CYBERCRIME

Martin Scharenborg

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 9789463428859)
- Afpakken & ontnemen (ISBN 9789463427043)
- Cybercrime (ISBN 9789463426923)
- Verkeersmisdrijven (ISBN 9789462546707)
- Bewijs in het strafrecht (ISBN 9789463425193)
- Vermogensmisdrijven (ISBN 9789463425827)

Voor meer informatie wordt verwezen naar de website www.fraudeknooppunt.nl.

M. Scharenborg
ISBN: 9789463426923

Voorwoord

Cybercrime vindt dagelijks plaats. Niet altijd met (zichtbare) schade, niet altijd merkbaar, maar de gevolgen voor *privacy* en de portemonnee kunnen groot zijn. *Cybercrime* voelt ondanks de impact als ongrijpbaar, niet in de laatste plaats door de fysieke afstand tussen crimineel en slachtoffer. *Cybercrime* is een van de weinige vormen van misdaad waarbij de dader niet fysiek op het plaats delict hoeft te zijn. Dit boek poogt een deel van het mysterie dat *cybercrime* heet te ontsluieren.

Dit boek richt zich op de juridische aspecten van *cybercrime*, niet op de technische. Dit laat onverlet dat enige basale kennis van de computer en het internet vereist is, anders kan het motief en de methoden van de cybercrimineel niet begrepen worden. De technische kant van *cybercrime* zal dan ook beperkt belicht worden.
Daarna wordt ingegaan op de historie van cyberwetgeving, om de ontwikkeling in wetgeving te kunnen begrijpen.
Vervolgens worden meer dan twintig vormen van *cybercrime* beschreven.
De kern van het boek wordt gevormd door de beschrijving van materieel en formeel cyberrecht: de cyberbepalingen en de cyberbevoegdheden.

De opzet van het boek is een praktische. Verschillende onderwerpen worden uitgewerkt, onderbouwt met vele voorbeelden, jurisprudentie en wet- en regelgeving. Voor wat betreft de rechtspraak is ervoor gekozen om zoveel mogelijk te beperken tot richtinggevende uitspraken, dus arresten van hoven en de Hoge Raad.
In dit boek is gebruik gemaakt van eigen werk, zoals de Geschiedenis van het Wetboek van Strafrecht, Bewijs in het strafrecht.

Een inhoudelijke opmerking dien ik te maken over de wijze van citeren in dit boek. In sommige gevallen zijn citaten letterlijk opgenomen maar in de meeste gevallen zijn teksten geparafraseerd of anderszins enigszins aangepast (verkort). Aangezien zo veel bronnen zijn geraadpleegd, werd de taalstijl te verschillend om de citaten in volle omvang letterlijk weer te geven. Dit betekent dat de lezer er goed aan doet althans kan doen om de oorspronkelijke uitspraken of teksten te raadplegen, zoals opgenomen in de voetnoten. Het gaat hier voor het overgrote deel om bronnen afkomstig van www.wetten.nl of www.rechtspraak.nl.

Martin Scharenborg, 2019

Inhoudsopgave

Hoofdstuk 1 Algemeen

1.1 Definitie

Cybercrime, computercriminaliteit of cybercriminaliteit, kan omschreven worden als criminaliteit met informatiecommunicatietechnologie (ICT)[1] als middel én doelwit.[2]
Als het doelwit niet de ICT is, maar het middel waarmee het delict gepleegd is is wel de ICT, dan wordt dit niet cybercriminaliteit genoemd, maar gedigitaliseerde criminaliteit.[3] Gedigitaliseerde criminaliteit is dus 'klassieke' criminaliteit die door computertechnologie een nieuwe impuls heeft gekregen. Nu is het duidelijk dat een (fysieke) inbraak waarbij gebruik is gemaakt van een digitale scanner om af te luisteren of er politie in de buurt is, gedigitaliseerde criminaliteit genoemd kan worden. Maar een afpersing van een ex die zich ooit voor de *webcam* vrijwillig heeft uitgekleed en wiens naaktbeelden worden verspreid door een wraakzuchtige partner als de ex niet doet wat de verdachte wil. Is dat gedigitaliseerde criminaliteit? Neen. Dit is *sextortion* en dat is een vorm van *cybercrime*, ook al is ICT hier alleen het middel.
Voormelde maakt duidelijk dat de scheiding tussen *cybercrime* en gedigitaliseerde criminaliteit een zekere helderheid tracht te verschaffen die er niet is.

Een andere benadering van wat *cybercrime* is is die van het *Cybercrime-verdrag* waarin onderscheid wordt gemaakt tussen computercriminaliteit in enge of in brede zin:

- Computercriminaliteit in enge zin: alle strafbare gedragingen die gericht zijn tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde processen en middelen (denk aan *hacken*, (D)dos-aanvallen, virussen).
- Computercriminaliteit in ruime zin: strafbare handelingen die zich richten op het verstoren of beïnvloeden van de werking van computersystemen of daarmee onderhouden geautomatiseerde processen. Denk aan elektronische vermogensdelicten (betalingsverkeer, telefoonfraude, afpersing), inhoudgerelateerde delicten, (kinderpornografie, illegale diensten zoals internetcasino's) en delicten op het gebied van intellectuele eigendom en de aantasting van de persoonlijke levenssfeer (*spam* en *cyberstalking*).[4]

---

1 ICT omvat niet alleen de computer, maar alles waar een *chip* in zit (zoals de *smartphone*, de *smart*-tv, een bankpas).
2 http://www.woorden.org/woord/cybercrime
3 http://www.mijndigitalewereld.nl/digital/wat-is-cybercrime.html
4 Http://nl.wikipedia.org/wiki/Verdrag_inzake_de_bestrijding_van_strafbare_feiten_verbonden_met_elektronische_netwerken

Weer een andere definitie is die van onze wetgever in de Wet computercriminaliteit III: "Computercriminaliteit kan worden omschreven als het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk."[5]
Hiermee wordt *cybercrime* (doelwit en middel) samengevoegd met gedigitaliseerde criminaliteit (middel) zodat de betrokkenheid van ICT wordt uitgebreid naar doel of middel. Het voordeel van deze omvangrijke definitie is dat er geen geforceerd onderscheid meer hoeft te worden gemaakt. Het nadeel: *everything becomes cybercrime*. Immers, waar zit tegenwoordig geen geautomatiseerd werk in? Kleding, telefoon, horloge, auto, huis, *pacemaker*. Hierdoor kan bij heel veel delicten een koppeling gemaakt worden met ICT: het vervalsen van een diploma middels scanner en printen via een internetdrukkerij; het plaatsen van een bestelling via een *app* om een pizza te laten afleveren en vervolgens de koerier te beroven.

Moet er een sluitende definitie van *cybercrime* zijn? Neen. Belangrijker is dat men zich bewust is hoe omvangrijk *cybercrime* kan zijn. Dat overheid en burger zich hier steeds bewuster van worden is winst. Wat precies onder *cybercrime* valt, tot in alle details, is minder belangrijk. Niemand zal stellen dat *hacking* of *bombing* geen *cybercrime* is, maar er zullen tal van discussiepunten blijven. Het heeft voor dit boek ertoe geleid dat het substantieel dikker is geworden omdat ik de ruime definitie aanhang. Daarom worden in dit boek ook klassieke delicten beschreven met een 'modern ICT-sausje' erover. Wat dat betreft gaat dit boek over *cybercrime,* in al zijn facetten.

1.2 Indeling

Nu de definitie niet kraakhelder is, heeft dat ook gevolgen voor de indeling van *cybercrime*. Ook dat is niet eenduidig. Zo wordt in het Cybercrimeverdrag de volgende indeling gehanteerd:

- *Delicten tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computergegevens en -systemen:*
  - Wederrechtelijke toegang (artikel 2);
  - Wederrechtelijke onderschepping (artikel 3);
  - Verstoring van computergegevens (artikel 4);
  - Verstoring van een computersysteem (artikel 5);
  - Misbruik van technische hulpmiddelen (artikel 6).
- *Computer-gerelateerde delicten:*
  - Computer-gerelateerde valsheid (artikel 7);
  - Computer-gerelateerde fraude (artikel 8);
- *Inhoudgerelateerde delicten:*
  - Delicten in verband met kinderpornografie (artikel 9).

[5] Tweede Kamer, vergaderjaar 2015–2016, 34 372, nr. 3, pag. 7.

- *Delicten met betrekking tot inbreuken op Auteursrecht en naburige rechten:*
    - Delicten met betrekking tot inbreuken op auteursrecht en naburige rechten (artikel 10).

Hoewel voormelde indeling een zeker logica bevat, opteer ik liever voor een indeling vanuit het gevoel, die vanuit het motief van de pleger:

- *technische cybercrime:* hier wordt ICT ingezet om gegevens te verkrijgen, om digitale vernieling te plegen, om systemen te saboteren. Denk aan *hacking*, *spamming*, ddos-aanvallen, *cyberdestruction*.
  Dit handelen is gericht op de techniek. Dit betekent niet dat de dader een computerexpert moet zijn. Criminelen verkopen kant-en-klare pakketten ('*plug and prey*')[6] op het *dark web* zodat ook leken direct aan de slag kunnen met *cybercrime*. *Hackers* noemen dit soort *wannabees* ook wel *script kiddies*. Niet ervaren, maar helaas maakt dat voor de schade die ze kunnen veroorzaken niet veel uit.
- *financiële cybercrime:* hier wordt ICT ingezet om financieel voordeel te behalen. Denk aan *cyberpiracy,* cyberdiefstal, identiteitsdiefstal, *skimming*, *ransomsoftware*, *online* handelsfraude.
  Dit handelen is gericht op het voordeel. Daarvoor wordt de technische kant van geautomatiseerde werken misbruikt. Dit alles dient het doel om rijker te worden. Zo is *skimmen* weliswaar zeer technisch van aard, maar er wordt niet geskimd om het skimmen (dan zou het technische *cybercrime* zijn), het wordt gedaan om er geld mee te verdienen.
- *psychische cybercrime:* hier wordt ICT ingezet om een (onweerstaanbare) innerlijke behoefte te bevredigen. Denk aan *revenge porn*, *sextortion*, *cyberbullying/shaming*, *cyberstalking*, filmen van geweld, kinderporno alsook dierenporno.
  Psychische druk (kwaadheid, zich gekwetst voelen, een innerlijke stem die bevredigd moet worden) leidt tot dit veelal irrationeel handelen, daar waar de andere twee vormen veelal het rationeel handelen raken.
  Nu kan hier wel degelijk een overlap met financiële *cybercrime* zijn. Een goed voorbeeld is *sextortion*. Als de afperser dit doet omdat hij een seksuele tegenprestatie verlangt, dan is het psychische *cybercrime*. Doet hij dit om er rijker van te worden, dan is het financiële *cybercrime*.

De indeling kan helpen het motief van de dader te begrijpen. Leer het motief, de beweegredenen van diens handelen en de dader wordt beter begrepen. En een dader die beter begrepen wordt, kan makkelijker aangepakt worden.

---

6 De klassieke uitdrukking is *plug and play*, hetgeen duidt op het gebrek aan complexiteit, het werkt direct; maar gelet op de enorme ellende die criminelen met deze standaardpaketten kunnen aanrichten is bidden dat het niet helemaal uit de hand loopt niet een overbodig uitgangspunt.

1.3 Cijfers

Het Centraal bureau voor de statistiek (Cbs) heeft moeite met het begrip *cybercrime*. Hieronder werd alleen begrepen computervredebreuk (*hacking*). Alleen daarvan werden cijfers bijgehouden:

	2012	**2013**	**2014**	**2015**	**2016**	**2017**
computervredebreuk	4.620	2.535	2.045	2.225	1.875	2.300
opgehelderd	300	295	235	195	210	220

Bron: Cbs, Cybersecuritymonitor 2018

Wat opvalt is een daling in het aantal (gemelde) zaken met 50%. Hieruit mag niet de conclusie getrokken worden dat er minder *cybercrime* is. Er wordt slechts in 8% van de gevallen aangifte gedaan.[7]
Een conclusie welke wel getrokken kan worden is dat slechts zo'n 10% van de zaken opgehelderd worden. Niet een hoog resultaat.

Inmiddels onderkent het Cbs dat *cybercrime* omvangrijker is dan alleen *hacking*. Vanuit de traditionele registratie van cijfers is dit niet af te leiden. Het Cbs registreert kinderporno als een zedendelict en marktplaatsoplichting als een vermogensmisdrijf. Daarom heeft het Cbs de *Cybersecuritymonitor* 2018 opgemaakt, waarin cijfers herleid worden naar enkele andere vormen van *cybercrime:* identiteitsfraude, (ver)koopfraude, *hacking* en cyberpesten.

per 100 inwoners	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
identiteitsfraude	1,6	1,3	0,7	0,6	0,4	0,4
koop- en verkoopfraude	3,4	3,9	4,1	4,2	4,1	4,6
hacken	8,8	9,3	7,9	7,6	7,4	7,5
cyberpesten	5,9	6,3	6,0	6,3	6,0	6,1

Bron: Cbs, Cybersecuritymonitor 2018

Dit betreft alleen een registratie in aantallen, niet van opgehelderde zaken.[8]
Omdat in relatief weinig zaken aangifte wordt gedaan is het trekken van conclusies voorbarig. Wel lijkt cyberpesten stabiel te zijn, *hacken* en identiteitsfraude af te nemen en *online* handelsfraude toe te nemen.

Nu zijn er andere bronnen met cijfers inzake *cybercrime*, maar die lijken nauwkeurigheid te ontberen. Duidelijk is dat *cybercrime* niet goed geregistreerd wordt, zodat de volle omvang van deze vorm van strafbaar handelen niet goed beoordeeld kan worden.

[7] Cybersecuritymonitor 2018, Een verkenning van dreigingen, incidenten en maatregelen
[8] Cybersecuritymonitor 2018, Een verkenning van dreigingen, incidenten en maatregelen

1.4 Hoe werkt informatie-communicatietechnologie?

1.4.1 De computer[9]

Om misdaad met ICT te begrijpen, moet een basale kennis van ICT aanwezig zijn. Hoe werkt een computer, hoe werkt internet en waar richt de misdaad binnen de ICT zich op? Daartoe zal op zeer beperkte wijze de technische kant van ICT nader toegelicht worden.

Vroeger was een computer zo groot dat alleen grote bedrijven er één hadden en die was zo groot dat het de hele kamer in nam. Tegenwoordig heeft een krachtige *laptop* meer rekenkracht. Wat met een computer kan worden gedaan is verbazingwekkend: het schrijven van een brief, het maken van berekeningen, het maken van tekeningen, het ontwerpen van objecten, het luisteren naar muziek, het bekijken van een film, het bellen met anderen. Een computer vervangt goederen zoals de platenspeler, cassetterecorder, typemachine, rekenmachine, kalender, dagboek, boekenkast. En dat alles is kleiner dan de telefoonhoorn van een ouderwetse telefoon (thans *smartphone* geheten).

De basis van dit alles zijn eentjes en nulletjes (*bits and bytes*), want feitelijk is een computer niet meer dan een rekenmachine, een rekenmachine dat beeld, muziek, tekst kan samenstellen. Hoe werkt een computer?
Een computer bestaat uit *hardware* en *software*. De *hardware* is de behuizing, de *chip*, de grafische kaart, het fysieke deel van de computer. De *software* is de taal, de instructie, waardoor programma's werken. Dit wordt de binaire code genoemd.
De binaire code wordt gevormd door eentjes en nulletjes (*bits*). Acht *bits* vormen 1 *byte*. Elke *byte* staat voor een teken of letter. Zo staat 01000001 voor A en 01100001 voor a.

> Elke *bit* is een 1 of 0. Dat betekent dat bij een *bit* er twee combinaties mogelijk zijn (1 of o); bij twee *bits* zijn vier combinaties mogelijk (00, 01, 10, 11), bij drie *bits* zijn acht combinaties mogelijk, bij acht *bits* zijn 256 combinaties mogelijk. Dus een *byte* bevat 256 combinaties, hetgeen voldoende is voor 26 kleine letters, 26 hoofdletters, alle leestekens en andere tekens. Hiermee kan programmeertaal gevoed worden.

Nu kan met één *byte* niet veel gedaan worden, maar één *megabyte* staat voor 1 miljoen *bytes* (een mp3 muziekbestand is enkele MB's), een *gigabyte* bevat 1 miljard *bytes* (een film is zo'n 2 GB), een *terabyte* is 1 biljoen *bytes*. De hoeveelheid informatie die daarmee opgeslagen kan worden is enorm.
Die eentjes en nulletjes staan voor tekens, letters en cijfers. Daarmee wordt het mogelijk een computer te programmeren, middels een programmeertaal zoals *visual basic*, cobol of oberon. En de programmeertaal is datgene waardoor de computer instructies uitvoert en dus werkt.

[9] https://www.nemokennislink.nl/publicaties/hoe-werkt-een-computer/

Door een grafische *interface* (zoals Windows) hoeft de gebruiker de programmeertaal niet te zien, die ziet alleen de schil. Onder het oude MS-dos besturingssysteem moest de gebruiker allerlei commando's invoeren. Nu klikt de gebruiker met een muis op datgene wat hij wil: het bekijken van een film, het gebruiken van een tekenprogramma.

De *hardware* omvat:

- een moederbord, zijnde een groene vierkante plaat met een processor, datgene wat alle *bytes* berekent;
- 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).

Met voormelde kan de gebruiker de computer gebruiken. Ten goede en ten kwade. Ten kwade als een *hacker* de computer van een slachtoffer iets anders wil laten doen dan de gebruiker van de computer wil. Zo kan de *hacker* eigen *software* schrijven dat de *software* van de gebruiker manipuleert, beschadigt of vernielt. Dit wordt een virus genoemd. De aanpassing van de originele *software* kan tal van doelen dienen: kopiëren van data, aanvullen van opdrachten zodat *live* meegekeken kan worden, aanpassen data zodat specifieke opdrachten uitgevoerd worden. Dit laatste kan zelfs fysieke gevolgen hebben: zo kan een *software*-opdracht om de ventilator uit te zetten tot oververhitting van de computer tot gevolg hebben waarop deze kapot gaat.

1.4.2 Het internet[10]

Nu duidelijk is hoe een computer werkt (de techniek voor pc, *laptop*, *tablet*, *smartphone*, een chip op een betaalpas is in de kern dezelfde), is het van belang te begrijpen hoe een netwerk werkt. Want *cybercrime* richt zich weliswaar op de computer, maar menig computer is verbonden met een netwerk, zoals het internet.

Een netwerk, of dat nu een bedrijfsnetwerk (intranet) of het openbare netwerk (internet) is, is in essentie niet meer dan een verzameling van gekoppelde computers. Maar net zoals mensen elkaar moeten begrijpen, is

[10] http://www.beautifulcode.nl/hoe-werkt-het-internet/

het van belang dat computers elkaar begrijpen en elkaar kunnen vinden. Het begrijpen geschiedt middels een communicatieprotocol (zoals tcp en ip) en het kunnen vinden via een ip-adres (ip staat voor internetprotocol). Het ip-adres is uniek en bestaat uit 4 series getallen van 0 tot en met 255 die worden gescheiden door een punt. 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 wisselend adres (dynamisch ip-adres).

> 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*.[11]
> Als sprake is van https:\\, dan gaat het om een versleutelde (*secure*) dataverbinding. Dit vereist een SSL-certificaat. Google informeert vanaf juli 2018 gebruikers van de *webbrowser* Google Chrome als een bezoeker een *website* bezoekt zonder ssl-certificaat.[12]

Om te communiceren tussen twee computers wordt gebruik gemaakt van een zogeheten *protocol stack*. Deze 'stapel' bestaat uit 4 lagen met elk een eigen doel om een bericht van computer A naar computer B te versturen:

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.

> Een bericht tussen computer A en B wordt als volgt verzonden: de data zal de reis beginnen in de applicatielaag van computer A om vervolgens via de transportlaag en internetlaag naar de hardwarelaag te gaan en daar vandaan naar het internet worden verstuurd. Vervolgens zal het bericht via de hardwarelaag binnenkomen op computer B en zal daar via de internetlaag en transportlaag in de applicatielaag van computer B terecht komen. De applicatie die computer B gebruikt kan het bericht nu gebruiken en tonen aan de gebruiker van computer B.[13]

Op deze wijze kunnen pakketjes data tussen de ene en de andere computer verzonden worden. Maar ook het internet bestaat uit lagen. Lokale netwerken van bedrijven en providers komen samen in een *Internet Exchange*,

---

11 https://nl.wikipedia.org/wiki/Hypertext_Transfer_Protocol
12 https://www.dotsolutions.nl/nieuws/het-hebben-van-een-ssl-certificaat-is-een-absolute-must
13 http://www.beautifulcode.nl/hoe-werkt-het-internet/

een knooppunt van netwerken. Een van de grootste internetknooppunten ter wereld is de *Amsterdam Internet Exchange.*
Elk van de kleine netwerken is middels een *router* gekoppeld aan een ander netwerk. Tezamen vormen deze kleine netwerken het internet. Elke *router* 'kent' het ip-adres van alle apparaten die in 'zijn' netwerk zijn aangesloten. Als vervolgens een pakketje wordt ontvangen door de *router* met een IP-adres dat het niet kent, dan stuurt de *router* het pakketje een niveau hoger. Als de *router* van dat hogere niveau het ip-adres wel kent, dan stuurt die het door. Zo niet, dan gaat het pakketje weer een niveau hoger, net zo lang tot het ip-adres bij een *router* wel bekend is en het pakketje kan worden afgeleverd.

Maar met voorgaande zijn alleen de ip-adressen bekend als getallen en mensen werken niet goed met getallen. Net zoals voor de programmeertaal een grafische schil is gemaakt (Windows in plaats van MS-dos), zo is ook voor het internet een schil gemaakt dat het ip-adres vertaalt naar een domeinnaam. Dit geschiedt door de *Domain Name Service* (DNS). DNS-*servers* beschikken over een database waarin domeinnamen en ip-adressen aan elkaar zijn gekoppeld. Er is niet één DNS-server met alle internetadressen. Net zoals bij de *router*, gaat een domeinnaam naar DNS-server A, kan die het niet vinden dan naar een hoger niveau DNS server B, net zolang totdat een *server* is gevonden die de domeinnaam kan vertalen naar een ip-adres.
Op deze wijze kan een computergebruiker een taalkundig adres opgeven, zoals www.nos.nl, waarop de computer zoekt naar het IP-adres, om vervolgens een verbinding te maken met die website.

Nu is het internet meer dan alleen maar *websites*. Het *world wide web* (www) is de grafische *interface* van het internet (de *websites*), maar e-mail (digitale post) gaat ook over het internet, zoals ook *usenet* (berichten die in nieuwsgroepen worden geplaatst) van het internet gebruik maakt.[14]
Kan iedereen dan zomaar alle opgeslagen informatie in het internet benaderen? Neen. Het *world wide web* bestaat uit meerdere lagen. De buitenste laag zijn de *websites* die door zoekmachines (zoals Google) doorzocht worden met zogeheten *spiders*. Die indexeren dat deel van het *world wide web.* Een zoekopdracht in Google gaat over de buitenste schil, het *surface web*.
Het grootste deel ligt echter onder de buitenste schil en dat wordt het *deep web* genoemd. Dit zijn de niet-geïndexeerde pagina's. Dit zijn veelal gevoelige gegevens: data van overheid, academische, medische en militaire databanken. Alleen met kennis van loginnamen en/of speciale ip-adressen kan toegang daartoe verkregen worden.
Het *dark web* betreft ook de niet-geïndexeerde pagina's. Maar in tegenstelling tot het *deep web* is de informatie in het *dark web* verre van legaal. Hier gaat het om illegaal handelen in wapens, drugs en kinderporno. Toegang tot dit

[14] http://nl.wikipedia.org/wiki/Internet

deel van het internet gaat via een specifieke browser om vervolgens met loginnamen en/of speciale adressen toegang te verkrijgen.[15] Een bekend deel van het *dark web* was de illegale marktplaats *Silk roads.* Deze is door de FBI opgerold.

Voormelde betreft het internet. Maar de kreet *the internet of all things* doet tegenwoordig ook de ronde. Wat omvat dit? Computers zitten tegenwoordig niet alleen meer in pc, *tablet* of *laptop*. Ook de *smart-tv*, de telefoon, de *smart watch*, de koelkast, de auto, het zijn allemaal computers geworden en dus allemaal te koppelen aan een netwerk. Bewakingscamera's, stofzuiger, koelkast, thermostaat, het is dan allemaal op afstand via het internet te benaderen en kan onderling met elkaar communiceren. Het is deze combinatie van apparaten en computers waardoor het kwetsbaar is voor een aanval van *hackers*. Hoe dit in zijn werk kan gaan, op niveau van computer en op niveau van netwerk (internet) wordt beschreven in de volgende paragraaf.

1.5 Hoe werkt *cybercrime*?

1.5.1 Inleiding

Een cybercrimineel maakt misbruik van kwetsbaarheden in computer of mens, om zo computerprocessen te manipuleren. De aard van de bedreiging verschilt: gericht op de pc (zoals *spyware*), gericht op het netwerk (zoals de dos-aanval), of gericht op de mens (zoals *social engineering*).
Veelal is manipulatie van *software* voldoende voor de cybercrimineel, maar soms is de aanval zo kwaadaardig dat ook fysieke apparaten kapot gaan (zoals het stuxnetvirus).

Om een indruk van de omvang van *cybercrime* te krijgen hoeft alleen maar de krant geraadpleegd te worden. Vervolging is lastig, omdat cybercriminelen zich niet aan landsgrenzen houden. Enkele voorbeelden.

> *Hackers* zijn binnengedrongen in een database van hotelketen Marriott. Daarbij kregen ze toegang tot 500 miljoen hotelreserveringen. Bij 327 miljoen reserveringen zijn de namen, mailadressen, telefoonnummers, e-mailadressen, paspoortnummers, accountgegevens, geboortedata gestolen. Bij een niet nader genoemd aantal klanten is ook (versleutelde) creditcardinformatie gestolen.[16]
>
> De hackersgroep *Snake*, die door inlichtingendiensten in verband wordt gebracht met de Russische overheid, nam in 2018 de Duitse overheid onder vuur. De hackersgroep zou het onder meer gemunt hebben op *e-mailaccounts* van Duitse parlementsleden, verschillende ambassades en de Duitse krijgsmacht.[17]

15 http://www.npofocus.nl/artikel/7642/wat-is-het-dark-web
16 https://www.nu.nl/internet/5603609/half-miljard-klantgegevens-van-hotelketen-marriott-gestolen-hackers. html
17 https://www.nu.nl/internet/5602526/russische-hackersgroep-valt-duitse-overheid-opnieuw-aan.html

> *Hackers* hebben toegang gekregen tot 32.000 *accounts* van diensten van mediabedrijf RTL, waaronder Buienradar en Videoland. Daarbij hebben zij toegang gekregen tot persoonlijke informatie op die *accounts*. Het gaat om namen, e-mailadressen, woonadressen en woonplaatsen van gebruikers.[18]

In plaats van het verzamelen van e-mailadressen voor *spamruns* kunnen *hackers* ook veel directer zijn, zoals informatie vergaren voor afpersing.

> De Amerikaanse ministerie van Financiën heeft twee bitcoinrekeningen op een sanctielijst geplaatst omdat twee Iraniërs door middel van afpersing miljoenen *dollars* doorsluisden via deze rekeningen. Zij worden verweten gelieerd te zijn aan SamSam *ransomware*. Beide mannen wordt verweten zes miljoen *dollar* afgeperst te hebben van 200 slachtoffers, waaronder de steden Atlanta, Georgia, Newark. Zij richtten zich vooral op ziekenhuizen en infrastructuur.[19]

> SamSam *ransomware* heeft ook in Nederland tientallen slachtoffers gemaakt. Het effectieve aan SamSam is dat criminelen eerst enkele dagen ongemerkt door het systeem gaan en bekijken of het bedrijf beschikt over voldoende geld. Als dat het geval is dan verwijdert de cybercrimineel de *back ups* zodat het bedrijf daar niet op kan terugvallen. Vervolgens wordt het systeem versleuteld. Het slachtoffer rest dan weinig keuze, betalen of alles kwijt zijn.[20]

Hoe erg de gevolgen van *sextortion* kunnen zijn blijkt wel uit het bericht van de Engelse politie.

> Vier Britse mannen hebben het afgelopen jaar zelfmoord gepleegd nadat ze slachtoffer waren geworden van *sextortion*. De slachtoffers werden tot wanhoop gedreven door hun afpersers. De toename is enorm: 385 in 2015 tot 864 dit jaar. Schotse aanklagers proberen momenteel een Filipijnse man aan te klagen voor de dood van een 17-jarige jongen. *Sextortion* is bedrieglijk eenvoudig. Jonge mannen worden benaderd door criminelen die zich voordoen als aantrekkelijke vrouwen via *datingapps* en aangezet tot seksuele handelingen. Vervolgens worden ze gechanteerd met de beelden van de *webcam*.[21]

Maar de *hack* kan ook gevolgen hebben waarvan menig telefoongebruiker zich niet bewust is. Het was al bekend dat veiligheidsdiensten een telefoon konden beluisteren dat niet in gebruik was. Ook was bekend dat een *webcam* overgenomen kon worden door *hackers* (wat beelden voor *sextortion* kan opleveren). Maar het gaat verder. Er bestaat *malware* om de locatie van de mobiele telefoon te bepalen en de microfoon van de telefoon open te zetten. Hierdoor wordt niet alleen meegekregen wat iemand zegt, maar ook waar hij is als hij dat zegt. De crimineel die iemand wil overvallen weet dan waar, wanneer iemand is en hoort via de telefoon of deze slaapt.

> Er is *malware* dat in staat is om de locatie van een slachtoffer te achterhalen en de microfoon te activeren. Hierdoor is het mogelijk om doelwitten alleen op specifieke locaties, zoals op kantoor of thuis, af te luisteren. Daarnaast is *software* in staat om berich-

---

18 https://www.nu.nl/internet/5602253/hackers-krijgen-toegang-duizenden-accounts-van-rtl-diensten.html

19 https://www.theverge.com/2018/11/28/18116213/iranian-hackers-samsam-ransomware-indictment-bitcoin-sanctions-wallet-atlanta

20 https://www.nu.nl/internet/5606015/uitbraak-samsam-gijzelsoftware-treft-tientallen-nederlandse-bedrijven.html

21 https://www.ad.nl/nieuws/sextortion-drijft-wanhopigen-tot-zelfmoord~a5486480/

> ten van Facebook Messenger, Skype, Viber en WhatsApp af te luisteren. Probeert de gebruiker de telefoon te ontgrendelen, dan wordt stiekem een foto gemaakt met de *frontcamera* van de *smartphone*. Is een slachtoffer in de buurt van een wifi-netwerk van de aanvaller, dan wordt hier mee verbonden. Volgens de onderzoekers wordt de *malware* verspreid op verschillende nepwebsites van *providers*, waar de *app* wordt gepresenteerd als een manier om internetsnelheid te verbeteren.[22]

Voorgaande voorbeelden zijn *cybercrime*. De overtreffende trap van *cybercrime* is cyberterrorisme (een computeraanval op een staat) of *cyberwarfare* (een computeraanval door een staat). Dat dit voorkomt blijkt bijvoorbeeld uit het stuxnetvirus. Dat een dergelijk virus dicht tegen een oorlogshandeling aan zit blijkt uit het volgende.

> Was het stuxnetvirus een digitaal wapen, bedoeld om een land aan te vallen? Een vraag waar brigade-generaal prof. dr. Ducheine op in gaat in het schrijven "Storing of oorlogsdaad"? Hij stelt dat afgevraagd moet worden of het gebruik van *stuxnet* gezien moet worden als een inbreuk op het geweldsverbod van art. 2(4) VN-Handvest. En als dat het geval is, kan Iran *Stuxnet* dan aanmerken als een 'gewapende aanval' uit artikel 51 VN-Handvest en zich vervolgens beroepen op zelfverdediging als rechtsbasis voor een reactie? Hoewel internationale experts het eens waren dat *Stuxnet* een vorm van geweldgebruik (art. 2(4) VN-Handvest) was, verdeelde de vervolgvraag de groep deskundigen. Slechts een minderheid typeerde de inzet van *Stuxnet* (die tot fysieke schade aan de Iraanse nucleaire opwerkingsfaciliteiten leidde) als een gewapende aanval (art. 51 VN-Handvest).[23]

Er is dus in de hackerswereld een overtreffende trap van *cybercrime* naar cyberterrorisme naar *cyberwarfare*. Dit boekt beperkt zich tot *cybercrime.*

Hoe omvangrijk *cybercrime* kan zijn blijkt uit de top tien van zwaarste *hacks*.[24]

TOP TIEN	
1	*Hack* bij websitebedrijf Yahoo: in 2014 zijn de gebruikersgegevens van 500 miljoen gebruikers gestolen (namen, geboortedata, telefoonnummers, wachtwoorden). Om later weer gehackt te worden, waarbij 32 miljoen gebruikersgegevens werden gestolen. Om weer later toe te geven dat de gegevens van 3 miljard gebruikers waren gehackt.
2	*Hack* bij IT-beveiligingsbedrijf *Hold Security*: in 2014 hebben Russische *hackers* 1,2 miljard gebruikersnamen en wachtwoorden verkregen voor 420.000 websites over de wereld.
3	*Hack* bij *Adult Friend Finder*: in 2015 is de *datingsite* gehackt en zijn 4 miljoen gebruikersgegevens publiek gemaakt via het tor-netwerk. Een jaar later gebeurde het weer. Toen ging het om 400 miljoen gebruikers, met 20 jaar aan gebruikersdata.
4	*Hack* bij kortingswinkel Target: data van 110 miljoen klanten werd gestolen. Opmerkelijk is dat niet het bedrijf hierachter kwam, het was de Amerikaanse geheime dienst die het bedrijf waarschuwde na abnormale bankactiviteiten. Het betrof een Oost-Europese hackersgroep. Zij hadden *malware* geïnstalleerd in kasregisters welke de creditcard lazen.

[22] https://www.nu.nl/apps/5090876/pas-ontdekte-android-malware-luistert-microfoon-en-whatsapp-berichten-af.html

[23] http://puc.overheid.nl/mrt/doc/PUC_68346_11/1/

[24] https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks

5	*Hack* in Zuid-Korea: in 2014 zijn de creditcardgegevens van 100 miljoen gebruikers gehackt alsook 20 miljoen bankgegevens. Uit voorzorg werden de *creditcards* van 2 miljoen gebruikers geblokkeerd. De dader bleek een medewerker van de Korea Credit Bureau te zijn. Hij kopieerde de data op een harde schijf en verkocht dit aan bedrijven in de *telemarketing.*
6	*Hack* bij creditcardbedrijf Equifax: gebruikersgegevens zoals namen, geboortedata, sofinummer, rijbewijsnummers van 143 miljoen Amerikanen, Canadezen en Britten zijn gestolen.
7	*Hack* bij Sony: in 2001 werd het netwerk van de *playstation* gehackt, waardoor de gegevens van 77 miljoen gebruikers op straat lag. Van tienduizenden waren ook de bankgegevens gestolen. Om later *Sony Pictures Entertainment* te *hacken*. Er werd 100 *terabyte* aan data gestolen, waaronder het nieuwe scenario van de James Bond film, data van 47.000 werknemers, alsook compromitterende e-mails.
8	*Hack* van Adobe: in 2013 zijn van 2,9 miljoen gebruikers de creditcardgegevens en vervaldata, namen, wachtwoorden en gebruikersnamen gehackt. Later bleek het te gaan om 150 miljoen gebruikers, waarvan 38 miljoen actieve gebruikers. Van Adobe zelf werd 40 *gigabyte* aan bronmateriaal van software gestolen.
9	*Hack* van Ashley Madison: in 2015 zijn 30 miljoen namen, telefoonnummers, e-mailadressen, maar ook de seksuele voorkeur van klanten uit 40 landen gehackt. Dat de seksuele voorkeur bekend was komt omdat dit een overspelwebsite is (hetgeen de deuren voor *sextortion* wagenwijd openzet). Gevolgen: meerdere ontslagen en drie zelfmoorden.
10	*Hack* van Instagram: in 2017 zijn telefoonnummers en e-mailadressen van 6 miljoen gebruikers gehackt.

Uit voorgaande blijkt dat niet alleen multinationals kwetsbaar zijn, zelfs IT-bedrijven worden gehackt, hetgeen aantoont hoe lastig het is *cybercrime* te voorkomen. Het gaat veelal om gebruikersdata, maar soms worden ook bedrijfsgeheimen gestolen. De vraag is natuurlijk waarom een bedrijf diens bedrijfsgeheimen toegankelijk maakt via het internet. Dat de gebruikersgegevens op het netwerk staan is begrijpelijk; als een gebruiker zich inlogt moet het systeem kunnen controleren of de gebruiker mag inloggen. Maar waarom moeten bedrijfsgeheimen via een openbaar netwerk bereikbaar zijn? Het toont aan dat ook grote bedrijven niet altijd even goed over *cybersecurity* nadenken.
Daar waar het klantgegevens betreft worden deze in de miljoenen verkocht aan telemarketingbedrijven die er gebruik van maken voor *spamming*. Maar het wordt ook gebruikt voor virusaanvallen verpakt als *spam*. Daar waar ze creditcardgegevens verkrijgen is het soms mogelijk om de creditcardsgegevens te gebruiken voor *online* aankopen. En daar waar het gaat om *datingsites* (zeker in geval van overspelsites) is er het risico van *sextortion*.

1.5.2 Aanvallen op de computer

Aanvallen op de *software* hebben tot gevolg dat de programmeertaal veranderd wordt. Er worden regels gewijzigd, toegevoegd, verwijderd. Dit zorgt ervoor dat het programma niet meer werkt zoals het hoort. Het doet wat de *hacker* wil en kan zelfs schade veroorzaken aan de *hardware*.

> Een voorbeeld is het beruchte *stuxnetvirus*. Dit virus is vermoedelijk van de hand van de Amerika en Israël en is bedoeld om de uranium verrijkende centrifuges van Iran te saboteren. Als virus ging het het internet over en besmette duizenden computers. Het viel echter niet alle computers aan. Het was gericht op een specifiek programma van Siemens, Simatic step 7 en Simatic WinCC. Deze programma's maken deel uit van een *industrial control system* en zijn controleprogramma's voor apparaten, waaronder uraniumverrijkende centrifuges van Iran. Door het virus werd het sturingsprogramma aangevallen, waardoor veel centrifuges kapot zijn gegaan.[25]

Veranderen programmeertaal

De verzamelnaam voor alle *software* met een opzettelijk kwaadaardige werking is *malware* (samenvoeging van malafide en *software*). Als de aanval specifiek gericht is op de computer kan gedacht worden aan het gebruik maken van virussen, wormen, of Trojaanse paarden:[26]

- Een virus is een programma dat de werking van de computer verstoort. Een virus kan gegevens op de computer beschadigen of verwijderen, het e-mailprogramma gebruiken om zichzelf te verspreiden of zelfs de gehele harde schijf wissen. Veel virussen worden per e-mail verspreid en zijn vermomd als onschuldige bijlage (een foto of een geluidsbestand).[27]
- Een computerworm is een zichzelf vermenigvuldigend computerprogramma. Via een netwerk worden kopieën van de worm doorgestuurd zonder tussenkomst van een tussengebruiker.[28]
- Een Trojaans paard is een functie dat verborgen is in een programma dat door de gebruiker wordt geïnstalleerd. Deze functie kan toegang tot de geïnfecteerde computer verschaffen aan kwaadwillenden en zo schade toebrengen aan computergegevens of de *privacy* van de gebruiker kan aantasten. De naam komt van het Paard van Troje. Het paard waarin Griekse soldaten waren verstopt om zo de stad Troje binnen te komen. Om vervolgens de poorten van de stad van binnenuit te openen en de stad te veroveren.[29]

Wat is het verschil tussen deze vormen van *malware*?

Een virus heeft een computerprogramma nodig om zich aan vast te hechten en voert een gerichte aanval uit op een computer.

Een worm kan zich zonder hulp van een gebruiker verspreiden en brengt schade toe aan een netwerk.

Een Trojaans paard lijkt op een worm in de zin dat het niet zelfstandig beschadigingen veroorzaakt. Maar terwijl de worm zich wel kopieert naar ander computers, moet een Trojaans paard door de gebruiker gekopieerd worden.[30]

---

25 http://mens-en-samenleving.infonu.nl/internationaal/163739-van-stuxnet-naar-cyberoorlog-hoe-een-virus-een-bom-vervangt.html

26 http://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/

27 http://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/

28 http://nl.wikipedia.org/wiki/Computerworm

29 http://nl.wikipedia.org/wiki/Trojaans_paard_(computers)

30 http://nl.wikipedia.org/wiki/Trojaans_paard_(computers); http://nl.wikipedia.org/wiki/Computerworm

Hoewel *spam* geen virus of worm is, betekent dat niet dat *spam* dat niet kan bevatten. *Spam* is bij *hackers* een populair transportmiddel voor *malware*. *Hackers* gebruiken de miljoenen gehackte e-mailadressen om daar *spam* naar te verzenden. In de *spam* is dan *malware* verstopt, waarbij bij het aanklikken van de *spam* een virus of Trojaans paard wordt geactiveerd.

> Verdachte heeft via een aantal *spamruns* onschuldig ogende e-mails verstuurd naar duizenden bedrijven. Deze e-mails bevatten een gemanipuleerd Word-bestand. Zodra een ontvanger dit Word-bestand opende, werd automatisch op de computer van de ontvanger *malware* (genaamd njRAT) geïnstalleerd. NjRAT is een variant van een *Remote Access/Administration Tool* (RAT), *software* waarmee op afstand toegang tot computers kan worden verkregen. Na installatie werd njRAT telkens bij het opstarten van de computer geactiveerd. Eenmaal geïnfecteerd meldden de besmette computers zich aan op het beheerderspaneel dat op de computer van de verdachte geïnstalleerd was. Op dat moment was het voor de verdachte mogelijk om mee te kijken op het computerscherm van het slachtoffer en kon de verdachte ook de controle over de muis en het toetsenbord overnemen. Ook hield de RAT bij welke toetsaanslagen op het toetsenbord van de besmette computer werden gemaakt (*keylogging*). Op deze wijze werden wachtwoorden en inloggegevens verkregen waarmee zij konden inloggen op de internetbankieromgevingen van de gehackte slachtoffers.[31]

Onderscheppen invoer

Het verkrijgen van vertrouwelijke gegevens hoeft niet via manipulatie van bestaande *software* in de computer. Via *spam* of *phising* wordt een *keylogger* geïnstalleerd. Dit is een programma dat alle toetsaanslagen registreert op de computer van het slachtoffer en die informatie doorstuurt naar de computer van de cybercrimineel. Als het slachtoffer dan (dagen later) naar zijn internetbank gaat om geld over te maken dan worden die gegevens onderschept zodat de cybercrimineel dat kan misbruiken.[32]

> Verdachte is veroordeeld voor het plaatsen van *keyloggers* tussen het toetsenbord en de computer waardoor inloggegevens verzameld konden worden. In een periode dat verdachte depressief was en 'klaar was met studeren', heeft hij *keyloggers* gebruikt en daarmee gebruikersnamen en wachtwoorden van medewerkers en studenten verworven.[33]

Behalve het registreren van toetsaanslagen zijn er ook programma's die vastleggen wat op het scherm wordt geprojecteerd. Dit zijn zogeheten *screenscrapers*.

Gluurprogramma's

Gluurprogramma's worden ook wel *spyware* genoemd. Deze registreren niet de aanslagen maar kijken mee. Het gedrag van de gebruiker wordt geregistreerd (welke *websites* worden bezocht, welke programma's worden gebruikt). Deze data wordt doorgestuurd naar een partij die die informatie gebruikt om er rijker van te worden (zoals telemarketeers).

---

31 Gerechtshof Den Haag 05-09-2017, ECLI:NL:GHDHA:2017:2519

32 https://nl.wikipedia.org/wiki/Phishing

33 Rechtbank Zeeland-West-Brabant 09-05-2018, ECLI:NL:RBZWB:2018:2991

Een probleem is dat *spyware* geen virussen zijn en als zodanig niet herkend worden door antivirusprogramma's. Daarvoor zijn anti-spywareprogramma's beschikbaar.[34]

Gijzelingsprogramma's
Een vorm van *malware* is *browser hijacking.* Dat type programma zorgt ervoor dat de instellingen van de *webbrowser* zonder toestemming van de gebruiker gewijzigd worden. Wijzigingen kunnen zijn het instellen van een andere *home page*, of een andere zoekmachine. Doel hiervan is de computer te dwingen naar een bepaalde *website* te gaan en zo het aantal bezoekers te verhogen. Omdat advertentie-inkomsten afgerekend worden op het aantal *hits* van de *website* levert dit geld op.
Maar *malware* is zelden een geïsoleerd programma. Het komt dan ook voor dat met dit gijzelingsprogramma tevens een *keylogger* wordt geïnstalleerd.[35]

Een zeer agressief gijzelingsprogramma is *software* dat de gebruiker geheel buitensluit, *ransomware* (gijzelsoftware) geheten. Gaat het specifiek om het versleutelen van bestanden, dan wordt dit *cryptoware* genoemd. Middels krachtige encryptie versleutelt de cybercrimineel op afstand de computer van het slachtoffer. Deze krijgt dan alleen tegen betaling (van bijvoorbeeld *bitcoins*) de sleutel om de data op de computer weer te kunnen openen. Maar zoals alle vormen van afpersing: er is geen enkele garantie dat na betaling niet een nieuwe geldsom wordt geëist of dat de sleutel wordt gegeven. Meestal is de beste optie om de computer geheel te wissen en dan opnieuw te installeren met een *back up* van de data (als deze is gemaakt natuurlijk).[36]

> Zo is een ziekenhuis gedwongen $ 55.000 te betalen om het gegijzelde IT-systeem te ontsleutelen. Hoewel de *malware* werd ontdekt, was het te laat om verspreiding naar het e-mailsysteem, de elektronische patiëntendossiers en het interne *operating system* tegen te houden. Het ging in totaal om 1.400 versleutelde bestanden. De Oost-Europese *hackers* hadden toegang tot het ziekenhuissysteem verkregen via een derde partij welke zaken deed met het ziekenhuis. Hoewel het ziekenhuis wel *back ups* had, leerde een simpele rekensom dat betalen goedkoper was dan herstellen.[37] Daarmee een groot risico nemende dat de ontsleutelingscode mogelijk helemaal niet verstrekt zou worden.

Voormeld voorbeeld maakt het gebrek aan moraliteit van cybercriminelen duidelijk: een ziekenhuis platleggen waardoor geen operaties meer kunnen worden uitgevoerd. Hoe hoger de druk, hoe hoger de kans op betaling, ongeacht de levens die verstoord worden of zelfs in gevaar worden gebracht.

---

34 http://nl.wikipedia.org/wiki/Spyware
35 https://en.wikipedia.org/wiki/Browser_hijacking
36 http://www.consumentenbond.nl/veilig-internetten/ransomware-cryptoware-gijzelsoftware
37 https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

Wachtwoordkrakers
In geval van *password cracking* richt de *hacker* zich op het wachtwoord. Als de voordeur open is (wachtwoord), waarom dan nog door de achterdeur gaan (virus)?
Het wachtwoord kan verkregen worden via *social engineering.* Een medewerker van een zogenaamde *helpdesk* belt de computergebruiker op en vraagt om het wachtwoord om op afstand te helpen met een probleem dat de verdachte heeft verzonnen (bijvoorbeeld het installeren van een *update* tegen een bepaald virus). Zodra het wachtwoord is gegeven, kan de *hacker* via de voordeur het systeem in.
Het wachtwoord kan ook gekraakt worden middels speciale software dat wachtwoorden genereert. Dit kan behoorlijk effectief zijn omdat veel mensen nogal voor de hand liggende wachtwoorden kiezen.

1.5.3 Aanvallen op het netwerk

Behalve de bron of het einddoel (de computers), kan ook het transport (het netwerk) aangevallen worden. Aanvallen op het netwerk kunnen actief of passief plaatsvinden.
Bij een passieve aanval wordt stromende data over het netwerk onderschept; bij een actieve aanval wordt het normale netwerkverkeer verstoord of wordt gepoogd toegang te krijgen tot data of objecten die benaderbaar zijn via het netwerk.[38]

Passieve netwerkaanvallen[39]
Voorbeelden van passieve netwerkaanvallen:

- Tappen, hiermee wordt de glasvezelkabel afgetapt waardoor de data over die kabel wordt onderschept. Dat kan passief plaatsvinden (alleen lezen van de data) of actief (het veranderen van verzonden data).[40]
- De *port scanner*, dit is is een applicatie welke ontworpen is om *servers* te controleren op open poorten. Hoewel dit legitiem kan zijn, kan het ook met criminele intentie worden gebruikt. Als een open poort is gevonden, dan kan data verzonden worden om een *buffer overflow* te creëren.[41]
- De *idle scan,* dit is een TCP poort-*scan* dat bestaat uit het versturen van *spoofed packets* aan een computer om vast te kunnen stellen welke diensten beschikbaar zijn. Dit wordt bereikt door te doen alsof het een andere computer is (een zombie genoemd) en vervolgens het gedrag van dat zombie-systeem te observeren.[42]

38 https://en.wikipedia.org/wiki/Network_security
39 https://en.wikipedia.org/wiki/Network_security
40 https://en.wikipedia.org/wiki/Telephone_tapping
41 https://en.wikipedia.org/wiki/Port_scanner
42 https://en.wikipedia.org/wiki/Idle_scan

- Encryptie, dit betreft het versleutelen van informatie op een wijze zodat deze niet door onbevoegde derden gelezen kan worden.[43]
- *Traffic analysis,* dit betreft het onderscheppen en onderzoeken van berichten om patronen te ontdekken in communicatie, zelfs als deze gecodeerd is. Dit wordt veelal gebruikt door militaire inlichtingendiensten.[44]

Actieve netwerkaanvallen[45]
Voorbeelden van actieve netwerkaanvallen:

- *Network eavesdropping*, dit is een aanval dat gericht is op het onderscheppen van kleine *packets* van het netwerk welke zijn verzonden door andere computers.[46]
- *(Distributed) denial-of-service,* een (D)dos-aanval heeft tot gevolg dat een computersysteem niet beschikbaar is voor gebruikers.[47] Dit kan veroorzaakt worden doordat een *botnet* tegelijkertijd diens zombiecomputers een specifieke *website* laat bezoeken.
- *DNS spoofing* of *DNA cache poisening,* dit is een aanval waarbij de domeinnamentabel (*Domain Name System*) van een *internetserver* wordt aangetast. Bij een DNS-vergiftiging worden de adressen vervangen door nepadressen. Wanneer dan een URL wordt opgevraagd in een aangetaste DNS-tabel, wordt dit verzoek niet doorgestuurd naar de legitieme URL, maar naar een vervalste pagina.[48]
- *Man in the middle-attack*, dit is een aanval waarbij informatie tussen twee partijen onderschept wordt zonder dat deze partijen zich hiervan bewust zijn. De cybercrimineel onderschept de informatie en kan deze lezen, wijzigen, maar kan het ook versturen alsof het bericht van een van de gebruikers afkomstig is.[49]
- *ARP (Address Resolution Protocol) poisoning, ARP spoofing, ARP cache poisoning* of *ARP poison routing,* dit is een techniek waarbij de *hacker* ARP- berichten verstuurt naar een lokaal netwerk. Het doel is het adres van de *hacker* te associëren met het IP-adres van een andere *host*, zodat het dataverkeer van de andere computer naar de computer van de *hacker* gaat.[50]
- VLAN (virtueel lokaal netwerk) *hopping,* dit is een aanvalsmethode waarbij het netwerk middels een virtueel lokaal netwerk wordt aangevallen,

43 https://en.wikipedia.org/wiki/Encryption
44 https://en.wikipedia.org/wiki/Traffic_analysis
45 https://en.wikipedia.org/wiki/Network_security
46 https://en.wikipedia.org/wiki/Eavesdropping
47 https://nl.wikipedia.org/wiki/Denial_of_service
48 https://nl.wikipedia.org/wiki/DNS-vergiftiging
49 https://nl.wikipedia.org/wiki/Man-in-the-middle-aanval
50 https://en.wikipedia.org/wiki/ARP_spoofing

zodat de *hacker* deze kan overnemen.[51]

- Een *smurf attack,* dit is een een dos-aanval tegen een *host*. De aanval werkt door ICMP *echo requests* (ook wel ping geheten) met een vervalst IP-bronadres naar een *broadcast* adres binnen het netwerk te sturen. De aangevallen *host* zal overspoeld worden met de antwoorden op deze verzoeken, waardoor het netwerkverkeer verstopt raakt.[52]
- *Buffer overflow,* dit is een aanval waardoor gegevens sneller bij een computer via het netwerk binnenstromen dan ze verwerkt kunnen worden door het systeem. De buffer is te klein voor de omvang van de verzonden data, hetgeen leidt tot een *buffer overflow*.[53]
- Een SQL (*structured query language*)-injectie, dit heeft tot doel dat de *server* informatie geeft dat valt buiten de reguliere vragenstructuur. Zo kan de url worden aangepast om vragen aan de database te stellen die niet via de reguliere *website* te stellen zijn. Als de webomgeving onvoldoende is afgeschermd, dan zal de vraag doorgestuurd worden aan de SQL-server. Die SQL-server vertrouwt de *webserver* en geeft antwoord. "Het gaat om gebruikmaking van een 'achteringang' tot de informatie op de server en daarmee naar 's Hofs oordeel derhalve tot die *server* zelf."[54]
- *Phising,* dit is het hengelen naar informatie om te misbruiken. Meestal geschiedt dit door het verzenden van een e-mail waarin de ontvanger een verhaal voorgeschoteld krijgt dat hij zijn inlogcode bij de bank moet controleren. Hiervoor moet op een *link* geklikt worden in de e-mail. Deze *link* lijkt verwijzen naar een legitieme *website* van de bank, maar verwijst in werkelijkheid naar een nagebouwde *website* van de cybercrimineel. Als daar de inlogcode van de bank ingevuld wordt, dan komt die code bij de criminelen, die vervolgens die code gebruiken om de bankrekening leeg te halen.
  Een variant is *spear fishing*. In dat geval wordt een e-mail aan een slachtoffer verzonden welke uit de eigen organisatie lijkt te komen. Daarin vraagt een 'directielid' om vertrouwelijke informatie van zijn werknemer.
- *URL-spoofing,* dit is het nabootsen van de URL van een legitieme *website*, zodat de gebruiker denkt de echte *website* te bezoeken terwijl de URL van een cybercrimineel is. Dit wordt gebruikt bij *phising*.
- *Pharming,* hierbij wordt een DNS-server aangevallen en wordt het IP-adres van een domeinnaam gewijzigd. Het slachtoffer voert het hem bekende webadres in, en komt dan op de valse *website* terecht. De term *pharming* is gekozen analoog met de term *phishing*. Hoewel *pharming* gelijkenissen vertoont met *phishing*, is deze techniek verraderlijker

51 https://en.wikipedia.org/wiki/VLAN_hopping
52 https://nl.wikipedia.org/wiki/Smurf_(computeraanval)
53 https://nl.wikipedia.org/wiki/Bufferoverloop
54 Rechtbank Rotterdam 14-04-2010, ECLI:NL:RBROT:2010:BM1172

omdat de gebruiker te goeder trouw naar een valse *website* kan worden doorgezonden.[55]

- *Cross-site scripting,* dit betreft een fout in de beveiliging van een web-applicatie. De invoer die de webapplicatie ontvangt (zoals *cookie*, *url*, *request parameters*) wordt niet juist verwerkt en komt hierdoor in de uitvoer terecht naar de eindgebruiker. Via deze *bug* kan kwaadaardige code geïnjecteerd worden. Hiermee kunnen onder meer *sessiecookies* worden bekeken, sessies van een gebruiker worden overgenomen, de functionaliteit van een *website* worden verrijkt of onbedoelde acties voor een gebruiker worden uitgevoerd.[56]

Onderwerping van computers
Botnets zijn netwerken van computers die zonder medeweten van hun eigenaar zijn overgenomen door de cybercrimineel. De computer van de *hacker* is de *master*, die van de slachtoffers zijn *slaves*. Hij kan dit *botnet* gebruiken voor het uitvoeren van dos-aanvallen, het versturen van *spam*, het delven naar *bitcoins* (*cryptomining* geheten).[57]
Als de computers tot *slaves* worden gemaakt voor het specifieke doel van *cryptomining* dan wordt die handeling *cryptojacking* genoemd (vernoemd naar *carjacking*, *hijacking*).[58]

1.5.4 Aanvallen op de mens

Aanvallen gericht op de mens kunnen bestaan uit het verkrijgen van gegevens (middels *social engineering, social hacking*), maar ook uit het ongevraagd moeten lezen van reclame (*spam*), of terroriseren/afpersen van mensen.

Social engineering is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid met als doel persoonlijke informatie in te winnen.[59]
Op deze wijze kunnen de best beveiligde systemen ge*hack*t worden omdat het slachtoffer vrijwillig de digitale sleutels van de voordeur van het systeem aan de verdachte geeft. Het slachtoffer denkt bijvoorbeeld dat hij een *helpdesk* aan de lijn heeft, geeft daar zijn wachtwoord en gebruikersnaam aan af, terwijl het een *hacker* is die zijn computer *hack*t.

Spam is een verzamelnaam voor ongewenste berichten en is ook bekend als *Unsolicited Commercial E-mail* en *Unsolicited Bulk E-mail.* Onder deze term vallen ongewenste e-mails en reclameboodschappen op *websites*. Niet iedere

55 http://nl.wikipedia.org/wiki/Pharming_(internet)
56 https://nl.wikipedia.org/wiki/Cross-site_scripting
57 http://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/
58 http://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/
59 www.fraudehelpdesk.nl/verklaring/p_Social_engineering_p.

e-mail van een bedrijf is *spam*. *Spam* is een bericht dat wordt gestuurd aan een groep die veel groter is dan de potentiële doelgroep. Bij *spam* wordt met hagel geschoten, in de hoop iets te raken. Dat veroorzaakt ook de overlast, omdat slechts een zeer kleine groep van ontvangers geïnteresseerd zou kunnen zijn. Dat dit toch voor de verzender effectief kan zijn komt door de omvang van de *spamrun* (miljoenen gebruikers). Bij digitale post zijn geen portokosten. Het kost slechts 150 euro om 20 miljoen spamberichten te verzenden.[60]

In geval van *revenge porn* (wraakporno) verspreidt de cybercrimineel pornografisch/naaktmateriaal van personen zonder diens toestemming. Dit materiaal kan gemaakt zijn door een ex-partner terwijl het slachtoffer in het verleden hieraan vrijwillig meewerkte, maar het kan ook heimelijk zijn gemaakt. Het verzamelde materiaal wordt gebruikt om wraak te nemen voor het beëindigen van de relatie.[61]
Als geld of seksuele handelingen geëist worden, dan is niet meer sprake van *revenge porn* maar van *sextortion*.

1.6 Cryptocurrency

Cryptocurrency staat voor digitale (virtuele) munteenheden. De cryptomunten worden als versleutelde series programmeercode verstuurd over het internet. Die versleuteling heet cryptografie. Cryptomunten zijn niet gereguleerd. Er bestaat geen plicht om deze munten aan te nemen, of om te wisselen voor fysiek (echt) geld. Dat laat onverlet dat mensen ervoor kunnen kiezen om dit geld wel te accepteren. En dan geldt, hoe meer mensen het accepteren, hoe meer ingeburgerd het raakt. Voorbeelden van cryptogeld zijn de *bitcoin*, *ethereum*, *litecoin* en de (digitale) gulden.[62]

Cryptocurrency heeft op zich niets met *cybercrime* van doen. Het is niet strafbaar om het te hebben, het wordt niet gebruikt om *cybercrime* mee te plegen (in de zin dat het geen *hackingtool* is). Dat betekent niet dat het niet een zeer centrale rol speelt bij *cybercrime*. De anonimiteit van de bezitter maakt cryptogeld ideaal voor criminelen. Bij een *ransomware* aanval wordt om betaling in *bitcoins* gevraagd, zo ook bij *sextortion*.

> Een politieambtenaar kijkt het wachtwoord van een collega af van het politiesysteem en gebruikt zonder diens toestemming diens wachtwoord om de kentekens van 77 auto's geparkeerd op een homo-ontmoetingsplaats op te vragen. Hij verstuurde aan 29 personen een brief waarin stond dat zij naar hun woning zijn gevolgd en dat de foto's van de activiteiten bij de parkeerplaats openbaar zouden worden gemaakt aan hun familie en omgeving, tenzij de slachtoffers *bitcoins* ter waarde van € 1.000 euro p.p. aan verdachte zouden geven. In totaal gaat het om twintig pogingen afdreiging.[63]

60 http://nl.wikipedia.org/wiki/Spam_(post)
61 http://en.wikipedia.org/wiki/Revenge_porn
62 https://www.simyo.nl/blog/cryptocurrency-en-bitcoins/
63 Gerechtshof Arnhem-Leeuwarden 23-02-2018, ECLI:NL:GHARL:2018:1959

Voor witwassen van criminele opbrengsten is de *bitcoin* dan ook van groot belang.
Nu is er een vorm van *cybercrime* waarbij het doel is om *bitcoins* te delven (*cryptojacking*). Dat is een fase voor het witwassen, het is de fase van verkrijging van het cryptogeld. Maar het strafbare feit is op zich niet de *bitcoin*, maar het op criminele wijze delven naar de *bitcoin*.

Hoofdstuk 2 Ontwikkeling cyberwetgeving

2.1 Algemeen

De wetgever is eind jaren tachtig bewust geworden van de steeds verdergaande impact van informatiecommunicatietechnologie op de maatschappij. Weliswaar was de Hoge Raad in staat om klassieke wetgeving (opgemaakt in een pre-computertijdperk) zo uit te leggen dat het ook toepasbaar was in de digitale wereld, maar het oprekken heeft zijn grenzen. Zo worden computerbestanden aangemerkt als geschriften in de zin van artikel 225 van het Wetboek van strafrecht. Maar er doemden al snel allerlei problemen op: het inbreken op een computersysteem is geen huisvredebreuk en vereist aparte strafbaarstelling. Ook is het stelen van gegevens geen diefstal. Dit soort problemen eisen nieuwe wetgeving.
Met de Wet computercriminaliteit I werd tegemoet gekomen aan een veranderende wereld. Internationaal werd het belang van regelgeving inzake *cybercrime* ook onderkend, resulterend in het Cybercrimeverdrag, welke in Nederland leidde tot de Wet computercriminaliteit II. De laatste loot aan de stam van computerregelgeving is de Wet computercriminaliteit III.

2.2 Wet computercriminaliteit I

In de jaren zeventig zijn strafbepalingen ingevoerd ter bescherming van de persoonlijke levenssfeer. Hierdoor is het afluisteren van gesprekken met een technisch hulpmiddel strafbaar gesteld, voor zover het mondelinge communicatie betrof. Datacommunicatie was toen nog niet aan de orde.[64]
De digitale ontwikkeling maakte de strafwetgeving gedateerd. Daarop is de Wet computercriminaliteit ingevoerd. Er is gekozen aansluiting te zoeken bij bestaande wetgeving. Daarom is er geen aparte titel in de strafwetten voor *cybercrime*-bepalingen. Computervredebreuk is geplaatst bij huisvredebreuk; computervernieling bij de zaaksbeschadiging.[65]

Hacking (was artikel 138a, thans 138ab Sr)
De basis voor bestrijding van *cybercrime* is het strafbaar stellen van *hacking*. "Het beschermt degeen die blijkens feitelijke beveiliging heeft duidelijk gemaakt dat hij zijn gegevens heeft willen afschermen tegen nieuwsgierige blikken. Het gaat hierbij om een uitwerking van het beginsel dat het medium wordt beveiligd. (…) Aansluiting is gezocht bij het bestaande artikel 138 van het Wetboek van Strafrecht betreffende de huisvredebreuk. Daar geldt in

64 Artikelen 139a tot en met 139g, 441 a en 441 b Sr en de artikelen 125f tot en met 125h Sv.
65 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 7.

beginsel dat een ieder vrij is te gaan waar hij wil. Zelfs wanneer iemand wederrechtelijk in een woning, besloten lokaal of erf vertoeft, is hij nog niet zonder meer strafbaar. Slechts na een weigering te voldoen aan de vordering van de rechthebbende of wanneer wederrechtelijk is binnengedrongen, ontstaat er strafbaarheid. Deze eisen zijn in de sfeer van de informatietechniek vertaald in de eis, dat een beveiliging moet zijn doorbroken."[66]
Nu kan het voorkomen dat er geen beveiliging wordt doorbroken. Omdat in die gevallen veelal ook sprake is van vernieling/beschadiging van gegevens is vervolging toch wenselijk. Daarom heeft de wetgever in deze wet computervernieling strafbaar gesteld (artikel 350 e.v. Sr).

Vernieling/beschadiging (artikel 350 e.v. Sr)
Er was overwogen om computervernieling aan te pakken via het bestaande artikel 350 Sr. Immers de data staat op gegevensdragers (cd-rom, *USB-stick*, harde schijf) en dat is een goed welke valt onder artikel 350 Sr.
De minister signaleert echter een probleem met betrekking tot tijdelijke versus permanente gegevensdragers: "Deze benadering acht ik onwenselijk omdat het leidt tot een overspanning van het begrip «goed». Hoewel inderdaad het beschadigen van een grammofoonplaat leidt tot het veranderen of wissen van gegevens, neergelegd in de groef, en zeer wel wegens zaaksbeschadiging zou kunnen worden vervolgd, sluit bij voorbeeld het wissen van een tekening op een schoolbord in mindere mate aan bij het gewone taalgebruik indien deze handeling zou worden aangemerkt als beschadiging van het schoolbord als informatiedrager. Het verschil ligt daarin dat de grammofoonplaat is vervaardigd uitsluitend met het doel om die specifieke informatie die daarop is vastgelegd, blijvend daarop ter beschikking te doen zijn, terwijl een schoolbord juist is ontworpen met het oog op de mogelijkheid gegevens tijdelijk vast te leggen en ook weer makkelijk te kunnen wissen. Dit gebruik overeenkomstig zijn bestemming kan men toch bezwaarlijk als beschadiging van het goed aanmerken.
Daarom geef ik er de voorkeur aan een afzonderlijke bepaling op te nemen gericht op de aantasting van gegevens ongeacht de wijze waarop zij zijn vastgelegd."[67]

Vernieling geautomatiseerde werken (artikel 161septies/sexies Sr)
Computers zijn veelal gekoppeld in een netwerk. De schade kan beperkt zijn tot één of enkele computers. Daarvoor is artikel 350a e.v. Sr geschikt. Maar wat als er algemene gevaarzetting is? Als een netwerk zwaar hinder ondervindt van de vernieling? Daarvoor zijn de artikelen 161septies (opzet) en 161sexies (schuld) Sr ingevoerd.

66 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 15-17.
67 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 23-25.

Skimming
Nu raken de vorige artikelen het *hacken* van de computer of het netwerk. Maar duidelijk werd dat ook betaalpassen gekopieerd kunnen worden om zo de betaalautomaat 'te *hacken'*. De wetgever vond het dan ook wenselijk om een speciale bepaling op te nemen ter bescherming van betaalpassen en waardekaarten.
"De wenselijkheid om een bijzondere bepaling op te nemen vindt zijn grondslag daarin dat sommige betaalpassen of waardekaarten zo kunnen zijn ingericht dat deze veelvuldige wijzigingen kunnen ondergaan, bij voorbeeld met het oog op de indicatie van het tegoed dat de betrokkene nog op een rekening heeft staan. Een bijzondere bepaling lijkt gewenst nu deze kaarten in de samenleving steeds meer zullen worden gebruikt, en de financiële voordelen die daarmee kunnen worden behaald, daardoor toenemen."[68]

Schending bedrijfsgeheimen (artikel 273 Sr)
De wetgever realiseerde zich dat bedrijfsgeheimen steeds vaker in computersystemen vastgelegd worden. Om die geheimen te beschermen is artikel 273 Sr aangepast.[69]

Wijzigingen Wetboek van strafvordering
Het bestrijden van *cybercrime* vereist een tweeledige aanpak: strafbaarstelling van specifieke handelingen, maar ook geven van specifieke bevoegdheden aan opsporingsambtenaren. Daarom zijn bepaalde bestaande bevoegdheden gewijzigd en nieuwe toegevoegd.
Zo is de term «afluisteren» vervangen voor «aftappen» zodat elke vorm van onderscheppen van gegevensverkeer hieronder valt, dus spraak, geschriften, beelden of data, zonder dat sprake is van vastleggen van deze gegevens." (artikel 125g Sr).[70]

Een nieuwe bevoegdheid die met de eerste computerwet is ingevoerd is de doorzoeking van een plaats ter vastlegging van gegevens (artikel 125i Sv).[71]
Nu regelt deze bevoegdheid de doorzoeking op een fysieke plaats, terwijl door netwerken gegevens zich zelden op dezelfde plaats als de computer bevinden. De data staat op de harde schijf van een *server* (de '*cloud'*). Daarom heeft de wetgever de netwerkzoeking als bevoegdheid opgenomen in artikel 125j Sv.
"De voorgestelde bepaling bevat de eis dat de elders zich bevindende geautomatiseerde werken slechts toegankelijk zijn voor een onderzoek in het kader van een huiszoeking, indien deze toegankelijk zijn voor de personen die regulier toegang hebben tot de locatie van huiszoeking. De band tussen de personen en de locatie is niet omschreven in de zin van pure feitelijkheid,

68 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 19-20.
69 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 21-22.
70 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 26.
71 Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 26-27.

noch in strikt juridische zin. Het gaat niet om personen die min of meer toevallig of incidenteel op de locatie aanwezig zijn of zijn geweest. Evenmin gaat het slechts om personen die rechtmatig toegang hebben tot de locatie. Een juridische band tussen een locatie en een persoon is niet altijd vast te stellen. De bepaling duidt op iets daar tussenin: personen die regelmatig verblijven op de locatie, hetzij doordat zij daar wonen, regelmatig werken of verblijven. Het wonen en verblijven sluit aan bij het voorschrift dat van de rechter eist iemands woon– of verblijfplaats vast te stellen. Bij computercriminaliteit zal het bovendien vaak gaan over personen die in dienst zijn van een bedrijf.
Samenvattend gaat het om een dubbele band. Er moet een feitelijke band zijn, in de zin van een gewoonte, tussen personen en de locatie waar de huiszoeking plaatsvindt. Er moet een juridische band zijn tussen deze personen en het geautomatiseerd werk waarin een onderzoek wordt gedaan. Zijn de voorwaarden voor deze dubbele band niet aanwezig, dan kan tijdens een huiszoeking geen onderzoek elders worden gedaan. De privacy van degeen die gegevens in een geautomatiseerd werk heeft opgeslagen, heeft dan de overhand."[72]
Nu kan in geval van een (fysieke) doorzoeking een kast op slot zijn. Geeft de bewoner de sleutel niet, dan kan de opsporingsambtenaar het slot verbreken. Dit geldt niet zomaar voor de digitale variant. Als een computer op slot zit, dan is hulp van een deskundige nodig. "Inherent aan de bevoegdheid tot onderzoek is daarom de bevoegdheid het bevel te geven toegang te verlenen."[73] Dit wordt ook wel het bevel tot decryptie genoemd (artikel 125k Sv).

Met voorgaande is de basis gelegd voor computerstrafrecht.

2.3 Cybercrimeverdrag

Het heeft acht jaar geduurd na invoering van de Wet Computercriminaliteit I voordat er een verdrag kwam met betrekking tot *cybercrime*. Dit is het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (het Cybercrimeverdrag).
Het doel van het verdrag is een mondiale aanpak van wetgeving inzake computercriminaliteit, om zo het opsporen en bestraffen van computercriminelen te vereenvoudigen. Het verdrag was in eerste instantie ondertekend door 38 staten, waaronder de Europese staten, de Verenigde Staten, Canada, Japan en Zuid-Afrika. Inmiddels is het toegenomen tot vijftig, maar Rusland is nog steeds geen lid.

De doelen van het verdrag zijn:
- constitutieve elementen harmoniseren inzake misdrijven van het nationale materiële strafrecht;

[72] Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 27-28.
[73] Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pag. 28.

- internationale samenwerking door grensoverschrijdende opsporingsbevoegdheden voor justitie en politie;
- verdragstaten voorzien in de bestraffing van computermisbruiken.[74]

2.4 Wet computercriminaliteit II

Nederland heeft gehoor gegeven aan de aangegane verplichtingen in het Cybercrimeverdrag door de Wet Computercriminaliteit II in te voeren.[75]

Vernietiging/ontoegankelijk maken van computergegevens
In de praktijk werd een probleem onderkend welke verbonden was aan de netwerkzoeking: computergegevens waarmee strafbare feiten werden gepleegd mochten worden gekopieerd voor waarheidsvinding, maar het origineel moest achter blijven bij de verdachte. Er mocht geen onttrekking of verbeurdverklaring plaatsvinden. Dit omdat de klassieke bepalingen voor beslag niet op gegevens van toepassing zijn (gegevens zijn geen goed).[76]
Daarop is in artikel 125o Sv de bevoegdheid opgenomen om computergegevens waarmee of met behulp waarvan een strafbaar feit is gepleegd, bij wijze van voorlopige maatregel ontoegankelijk gemaakt worden. Ook kan bij de einduitspraak of bij afzonderlijke beschikking door de rechter besloten worden de gegevens te doen vernietigen.[77]

E-mail
Een grondwetswijziging van artikel 13 om e-mail dezelfde bescherming te geven als de brief of de telefoon is er niet gekomen. Daarop besloot de minister de strafrechtelijke bescherming van e-mail te onderzoeken en daar waar nodig aan te passen.
Uit het onderzoek bleek dat de bescherming van het transport van e-mail nagenoeg compleet is. De minister wijst op het tapverbod van artikel 139c Sr, dat ook geldt voor e-mail verzonden via het internet. Gaat e-mail over een intern netwerk, dan zijn de aftapverboden van toepassing in de artikelen 139a en 139b. Bovendien is er nog de strafbaarstelling artikel 374bis Sr. Voor wat betreft de onderzoeksbevoegdheden voor e-mail in transport is dit afdoende geregeld in de artikelen 125g, 126m en 126t Sv.
De bescherming van opgeslagen e-mail (op computer, *server*) wordt geboden via de algemene verboden van artikel 138ab Sr. De bevoegdheden voor onderzoek van opgeslagen e-mail zijn geregeld in de artikelen 125i, eerste lid en 125j, eerste lid, Sv. De minister wijst wel op een manco. Voor fysieke post worden extra eisen gesteld aan het vervoersbedrijf. Een soortgelijke

74 nl.wikipedia.org/wiki/Verdrag_inzake_de_bestrijding_van_strafbare_feiten_verbonden_met_elektronische_netwerken
75 Tweede Kamer, vergaderjaar 2015–2016, 34 372, nr. 3, pag. 2.
76 Hoge Raad 03-12-1996, NJ 1997, 574
77 Tweede Kamer, vergaderjaar 1998–1999, 26 671, nr. 3, pag. 19-20.