deep fakes
- Digital espionage
- Ethical hacking
- Grooming
- Hacking
- Internet of people
- Internet of things
- Malware
- Money laundering (online)
- Online fraud
- Phishing
- Ransomware
- Revenge porn
- Sexting
- Sextortion
- (Virtual) child pornography

Annex: Relevant provisions of the Convention on Cybercrime

Article of law	Name	Text of Treaty (Convention on Cybercrime)
Article 1	Definition of a 'computer system' and 'computer data'	For the purposes of this Convention: a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
Article 2	Illegal access	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
Article 3	Illegal interception	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.
Article 4	Data interference	1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Article 5	System interference	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Article 6	Misuse of devices	1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being

Article of law	Name	Text of Treaty (Convention on Cybercrime)
		accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 of this article.
Article 7	Computer-related forgery	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.
Article 8	Computer-related fraud	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Article 9	Offences related to child pornography	1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another person; e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term ‘child pornography’ shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit

Article of law	Name	Text of Treaty (Convention on Cybercrime)
		conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term 'minor' shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.
Article 10	Offences related to the infringements of copyright and related rights	1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.