Cybercrime 2.0

Martin Scharenborg

tweede druk

Heruitgave van de Geschiedenis van het WvSr, geschreven door mr. H.J. Schmidt:
1. Geschiedenis van het wetboek van strafrecht (1881-1886), ISBN 9789463426718
2. Geschiedenis van het wetboek van strafrecht (1881-1886), ISBN 9789463426749
3. Geschiedenis van het wetboek van strafrecht (1881-1886), ISBN 9789463426756
4. Geschiedenis van het wetboek van strafrecht (1881-1886), ISBN 9789463426763
5. Geschiedenis van het wetboek van strafrecht (1886-1901), ISBN 9789463426770

Serie geschiedenis van het strafrecht:
1. Geschiedenis van het wetboek van strafrecht (1886-2017), ISBN 9789462546677
2. Geschiedenis van het wetboek van strafrecht (1886-2017), ISBN 9789462546684
3. Geschiedenis van het wetboek van strafrecht (1886-2017), ISBN 9789462546691

Serie fraude en integriteit:
- Onderzoeken van fraude (ISBN 9789463185141)
- Voorkomen van fraude (ISBN 9789463185172)
- Fraude door ambtenaren (ISBN 9789463185271)
- Fraude door werknemers (ISBN 9789463185240)
- Fraude en accountant (ISBN 9789463185325)
- Uitkeringsfraude (ISBN 9789463185011)
- Faillissementsfraude (ISBN 9789463185073)
- Fraude in het strafrecht (ISBN 9789463185301)

Serie tuchtrecht:
- Tuchtrecht voor accountants (ISBN 9789463185905)
- Tuchtrecht voor advocaten (ISBN 9789463185943)
- Tuchtrecht voor gerechtsdeurwaarders (ISBN 9789463185929)
- Tuchtrecht voor notarissen (ISBN 9789463185882)

Serie strafrecht:
- Witwassen (ISBN 9789403625409)
- Afpakken en Ontnemen (ISBN 9789403641584)
- Cybercrime (ISBN 9789403742939)
- Verkeersmisdrijven (ISBN 9789462546707)
- Bewijs in het strafrecht (ISBN 9789463425193)
- Vermogensmisdrijven (ISBN 9789463425827)
- Terrorisme (ISBN 9789463987240)
- Materieel strafrecht (ISBN 9789403634906)
- Overtredingen strafrecht (ISBN 9789403629094)
- Drugsdelicten (ISBN 9789403641577)
- Geweldsmisdrijven (ISBN 9789403629100)
- Zwijgen en verschoning (ISBN 9789403701141)
- Zedenmisdrijven (ISBN 9789403742922)

M. Scharenborg
ISBN: 9789403742939

Voorwoord

Cybercrime vindt dagelijks plaats, en dit gebeurt niet altijd met direct zichtbare schade. Soms is het niet eens merkbaar voor het slachtoffer, maar de gevolgen voor privacy en financiën kunnen aanzienlijk zijn. Cybercrime lijkt vaak ongrijpbaar, mede door de fysieke afstand tussen de crimineel en het slachtoffer. De schade kan variëren van financiële verliezen tot langdurige imagoschade, aangezien informatie op het internet blijft circuleren.
Dit boek richt zich op de strafrechtelijke aspecten van cybercrime, niet op de technische aspecten ervan. Desalniettemin is enige basiskennis van computers en het internet vereist om het motief en de methoden van de cybercrimineel te kunnen begrijpen.
In deze tweede druk zijn de wetgeving en jurisprudentie bijgewerkt en zijn relevante richtlijnen integraal opgenomen. Met de vele wetswijzigingen sinds de invoering van de wetten Computercriminaliteit I, II en III, is ook de regeling inzake verjaring uitgewerkt en zijn oude wetteksten opgenomen, zodat altijd de toepasselijke wetgeving in een zaak geraadpleegd kan worden. Daarnaast zijn ontwikkelingen op het gebied van informatie- en communicatietechnologie (ICT) uitgebreider toegelicht.

De opzet van dit boek is praktisch van aard. Verschillende onderwerpen worden uitgewerkt en voorzien van voorbeelden, jurisprudentie en wet- en regelgeving. Wat betreft de rechtspraak is ervoor gekozen om uitspraken van hoven en de Hoge Raad te gebruiken vanwege hun rechtsvormende karakter. Lezers die de bronnen willen raadplegen kunnen gebruikmaken van de website www.rechtspraak.nl. Voor wat betreft de wetgeving is gebruikgemaakt van de website www.wetten.nl. Hier zijn oude, huidige en toekomstige wetten te vinden. Bovendien kan via de informatieknop bij elk artikel de parlementaire geschiedenis worden geraadpleegd.
Voor dit boek is gebruik gemaakt van eigen werk, waaronder "Geschiedenis van het Wetboek van Strafrecht", "Bewijs in het strafrecht" en "Materieel strafrecht". Allen uit de Serie strafrecht.
Een inhoudelijke opmerking betreft de wijze van citeren in dit boek. In sommige gevallen zijn citaten letterlijk opgenomen, maar vaak zijn teksten geparafraseerd of verkort. Door het raadplegen van vele bronnen werd de taalstijl te divers om alle citaten in volle omvang weer te geven. Het is daarom raadzaam voor de lezer om de oorspronkelijke uitspraken of teksten te raadplegen, die te vinden zijn via de verwijzingen in de voetnoten.
Ten slotte het weergeven van Engelstalige woorden. Deze zijn cursief weergegeven, tenzij het gaat om Engelse namen, Engelse woorden die als Nederlandse woorden zijn vervoegd (zoals "gehackt") en vernederlandste Engelse woorden (zoals creditcard, cybercrime).

Martin Scharenborg, 2024

Inhoudsopgave

Hoofdstuk 1 Algemeen

1.1 Cybercrime/computercriminaliteit

1.1.1 Definitie

Cybercrime, zoals beschreven in het woordenboek Van Dale, verwijst naar computercriminaliteit. Computercriminaliteit wordt gedefinieerd als: “met behulp van computers gepleegde misdrijven”. Dit omvat een scala aan activiteiten, zoals diefstal van gegevens of verspreiding van virussen.[1]
Het Centraal Bureau van de Statistiek (CBS) hanteert een bredere definitie, waarbij cybercrime wordt omschreven als “alle delicten die worden gepleegd met behulp van ICT”[2] ICT staat voor Informatie- en Communicatietechnologie. Dit omvat dus ook misdrijven die niet per se direct gerelateerd zijn aan computers, maar wel gebruik maken van digitale technologieën.
Deze ruime beschrijvingen maken het lastig om strafwetgeving voor cybercrime op te baseren. Daarom is er behoefte aan een nauwkeurige definitie voor computercriminaliteit. Deze kwam er in 2001. Toen werd het eerste internationale verdrag inzake cybercrime opgesteld, het Verdrag van Boedapest.[3] Dit verdrag maakt onderscheid tussen twee vormen van computercriminaliteit: computercriminaliteit in enge zin en in ruime zin.

computercriminaliteit	
computercriminaliteit in enge zin	**computercriminaliteit in ruime zin:**
= alle strafbare gedragingen die gericht zijn tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde processen en middelen.	= strafbare handelingen die zich richten op het verstoren of beïnvloeden van de werking van computersystemen of daarmee onderhouden geautomatiseerde processen.
Voorbeelden: • hacking • (D)dos-aanvallen • virussen	Onder te verdelen in: • elektronische vermogensdelicten (betalingsverkeer, telefoonfraude, afpersing), • inhoudgerelateerde delicten (kinderpornografie, illegale diensten zoals internetcasino's) • delicten op het gebied van intellectuele eigendom en de aantasting van de persoonlijke levenssfeer (spam en cyberstalking).

Onze wetgever heeft het verdrag omgezet naar nationaal recht, maar heeft zich door de taalkundige beschrijving laten inspireren. De definitie van computercriminaliteit zoals opgenomen in de memorie van toelichting van de Wet computercriminaliteit III luidt: "Computercriminaliteit kan worden

1 www.vandale.nl/
2 www.cbs.nl/nl-nl/longread/rapportages/2022/*cyber*securitymonitor-2021/
3 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest van 23 november 2001.

omschreven als het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk."[4]
Deze definitie kan verfijnd worden. Zo is het plegen van strafbare feiten hetzelfde als het plegen van delicten. Daarnaast is het begrip geautomatiseerd werk[5] een juridisch begrip. Het maakt duidelijk dat het meer dan alleen een computer omvat. Taalkundig zou dit vervangen kunnen worden door het begrip ICT. Dan zou het gaan het om de volgende beschrijving:

computercriminaliteit	
doel	**middel**
het plegen van delicten gericht op ICT	het plegen van delicten met behulp van ICT

Een ogenschijnlijk eenvoudige edoch alomvattende definitie. ICT bij hacken wordt beschouwd als het doel, terwijl de ICT bij WhatsApp-fraude wordt gezien als het middel. Dit zorgt voor een heldere scheiding. Echter, de formulering, waarbij het één of het ander is, brengt een probleem met zich mee. Als ICT alleen als doel wordt beschouwd, zou bijvoorbeeld het stelen van een computer ook als computercriminaliteit kunnen worden beschouwd, hoewel dat niet het geval is. Dit probleem doet zich niet voor bij de definitie die de politie hanteert, omdat die iets anders is.[6]

computercriminaliteit	
cybercrime (doel + middel)	**gedigitaliseerde criminaliteit (middel)**
= criminaliteit waarbij ICT zowel het middel als het doelwit is.	= ICT is een middel om (traditionele vormen van) criminaliteit te plegen.
Voorbeelden: hacking, DDos-aanvallen	Voorbeelden: bankhelpdeskfraude, cyberstalking

De interpretatie van de politie is correct, aangezien het stelen van een computer niet wordt beschouwd als cybercrime. Als gevolg van deze classificatie wordt cybercrime gezien als een deelverzameling van computercriminaliteit.

computercriminaliteit = cybercrime + gedigitaliseerde criminaliteit

Dit terwijl taalkundig, alsook in de vertaling van het Cybercrimeverdrag, geldt dat computercriminaliteit een synoniem is van cybercrime.

Dit kan tot verwarring leiden als gesproken wordt over cybercrime. Bijvoorbeeld, dit boek heet cybercrime, maar ook gedigitaliseerde criminaliteit wordt behandeld. Deze keuze is gemaakt omdat de termen 'computercrimi-

4 Tweede Kamer, vergaderjaar 2015–2016, 34 372, nr. 3, pag. 7.

5 Artikel 80sexies Sr: Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.

6 www.politie.nl/binaries/content/assets/politie/onderwerpen/nationaal-dreigingsbeeld/2017/nbd2017-deel-3-h2.pdf

naliteit' en 'gedigitaliseerde criminaliteit' niet ingeburgerd zijn. Nu de verschillen zijn toegelicht, zal in het vervolg van het boek de term cybercrime worden gebruikt als een deelverzameling van computercriminaliteit. Daarom zijn in hoofdstuk 4 de bepalingen met betrekking tot cybercrime uitgewerkt, en in hoofdstuk 5 die van gedigitaliseerde criminaliteit. In gevallen waar beide vormen aan bod komen, zal de term 'computerdelicten' of 'computercriminaliteit' worden gebruikt.

1.1.2 Indeling

Hoewel computercriminaliteit geen specifiek bestanddeel vormt van enige strafbepaling, is het toch van belang om het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit te begrijpen.[7]
Cybercrime omvat technische misdrijven (want doel en middel) zoals computervredebreuk, *bombing* en computervernietiging, terwijl gedigitaliseerde criminaliteit klassieke misdrijven omvat die worden gepleegd met een 'digitaal sausje' (alleen middel).
Het onderscheid tussen deze vormen van criminaliteit is van waarde omdat het zorgt voor een vollediger begrip van strafbaar gedrag. Terwijl specifieke bestanddelen moeten worden bewezen bij cybercrime, zijn de artikelen voor gedigitaliseerde criminaliteit doorgaans algemener van aard, waardoor ze van toepassing kunnen zijn op meer handelingen.[8]
Een juiste definiëring van computercriminaliteit is ook van belang voor statistische doeleinden, zoals bij het Centraal Bureau voor de Statistiek (CBS), dat gegevens bijhoudt over computerdelicten. Afwijkingen tussen de definitie van het CBS en de juridische definitie kunnen resulteren in onjuiste vergelijkingen en evaluaties van de effectiviteit van computerwetgeving door de wetgever.
Voor de politie is een duidelijke afbakening van belang om te bepalen welke eenheid de zaak dient te behandelen. Eenvoudige/kleine zaken worden doorgaans afgehandeld door het basisteam, standaard/middelgrote zaken door de districtsrecherche, terwijl grote/complexe zaken worden toegewezen aan gespecialiseerde eenheden zoals high tech crime-teams.
Tot slot is eenduidigheid van begrippen van belang voor opsporingsdoeleinden. Afwijkingen tussen de definitie van de politie en de juridische definitie kunnen leiden tot problemen bij de vervolging van zaken als men niet eenzelfde begrip gebruikt. In de praktijk zal dit meevallen omdat de definitie van de politie beperkter van omvang is dan de juridische definitie.

---

[7] Zo is het (ruime) begrip fraude niet gedefinieerd, maar het begrip komt wel voor in artikel 273f Sr. De vraag is daar: wat valt onder fraude? Bij computercriminaliteit geldt het omgekeerde: wel een definitie maar niet opgenomen in enig delict.

[8] De brede toepasbaarheid van algemene bepalingen heeft wel grenzen. Zo moesten de delicten verduistering van niet-openbare gegevens en *doxing* ingevoerd worden omdat er vrijspraken volgden voor vervolging wegens (reguliere) diefstal. Gegevens zijn geen goed.

Er bestaat een duidelijk verschil tussen de verschijningsvorm van het computerdelict en het computerdelict zelve. Een verschijningsvorm kan vallen onder meerdere computerdelicten uit het wetboek van strafrecht.
De verschijningsvorm verwijst naar de manier waarop computercriminaliteit zich manifesteert in de maatschappij. In hoofdstuk 3 worden vele vormen beschreven, zoals *sexstortion*, *sexting*, wraakporno, hacking en *bombing*.
Het computerdelict betreft de delictsomschrijving in het wetboek van strafrecht. In hoofdstukken 4 en 5 worden de delicten met betrekking tot computercriminaliteit beschreven.

Enkele voorbeelden van verschijningsvormen die beide aspecten kunnen omvatten zijn de volgende:

vorm	cybercrime	gedigitaliseerde criminaliteit
digitale belaging	hacken sociale media-account om het slachtoffer te belagen	plaatsen apple *air tag* onder de auto en volgen van reisbewegingen
sex-stortion	hacken systeem om het slachtoffer te chanteren met naaktbeelden	afpersen met vrijwillig gemaakte *webcam*-seksbeelden
cyber-pesten	hacken sociale media-account om *fake* berichten te plaatsen als gebruiker	op sociale media beledigende reacties geven op berichten van het slachtoffer
doxing	hacken systeem om de verkregen persoonlijke gegevens te publiceren	de adresgegevens van het slachtoffer publiceren op sociale media
wraak-porno	hacken systeem om naaktbeelden te verspreiden aan vrienden en kennissen.	vrijwillig in de relatie verstrekte naaktbeelden publiceren

.

1.1.3 Computerdelicten

Voor cybercrime moet ICT het doel en middel zijn. De wetgever heeft dit verwerkt in strafwetgeving door in de delictsomschrijving het bestanddeel «geautomatiseerd werk» op te nemen. Deze delicten zijn – in beginsel - cybercrime.

> **toelichting**
> In beginsel omdat enkele artikelen met dit bestanddeel geen cybercrime zijn:
> - er twee definitiebepalingen (artikelen 80sexies en 80quinquies Sr);
> - artikel 139a Sr betreft een strafuitsluitingsgrond;
> - artikel 317, tweede lid, Sr is een geweldsdelict (dreigen *ransomware*, niet uitvoeren);
> - artikel 441a Sr betreft een verbod voor reclamemaken voor hackingapparatuur.

Maar dit bestanddeel is niet het enige dat een delict als een computerdelict classificeert. Door het criterium 'doel/middel' zijn er andere delicten die als computerdelicten geduid kunnen worden. Zo is digitaal kinderlokken een zedendelict maar ook een computerdelict. En *skimming* mag een vermogensdelict zijn, het is ook een computerdelict. Deze delicten kunnen als 'overige computerdelicten' geduid worden.

Los van voorgaande kunnen 'klassieke' delicten, de delicten die niet opgesteld zijn om computercriminaliteit mee aan te pakken, in bepaalde gevallen wel gebruikt worden bij de vervolging van computercriminaliteit. Zo zal *sexstortion* het gevolg kunnen zijn van een hack (artikel 138 ab Sr), maar het afpersen zelf is afdreiging (artikel 318 Sr). En diefstal van een virtueel amulet is strafbaar via artikel 310 Sr. Deze 'klassieke' delicten kunnen geduid worden als gedigitaliseerde criminaliteit (in ruime zin).

Voorgaande leidt tot het volgende overzicht:

computerdelicten		
cybercrime	**gedigitaliseerde criminaliteit**	
	in enge zin	**in ruime zin**
«geautomatiseerd werk»		**'klassieke' delicten**
computervredebreuk (138ab Sr)	verduistering niet-openbare gegevens (138c Sr)	opruiing (131 t/m 134 Sr)
belemmeren toegang/*spam bombing* (138b Sr)	toegang krijgen tot kipo (240b Sr)	discriminatie (137c t/m 137g Sr)
aftappen gegevens/tapapp./ bezit (139c/139d/139e Sr)	digitaal kinderlokken/*grooming* (248e Sr)	zedendelicten (titel 15)
vernielen geautomatiseerde werken (161sexies/septies Sr)	online handelsfraude (326e Sr)	belediging (titel 16)
schenden bedrijfsgeheim (273 Sr)		dwang (248 Sr)
computervernieling, vernieling geautomatiseerd werk, bezit middelen (350a, 350b, 350c, 350d Sr)		bedreiging (285 Sr)
vernieling werken algemene nutte (351/351bis Sr)		belaging ((285b Sr)
overige computerdelicten		diefstal (titel 22)/ verduistering (titel 24)/ begunstiging (titel 30)
vervalsen bankpas (skimming)/bezit apparatuur (232/234 Sr)	heling van niet-openbare gegevens (139g Sr)	afpersing/afdreiging (titel 23)
aftappen medewerker telecom (273d Sr)	139h Sr misbruik seksueel beeldmateriaal (139h Sr)	oplichting (326 Sr)
bedrog d.m.v. telecom (326c Sr)	Identiteitsfraude (231a/231b)	witwassen (titel 30a)
	ontucht minderjarige (248a Sr)	auteurswet
	doxing (285d Sr)	

1.1.4 Drijfveer

1.1.4.1 Overzicht

Er zijn drie belangrijke drijfveren voor het plegen van computerdelicten:[9]

	drijfveren		
	activistisch (hacktivisme)	**psychologisch**	**financieel**
waarom	Inzet ICT om een politiek, maatschappelijk, religieus of levensbeschouwelijk doel te bereiken.	Inzet ICT om een innerlijke behoefte te bevredigen, zoals kwaadheid, zich gekwetst voelen, eenzaamheid, innerlijke stem, seksuele behoefte.	Inzet ICT om financieel voordeel te behalen.
wie	rationeel (groeps)belang	irrationeel (individueel) belang	rationeel (individueel) belang
welke	Denk aan hacking, *spamming*, ddos-aanvallen, *defacing*.	Denk aan *revenge porn, sextortion, cyberbullying, cyberstalking, sexting, doxing.*	Denk aan *cyberpiracy*, cyber-diefstal, *skimming, ransomware*, online handelsfraude.
overlapping	*Defacing* als protestactie: dit bedrijf verkoopt slechte producten.	*Defacing* komt voor als onderdeel van wraakporno: een ex hackt het meta-account en wijzigt de profielfoto met een naaktfoto.	*Defacing* als onderdeel *ransomware:* er worden betalingsinstructies achtergelaten op de gehackte website.
	Doxing kan gebruikt worden om de mening van het slachtoffer te beïnvloeden: werk mee of wordt genageld aan de publieke schandpaal.	*Doxing* als wraak: de ex is kwaad dat de relatie over is en publiceert haar telefoonnummer op een pornosite.	*Doxing* als afpersing: als niet x euro wordt betaald dan worden de adressen van woning, werk en school gepubliceerd op sociale media.
	Cyberpiracy wordt hier gepleegd met de gedachte dat informatie vrij moet zijn (denk aan Wikileaks).	*Cyberpiracy* kan hier gepleegd worden als een gebruiker van het product zich niet goed behandeld voelt en uit wraak illegale kopieën verspreid.	*Cyberpiracy* wordt hier gepleegd om geld te besparen.

Voordat ingegaan wordt op de drie drijfveren moet opgemerkt worden dat het motief niet exclusief te koppelen is aan een computerdelict. In voormelde rubriek 'welke' zijn voorbeelden opgenomen van delicten die normaal gesproken geassocieerd worden met een bepaald motief. Maar, zoals de rubriek 'overlapping' duidelijk maakt, daders van computerdelicten kunnen andere motieven hebben.

[9] In de vorige druk gebruikte ik de indeling technisch – psychologisch – financieel. Maar technische cybercrime is geen motief maar een manier (een 'hoe') om cyberdelicten te plegen. Technische cybercrime komt ook voor bij de andere twee vormen. Daarom is de indeling herzien in voormelde.

Waarom is het belangrijk om de drijfveer (het motief) te begrijpen? Het biedt inzicht. Door het motief van de dader te kennen, kan de dader beter begrepen worden. Als duidelijk is waarom de dader het delict pleegt, wordt ook duidelijk hoe het opsporingsonderzoek moet worden uitgevoerd en hoe de dader het beste kan worden afgestraft.

> **toelichting**
> Bij een financieel motief richt de bewijsgaring zich op de geldstromen van de dader, zoals zijn bankrekeningen en contante aankopen. De afstraffing is gericht op het ontnemen van het wederrechtelijk verkregen voordeel.
> Bij een psychologisch motief wordt de afstraffing gericht op het voorkomen van nieuwe delicten. Er kan psychologisch onderzoek worden uitgevoerd, en als het indammen van de risico's niet goed mogelijk is, kunnen alternatieven zoals de tbs-maatregel worden onderzocht.
> Bij een activistisch motief kan het van belang zijn om de reclassering in kaart te laten brengen hoe het recidiverisico verlaagd kan worden. Denk aan een contactverbod voor foute vrienden, een gebiedsverbod voor foute plaatsen en/of het aanleggen van een elektronische enkelband ter controle.

.

1.1.4.2 Activistisch

De eerste drijfveer wordt geduid als activistisch en wordt ook wel hacktivisme genoemd. Hacktivisme is “het gebruik van computergebaseerde technieken zoals hacken als een vorm van burgerlijke ongehoorzaamheid om een politieke agenda of sociale verandering te bevorderen. Met wortels in de hackercultuur en de hackerethiek, houden de doelen ervan vaak verband met de vrijheid van meningsuiting, de mensenrechten of de vrijheid van informatieverkeer.”[10]

> **voorbeelden**
> Een hacker die velen kennen (vooral zij die in de jaren 80 naar de bioscoop zijn geweest) is Kevin Mitnick. De film Wargames is op hem gebaseerd. Hij was degene die in 1982 Norad hackte. Mitnick hackte 'alles wat los en vast zat', maar verdiende nooit geld aan zijn hacks. Hij was een *gray hat* hacker.[11]
>
> Een groepering van hackers die (vermeende) misstanden aanpakken is Anonymous. Onder de naam *Operation Payback* vielen zij de website van PayPal aan toen die weigerde nog langer donaties voor WikiLeaks te verwerken. Dit nadat WikiLeaks geheime informatie op de website gepubliceerd had.[12]

Het doel van hacktivisme is het veranderen van de status quo, vaak in samenwerking met anderen (zoals Anonymous), maar het kan ook individueel worden uitgevoerd (zoals in het geval van Kevin Mitnick). Dus, de 'wie' verwijst hier niet naar de uitvoerder van de hack, maar naar het doel van de actie. De hacktivist dient hierbij de groep waarvan hij vindt of voelt dat hij deel uitmaakt. Een individuele hacker kan bijvoorbeeld een website hacken

10 www.en.wikipedia.org/wiki/Hacktivism
11 www.wired.com/2008/07/ff-wargames/
12 www.en.wikipedia.org/wiki/Operation_Payback

en de gestolen informatie delen omdat hij van mening is dat er een algemeen belang is bij vrije informatiedeling.

> **voorbeeld**
> Chelsea Manning werd veroordeeld voor schending van de Spionagewet omdat zij bijna 750.000 geheime of gevoelige militaire en diplomatieke documenten met WikiLeaks heeft gedeeld.[13]

Dit betekent niet dat elke hacker een hacktivist is. Een internettrol die een website hackt om te 'defacen' handelt niet activistisch. Hij wordt psychologisch gedreven, waarbij hij een individueel en irrationeel belang dient, de wens om chaos te veroorzaken. Als een hacker daarentegen data steelt om deze te verkopen, dient hij een rationeel eigen belang. Dit is een financieel motief en geen activistisch motief.

> **voorbeeld**
> Doxing kan alle drie de drijfveren omvatten:
> Activistisch: Een voorbeeld hiervan is toen het weekblad Bluf! de woonadressen van hoge ambtenaren plaatste in het weekblad omdat de redactie van het weekblad (een krakersblad) zich verzette tegen de politiek.
> Financieel: Iemand kan dreigen met het openbaar maken van verkregen persoonsgegevens tenzij er een betaling wordt gedaan.
> Psychologisch: Het openbaar maken van persoonsgegevens kan wraak zijn van een expartner omdat die het niet eens is met de relatiebreuk.

1.1.4.3 Psychologisch

De tweede drijfveer is psychologisch van aard. Dit betekent dat het individu handelt vanuit een irrationeel individueel belang, wat wil zeggen dat het strijdig is met het gezonde verstand.[14] Hierbij tracht iemand zijn eigen innerlijke drang te bevredigen.

Internettrollen vallen onder deze categorie. Dit zijn individuen, vaak tieners, die vanwege de anonimiteit op het internet normen in de maatschappij schenden, aangezien er voor hen nauwelijks sociale gevolgen zijn. Zij gaan doelbewust conflicten aan op sociale media om reacties uit te lokken, wat kan worden gezien als het creëren van sociale onrust. Het empathisch vermogen van trollen is vaak beperkt.

> **toelichting**
> Internettrollen zijn van een andere orde dan trollenfabrieken. De eerste groep bestaat uit individuen die alleen chaos willen veroorzaken. De tweede groep zijn betaalde medewerkers die in grote ruimtes de hele dag samenwerken met tientallen andere trollen om het belang van hun werkgever te dienen, meestal een staat. Het motief van deze werknemers is financieel, niet psychologisch.
> Rusland heeft trollenfabrieken om de westerse maatschappij te polariseren. Hier wordt een koude digitale oorlog uitgevochten (= *cyberwarfare*).

---

13 www.en.wikipedia.org/wiki/Chelsea_Manning

14 www.vandale.nl/gratis-woordenboek/nederlands/betekenis/irrationeel

> Er zijn meer landen met trollenfabrieken, zoals Saoedi-Arabië. Daar gaat het om propaganda. Zij overstelpen sociale media met positieve berichtgeving om negatieve berichten digitaal te begraven. Daarnaast proberen zij de toon op sociale media te sturen, met een activistisch doel.

Pedofielen die kinderporno downloaden vallen ook onder deze categorie. Zij kunnen in groepen samenwerken, zoals op uitwisselingssites op het *dark web*, maar de geestelijke kriebel die zij willen bevredigen is individueel van aard en irrationeel.

1.1.4.4 Financieel

De derde drijfveer is financieel van aard. Hierbij wordt een rationeel individueel belang nagestreefd: de cybercrimineel streeft ernaar om rijk te worden ten koste van het slachtoffer dat hem geld gaat geven. Het overgrote deel van computerdelicten valt binnen deze categorie. Denk hierbij aan *ransomware*, *exit scams* en marktplaatsfraude.

Ook hier geldt dat de fraudeur kan samenwerken met anderen, maar het belang dat hij dient is van hemzelf. Hij wil financieel gewin behalen.

1.2 Cyberspace

1.2.1 Overzicht

Nu duidelijk is wat computerdelicten zijn moet geduid worden hoe dit zich verhoudt tot andere activiteiten in *cyberspace*.

cyberspace[15]				
cybercrime[16]	***cyberactivism***	***cyberspying***	***cyberwarfare***	***cyberterrorism***
= delicten waarbij ICT doel en/of middel is	= gebruik van op internet gebaseerde socialisatie- en communicatietechnieken om (elk soort) activisme te creëren, exploiteren en beheren.	= infiltreren van systeem of database om geheime of bedrijfseigen informatie te stelen die wordt gebruikt door overheids- of particuliere organisaties.	= gebruik van cyberaanvallen tegen een vijandige staat, waarbij schade wordt toegebracht aan vitale computersysteem.	= ontwrichtende aanvallen op informatiesystemen met als primair doel het veroorzaken van alarm, paniek of fysieke ontwrichting.
• burgers • bedrijven • Staat (immuun)	• burgers • bedrijven • Staat (propaganda)	• bedrijven • buitenlandse Staat	• buitenlandse Staat	• buitenlandse Staat • terroristen

Dit boek gaat het over cybercrime, maar dit laat onverlet dat andere acties in *cyberspace* kunnen worden aangemerkt als computerdelicten als daarbij artikelen in het wetboek van strafrecht worden geschonden.

1.2.2 Cybercrime

Computerdelicten zijn strafrechtelijke zaken waarbij burgers of bedrijven[17] betrokken zijn en die het openbaar ministerie kan vervolgen. In sommige gevallen kan zelfs de staat worden beschuldigd van strafbare feiten, maar vanwege immuniteit is vervolging van de staat in beginsel niet mogelijk.[18]

> **voorbeeld**
> In 2023 oordeelde de Amerikaanse *Foreign Intelligence Surveillance Court* dat de FBI gedurende meerdere jaren maar liefst 278.000 keer ten onrechte informatie had gezocht in een Amerikaanse database van buitenlandse inlichtingen.[19]

15 Zie ook *Cyberwarfare and Cyberterrorism: In Brief* van het *Congressional Research Service;* www.sgp.fas.org/crs/ natsec/R43955.pdf; www.en.wikipedia.org/wiki/Cyberterrorism# en *cyberwarfare; www.techopedia.com/definition/27973/cyberactivism; www.makeuseof.com/what-are-cyberwarfare-cyberterrorism-and-cyberespionage/*

16 Bedoeld wordt de Engelse term voor computercriminaliteit, dit omvat ook gedigitaliseerde criminaliteit.

17 Hiermee worden alle vormen van samenwerkingverbanden bedoeld, ook organisaties, ondernemingen e.d.

18 Hierop geldt een uitzondering maar dat voert te ver om in een boek over *cybercrime* toe te lichten. Daarvoor wordt verwezen naar het boek Materiaal strafrecht uit dezelfde serie.

19 www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/

De nationaliteit van de dader heeft geen invloed op de strafbaarheid van het delict, zolang het delict hier ten lande land is gepleegd. Echter, de nationaliteit kan het onderzoek en de vervolging van het delict wel complex of zelfs onmogelijk maken.

1.2.3 Cyberactivisme

Aangezien geografische grenzen in *cyberspace* irrelevant zijn, kan het verzet afkomstig zijn van burgers uit alle delen van de wereld. Dit verzet manifesteert zich vaak via sociale mediaplatforms, waarbij het snel viraal kan gaan en tijdelijk de online wereld domineert. Soms resulteert dit online verzet ook in acties in de fysieke wereld.

> **voorbeeld**
> De #metoo-beweging begon in 2017 met een artikel in het tijdschrift The New Yorker waarin filmproducent Harvey Weinstein werd beschuldigd van het seksueel misbruiken van actrices (hij is veroordeeld tot 23 jaar gevangenisstraf in New York en 16 jaar in Los Angeles). Deze beschuldigingen leidden tot talloze berichten op sociale media die viraal gingen en wereldwijd protesten veroorzaakten tegen het misbruik van vrouwen. Deze beweging had ook invloed op de strafwetgeving in Nederland, wat resulteerde in de totstandkoming van de nieuwe Wet seksuele misdrijven.

Zolang de actievoerders binnen de grenzen van de grondrechten blijven, blijft deze vorm van verstoring in *cyberspace* in principe ongestraft. Gaat men te ver met protesteren, dan kan het strafbaar worden. Dit geldt zowel voor de fysieke wereld als voor de digitale wereld. In het laatste geval kan het om computercriminaliteit gaan. Hoewel er nog steeds een algemeen belang kan zijn, is dit dan ondergeschikt aan het strafbare handelen. Bij de strafmaat kan clementie worden getoond door bijvoorbeeld een voorwaardelijke straf op te leggen of artikel 9a van het Wetboek van Strafrecht toe te passen.

> **voorbeeld**
> In 2014 heeft Denemarken bestialiteit strafbaar gesteld. Voor die tijd waren er in het land dierenbordelen waar sekstoeristen naartoe kwamen. De minister van Voedsel en Landbouw gaf aan dat de schade die aan de reputatie van Denemarken werd toegebracht door het toestaan van seks met dieren een factor was in zijn beslissing.
> Wat bracht de regering ertoe om dit te verbieden? Hackers werkten samen met dierenactiegroepen en haalden zo'n 20 websites over bestialiteit uit de lucht. Vervolgens werd dit gedeeld op Twitter en werden foto's van wreed mishandelde honden verspreid.[20] Uiteindelijk veranderde de publieke opinie: seks met dieren moest verboden worden. Het illegale protest bleek effectief.

De staat kan ook gebruik maken van cyberactivisme. Rusland heeft bijvoorbeeld trollenlegers om buitenlandse democratieën te ondermijnen. Dit kan worden beschouwd als een aanval op een andere staat, een vorm van cyberoorlogvoering (*cyberwarfare*). Maar sommige landen hebben trollen-

[20] www.mirror.co.uk/news/technology-science/technology/anti-bestiality-*hackers*-target-vile-dog-5310038; www.independent.co.uk/news/weird-news/denmark-moves-to-ban-bestiality-controversial-right-to-have-sex-with-animals-will-be-outlawed-9790829.html?loadcomments=true

legers om critici het zwijgen op te leggen en propaganda te verspreiden, gericht tegen de eigen bevolking.

> **voorbeeld**
> In een trollenfabriek in Riyaad, Saoedi-Arabië, werken honderden mensen die door de staat worden betaald. Hun taak is om protesteerders via sociale media te trollen. Deze groep staat bekend als *The Flies*. Journalist van The Washington Post, Khashoggi, gebruikte de methoden van deze groep tegen hen. Samen met duizenden anderen noemden zij zichzelf *The Bees* en gingen ze in de aanval tegen de propaganda van de staat. De journalist tweette: *"The bees are coming."* Ongeveer twee weken na dit bericht werd hij vermoord in de Saoedische ambassade in Turkije. [21]

1.2.4 Cyberspying

Er zijn twee soorten spionnen: de staatsspion en de bedrijfsspion.
De bedrijfsspion steelt bedrijfsinformatie in opdracht van een concurrerend bedrijf. Dit kan variëren van receptuur en technische beschrijvingen tot prototypes.
Een staatsspion kan soortgelijke activiteiten uitvoeren. Bijvoorbeeld, ASML beschuldigde een Chinese werknemer ervan bedrijfsdata te hebben gestolen. Een ander voorbeeld is Noord-Korea, dat Sony hackte en bedrijfsdata stal als wraak voor de film "*The Interview*".[22]

> **voorbeeld**
> De VN voerde een onderzoek uit naar Noord-Korea, waarbij werd vastgesteld dat zij achter 58 cyberaanvallen zaten waarbij 3 miljard dollar aan cryptomunten werd gestolen door de Lazarus Group. Deze hackersgroep wordt geassocieerd met het Noord-Koreaanse leger. De motivering voor de hacks lijkt gerelateerd te zijn aan de financiering van hun raketprogramma's.[23]

Bedrijfsspionage wordt vaak beschouwd als een neventaak voor inlichtingendiensten. De primaire taak van staatsspionnen is het verzamelen van inlichtingen over buitenlandse staten op het gebied van defensie, veiligheid en politiek.

> **voorbeeld**
> Russische hackers zijn Nederland uitgezet wegens hun betrokkenheid bij het hacken van de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag. Deze poging tot hacken werd verijdeld door de militaire inlichtingendienst MIVD. De hackers achter de aanval werden geïdentificeerd als gelieerd aan de Russische overheid.[24]

Een andere belangrijke taak van staatsspionnen is sabotage. Een bekend voorbeeld hiervan is het loslaten van het Stuxnet-virus.

---

21 www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html
22 www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack
23 www.nl.beincrypto.com/markten/deze-natie-stal-miljard-crypto/
24 www.nu.nl/*internet*/5507720/kaspersky-veel-meer-buitenlandse-overheids*hackers*-in-nederland-actief.html

voorbeeld
Het Stuxnet-virus is een vorm van *malware*, specifiek een worm, die opzettelijk ontworpen was om de werking van Iraanse ultracentrifuges te verstoren. Hierdoor raakten de motoren beschadigd en functioneerde zij niet meer naar behoren. De worm werd verspreid met als doel het nucleaire programma van Iran te saboteren. Het feit dat het virus voornamelijk in Iran werd aangetroffen, waarbij 58% van de computers besmet was, suggereert dat het specifiek gericht was op Iran. Andere landen, zoals Indonesië en India, werden in mindere mate getroffen, met respectievelijk 18% en 8% van de besmette computers.[25]

De strafbaarstelling van spionage wordt behandeld in het wetboek van strafrecht. Echter, bij de vervolging van spionage kunnen complicaties ontstaan, afhankelijk van de diplomatieke status van de spion en eventuele politieke kwesties die ermee gemoeid zijn. Hoewel strikt genomen politieke factoren de vervolging niet zouden moeten beïnvloeden, aangezien politiek en rechtspraak gescheiden zouden moeten zijn, is de praktijk weerbarstig. .

voorbeeld
Khan was een Pakistaanse atoomgeleerde die in de jaren zeventig werkzaam was bij het Almelose bedrijf Urenco, dat verrijkt uranium produceerde met behulp van ultracentrifugetechnologie. Dit verrijkte uranium is zowel nodig voor kernenergie als voor de productie van atoombommen. Khan stal atoomgeheimen bij het bedrijf, wat leidde tot de ontwikkeling van een atoombom door Pakistan. Later volgden ook China, Noord-Korea en Iran was op weg, allemaal mede dankzij Pakistan. Dit alles gebeurde met medeweten van Amerika...
Na het stelen van de atoomgeheimen vluchtte Khan uit Nederland. Hij werd vervolgd en in eerste aanleg bij verstek veroordeeld tot vier jaren gevangenisstraf. Echter, het hof vernietigde de dagvaarding wegens een vormfout en het openbaar ministerie koos ervoor om niet opnieuw te dagvaarden. Khan hoefde dus niet de cel in van Nederland.
Later bleek dat er al drie meldingen over spionage door Khan waren gedaan door een medewerker bij Urenco, waardoor hij eerder had kunnen worden aangehouden voordat de situatie escaleerde. Oud-premier Van Agt verklaarde bij VPRO-radio dat "de Amerikaanse inlichtingendienst er de voorkeur aan gaf om de man niet vast te zetten, maar te volgen". Hierdoor werd niet tijdig ingegrepen omdat Amerika Pakistan te vriend wilde houden, zonder te voorzien dat de atoomkennis zou worden doorgespeeld naar andere landen dan Pakistan.[26]

Er komt een wetswijziging aan om verschillende vormen van spionage beter aan te pakken: de Wet uitbreiding strafbaarheid spionageactiviteiten.

wetgever
"Over het algemeen wordt bij «spionage» gedacht aan het heimelijk of onrechtmatig vergaren van (gevoelige) informatie of objecten door, of in opdracht van een buitenlandse mogendheid. Er zijn echter ook andere gedragingen die in verband kunnen worden gebracht met spionage (hierna: spionageactiviteiten), zoals sabotage, het interveniëren in (besluitvormings)processen of beïnvloeding van personen. Spionageactiviteiten kunnen zich zowel richten op overheden en volkenrechtelijke organisaties als op bijvoorbeeld bedrijven en universiteiten. Steeds vaker worden daarbij ook digitale en andere technische middelen ingezet."[27]

25 www.nl.wikipedia.org/wiki/Stuxnet

26 www.clingendael.org/nl/publicatie/nieuwe-lagen-verhaal-pakistaanse-atoomspion-khan; nl.wikipedia.org/wiki/Abdul_Qadir_Khan

27 Tweede Kamer, vergaderjaar 2022–2023, 36 280, nr. 2, pag. 1-2

Een van de voorgestelde maatregelen is de invoering van artikel 98d Sr.

Artikel 98d Sr [voorstel]
1. Met een gevangenisstraf van ten hoogste acht jaar of geldboete van de vijfde categorie wordt gestraft hij die, wetende dat daarvan gevaar is te duchten voor de veiligheid van de staat, van zijn bondgenoten of van een volkenrechtelijke organisatie, voor de vitale infrastructuur, voor de integriteit en exclusiviteit van hoogwaardige technologieën, of voor de veiligheid van een of meer personen, opzettelijk in heimelijke betrokkenheid met een buitenlandse mogendheid 1°. schadetoebrengende handelingen verricht ten behoeve van die buitenlandse mogendheid; of 2°. aan die buitenlandse mogendheid onmiddellijk of middellijk inlichtingen, een voorwerp of gegevens verstrekt.
2. Met dezelfde straf wordt gestraft hij die een ander beweegt tot de in het eerste lid bedoelde handelingen.

Dit artikel valt niet onder computercriminaliteit maar onder staatsveiligheid. Dit wordt verder niet behandeld in dit boek.

1.2.5 Cyberwarfare

In een oorlog kan een land in *cyberspace* een aanval uitvoeren op een ander land. Cybereenheden van het leger kunnen daardoor de digitale infrastructuur van de vijand platleggen. Het leger kan ook de ''klassieke' eenheden inzetten voor de *cyberwar*. Denk aan het neerhalen van gps-satellieten met raketten of het tot ontploffing brengen van een atoombom in de ruimte om de elektronica van satellieten te verstoren met een elektromagnetische impuls. Dit valt onder het oorlogsrecht en wordt verder niet behandeld.
De grens tussen cyberspionage en cyberoorlogvoering is soms vaag, vooral als het gaat om sabotage. Wat het ene land aanmerkt als spionage, kan door het andere land worden beschouwd als een daad van oorlog.

> **voorbeeld**
> Brigade-generaal Ducheine vroeg zich af of het gebruik van het *Stuxnet*-virus gezien moest worden als een inbreuk op het geweldsverbod van art. 2(4) VN-Handvest. En zo ja, kon Iran dit dan aanmerken als een 'gewapende aanval' uit artikel 51 VN-Handvest en zich beroepen op zelfverdediging als rechtsbasis voor een reactie?
> Hoewel internationale experts het eens waren dat het *Stuxnet*-virus een vorm van geweldgebruik (art. 2(4) VN-Handvest) was, typeerde een minderheid van de groep deskundigen de inzet ervan (dat tot fysieke schade aan de Iraanse nucleaire opwerkingsfaciliteiten leidde) als een gewapende aanval (art. 51 VN-Handvest).[28]

Een vorm van *cyberwarfare* is *psyops (psychological operations).*[29] Het is al lange tijd bekend dat Rusland trollenfabrieken inzet om democratieën te ondermijnen, hetgeen een vorm van psychologische (koude) digitale oorlogsvoering is.

---

28 www.puc.overheid.nl/mrt/doc/PUC_68346_11/1/

29 Dit zijn"operaties om geselecteerde informatie en indicatoren aan het publiek over te brengen om hun motieven en objectieve redeneringen, en uiteindelijk het gedrag van regeringen, organisaties, groepen en grote buitenlandse machten, te beïnvloeden.";www.en.wikipedia.org/wiki/Psychological_operations_(United_States)

voorbeeld
Het centrum van het Russische trollenleger bevindt zich in Sint-Petersburg. De trollen opereren met name op sociale media en reageren op berichten op websites. Zij zaaien onrust met als doel polarisatie en verdeeldheid in de samenleving te veroorzaken. In reactie op gepubliceerd onderzoek hierover verklaarde de voormalige Britse premier Truss: "We zullen nauw samen blijven werken met bondgenoten en mediaplatforms om de Russische informatieoperaties te ondermijnen."[30]

1.2.6 Cyberterrorisme

Het is evident dat terroristen streven naar het zaaien van angst en daarbij *cyberspace* kunnen misbruiken. Het uitschakelen van luchtverkeersleiding, het verstoren van de beurzen, of het saboteren van kerncentrales behoren tot de (potentiële) mogelijkheden. In al deze gevallen gaat het om het hinderen van de toegang tot of het gebruik van een geautomatiseerd systeem, of om de vernietiging ervan.
Dergelijke handelingen zijn strafbaar gesteld in artikelen 138b, 161sexies en 350 tot en met 351 van het wetboek van strafrecht. Bij deze delicten zijn er strafverzwarende bepalingen van toepassing wanneer er sprake is van de voorbereiding van een «terroristisch misdrijf» of wanneer het delict wordt gepleegd met een «terroristisch oogmerk». Deze specifieke elementen worden niet verder behandeld in dit boek. Voor meer informatie hierover wordt verwezen naar het boek 'Terrorisme' uit de Serie strafrecht.

Het label "digitaal terrorisme" wordt vaak te snel toegepast op internetacties, terwijl hiervan bijna nooit sprake is. Bijvoorbeeld, *ransomware* die bestanden van een bedrijf of ziekenhuis versleutelt, kan niet worden beschouwd als digitaal terrorisme. Het betreft hier criminele activiteiten, zoals hacking en afpersing, waarbij het doel is om geld te verdienen door middel van computercriminaliteit. Er is geen intentie om maatschappelijke terreur te zaaien. Hoewel dit als gevolg kan hebben dat maatschappelijke onrust ontstaat, nemen de daders dit risico misschien wel op de koop toe, maar dat is voorwaardelijke opzet. Voor terrorisme is «terroristisch oogmerk» vereist.

voorbeeld
In 2021 werd de *Colonial Pipeline* het doelwit van een cyberaanval, wat resulteerde in verstoring van de oliedistributie in de Verenigde Staten. Deze pijpleiding transporteert 45% van de olie aan de oostkust. Als reactie op de aanval moest de pijplijn worden stilgelegd, wat leidde tot een *rush* op benzinestations doordat veel mensen hun tanks wilden vullen. Uiteindelijk betaalde het bedrijf 5 miljoen *dollar* aan bitcoins.[31]
Het primaire doel van deze aanval was afpersing, niet het ontwrichten van de economische structuur van het land (zoals vereist in artikel 83a Sr). Hoewel de gevolgen van de aanval zo ernstig kunnen zijn dat het ontwrichting tot gevolg heeft bij niet-betaling, is dit eerder het op de koop toenemen van dit gevolg (= voorwaardelijk opzet) en niet oogmerk daartoe. De aanvallers wilden geen ontwrichting, maar enkel geld verkrijgen en dreigden met ontwrichting om dit doel te bereiken (een financieel doel, geen terroristisch doel).

30 www.rtlnieuws.nl/tech/artikel/5305529/rusland-nepnieuws-russische-trollen
31 www.dataconomy.com/2022/06/17/what-is-cyberterrorism/

1.3 Cijfers

Het Centraal Bureau voor de Statistiek hanteert een breed begrip van computercriminaliteit, zoals beschreven in paragraaf 1.1.1. Toch houdt het bureau geen specifieke gegevens bij over de verschillende soorten computercriminaliteit. Alleen voor computervredebreuk, ook wel bekend als hacking, worden cijfers bijgehouden.

	2015	2016	2017	2018	2019	2020	2021	2022	2023
computervredebreuk	2.225	1.875	2.320	2.945	4.865	11.270	14.645	14.165	12180
opgehelderd	165	170	185	390	380	1.010	1.110	695	385
opgehelderd (%)	7,4%	9,1%	8,0%	13,2%	7,8%	9,0%	7,6%	4,9%	3,2%

Bron: Cbs

Wat opvalt is de aanzienlijke toename van het aantal computerinbraken, evenals het zeer lage oplossingspercentage. Terwijl het oplossingspercentage in eerdere jaren rond de 10% lag, is het nu gedaald tot onder de 5%.

Uit de cijfers blijkt niet waarom het oplossingspercentage zo laag is. Het is aannemelijk dat beperkte capaciteit bij de politie hier een rol in speelt, gezien de sterke stijging van het aantal zaken. Basisteams zijn zelden uitgerust om hackingszaken aan te pakken, en zelfs voor veel rechercheteams kan dit een uitdaging zijn. Hoewel er speciale teams voor *high tech crime* zijn opgericht, is het aantal van 14.000 zaken dat zij moeten behandelen simpelweg te veel.
Het is voorzienbaar dat deze situatie nog erger zal worden. De maatschappij wordt steeds verder gedigitaliseerd en mensen worden op steeds jongere leeftijd vertrouwd met ICT. Bovendien worden *hackingtools* steeds meer gestandaardiseerd. Waar een hacker vroeger een technisch onderlegde programmeur moest zijn, kan tegenwoordig een *script kiddie* eenvoudig kant-en-klare pakketten van het *dark web* downloaden en gebruiken: *plug and play* (bij *malware* ook wel genoemd: *plug and pray*).

1.4 Werking computers

1.4.1 De computer

1.4.1.1 Algemeen

Om een goed begrip te krijgen van computercriminaliteit is basale kennis van ICT essentieel. Men moet begrijpen hoe een computer werkt, hoe software functioneert en welke mogelijkheden een crimineel heeft. In deze paragraaf wordt in grote lijnen uitgelegd wat hardware en software inhouden. De volgende paragraaf zal ingaan hoe deze kennis kan worden misbruikt.

Een computer bestaat uit twee hoofdcomponenten: hardware en software. De hardware voert taken uit, terwijl de software instructies geeft aan de hardware. Dit betekent dat een hacker kan proberen direct invloed uit te oefenen op de hardware, maar het is doorgaans eenvoudiger om zich te richten op de software, aangezien dat bepaalt hoe de hardware functioneert.
Met inachtneming van zowel oude als nieuwe ontwikkelingen kan de structuur van een computer als volgt worden weergegeven:

<table>
<tr><th colspan="5">computer
[opdrachten worden achter elkaar uitgevoerd]</th></tr>
<tr><th>[verleden]
analoog</th><th colspan="3">[heden]
digitaal</th><th>[toekomst]
organisch</th></tr>
<tr><td></td><td></td><td>software</td><td>hardware</td><td>wetware[32]</td></tr>
<tr><td>systeem</td><td>applicaties</td><td>malware</td><td rowspan="2">– moederbord
– intern geheugen
– BIOS
– videokaart
– extern geheugen
– muis
– toetsenbord,
– monitor</td><td rowspan="2">Maakt gebruik van levende neuronen in organismen, zoals schimmels (vandaar ook de naam mushroom computers)
=> experimenteel [toekomst]</td></tr>
<tr><td>– besturing-systeem
– drivers
– utilities</td><td>– tekstverwerker
– fotobewerking
– e-mail
– browser
– mp3-speler
– filmspeler</td><td>– virussen
– spam
– ransomware</td></tr>
<tr><td colspan="3">nieuw</td><td colspan="2" rowspan="2">Met organisch [in de zin van heden] wordt ook de interface tussen levend wezen (wetware) en computer (hardware) bedoeld.</td></tr>
<tr><td colspan="3">- metaverse
- artificial intelligence: chat GPT 5, Midjourney
- internet of things</td></tr>
<tr><td colspan="3"></td><td>buiten het lichaam</td><td>in het lichaam</td></tr>
<tr><td colspan="3"></td><td>- exoskeleton
- Apple Vision</td><td>- pacemaker
- neurolink</td></tr>
</table>

↓

kwantumcomputer [opdrachten worden parallel uitgevoerd]
[toekomst]

[32] Zie ook www.interestingengineering.com/science/what-are-mushroom-computers

1.4.1.2 Computer vs. kwantumcomputer

Er zijn twee soorten computers te onderscheiden op basis van de manier waarop ze opdrachten verwerken: de normale computer en de kwantumcomputer.

De normale computer maakt gebruik van binaire code, die wordt gevormd door eentjes en nulletjes (bits). Acht bits vormen samen 1 byte. Elke byte vertegenwoordigt een teken of letter. Bijvoorbeeld, 01000001 staat voor de hoofdletter A en 01100001 staat voor de kleine letter a. Belangrijk om op te merken is dat de computer deze code sequentieel leest en uitvoert, oftewel in een volgtijdelijke volgorde.

> **toelichting**
> Elke bit kan de waarde 1 of 0 hebben, wat betekent dat er bij één bit twee mogelijke combinaties zijn (1 of 0). Bij twee bits zijn er vier mogelijke combinaties (00, 01, 10, 11), bij drie bits zijn er acht combinaties mogelijk, en bij acht bits zijn er 256 combinaties mogelijk. Dus een byte bevat 256 combinaties, wat voldoende is om alle 26 kleine letters, 26 hoofdletters, leestekens en andere tekens weer te geven. Hiermee kan programmeertaal worden gecodeerd.

Nu kan met één byte niet veel worden gedaan, maar één megabyte staat voor 1 miljoen bytes (een mp3 muziekbestand is enkele MB's), een gigabyte bevat 1 miljard bytes (een film is enkele GB), een terrabyte is 1 biljoen bytes. De hoeveelheid informatie die daarmee kan worden opgeslagen, is enorm.
Die eentjes en nulletjes vertegenwoordigen tekens, letters en cijfers. Hierdoor wordt het mogelijk een computer te programmeren, met behulp van een programmeertaal zoals Visual Basic, COBOL of Oberon. De programmeertaal is het middel waarmee de computer instructies uitvoert en dus werkt.
Dankzij een grafische *interface*, zoals Windows, hoeft de gebruiker de programmeertaal niet te zien; deze ziet alleen de visuele schil. Onder het oude MS-DOS-besturingssysteem moest de gebruiker allerlei commando's invoeren. Nu kan de gebruiker met een muis klikken op wat hij wil doen: het bekijken van een film, het gebruiken van een tekenprogramma, enzovoort.

Al jaren wordt er onderzoek gedaan naar een volgende fase in computertechnologie: de kwantumcomputer. Terwijl een normale computer berekeningen achter elkaar maakt (sequentieel), voert de kwantumcomputer deze gelijktijdig uit. Waar een normale computer moet kiezen tussen een 0 of 1, gebruikt de kwantumcomputer zowel de 1 als de 0 tegelijkertijd. De bits worden hier qubits genoemd. Dit heeft bij één berekening weinig impact, maar de rekenkracht stijgt exponentieel met het aantal qubits. Dit zou leiden tot een computer die 100 miljard keer sneller is.[33]

[33] www.nl.wikipedia.org/wiki/Kwantumcomputer

Hoewel dit op dit moment nog lijkt op sciencefiction, wordt er veel geld geïnvesteerd in de ontwikkeling ervan omdat de eerste die beschikt over een kwantumcomputer alles digitaal kan. Dit zal verstorend werken: alles wat digitaal werkt kan met een kwantumcomputer ongelooflijk veel sneller worden verwerkt. En als het bedrijf kwade bedoelingen heeft, of als criminelen de kwantumcomputer stelen… De beveiliging van banken, ministeries van defensie, beurzen, waterzuiveringsinstallaties, kerncentrales, luchtverkeersleidingen - alles kan worden gehackt. Geen enkele beveiliging zal meer afdoende zijn. De eerste kwantumcomputer is als een universele sleutel die past op elk digitaal slot.

1.4.1.3 Analoog, digitaal, organische computers

Als alleen gekeken wordt naar computers die sequentiële bewerkingen maken, dan kunnen in de loop van de tijd drie soorten onderscheiden worden: de analoge, de digitale en de organische computer. Voordat de laatste computer toegelicht wordt, moet eerst duidelijk gemaakt worden wat een computer is.
Een computer is een "elektronisch apparaat voor het opslaan en verwerken van gegevens."[34] Hoewel de elektronische computer pas enkele tientallen jaren bestaat, zijn er al duizenden jaren apparaten die gegevens kunnen verwerken en opslaan. Dit zijn analoge computers. Een bekend voorbeeld hiervan is het telraam (*abacus*), dat al door de Romeinen werd gebruikt.

> **toelichting**
> Het telraam is "een mechanisme met kralen die afhankelijk van het type *abacus*, heen en weer geschoven kunnen worden in horizontale of verticale richting, om sommen en andere wiskundige berekeningen mee uit te voeren. Het is een voorloper van de rekenmachine en de computer. In de westerse wereld wordt de abacus tegenwoordig hoofdzakelijk gebruikt als didactisch hulpmiddel bij het leren rekenen."[35]

Een ander voorbeeld van een analoge computer is de rekenliniaal.

> **toelichting**
> "Een rekenliniaal is een analoog wiskundig instrument waarmee men berekeningen kan uitvoeren. Samen met de logaritmetafel en een handboek met de meest voorkomende wiskundige functies, zoals 'de' Abramowitz & Stegun, vormde de rekenliniaal tot circa 1980 (toen goedkope elektronische, digitale rekenmachines op de markt verschenen) het standaard rekengereedschap van technici, natuurkundigen en ingenieurs."[36]

Het moge duidelijk zijn dat er vele soorten analoge computers zijn en dat deze nog steeds worden gebruikt. Maar voor het serieuzere werk wordt de digitale computer gebruikt. Hoe de digitale computer werkt wordt hierna onder de kop "hardware vs. software" uitgelegd.

---

34 www.vandale.nl/*grat*is-woordenboek/nederlands/betekenis/computer
35 www.nl.wikipedia.org/wiki/Abacus_(rekentuig)
36 www.nl.wikipedia.org/wiki/Rekenliniaal

Blijft over de organische computer. Een normale computer gebruikt anorganische materialen zoals metaal en plastic, terwijl een organische computer de bouwstenen van het leven gebruikt. Zo werd al in 1994 een DNA-computer gebouwd.[37] Dit wordt een *wetware* computer genoemd, waarbij hardware en software samensmelten met levend weefsel.

> **toelichting**
> Een *wetware*-computer is een organische computer samengesteld uit organisch materiaal, zoals levende neuronen. Dit onderzoek begon met name in 1999 toen het Georgia Institute of Technology erin slaagde om een eenvoudige neurocomputer te laten werken met bloedzuigerneuronen.[38]
> Tegenwoordig zijn onderzoekers ook bezig met paddenstoelen. Het wortelnetwerk van paddenstoelen, *mycelium* genaamd, vertoont veel overeenkomsten met het menselijk brein. "*Mycelia* zijn dunne haarachtige delen van het wortelsysteem van een schimmel die elektrische impulsen kunnen overbrengen, vergelijkbaar met synapsen. Paddenstoelen die verbonden zijn met hetzelfde ondergrondse *mycelia*netwerk kunnen soms over aanzienlijke afstanden communiceren met elektrische signalen."[39]

Als het begrip "organisch" breder wordt getrokken, meer in de stijl van *cyberpunk*, dan kan een organische computer ook worden gezien als het verbinden van het lichaam met een geautomatiseerd werk (cybernetica). Deze ontwikkeling vindt al veelvuldig plaats. Hoewel de mens nog geen *cyborg* is, zijn er wel ontwikkelingen in die richting. Zo vervangt een pacemaker al jarenlang het hart, en het bedrijf van Elon Musk heeft inmiddels de eerste neurolink geïmplementeerd in de hersenen van een mens.[40]
Maar ook buiten het lichaam worden computers ingezet om de mens te helpen. Denk aan de digitale bril van Apple, waarbij de echte wereld wordt gefilmd en vervolgens wordt afgespeeld binnen de bril op twee kleine computerschermen, waardoor het lijkt alsof het computerscherm in de echte wereld voor de ogen van de gebruiker verschijnt. Dit opent veel mogelijkheden voor interactie tussen de digitale en de echte wereld.
Dus terwijl de digitale computer de opvolger is van de analoge computer, kan dat nog niet gezegd worden van de organische computer. Deze ontwikkeling is nog niet ver genoeg gevorderd. Bovendien lijkt het eerder te gaan om een samensmelting tussen beide computervormen.

1.4.1.4 Software versus hardware

De hardware is het fysieke deel van de computer en omvat onder andere:

- een moederbord, zijnde een groene vierkante plaat met een processor, datgene dat alle bytes berekent;

---

37 www.weforum.org/agenda/2015/09/what-are-organic-computers/
38 www.en.wikipedia.org/wiki/Wetware_computer
39 www.techspot.com/news/97836-scientist-have-developed-living-pc-made-mushrooms.html
40 www.scientificamerican. com/article/elon-musks-neuralink-has-implanted-its-first-chip-in-a-human-brain-whats-next/

- intern (RAM) geheugen waar de berekeningen van de processor tijdelijk op worden opgeslagen;
- extern geheugen (harde schijf) waarop software wordt opgeslagen en het resultaat van het werk van de gebruiker (tekst, film, muziek);
- een videokaart dat de data vertaalt naar beeld;
- Bios (*Basic Input/Output System*), wat ervoor zorgt dat bij het opstarten van de computer het besturingsprogramma wordt geladen (Windows, Linux);
- de ventilator, dat de hitte afkoelt dat het computerproces genereert;
- dit geheel is verbonden met het inputsysteem (toetsenbord en muis) en het outputsysteem (monitor, printer, opslagmedium).

Software is de taal, de instructie, die programma's laat werken door middel van binaire code. Software kan worden onderverdeeld in drie groepen: het besturingssysteem, applicaties en *malware*.
Het besturingssysteem is een verzameling van samenwerkende programma's die na het opstarten van een computer in het geheugen worden geladen en de hardware aansturen. Het fungeert als een medium tussen de hardware en de computergebruiker, met als doel dat de gebruiker programma's op een gemakkelijke en efficiënte manier kan uitvoeren.[41]

> **toelichting**
> Voorbeelden van besturingssystemen zijn Microsoft Windows voor pc's, Apple macOS voor Mac-computers, Android voor *smartphones* en *tablets*, en Linux voor *servers*. Er bestaat niet één universeel besturingssysteem voor alle computers; verschillende systemen worden gebruikt afhankelijk van het apparaat en het gebruiksdoel.

Toepassingssoftware, ook wel applicaties genoemd, zijn programma's ontworpen voor specifieke taken die gebruikers willen uitvoeren.
Voorbeelden hiervan zijn tekstverwerkingsprogramma's voor het schrijven van brieven, mp4-spelers voor het afspelen van videobestanden, e-mailclients voor het versturen van e-mails, en webbrowsers voor het surfen op internet.

> **toelichting**
> Wanneer een computergebruiker muziek wil beluisteren, opent hij een mp3-speler. Dit programma geeft instructies aan het besturingssysteem om een specifiek bestand te openen en af te spelen. De *driver* van de geluidskaart zet de digitale gegevens om in geluidssignalen. De mp3-speler zelf is toepassingssoftware, terwijl de andere softwarecomponenten bij het besturingssysteem horen.

Malware is een derde categorie software. Dit is software dat de gebruiker niet wil toepassen. Het wordt ongewenst geïnstalleerd door de hacker en heeft meestal nadelige gevolgen voor de werking van het besturingssysteem en/of toepassingssoftware.

---

41 www.nl.wikipedia.org/wiki/Besturingssysteem

Bijvoorbeeld, *ransomware* kan de gebruiker buitensluiten van zijn eigen computer en een virus kan bestanden beschadigen, waardoor data onleesbaar wordt. *Malware* wordt toegelicht in paragraaf 1.5.

1.4.2 Digitalisering

1.4.2.1 Algemeen

De digitalisering van de samenleving kent een snelle opmars. De eerste elektromechanische computer, de Z3, werd in 1941 gebouwd door Zuse. In de periode van 1950 tot 1980 vulden *mainframe*computers hele kamers in bedrijven. Bedrijven als Commodore en Apple begonnen zich ook te mengen in de wereld van computers, maar het was in 1981 dat IBM de eerste personal computer op de markt bracht, waardoor computers hun intrede deden in huishoudens.[42] Na de personal computer volgden al snel de laptop, tablet, *smartphone* en *smartwatch*, allemaal geautomatiseerde apparaten die vatbaar zijn voor hacking.

Het duurde niet lang voordat de digitalisering zich verspreidde naar verschillende apparaten. Het is verbazingwekkend hoeveel apparaten gedigitaliseerd kunnen worden. Analoge apparaten, zoals walkmans, platenspelers, cassettespelers en videospelers, waren nogal omslachtig. Zij hadden geen eigen geheugen, dus moest er altijd een fysieke gegevensdrager (zoals een langspeelplaat, muziekcassette, compact disc of videoband) in het afspeelapparaat worden geplaatst. Dit bracht niet alleen het risico op beschadiging met zich mee, maar de apparaten waren ook niet mobiel. Bijvoorbeeld, in de auto zat een cd-speler, wat betekende dat men tijdens elke autorit naar dezelfde cd moest luisteren of een stapel cd's moest meenemen. Een grote verbetering kwam toen analoge signalen konden worden omgezet in digitale signalen.

> **toelichting**
> "Analoge signalen zijn continu variërende signalen, zoals die van geluid of licht, in tegenstelling tot digitale signalen die bestaan uit discrete waarden."[43]
> Oftewel, bij een langspeelplaat wordt de muziek opgenomen door een microfoon om de geluidssignalen op te vangen, die vervolgens worden verwerkt in groeven op de plaat. De naald van de platenspeler kan deze groeven lezen en het oorspronkelijke geluid reproduceren.
> Bij digitale recorders daarentegen worden de geluidssignalen bij opname omgezet in eentjes en nulletjes, die vervolgens worden opgeslagen op een gegevensdrager, zoals een harde schijf, CD of USB-stick. Deze digitale bestanden kunnen worden afgespeeld met behulp van software, zoals een mp3-speler, dat de digitale informatie omzet in geluidssignalen die door speakers kunnen worden weergegeven. Een groot voordeel van digitale opslag is dat de informatie gemakkelijk over grote afstanden kan worden verplaatst, bijvoorbeeld via het internet.

---

42 www.nl.wikipedia.org/wiki/Computer
43 www.ensie.nl/betekenis/analoog

Analoge apparaten werden snel vervangen door digitale varianten, die minder leesfouten hadden, compacter waren, mobiel werden dankzij batterijvoeding en met intern geheugen de mogelijkheid boden om een grote hoeveelheid aan informatie op te slaan, zoals een muziekcollectie. Verscheidene apparaten, zoals fotocamera's, videocamera's, muziekspelers en antwoordapparaten, ondergingen deze digitale transformatie. Echter nog steeds een enkele functie vervullend.
De opkomst van de *smartphone* bracht een radicale verandering teweeg. Ondanks het kleine formaat biedt de *smartphone* een ongelofelijke variëteit aan functies die voorheen door meerdere afzonderlijke apparaten werden vervuld. Hoewel de prijs van ongeveer 1.000 euro hoog lijkt, moet worden bedacht dat de *smartphone* in feite een koopje is, gezien de veelzijdigheid ervan en het aantal apparaten dat het vervangt. Hoewel gespecialiseerde apparaten nog steeds meer mogelijkheden bieden dan een *smartphone*, voldoet de *smartphone* voor veel mensen aan al hun behoeften. Het is als een digitaal Zwitsers zakmes, een alleskunner.

> **toelichting**
> Het is opmerkelijk hoe *smartphones* talloze functies hebben overgenomen die voorheen door verschillende afzonderlijke apparaten werden vervuld. Enkele van deze functies omvatten: horloge/klok, antwoordapparaat, fotocamera, fotoboek, videocamera, videotheek, agenda, wekker, stopwatch, telefoon, videofoon, navigatiesysteem, telegraaf (tekstberichten), e-mailprogramma, browser, *tracker* (*find my phone*), rekenmachine, zaklamp, waterpas, kompas, transacties betalen, stappenteller, radio en kladblok.

Inmiddels lijkt het erop dat in bijna elk apparaat een computer is ingebouwd. Of het nu gaat om tv's, telefoons, horloges, brillen, muziekspelers, auto's, vaatwassers, koelkasten, luidsprekers, slimme thermostaten, slimme deurbellen, drones, printers of slimme verlichting. Maar let wel, elk geautomatiseerd werk brengt zijn eigen risico's met zich mee, omdat het vatbaar is voor hacking.

1.4.2.2 De gevaren

De groeiende digitalisering betekent dat elk geautomatiseerd apparaat gegevens verzamelt, wat resulteert in een schat aan informatie die toegankelijk is voor wie er maar toegang toe heeft. Veel van deze producten hebben onderhoudscontracten, abonnementsdiensten of andere klantrelaties die hen toegang geven tot de gegevens van het product en het gebruik ervan door de klant. Wanneer een informatiebedrijf deze bedrijven overneemt, verwerft het een aanzienlijke informatiepositie. Een treffend voorbeeld hiervan is Google. Dit techbedrijf beschikt over veel producten waaruit klantgegevens kan worden verzameld. Maar door bedrijven over te nemen heeft Google zijn informatie-arsenaal verder vergroot.

toelichting
Google heeft een sterke informatiepositie opgebouwd via haar eigen producten, zoals de zoekmachine, de Chrome-browser, Gmail, Google Pay, enzovoort. Maar ook door de overname van verschillende bedrijven, zoals YouTube, Waze, Nest, Fitbit, Motorola en HTC, heeft Google toegang tot een breed scala aan gebruikersgegevens.
Deze overnames hebben Google in staat gesteld om informatie te verzamelen over waar gebruikers wonen en werken (Waze), wanneer zij thuiskomen en thuis zijn (Nest, Siri), sportactiviteiten (Fitbit), kijkgedrag op YouTube en meer. Bovendien is er de continue luisterfunctie van Siri, die alles in huis opvangt om commando's te horen en erop te reageren. Hoewel beweerd wordt dat dit niet wordt opgenomen voor enig ander doel dan de werking van Siri, blijft de mogelijkheid van misbruik altijd aanwezig (denk aan microfoon-hacking).

Nu heeft Google geen kwaadwillende bedoelingen met de verzamelde informatie, maar het gebruikt deze gegevens wel om zijn eigen belangen te dienen. Een van de belangrijkste inkomstenbronnen voor Google is reclame. Voor adverteerders geldt dat hoe gerichter de advertenties zijn, hoe groter de kans is dat klanten het product kopen. Daarom streeft Google ernaar om zoveel mogelijk informatie over gebruikers te verzamelen, zodat advertenties nog gerichter kunnen worden gebracht.

toelichting
Google verzamelt veel informatie, waaronder zoekgedrag, locatiegegevens, apparaatinformatie, app-gebruik, e-mailinhoud (wordt gescand voor optimalisatie van gepersonaliseerde advertenties zonder de inhoud daadwerkelijk te lezen), YouTube-kijkgeschiedenis, advertentie-interacties, *cookies* en *tracking*, en aankoopgeschiedenis (in het geval van gebruik van Google Pay).
Het is belangrijk op te merken dat dit allemaal legaal is, omdat gebruikers vrijwillig toestemming geven voor het gebruik van deze informatie. Dit gebeurt meestal door akkoord te gaan met de algemene voorwaarden, zelfs als zij deze niet hebben gelezen. Het is uiteindelijk aan de gebruiker om te beslissen of het gebruik van de dienst de opoffering van een deel van de privacy waard is.

Voorgaande duidt erop dat grote hoeveelheden informatie kunnen worden verzameld van individuele gebruikers. Welke partijen hebben hier belang bij?

	belanghebbenden gebruikersinformatie			
	opsporingsdienst	**bedrijven**	**informatiemakelaars**	**criminelen**
waarom	vergaart de informatie voor opsporings-onderzoek.	– advertenties – klantenservice – verbeteren producten	kopen informatie via bedrijven om te verkopen aan andere bedrijven (zoals verzekeraars, adverteerders, banken)	om voordeel uit te halen ten nadele van de gebruiker
waarborg	mag pas na een verdenking (artikel 27 sv) + controle door strafrechter in geval van vervolging.	toestemming gebruiker (meestal via de acceptatie van de algemene voorwaarden)	wordt toestemming voor gegeven bij algemene voorwaarden van informatievergarend bedrijf (verstrekking aan derden)	geen (illegaal)
boek	uitgewerkt in hoofdstuk 6	uitgewerkt in hoofdstuk 2	uitgewerkt in hoofdstuk 2	uitgewerkt in hoofdstuk 3

Gebruikers verstrekken aanzienlijke hoeveelheden informatie over hun leven door de algemene voorwaarden te accepteren. Deze voorwaarden zijn vaak zo breed geformuleerd dat bedrijven aanzienlijke vrijheden hebben om deze gegevens te gebruiken, zelfs voor doorverkoop aan derden, zoals informatiemakelaars. Deze makelaars verkopen de gegevens door aan partijen die specifieke doeleinden hebben, niet altijd in het belang van de oorspronkelijke verstrekker van de informatie.
Zo meldde de krant The New York Times dat informatiemakelaar Lexus Nexus rijgegevens van klanten van autofabrikant General Motors (GM) kocht en deze doorverkocht aan verzekeraars. Dit resulteerde in een verhoging van de autoverzekeringspremie van een klant met 21%.

> **voorbeeld**
> De overdracht van persoonlijke auto-informatie van autofabrikant GM naar een verzekeraar, via informatiemakelaar Lexus Nexis, werd ontdekt toen de heer Dahl plotseling een verhoging van 21% op zijn autoverzekeringspremie kreeg. Zijn verzekeraar meldde dat dit te wijten was aan een rapport van informatiemakelaar Lexus Nexis dat de verzekeraar had gebruikt. Volgens de Amerikaanse wetgeving is de informatiemakelaar verplicht om het dossier openbaar te maken dat zij over burgers bijhouden wanneer daarom wordt gevraagd. Dahl ontving op zijn verzoek 258 pagina's, waarvan meer dan 130 pagina's details bevatten over de autoritten van hemzelf en zijn vrouw in de afgelopen zes maanden. Deze informatie omvatte start- en eindtijden van elke rit, de afgelegde afstand, evenals gegevens over snelheid, hard remmen of versneld optrekken. Alleen de locatie werd niet vermeld. General Motors had deze gegevens verstrekt aan Lexus Nexis.[44]

Grote techbedrijven schipperen met het gebruik van informatie van haar klanten. Grenzen worden opgezocht en soms overtreden.

> **voorbeelden**
> Google verzekert dat het de gezondheidsgegevens van de 27 miljoen Fitbit-gebruikers niet zal gebruiken voor advertentiedoeleinden. Dit biedt echter nauwelijks geruststelling, aangezien het bedrijf niet uitsluit dat de data op andere manieren worden gebruikt. Zoals de non-profit organisatie *Patient Privacy Rights* stelt, gezondheidsdata is bijzonder waardevol. Farmaceutische bedrijven hebben interesse in deze gegevens om investeringsbeslissingen te nemen en reclamecampagnes te plannen. Hoewel Google bezweert de data geanonimiseerd te verstrekken, blijkt uit onderzoek dat in bepaalde gevallen de identiteit van individuen kon worden achterhaald.[45]
>
> Google is zich ervan bewust dat een deel van de gebruikers privacy hoog in het vaandel draagt. Om tegemoet te komen aan deze zorgen, heeft het de optie voor de privémodus in de Chrome-browser opgenomen. Echter, aangezien Google geld verdient door gebruikersinformatie te verkopen, brengt deze optie verlies aan advertentieopbrengsten met zich mee. Het verwijt is dat Google toch gegevens van gebruikers in de privémodus heeft vastgelegd. Of dit daadwerkelijk is gebeurd, blijft onduidelijk omdat Google de zaak heeft geschikt door 5 miljard *dollar* te betalen aan de klagers.[46] Vijf miljard *dollar* wordt niet zonder reden betaald.

---

44 www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html
45 www.pbs.org/newshour/economy/making-sense/google-bought-fitbit-what-does-that-mean-for-your-data-privacy
46 www.reuters.com/legal/google-settles-5-billion-consumer-privacy-lawsuit-2023-12-28/

Facebook (Meta) kreeg in 2023 een boete van 1,3 miljard *dollar* opgelegd door de Ierse *Data Protection Commission* (DPC) wegens schending van de Algemene Verordening Gegevensbescherming (AVG) van de Europese Unie. Deze beslissing volgde op een rechtszaak aangespannen door de Oostenrijkse privacyactivist Max Schrems, die zich zorgen maakte over de waarschuwingen van Edward Snowden. Snowden had gewaarschuwd dat de gegevens van Europese gebruikers mogelijk onvoldoende beschermd waren tegen Amerikaanse inlichtingendiensten. Schrems won de zaak, waarna Meta in hoger beroep ging.[47]

In de lopende rechtszaak (Klein v. Meta Platforms, Inc., No. 3:20-cv-08570-JD (N.D. Cal.)) eisen de eisers, waaronder adverteerders, documenten op van de oprichter van Netflix (tevens bestuurslid van *Facebook*). In de vordering wordt beweerd (maar nog niet bewezen): *"By 2013, Netflix had begun entering into a series of "Facebook Extended API" agreements, including a so-called "Inbox API" agreement that allowed Netflix programmatic access to Facebook's user's private message inboxes, in exchange for which Netflix would "provide to FB a written report every two weeks that shows daily counts of recommendation sends and recipient clicks by interface, initiation surface, and/or implementation variant (e.g., Facebook vs. non-Facebook recommendation recipients)."*[48]

Het is zeer verontrustend dat sommige bedrijven geen enkele scrupules lijken te hebben als het gaat om het schenden van de privacy van gebruikers, vooral wanneer deze gebruikers psychische patiënten zijn. Dit roept ernstige ethische en juridische kwesties op, aangezien het exploiteren van de privacy van kwetsbare individuen onaanvaardbaar is.

voorbeeld
Het is zorgwekkend om te zien dat BetterHelp, een online platform voor psychologische hulp, betrokken is bij het delen van gezondheidsgegevens met derden voor reclamedoeleinden. Het feit dat de Federal Trade Commission (FTC) een schikkingsvoorstel heeft gedaan van 7,8 miljoen dollar, samen met het verbod op het delen van dergelijke gegevens (met *Facebook* en *Snapchat*), onderstreept de ernst van de situatie. Het is van cruciaal belang dat platforms voor psychologische hulp de vertrouwelijkheid van gezondheidsgegevens van hun gebruikers respecteren en beschermen. Dergelijke praktijken ondermijnen niet alleen het vertrouwen van de gebruikers, maar kunnen ook schadelijke gevolgen hebben voor hun welzijn en privacy.[49]

Sommige bedrijven zijn bereid om criminele handelingen te verrichten met betrekking tot persoonlijke informatie, waarbij het streven naar primeurs en winstgevendheid boven ethiek wordt geplaatst.

voorbeeld
Het schandaal rond News of the World, waarbij voicemails van beroemdheden werden gehackt, heeft geleid tot een golf van rechtszaken en heeft de krant uiteindelijk tot sluiting gedwongen. Het hacken van voicemails was schrikbarend eenvoudig: door het bellen van het nummer van de telefoon en het raden van de viercijferige code van de voicemail konden hackers toegang krijgen tot gevoelige

47 www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta
48 www.storage.courtlistener.com/recap/gov.uscourts.cand.369872/gov.uscourts.cand.369872.739.0_1.pdf
49 www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook

informatie. Dit leidde tot een enorme juridische nasleep, met honderden rechtszaken tegen News Group Newspapers, de uitgever van News of the World en The Sun. Als reactie hierop heeft de uitgever maar liefst 127 miljoen pond opzijgezet om de kosten van deze rechtszaken te dekken.
Het schandaal betekende het einde van News of the World, een krant met een geschiedenis van 168 jaar. James Murdoch, van News Corporation, erkende de verwerpelijke aard van het gedrag en benadrukte dat dergelijke praktijken geen plaats hebben binnen het bedrijf. Het hacken van voicemails was niet alleen immoreel, maar ook in strijd met zowel civiele als strafrechtelijke normen. De schending van privacy en ethiek door de krant en sommige van haar journalisten illustreert de noodzaak van strenge regelgeving en ethische normen in de journalistiek en daarbuiten.[50]

Soms kan gebruik van persoonlijke informatie levensgevaarlijk zijn.

voorbeelden
Een GPS-trackingbedrijf dacht dat het een slim idee was om een wereldwijde *heat map* te publiceren op het internet. Dat was totdat de krant The Washington Post in 2018 ontdekte dat zij op deze manier de locaties van Amerikaanse militaire bases in Irak en Syrië konden achterhalen, simpelweg door het gebruik van Fitbits. De sportieve activiteit lichtte op als puntjes op de kaart. Hoewel het in Europa of de VS niet duidelijk was, waren de enige gebruikers van Fitbits in de woestijn Amerikaanse militairen. Iedereen met toegang tot de kaart kon zien waar de (geheime) bases zich bevonden.[51]

"Rusland en Oekraïne gebruiken beide mobiele telefoons als wapen om troepen te volgen".[52] De metadata die wordt verzonden kan worden gebruikt om locaties te achterhalen. Vervolgens is het een kwestie van bewapende drones of artillerievuur richten op die locaties.

1.4.3 AI

1.4.3.1 Algemeen

Een snel evoluerende ontwikkeling is die van kunstmatige intelligentie (AI). Een voorbeeld hiervan is ChatGPT, een AI-model dat functioneert als een groot taalmodel. Achter ChatGPT zit een uitgebreid neuraal netwerk dat enorme hoeveelheden informatie kan verwerken en daardoor menselijk aandoende antwoorden kan genereren.

toelichting
Het is opmerkelijk hoe ChatGPT werkt. Een vraag kan gesteld worden in het Nederlands, waarna de computer de Nederlandse bronnen doorzoekt om een antwoord te vinden. Vervolgens wordt het antwoord gestructureerd en in behapbare stukken gepresenteerd. Echter, uit de gebruikte bronnen blijkt dat ook Engelse teksten worden geraadpleegd. De Nederlandse vraag wordt dan ook vertaald naar het Engels en worden de Nederlandse en Engelse bronnen samengevoegd, waarna het antwoord weer wordt vertaald naar het Nederlands om een begrijpelijk antwoord te geven.

---

50 www.bbc.com/news/business-65207881

51 www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

52 www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/

Inmiddels kan ChatGPT ook een vraag beantwoorden die met een stem is gesteld, waarna de AI het ook met een stem beantwoord.[53]

De voordelen van ChatGPT zijn duidelijk: het biedt hulp bij het verkrijgen van kookrecepten, het schrijven van een brief, het samenvatten van een tekst, en zelfs het schrijven in programmeertaal.
Echter, de risico's zijn inmiddels ook duidelijk: oplichters maken gebruik van ChatGPT om beter ogende scripts te verkrijgen om mensen op te lichten, studenten laten ChatGPT hun huiswerk maken, en AI wordt gebruikt om desinformatie te verspreiden.[54]

voorbeeld
Tijdens het schrijven van dit boek vroeg ik aan de chatbot om voorbeelden van cybercrime te geven. Ik wilde controleren of ik geen vormen van cybercrime had gemist. Blijkbaar was mijn prompt niet specifiek genoeg geformuleerd, want de AI begon een script te schrijven over hoe mensen klant konden worden bij een bepaalde webwinkel en vervolgens afgeperst konden worden. Voordat het klaar was, wiste het alle tekst en gaf het aan dat deze vraag ongepast was. Hoewel er herstellend vermogen is, blijft het eenvoudig om dit te omzeilen door de prompt anders te formuleren. Het verontrustende was dat hoewel het advies wat knullig was, het zou kunnen werken.

ChatGPT kan vragen beantwoorden, teksten verbeteren en vertalen. Maar het gaat verder dan dat. Dankzij AI is het nu mogelijk om tekst om te zetten naar spraak (en vice versa), naar beeld, video of muziek.
Er zijn inmiddels AI waarbij een foto geüpload kan worden en de AI het laten omzetten naar bewegend beeld, waarbij de 'persoon' op de foto zelfs kan zingen. De gevolgen hiervan zijn duidelijk, vooral vanuit een crimineel perspectief: het wordt veel gemakkelijker om stemmen te hacken, niet alleen om beveiligingsapparatuur te omzeilen, maar ook om mensen te misleiden om bepaalde opdrachten uit te voeren, zoals banktransacties. En wanneer beeld toegevoegd wordt aan het geheel, wordt terrein van *deepfakes* betreden, met talloze mogelijkheden voor criminelen.

toelichting
De ontwikkelingen op het gebied van robotica zijn nauwelijks bij te houden. Er is al geruime tijd bekend dat er robots in ontwikkeling zijn, vooral door bedrijven zoals Boston Robotics. Maar door een samenwerking tussen OpenAI en een opkomende robotics startup, is nu Figure ontwikkeld.[55] Dit is een humanoïde robot die in staat is om stemmen te herkennen, daarop te reageren en zelfs taken uit te voeren.
In de interactie tussen mens en robot spreekt de mens tegen de robot, die vervolgens de stem omzet in tekst, deze tekst in bytes converteert, het grote taalmodel raadpleegt voor een passend antwoord, de bytes weer omzet in tekst en tenslotte de tekst in stemgeluid. In demonstraties heeft de robot laten zien dat het in staat is om op een begrijpelijke manier te communiceren en vervolgens opdrachten uit te voeren. Dit lijkt rechtstreeks uit een sciencefictionverhaal te komen.
Echter, bij deze ontwikkelingen rijzen ook zorgwekkende implicaties. Wat als de robot gehackt wordt en opdrachten gaat uitvoeren die niet gewenst zijn?

53 www.nu.nl/tweakers/6307188/chatgpt-maker-onthult-ai-tool-die-stemmen-kan-imiteren.html
54 www.pcmag.com/how-to/what-is-chatgpt-a-basic-explainer
55 www.figure.ai/

1.4.3.2 Deepfakes

"*Deepfake* (een samentrekking van de Engelse woorden *deep learning* en *fake*) is een techniek voor het samenstellen van menselijke beelden op basis van kunstmatige intelligentie. Het wordt gebruikt om bestaande afbeeldingen en video te combineren en over elkaar te zetten met een techniek bekend als generatief antagonistennetwerk.
Door deze mogelijkheid werden *deepfakes* al gebruikt om niet-bestaande pornografische video's te maken van bekendheden. *Deepfakes* kunnen ook gebruikt worden om nepnieuws en misleidende *hoaxen* te maken."[56]

soorten deepfakes[57]	
tekst	AI is in staat om teksten te produceren op basis van een voorzet (prompt) die niet alleen lijken te zijn geschreven door een mens, maar ook specifieke eigenaardigheden kan overnemen waardoor het lijkt alsof het door een specifiek persoon is geschreven. Het bronmateriaal hiervoor kan gevonden worden op sociale media. Een voorbeeld hiervan is dat studenten chat GPT gebruiken om hun huiswerk te laten maken, waarbij zij als prompt aangeven dat de schrijfstijl moet lijken op die van een 14-jarige.
foto/video	AI kan het gezicht en lichaam van een bestaan persoon namaken en deze handelingen laten verrichten die zij niet verricht heeft. Zeer recentelijk is er een *deepfake*-naaktfoto gemaakt van Taylor Swift.
audio	AI kan op basis van slechts enkele minuten stemgeluid een menselijke stem klonen. Vervolgens kan tekst worden ingevoerd die de nepstem moet voorlezen, waardoor het lijkt alsof de persoon het zegt (voice hacking).
social media	AI kan een nepprofiel aanmaken. Een voorbeeld hiervan is een vals profiel dat werd aangemaakt door iemand die zich voordeed als een journalist van Bloomberg op sociale mediasites zoals LinkedIn en Twitter. Dit profiel probeerde in contact te komen met beleggers die speculeerden in aandelen Tesla, waarbij koersmanipulatie leek te worden nagestreefd.
Live/ real-time	AI is in staat om *live* klonen te genereren, waardoor het lijkt alsof men *live* in gesprek is via Zoom met de heer A, terwijl in werkelijkheid een kloon wordt gebruikt die wordt geïnstrueerd door een crimineel.

Een *deepfake* is een manipulatie van beeldmateriaal of video waarbij het lijkt alsof iemand iets doet of zegt wat in werkelijkheid niet het geval is. Het is nep. In het begin werden *deepfakes* vaak gebruikt voor grappige doeleinden, zoals een foto van de paus met een dikke witte gewatteerde jas aan. Tegenwoordig zijn *deepfakes* niet meer zo grappig. Het wordt steeds vaker ingezet voor misleidende doeleinden zoals de presidentsverkiezingen in de Verenigde Staten.

56 www.nl.wikipedia.org/wiki/deepfake
57 www.spiceworks.com/it-security/*cyber*-risk-management/articles/what-is-deepfake/

voorbeelden
In de voorverkiezingen van de Amerikaanse verkiezingen in de staat New Hampshire werden *robocalls* uitgevoerd met de stem van president Biden, waarin Democraten werden ontmoedigd om te stemmen. Het verraderlijke was dat deze stem niet echt van Biden was, maar een nepstem die gegenereerd was door AI. Zelfs de veelgebruikte term *malarkey* van Biden werd door de computer gebruikt om de stem authentiek te laten lijken. Tot op heden heeft niemand de verantwoordelijkheid voor deze verkiezingsmanipulatie opgeëist.[58]

Aan de andere kant van het politieke spectrum zijn valse foto's opgedoken. Zo circuleerden er foto's waarop het leek alsof voormalig president Trump gearresteerd werd omdat hij zou worden aangeklaagd voor het betalen van zwijggeld aan een pornoster, wat mogelijk als misbruik van campagnegeld zou kunnen worden beschouwd. Deze foto's waren *fake* aangezien Trump op dat moment nog niet was aangeklaagd.[59]

Ook beroemdheden zijn hier slachtoffer van. Van velen circuleren naakte *deepfakes* op het internet. Toen in 2024 *deepfake* naaktfoto's opdoken van zangeres Taylor Swift was dat voor de Amerikaanse congres reden om op te roepen tot de strafbaarstelling van *deepfakes*.[60] In Nederland is dit reeds strafbaar als pornografie (artikel 240 Sr).[61]

voorbeeld
De toespraak van Leonardo DiCaprio voor de Verenigde Naties over klimaatverandering is met behulp van *AI-voice cloning* omgezet. Men ziet en hoort de acteur spreken, maar hoort achtereenvolgens de stemmen van Joe Rogan, Steve Jobs, Robert Downey Jr., Bill Gates en Kim Kardashian. Het is grappig, maar zoals het artikel opmerkt: doodenge AI.[62]

Oplichters hebben ook de mogelijkheden van *deepfake* ontdekt als het gaat om *voice hacking*. OpenAI heeft een AI-stemkloon ontwikkeld, genaamd de *voice engine*, die met slechts 15 seconden stemgeluid een stem kan nabootsen, inclusief emoties en intonatie.[63]

voorbeeld
De filiaalmanager van een Japans bedrijf in Hong Kong kreeg in 2020 een telefoontje van de directeur van het moederbedrijf. De directeur stelde bezig te zijn met een overname en drong aan op een betaling van 35 miljoen *dollar*. De filiaalmanager werd verzekerd dat een advocaat alle details zou regelen en dat hij binnenkort e-mails zou ontvangen ter bevestiging. Toen de e-mails arriveerden met de betalingsinstructies, maakte de filiaalmanager het geld over. Echter, bleek al snel dat de stem van de zogenaamde directeur was gekloond en dat de hele transactie een zwendel was.[64]

58 wwww.edition.cnn.com/2024/01/24/politics/deepfake-politician-biden-what-matters/index.html
59 www.bbc.com/news/world-us-canada-65069316
60 www.bbc.com/news/technology-68110476
61 Het internet is een openbare plaats en een nepnaaktfoto is in strijd met de eerbaarheid.
62 www.manners.nl/leonardo-dicaprio-speech-vn-ai-voice-cloning/
63 www.nu.nl/tweakers/6307188/chatgpt-maker-onthult-ai-tool-die-stemmen-kan-imiteren.html
64 www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/

voorbeeld
In maart 2019 werd de leidinggevende van een Britse energieleverancier gebeld door de directeur, die dringend verzocht om 243.000 *dollar* over te maken naar een Hongaarse leverancier. De stem bleek later te zijn nagemaakt met *deepfake*-technologie. Het geld werd overgemaakt, maar het bleek al snel dat het een zwendel was.[65]

1.4.3.3 Auteursrechtelijke aspecten

Het aanleren van AI-systemen met behulp van auteursrechtelijk beschermd materiaal kan als strafbaar worden beschouwd vanwege schending van auteursrechten. Deze modellen maken vaak gebruik van grote datasets waarin auteursrechtelijk beschermd werk voorkomt, soms zonder de benodigde toestemming van de rechthebbenden.
AI-ontwikkelaars verdedigen dit vaak met het argument van algemeen belang, maar dit neemt niet weg dat auteurs van werken zoals boeken, foto's en kunstwerken wettelijk recht hebben op bescherming van hun werk en controle over hoe het wordt gebruikt door derden. Het is juridisch wel lastig omdat AI-systemen het werk niet reproduceren, maar aanpassen en gebruiken voor nieuwe doeleinden.
In de Verenigde Staten zijn meerdere civiele rechtszaken aangespannen tegen bedrijven zoals Microsoft, GitHub en OpenAI vanwege hun AI-modellen, zoals *Copilot*, die getraind zijn met mogelijk auteursrechtelijk beschermd materiaal. Ook de de krant The New York Times heeft OpenAI aangeklaagd wegens vermeende schending van auteursrecht.

Het is niet duidelijk of al strafrechtelijke vervolgingen zijn ingesteld wegens schending van auteurswetgeving door gebruik van AI-modellen.

1.4.4 Internet

1.4.4.1 Algemeen

Communicatie tussen computers vereist een netwerk. De volgende netwerken kunnen worden onderscheiden:

	geen	netwerk[66]				
wat	*stand alone*	*personal area network (pan)*	*local area network (lan)*	*metropolitan area network (man)*	*wide area network (wan)*	*internet*
afstand	-	< 10 meter	10 m – 5 km	5-50 km	> 50 km	wereldwijd
voorbeeld	geen	wifi-netwerk	lokaal bedrijfsnetwerk	• ziekenhuis • universiteit • fabriek	grote bedrijfsnetwerken	

65 www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
66 www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/

Door ontwikkelingen zoals het Internet der Dingen zijn veel geautomatiseerde processen nu verbonden met het internet. Terwijl vroeger een wifinetwerk beperkt was tot een *Personal Area Network* (PAN) met bijvoorbeeld computers en opslagschijven, kunnen tegenwoordig zelfs televisies rechtstreeks verbinding maken met het internet.
Een reden voor het bestaan van een *Metropolitan Area Network* (MAN) is de behoefte aan een stabiele verbinding met zeer hoge snelheden. Deze netwerken zijn kostbaar vanwege de hoge kwaliteitseisen en het relatief lage aantal gebruikers.
Hoewel het internet technisch gezien een *Wide Area Network* (WAN) is, worden met WAN's ook netwerken bedoeld die niet wereldwijd zijn, maar beperkt zijn tot een provincie of land.
De verschillende netwerken kunnen met elkaar worden verbonden, maar dit maakt het kwetsbaar voor hackers. Daarom kiezen bedrijven en overheidsinstanties ervoor om zeer gevoelige informatie op te slaan op *stand-alone* computers[67], die niet zijn verbonden met enig netwerk. Op deze manier hoeven de bedrijven alleen de fysieke ruimte waar de computer zich bevindt en de computer zelf te beveiligen. Hoewel inbreken in de computer nog steeds mogelijk is, vereist het dan fysieke toegang of omkoping van medewerkers. Dit wordt uitgewerkt bij het onderwerp *social engineering*.

In een netwerk moeten computers elkaar kunnen vinden voordat zij met elkaar kunnen communiceren. Dit vinden gebeurt aan de hand van IP-adressen (IP staat voor Internet Protocol). Een IP-adres is uniek en bestaat uit vier series getallen van 0 tot en met 255, gescheiden door punten. Bijvoorbeeld: 100.052.114.234. De toegang tot het internet wordt geregeld door internetproviders. De provider koppelt het IP-adres aan een computer of netwerkapparaat, zoals een netwerkprinter. Dit kan een vast adres zijn (statisch IP-adres) of een adres dat regelmatig verandert (dynamisch IP-adres).

> **toelichting**
> Een www-adres begint altijd met http:\\ Dat staat voor *Hypertext Transfer Protocol* (HTTP) en is het protocol voor de communicatie tussen een webcliënt (zoals een webbrowser of een app) en een webserver.[68]
> Bij https:\\ gaat het om een versleutelde dataverbinding. Dit vereist een SSL-certificaat. Google informeert gebruikers van de webbrowser Google Chrome als een bezoeker een website bezoekt zonder SSL-certificaat.[69]

Na het vinden van de bestemming begint de communicatie. Hiervoor wordt gebruikgemaakt van een communicatieprotocol, zoals TCP/IP. Daarbij wordt een *protocolstack* gebruikt. De *stack* bestaat uit vier lagen:[70]

---

67 Daarom moest Tom Cruise in de film *Mission Impossible* aan een touw afdalen in een beveiligde ruimte. Hij wilde een *stand alone computer* hacken en dat kan alleen door fysiek op de computer in te breken.
68 www.nl.wikipedia.org/wiki/Hypertext_Transfer_Protocol
69 www.dotsolutions.nl/nieuws/het-hebben-van-een-ssl-certificaat-is-een-absolute-must
70 www.beautifulcode.nl/hoe-werkt-het-*internet*/

1. De eerste laag is die van de applicatie. Hierin zitten protocollen die specifiek voor applicaties zijn bedoeld (bijvoorbeeld http of smtp).
2. De tweede laag is die van TCP/Transport. Deze laag zorgt ervoor dat door het gebruik van poortnummers voor de informatie bij de juiste applicaties terecht komt.
3. De derde laag is die van IP/internet. Deze laag zorgt ervoor dat met behulp van ip-adressen voor dat pakketjes met data bij de juiste computer terecht komen.
4. De vierde laag is die van de hardware. Deze laag zorgt ervoor dat data wordt omgezet in signalen die verstuurd kunnen worden met bijvoorbeeld een netwerkkaart.

> **toelichting**
> Een bericht tussen computer A en B wordt als volgt verzonden: de data begint zijn reis in de applicatielaag van computer A, gaat vervolgens via de transportlaag en internetlaag naar de hardwarelaag, waar het naar het internet wordt verstuurd. Daarna komt het bericht binnen via de hardwarelaag op computer B, gaat via de internetlaag en transportlaag naar de applicatielaag van computer B. De applicatie op computer B kan het bericht nu gebruiken en tonen aan de gebruiker van computer B.[71]

Op deze manier kunnen datapakketjes tussen verschillende computers worden verzonden. Het internet zelf bestaat ook uit lagen. Lokale netwerken van bedrijven en internetproviders komen samen op internetknooppunten, zoals de *Amsterdam Internet Exchange*, een van de grootste ter wereld.
Elk lokaal netwerk is verbonden met een ander netwerk via een router. Gezamenlijk vormen deze netwerken het internet. Elke router heeft kennis van de IP-adressen van de apparaten die op zijn netwerk zijn aangesloten. Wanneer een router een pakketje ontvangt met een IP-adres dat het niet herkent, stuurt hij het pakketje naar een hoger niveau. Als de router op dat niveau het IP-adres wel kent, stuurt hij het pakketje door. Als dat niet het geval is, gaat het pakketje verder naar een nog hoger niveau, totdat het IP-adres bij een router bekend is en het pakketje kan worden afgeleverd.

Nu zijn voor mensen IP-adressen in numerieke vorm moeilijk te onthouden. Daarom is er een systeem ontwikkeld dat IP-adressen vertaalt naar domeinnamen, genaamd het *Domain Name System* (DNS). DNS-servers hebben een database waarin domeinnamen en IP-adressen aan elkaar zijn gekoppeld. Er is niet één DNS-server met alle internetadressen. Net zoals bij routers gaat een domeinnaam naar DNS-server A. Als die het niet kan vinden, wordt het doorverwezen naar een hoger niveau DNS-server B, enzovoort, totdat een server wordt gevonden die de domeinnaam kan vertalen naar een IP-adres.
Op deze manier kan een computergebruiker een eenvoudig te onthouden adres opgeven, zoals www.bank.nl, waarna de computer het bijbehorende IP-adres opzoekt en verbinding maakt met die website. Hackers kunnen dit manipuleren (DNS-spoofing) door de adreslocatie te veranderen. De compu-

71 www.beautifulcode.nl/hoe-werkt-het-*internet*/

tergebruiker denkt naar de bankwebsite te gaan, maar wordt naar een nagemaakte site geleid waar de gebruiker zijn inloggegevens invoert, die vervolgens door de hacker worden gebruikt op de echte bankwebsite.

1.4.4.2 Internet

Het internet, afkorting voor *Interconnected Network*, omvat meer dan alleen websites. Het *World Wide Web* (WWW) vertegenwoordigt de grafische interface van het internet, met daarin de websites. Echter, e-mail (digitale post) wordt ook via het internet verzonden, net zoals Usenet (berichten die in nieuwsgroepen worden geplaatst) gebruikmaakt van internet.[72]

	internet						
	world wide web			***usenet***	***e-mail***	***voip***	***file sharing***
wat	*surface web*	*deep web*	*dark web*	nieuws-groepen	berichten	bellen	data uitwisselen
hoe	*web-browser*	*afgeschermd met login/ wachtwoord*	*tor-browser*	*Usenet-serviceprovider/news-reader*	*e-mail-*programma	VoIP-*provider*	*file hosting service*

N.B. Er zijn andere toepassingen (zoals opereren op afstand), maar dat komt niet veel voor.

Het *World Wide Web* bestaat uit verschillende lagen. De buitenste laag omvat de websites die worden doorzocht door zoekmachines zoals Google, die gebruikmaken van *spiders* om deze te indexeren. Zoekopdrachten in Google zoeken met name in de buitenste laag, ook wel het *surface web* genoemd.
Het internet is als een ijsberg. Het grootste deel zit onder water. Het grootste deel van het web (ongeveer 90-95%) bevindt zich onder deze buitenste schil en staat bekend als het *deep web*. Dit zijn pagina's die niet zijn geïndexeerd en vaak gevoelige informatie bevatten, zoals gegevens van overheden, academische instellingen, medische dossiers en militaire databases. Toegang tot het *deep web* vereist specifieke inloggegevens en IP-adressen.
Een subcategorie van het *deep web* is het *dark web*, dat alleen toegankelijk is via speciale browsers zoals de *Onion Browser* (TOR). Het *dark web* wordt vaak geassocieerd met illegale activiteiten en anonimiteit.
Het *World Wide Web* maakt gebruik van de programmeertaal HTML (*Hypertext Markup Language*). Webpagina's kunnen hyperlinks bevatten waarmee gebruikers van de ene pagina naar de andere kunnen navigeren, zowel binnen dezelfde site als naar andere websites. Deze pagina's worden gehost op internetservers en vormen gezamenlijk het geheel van het *World Wide Web.*[73]

---

72 www.nl.wikipedia.org/wiki/*internet*
73 www.nl.wikipedia.org/wiki/Wereldwijd_web

Usenet (*User's Network*) is een minder bekend deel van het internet, bestaande uit een netwerk van servers die nieuwsgroepen hosten, met meer dan 120.000 groepen in totaal. Het is over het algemeen sneller dan het traditionele internet, maar toegang vereist een *Usenet-serviceprovider*. Met behulp van een *newsreader* kunnen gebruikers informatie op Usenet doorzoeken en vinden. Naast het delen van allerlei soorten informatie wordt Usenet vaak gebruikt voor het downloaden van films, muziek en software. Berichten worden uitgewisseld via het NNTP-protocol.

Een andere veelgebruikte optie op het internet is e-mail (electronic mail), waarbij berichten kunnen bestaan uit tekst en bijlagen. Dit systeem maakt gebruik van het SMTP-protocol voor het verzenden van berichten.[74]

Het internet wordt ook gebruikt voor het uitwisselen van data, ook wel bekend als *filesharing*. De bestanden die worden gedeeld kunnen van alles zijn, zoals muziek, boeken, films en software. Dit systeem kan veel meer data verwerken dan e-mail.
Een gebruiker selecteert een *filesharing*-netwerk of -dienst en genereert een link die vervolgens per e-mail wordt verzonden, al dan niet beveiligd met een wachtwoord. Tegelijkertijd wordt het bestand geüpload naar de server, zodat de ontvanger de link kan gebruiken om het bestand te downloaden zodra de e-mail is ontvangen.
Filesharing vindt vaak plaats via *peer-to-peer* (P2P) netwerken, cloudopslagdiensten en bestandsdelingsprotocollen zoals BitTorrent. Dit kan illegaal zijn wanneer auteursrechtelijk beschermd materiaal wordt gedeeld.[75]

Een ander gebruik van het internet is digitaal bellen, mogelijk gemaakt door *Voice over Internet Protocol* (VoIP). Dit kan via computers, speciale VoIP-telefoons of soms zelfs reguliere telefoons met een VoIP-adapter.
De VoIP-service zet analoge stemmen om in digitale signalen die via het internet worden verzonden en vervolgens aan de ontvanger worden afgeleverd als hoorbare stemgeluiden.[76]

1.4.4.3 Dark web

Het *dark web*, ook bekend als het *darknet*, maakt deel uit van het *deep web* en staat bekend om zijn verborgen karakter. De pagina's zijn niet geïndexeerd en toegang is alleen mogelijk via een speciale browser genaamd *The Onion Router* (TOR), vernoemd naar een ui vanwege de meerdere lagen van anonimiteit die het biedt.

---

74 www.usenet.com/what-is-the-difference-between-usenet-and-the-*internet*/
75 www.mafaweb.nl/wat-is-filesharing/
76 www.fcc.gov/general/voice-over-internet-protocol-voip