Samenvatting

In het digitale tijdperk waarin wij leven worden kernprocessen in de hele samenleving veelvuldig aangestuurd door ICT en digitale technieken. Wereldwijd neemt in het laatste decennium het gebruik van ICT en het internet, zowel door bedrijven als door particulieren, steeds verder toe. Onze samenleving is voor haar functioneren sterk afhankelijk geworden van een goed functionerend netwerk van digitale en interconnectieve systemen. Deze afhankelijkheid wordt gaandeweg groter naarmate meer overheden, bedrijven, organisaties en natuurlijke personen hiervan gebruik zullen maken. De specifieke omstandigheden die hiermee gepaard gaan, zoals het toenemende gebruik van netwerken met een open verbinding met het internet, maar ook de anonimiteit en brede bereik van het internet, bieden echter lucratieve mogelijkheden voor het criminele circuit (Van Amersfoort e.a., 2002). De mogelijkheden voor het plegen van allerlei criminele activiteiten, hier beschreven als 'high-tech crime', zijn de laatste jaren fors toegenomen (NHTCC/NPAC, 2006a: 6). De financiële, economische en maatschappelijke gevolgen van high-tech crime kunnen voor onze samenleving vérdragende consequenties hebben. Niet alleen is het zaak dat de kernprocessen in onze samenleving goed kunnen blijven functioneren en zich verder kunnen blijven ontwikkelen, ook het vertrouwen van de gebruiker in een veilige ICT-wereld is van cruciaal belang. De preventie en bestrijding van high-tech crime vormt dan ook één van de speerpunten in het Nederlandse en Europese veiligheidsbeleid. Het gebrek aan kennis over de daders van high-tech crime en over de betrokkenheid van de georganiseerde criminaliteit vormen een belangrijke lacune voor een efficiënte en effectieve aanpak. Dat was voor het Ministerie van Justitie aanleiding om een *literatuur*inventarisatie uit te laten voeren, waarin de stand van zaken en kennis op het gebied van high-tech crime en in het bijzonder kennis over de daders ervan (de georganiseerde misdaad inbegrepen) in kaart wordt gebracht. De volgende zes onderzoeksvragen staan centraal in deze studie:

- Wat verstaan we onder het begrip high-tech crime?
- Welke verschijningsvormen van high-tech crime kunnen worden onderscheiden?
- Hoe zijn de daders (of dadergroepen) van high-tech crime te karakteriseren?
- In hoeverre is de georganiseerde misdaad betrokken bij high-tech crime?
- Wat zijn de lacunes in de literatuur in kennis over daders van high-tech crime?
- Welke ontwikkelingen op het gebied van high-tech crime zijn de eerstkomende jaren te verwachten?

Per onderzoeksvraag worden de belangrijkste bevindingen samengevat en enkele aandachts- en discussiepunten worden geëvalueerd voor de nadere invulling van de onderzoeks- en beleidsprogrammering op het gebied van high-tech crime.

Wat is high-tech crime?

Uit de literatuur is gebleken dat het niet eenvoudig is om het criminaliteitsterrein van high-tech crime eenduidig te definiëren. Een gemeenschappelijk begrippenkader ontbreekt en verschillende definities worden door elkaar heen gebruikt. De grote verwevenheid tussen klassieke vormen van criminaliteit (zoals fraude en diefstal) met geavanceerde ICT- en digitale technieken en tegelijkertijd het ontstaan van nieuwe criminele markten, maakt het criminaliteitsterrein oneindig breed en moeilijk af te bakenen. Het resultaat is dat onderzoekers en beleidsmakers, maar ook mensen binnen de opsporing, bestrijding en vervolgingsketen geneigd zijn om langs elkaar heen te praten: identieke begrippen ter omschrijving van een fenomeen kunnen voor betrokkenen een andere betekenis hebben en omgekeerd (uiteenlopende begrippen worden gebruikt terwijl ze feitelijk refereren aan hetzelfde probleem) en sommigen hanteren een smaller definitiekader dan anderen. Het criminaliteitsterrein zelf wordt door verschillende mensen ook uiteenlopend bestempeld. Zo zien we dat begrippen als cybercrime (of cybercriminaliteit) en high-tech crime veelvuldig als equivalenten van elkaar worden gebruikt, maar ook andere terminologieën als ICT-, internet-, digitale, e- of informatiecriminaliteit zijn begrippen die geregeld opduiken. Dit gebrek aan overzicht en consistentie schept verwarring en komt de aanpak, kennisuitwisseling en samenwerking op het gebied van high-tech crime niet ten goede.

In dit rapport hanteren wij '*high-tech crime*' als overkoepelend containerbegrip dat verwijst naar een veelheid aan criminele activiteiten waarbij gebruik wordt gemaakt van ICT. De criminele activiteiten kunnen gericht zijn tegen personen, eigendommen en organisaties (waarbij ICT als middel wordt ingezet), of tegen elektronische communicatienetwerken en informatiesystemen (waarbij ICT zowel middel als doelwit is). Ten opzichte van de term cybercrime biedt high-tech crime een breder en meer dynamisch perspectief dat beter aansluit bij de snelle technologische ontwikkelingen in de tijd. Nieuwe criminaliteitsvormen die kunnen ontstaan door innovaties van ICT (en niet alleen het internet) worden door dit containerbegrip afgedekt, wat per definitie inhoudt dat high-tech crime geen statisch containerbegrip is. Voor een nader onderscheid tussen klassieke delicten en nieuwe criminaliteitsvormen die door ICT zijn ontstaan maken we in dit rapport nog onderscheid tussen twee subcategorieën van high-tech crime. Daar waar ICT expliciet als middel én doelwit kan worden aangemerkt, spreken we van *computercriminaliteit*. Bij alle overige aan ICT gerelateerde (vaak klassieke) delicten spreken we van *cybercriminaliteit*. Beide subcategorieën kennen verschillende verschijningsvormen die sterk met elkaar verweven zijn en veelal in combinatie met elkaar worden gepleegd. Kenmerkend aan de verschijningsvormen

van computercriminaliteit (bijvoorbeeld hacking en het verspreiden van virussen) is dat zij een sterk technisch, virtueel karakter hebben: zij zijn ontstaan door, en kunnen niet bestaan zonder ICT. De verschijningsvormen van cybercriminaliteit daarentegen zijn doorgaans traditionele delicten die ook zonder tussenkomst van ICT gepleegd kunnen worden (bijvoorbeeld kinderporno en afpersing) maar door het gebruik van ICT een nieuwe (efficiëntere) uitvoering hebben gekregen door de inzet van geavanceerde technische middelen.

Wat zijn de verschijningsvormen van high-tech crime?

In dit rapport wordt een holistisch perspectief gehanteerd om zoveel mogelijk kennis te inventariseren over daders van high-tech crime. Daartoe hebben we de verschillende verschijningsvormen van cyber- en computercriminaliteit aan de hand van de literatuur in acht themaclusters als volgt gecategoriseerd (zie ook schema 2 in hoofdstuk 2).

Cybercriminaliteit:
1. legale communicatie en afscherming;
2. illegale handel;
3. financieel-economische criminaliteit;
4. illegale communicatie.

Computercriminaliteit:
5. ongeautoriseerde toegang tot ICT;
6. ICT-storing door gegevensverkeer;
7. ICT-storing door manipulatie van data en systemen;
8. dienstverleners.

Deze indeling is een voorlopige inventarisatie en dient als kapstok voor de doorontwikkeling van een typologie van high-tech crime. Dit overzicht is nodig om een aanzet te kunnen geven voor de verdere kennisopbouw en beleidsvorming in de preventie en bestrijding van high-tech crime. De indeling kan echter te allen tijde worden aangepast en gevoed met nieuwe en aanvullende inzichten. Voor elk van bovengenoemd themacluster en de bijbehorende verschijningsvormen volgt hierna een korte beschrijving.

Cybercriminaliteit

Cybercriminaliteit refereert aan het gebruik van ICT als instrument voor het plegen van uiteenlopende delicten. In veel gevallen gaat het om de ondersteunde functie van ICT ten behoeve van communicatie (tussen daders onderling of tussen daders en slachtoffers), maar bijvoorbeeld ook

voor het verrichten van (vrijwillige of onvrijwillige) transacties met goederen en diensten en financiële transacties.

Legale communicatie en afscherming
ICT heeft een veelheid aan gebruiksfuncties. In het kader van criminaliteit fungeert het internet bijvoorbeeld als virtuele inspiratiebron, als virtuele ontmoetingsplaats en als platform voor kennisuitwisseling en (afgeschermde) communicatie. Wanneer deze gebruiksfuncties worden ingezet in het kader van *illegale* doelstellingen (bijvoorbeeld rekrutering van radicale jongeren), spreken we in dit rapport van cybercriminaliteit. We onderscheiden binnen dit cluster drie thema's: radicalisering en extremisme, terrorisme en ideologisch gemotiveerde misdaad, en innovatieve afscherming met behulp van ICT. Zowel bij radicalisering als bij terrorisme speelt het internet een prominente rol. Het internet leeft, vooral onder jongeren, en zij laten zich over en weer inspireren en motiveren tot extremistische uitingen. Ook wordt het internet gebruikt om kennis te vergaren (handboeken die worden geraadpleegd of andere operationele kennis) en mensen te mobiliseren. In de literatuur is een tendens waarneembaar van publicaties die gericht zijn op de invloed van het islamistisch radicalisme (en in mindere mate van andere radicale stromingen). Dit kan ten koste gaan van de kennisontwikkeling in brede zin en leiden tot tunnelvisie waardoor belangrijke trends en indicaties aan het bewustzijn voorbij gaan. Radicalen, terroristen en mensen in het criminele circuit maken gebruik van innovatieve technieken om de communicatie mee af te schermen voor onbevoegden (waaronder de opsporing). Dit varieert van slimme vindingen (zoals het voortdurend wisselen van niet-geregistreerde mobiele telefoons of het gebruik van 'dead letter boxes' waarbij concept-e-mailberichten door meerdere gebruikers kunnen worden ingezien en aangepast zonder dat berichten daadwerkelijk worden verzonden) tot geavanceerde technieken als encryptie (waarbij de inhoud van berichten wordt versleuteld met codes) en steganografie (waarbij het hele bestaan van een bericht wordt verhuld door deze bijvoorbeeld in een afbeelding of digitale clip te verwerken). In sommige gevallen worden hiervoor experts ingehuurd.

Illegale handel
Via het internet kan onbeperkt en zonder veel moeite een diversiteit aan handel worden gedreven. Dit is een groeimarkt in onze huidige economie, maar gaat net zo goed op voor illegale goederen en diensten die via digitale weg worden verhandeld. De (inter)nationale literatuur biedt weinig zicht op de illegale handel in drugs, vuurwapens en explosieven, en mensenhandel- en smokkel. Op grond van deze studie is niet te bepalen of dit indicatief is voor de *mate* waarin gebruik wordt gemaakt van het internet of dat er een gebrek is aan opsporing, onderzoek en publicaties waardoor de kennis ontbreekt. Vooralsnog lijkt ICT bij deze handelsvormen vooral

een ondersteunende *communicatieve* functie te hebben. De relatieve anonimiteit van internetgebruikers en het gebrek aan sociale controle en face-to-face contact kunnen voor deze criminele markten het gebruik van internet juist tegengaan. Er zijn echter verschijningsvormen waarvoor het internet wel een belangrijke economische marktplaats en distributiekanaal is voor het verhandelen van goederen en diensten. Zo worden er op grote schaal merkvervalste geneesmiddelen, geneesmiddelen zonder recept, kinderporno, gestolen goederen, illegale software (softwarepiraterij) en illegale kansspelen aangeboden. Met name de grote afzetmarkten en de relatief geringe pakkans voor deze handel maakt het internet een populair en veelgebruikt middel. Vooral de handel in kinderporno, waarbij ook het materiaal zelf in digitale vorm wordt aangeboden, wordt in toenemende mate afgeschermd met behulp van geavanceerde technieken.

Financieel-economische criminaliteit
Bij financieel-economische criminaliteit wordt onrechtmatig voordeel behaald door fraude, oplichting en bedrog. Met name internetfraude is een veelvoorkomend probleem en vormt een bedreiging voor de Nederlandse samenleving. Mensen wordt onder valse voorwendselen geld uit de zak geklopt (voorschotfraude) of met behulp van ICT wordt op slinkse wijze vertrouwelijke informatie verkregen (identiteitsfraude) waarmee vervolgens bank- en creditcardfraude kan worden gepleegd. Identiteitsfraude met behulp van phishing, dat eerder een crimineel middel dan doel is, wordt beschouwd als een van de snelst groeiende vormen van niet-gewelddadige criminaliteit. Van de andere thema's (oplichting door marktmanipulatie, afpersing en chantage, en witwassen) is in de literatuur minder informatie terug te vinden. Door de toenemende virtuele geldstromen in het maatschappelijk-economische verkeer (via online veilingsites, elektronische en mobiele commercie) zou witwassen met behulp van ICT in de toekomst een aanzienlijke vlucht kunnen gaan nemen.
Ook afpersing van bedrijven die in hun bedrijfsvoering sterk afhankelijk zijn van het internet (e-commerce), of van bedrijven en burgers waarvan belangrijke bestanden en gegevens dreigen te worden beschadigd, openbaar gemaakt of misbruikt, vormt een potentiële bedreiging. Opvallend hier is de sterke verwevenheid tussen varianten van cyber- en computercriminaliteit. Zo kent internetfraude (cybercriminaliteit) een diversiteit aan werkwijzen en technieken zoals phishing, spamming, malware en pharming (zie computercriminaliteit), en de cybervorm van afpersing en chantage is vaak gerelateerd aan het hacken van systemen en het dreigen met een dDoS-aanval waarmee hele systemen kunnen worden gecorrumpeerd (zie computercriminaliteit).

Illegale communicatie
De veelheid aan gebruiksfuncties van ICT en het internet kunnen ook worden gebruikt om boodschappen van *illegale inhoud* uit te dragen.

Het gaat hier met name om activiteiten waarmee de publieke moraal of de persoonlijke levenssfeer van slachtoffers daadwerkelijk wordt aangetast (bijvoorbeeld stalking, discriminatie, of grooming). In dit rapport spreken we dan van illegale communicatie. Wat inhoud betreft verschillen deze digitale gedragsdelicten weinig van de varianten ervan in de 'fysieke wereld'. Vooral discriminatie (of haatzaaien) via het internet is een trend geworden, waarbij verschillende groeperingen elkaar voortdurend provoceren via discussiefora en chatboxen. Een toenemend probleem dat verontwaardiging binnen de samenleving oproept is grooming, waarbij kinderen via chatsites door volwassenen worden benaderd met oneerbare seksuele bedoelingen. In sommige gevallen leidt dit tot een fysieke ontmoeting waarbij daadwerkelijk sprake kan zijn van ontucht en verkrachting van minderjarigen. Van illegale communicatie is ook sprake wanneer op illegale wijze, zonder toestemming computer- en telefoongegevens van derden ongemerkt worden onderschept (spionage). Daarvoor worden methoden en middelen ingezet als hacking, spyware en malware, en kan gebruik worden gemaakt van dienstverleners (bijvoorbeeld corrupt personeel). Ook hier zien we weer de sterke verwevenheid terug tussen cyber- en computercriminaliteit, waarvan vooral het gebruik van spyware (ongemerkt op de computer geïnstalleerde software die gegevens verzamelt en doorstuurt naar een derde partij) en keyloggers (waarbij toetsaanslagen en muisklikken worden doorgestuurd naar een derde partij) in de toekomst zal kunnen gaan toenemen.

Computercriminaliteit

Met computercriminaliteit refereren we in dit rapport aan alle nieuwe vormen van criminaliteit die zonder het bestaan van ICT niet mogelijk waren geweest. Bij de criminele activiteiten wordt ICT niet alleen ingezet als instrument maar is de ICT zelf tevens expliciet doelwit. In de meeste gevallen gaat het om het inbreken, verstoren, manipuleren of wijzigen van systemen dan wel om het ontwikkelen en voorzien van instrumentele middelen die hierbij helpen. We onderscheiden vier themaclusters die hierna worden besproken.

Ongeautoriseerde toegang tot ICT
Voor het ongeautoriseerd toegang verschaffen tot ICT, feitelijk het inbreken op systemen, staan twee elementen centraal: hackers en botnets. Hackers hebben in toenemende mate criminele bedoelingen, zijn steeds vaker financieel gemotiveerd, en verrichten multifunctionele activiteiten die kunnen worden ingezet bij meerdere varianten van computercriminaliteit. Zij kunnen inbreken op (beveiligde) systemen, instrumenten ontwikkelen om ICT-storingen mee te veroorzaken, en verrichten maatwerk waar een grote mate van expertise en technische kennis voor nodig is.

Er is sprake van een 'ondergrondse' subcultuur die overeenkomsten vertoont met het ondergrondse criminele circuit: er is sprake van een eigen identiteit, status is een hoog goed, en er gelden eigen normen en waarden. In toenemende mate laten hackers zich inhuren door traditionele CSV's en in sommige gevallen maken ook Nederlanders deel uit van georganiseerde (Oost-Europese) criminele netwerken in de rol van dienstverlener. Een van de belangrijkste criminele instrumenten die door hackers kunnen worden opgezet zijn botnets. Dit zijn verzamelingen van op afstand bestuurbare computers die instrumenteel zijn voor het plegen van diverse varianten van high-tech crime, vooral spamming, phishing en (afpersing met behulp van) dDoS-aanvallen.

ICT-storing door gegevensverkeer
Het verstoren van de werking van systemen (bijvoorbeeld websites, e-maildiensten of computernetwerken) kan op verschillende manieren worden bereikt. Twee belangrijke varianten die wereldwijd enorm zijn toegenomen zijn (d)DoS-aanvallen en spamming. Bij een (distributed) Denial of Service of (d)DoS-aanval worden bewust massale hoeveelheden gegevens verzonden naar systemen waardoor deze overbelast raken en onbereikbaar worden. Het is een middel dat onder meer voor afpersing van bedrijven wordt ingezet, maar ook een uiting kan zijn van protest, wraak, concurrentie of vandalisme. Bij spamming kunnen ook storingen worden veroorzaakt door het versturen van massale e-mails, maar dit is eerder een neveneffect van digitale marketing en reclame (voor bijvoorbeeld life-style producten en geneesmiddelen zonder recept) dan een concreet doel. Bij internetfraude worden phishing e-mails massaal verzonden om vertrouwelijke informatie van mensen te ontlokken waarmee ze vervolgens worden opgelicht. Hackers bieden zowel bij dDoS-aanvallen als spamming ondersteuning of verrichten deeltaken bij het veroorzaken van doelgerichte storingen.

ICT-storing door manipulatie van data en systemen
Storingen kunnen ook direct worden veroorzaakt door het daadwerkelijk manipuleren (beschadigen, verwijderen, wijzigen of vernietigen) van gegevens en systemen. Malware is het bulkbegrip voor dubieuze '*…computerprogramma's die zonder toestemming van de eigenaar of beheerder draaien op een computer en het systeem iets laten doen naar de wens van een buitenstaander*' (KLPD, DNRI, 2007a: 15). Dergelijke programma's worden door specialisten op maat gemaakt en kunnen ongemerkt vertrouwelijke informatie van gebruikers verzamelen, data en systemen beschadigen (de bekende virussen), of externe toegang verlenen op computers (via de moderne virussen, zogenoemde Trojaanse paarden). Ook complete websites kunnen worden geblokkeerd of gewijzigd (defacing), onder meer als instrument om mensen mee op te lichten (bijvoorbeeld internetfraude door middel van nepwebsites), af te persen, of om uiting te

geven aan protest (hacktivisme). Wanneer ICT-systemen die vitale infrastructuren aansturen (bijvoorbeeld transportsystemen, besturingssystemen in de chemische sector of belangrijke crisis- en informatiediensten) om politieke redenen worden aangetast om grootschalige maatschappelijke ontwrichting te veroorzaken, spreken we in dit rapport van een cyberterroristische aanval. Hoewel er tot op heden nog geen concrete pogingen zijn geweest, vormen vooral de (wraakzuchtige) insiders met kennis en toegang tot de besturingssystemen een bedreiging (zie ook dienstverleners).

Dienstverleners
De inzet van ICT-dienstverleners staat in directe relatie tot de georganiseerde misdaad Niet alleen criminelen maar ook terroristen huren de kennis in van experts om bijvoorbeeld communicatie veilig te stellen voor de opsporing of om instrumenten te ontwikkelen waarmee criminele of terroristische activiteiten worden gefaciliteerd (zoals het opzettelijk vervaardigen, verkopen, verspreiden of ter beschikking stellen van een technisch hulpmiddel, wachtwoord of code waarmee toegang kan worden verkregen tot een geautomatiseerd systeem). In dit rapport onderscheiden we drie vormen van dienstverlening: corruptie van ICT-personeel, infiltratie van criminele ICT'ers, en het inhuren ICT-experts. Werknemers met ICT-bevoegdheden die toegang hebben tot gevoelige bedrijfsgegevens kunnen (door omkoping of bedreiging) hulp verlenen aan criminele partijen van binnenuit een organisatie. We spreken dan van corruptie en verwevenheid tussen boven- en onderwereld. Hoewel de dreiging van corrupte IT'ers in Nederland nog beperkt lijkt, vormen het infiltreren van criminelen als ICT-consultant en het inhuren van experts voor het verlenen van hand- en spandiensten (bijvoorbeeld hackers) een aanzienlijk veiligheidsrisico.

Wat is bekend over de daders?

Het systematisch in kaart brengen van daderkenmerken in de vorm van risico-indicatoren (het prototype daderprofiel) staat bekend als '*profiling*'. Profiling-technieken staan qua ontwikkeling en bruikbaarheid echter nog in de kinderschoenen. Deze techniek leidt niet direct tot het identificeren van de dader(s) van een delict maar geeft een omschrijving van *combinaties van kenmerken* waar dader(s) naar alle waarschijnlijkheid aan voldoen. De effectiviteit van het gebruik van risicoprofielen is tot op heden nog onvoldoende onderzocht (zie ook Van Donselaar en Rodrigues, 2006: 43, 58). Duidelijk is dat het moet gaan om een combinatie van algemene en specifieke kenmerken van daders die voldoende onderscheidend zijn.

Het nadeel van risicoprofielen is dat vooroordelen over bepaalde mensen en groepen worden bevestigd. Zowel in de preventie als in de opsporing zal er onevenredig veel aandacht uitgaan naar bekende risicogroepen. Dit kan leiden tot stigmatisering van onschuldige personen (die toevallig aan deze kenmerken voldoen) en tegelijkertijd tot criminelen die 'onzichtbaar' blijven en dus ten onrechte over het hoofd worden gezien wanneer zij toevalligerwijze niet aan het profiel voldoen. De profiling-techniek is dus beslist niet feilloos en het gebruik ervan vraagt om de nodige voorzichtigheid en nuances. Het gebruik van risicoprofielen als preventief en opsporingsinstrument verdient grote zorgvuldigheid en dient met terughoudendheid te worden gehanteerd. Dit neemt echter niet weg dat inzicht in daderkenmerken aanknopingspunten kan bieden in zowel de preventie als opsporing van high-tech crime. Nader onderzoek zal dit moeten uitwijzen. Omdat de inventarisatie van daderkenmerken in termen van profielen nog niet empirisch wordt ondersteund en gevalideerde instrumenten tot op heden ontbreken, spreken wij in dit rapport van inzicht in het soort daders van high-tech crime en niet van daderprofielen.

Het gebrek aan kennis over daders in een zogenoemde 'intelligence database' is een belangrijke reden voor het gebrek aan ontwikkeling van daderprofielen. Een van de doelstellingen van deze studie was dan ook om de kennis over daders van high-tech crime te inventariseren op basis van (inter)nationale literatuur. In hoofdstuk 3 zijn daderkenmerken in kaart gebracht voor een selectie van verschijningsvormen van high-tech crime waarvoor de dreiging en risico's voor de Nederlandse samenleving als meest urgent worden beschouwd:[2]

1. radicalisering en extremisme;
2. terrorisme en ideologisch gemotiveerde misdaad;
3. kinderporno;
4. grooming;
5. softwarepiraterij;
6. internetfraude;
7. witwassen;
8. cyberterrorisme;
9. hacking;
10. malware;
11. ICT-dienstverleners.

Uit deze inventarisatie bleek onder meer dat vooral *internetfraude* en *hacking* criminele verschijnselen zijn die veelal in combinatie met andere vormen van high-tech crime worden gepleegd. Bij terrorisme, kinderporno, grooming, softwarepiraterij en internetfraude zijn hoofdzakelijk

2 De daderkenmerken van de overige verschijningsvormen van high-tech crime staan in bijlage 6 beschreven.

mannelijke daders betrokken. Het gros van de zedendelicten (kinderporno en grooming) wordt gepleegd door blanke daders terwijl bij terrorisme en internetfraude vooral daders betrokken zijn van Afrikaanse en/of Aziatische afkomst. Hoewel een aanzienlijk deel van de high-tech crimes financieel gemotiveerd is, hebben vooral hackers en schrijvers van malware nogal uiteenlopende motieven voor hun criminele activiteiten (men doet het bijvoorbeeld ook voor de uitdaging, uit ideologie, macht, wraak of vandalisme). Opvallend is dat corrupte ICT'ers en criminelen die actief zijn op het gebied van terrorisme, internetfraude, kinderporno en hacking nogal eens over een strafblad blijken te beschikken. Door de variëteit aan verschijningsvormen en de (summiere) aanwijzingen over de daders, is duidelijk dat er niet kan worden gesproken van 'de' high-tech crimineel maar dat criminelen zich specialiseren op een bepaald vlak. Doordat sommige delicten echter door dezelfde digitale technieken worden gefaciliteerd, wordt het voor de crimineel echter makkelijker om grotere winsten te behalen door dezelfde technieken in te zetten voor meerdere delicten tegelijk.

We moeten echter constateren dat er betrekkelijk weinig bekend is in de literatuur over individuele daders van high-tech crime. De literatuurinventarisatie biedt slechts grove en onvolledige schetsen van daders op basis van een beperkt aantal kenmerken. Vergelijken we bijvoorbeeld de profielschets met indicatoren zoals die werden ontwikkeld voor de FBI (zie bijlage 7), dan ontbreekt het in de literatuur sterk aan specifieke daderkennis, zowel in termen van organisatie (zoals rekrutering), uitvoering (expertise), gedrag (waaronder persoonlijke kenmerken) als van de gebruikte resources. In zijn algemeenheid geldt voor de meeste verschijningsvormen bovendien dat het inzicht ontbreekt in de criminele carrières van daders en in de overlap tussen de verschillende verschijningsvormen van high-tech crime. De informatie die wel te vinden is in de literatuur is doorgaans oppervlakkig, ongestructureerd en summier, en in sommige gevallen deels gebaseerd op anekdotes en hypothesen waarvan de betrouwbaarheid en validiteit niet of nauwelijks te bepalen zijn. Het ontbreekt al met al aan empirisch-wetenschappelijk onderzoek naar daderkenmerken waarin duidelijk onderscheid wordt gemaakt tussen afzonderlijke verschijningsvormen van high-tech crime. Nader inzicht in daders kan worden verkregen door meer probleemgerichte onderzoeken (bijvoorbeeld casestudies). Een literatuurinventarisatie is niet afdoende om gefundeerd uitspraken over daders van high-tech crime te kunnen doen.

Is er sprake van georganiseerde high-tech crime?

Van sommige verschijningsvormen van high-tech crime zijn aanwijzingen dat er sprake is van georganiseerde criminaliteit. We spreken in dit rapport van georganiseerde criminaliteit als: '…*groepen primair gericht zijn op illegaal [financieel of materieel] gewin en systematisch misdaden plegen met ernstige gevolgen voor de samenleving*' (Parlementaire Enquêtecommissie Opsporingsmethoden, Bijlage VII, 1996; Fijnaut e.a., 1998; Kleemans e.a., 1998: 22-23). Hoewel er in de literatuur weinig bekend is over dadergroepen van high-tech crime (het zicht op daders is relatief beperkt), zijn er aanwijzingen dat zowel traditionele CSV's (zoals de Russische en Oost-Europese maffia) betrokken zijn die de benodigde expertise extern inhuren, als nieuwe fluïde HT-CSV's waarbinnen experts (zoals hackers en schrijvers van malware) deeltaken verrichten en hun krachten bundelen. Het KLPD (Boerman en Mooij, 2006) spreekt van een trend naar *diversificatie* waarbij verschillende criminaliteitsvormen in combinatie met elkaar worden gepleegd (bijvoorbeeld hacking, botnets, spamming, malware, pharming, dDoS-aanval, internetfraude, afpersing) en van een trend naar *taakspecialisatie* waarbij criminelen experts inzetten die verantwoordelijk zijn voor verschillende deeltaken voor het plegen van een delict (bijvoorbeeld het ontwikkelen van de instrumenten of het maken van bijvoorbeeld nepwebsites).

In hoofdstuk 4 is een inventarisatie gemaakt van de betrokkenheid van de georganiseerde criminaliteit voor de verschijningsvormen van high-tech crime die eerder als bedreiging voor de Nederlandse samenleving waren gekwalificeerd (zie paragraaf 5.3). Van de in hoofdstuk 3 geprioriteerde verschijningsvormen zijn vooral kinderporno, softwarepiraterij, internetfraude (voorschotfraude en identiteitsfraude), witwassen, hacking en malware financieel lucratieve werkterreinen voor CSV's en HT-CSV's. De opbrengsten zijn groot, zeker als deze worden afgezet tegen de geringe investeringen en risico's. Ook ICT-dienstverleners hebben in toenemende mate criminele bedoelingen en raken betrokken bij georganiseerde criminaliteit. Jongeren met kennis van ICT op universiteiten, computerclubs en via het internet gerekruteerd om te ondersteunen bij malafide praktijken van criminelen. Hetzelfde geldt voor afgestudeerden en computermedewerkers. Dit neemt echter niet weg dat er ook binnen het criminele circuit zelf inmiddels voldoende technische kennis aanwezig kan zijn om zonder hulp van buitenaf een grote slag te slaan. Vooral de handel in botnets is een belangrijke criminele markt binnen de georganiseerde misdaad In Nederland zijn HT-CSV's vooral actief op het gebied van internet- en voorschotfraude. Nederland is bovendien een belangrijke toeleverancier van botnets (die tegen forse betaling te huur worden aangeboden) en belangrijk doelwit van dDoS-aanvallen. Vooral virusschrijvers (van malware en Trojaanse paarden) spelen in dit kader een prominente rol om de

controle over andermans systemen te krijgen en deze te bespioneren. Ook het aanpassen of vernielen van websites (defacing) of het ontwikkelen van nepwebsites waarnaar mensen worden omgeleid (pharming) zijn in toenemende mate activiteiten waarmee grof geld kan worden verdiend.

Voor radicalisering en terrorisme geldt dat activiteiten weliswaar (lokaal) georganiseerd plaatsvinden, maar dat traditionele CSV's hierbij niet betrokken zijn. Van georganiseerde high-tech crime is ook geen sprake bij grooming (dat doorgaans individueel wordt gepleegd) en voor cyberterrorisme geldt dat tot op heden nog geen concrete activiteiten zijn waargenomen. Onderzoek van het KLPD heeft bovendien geen aanwijzingen opgeleverd van samenwerking tussen criminele en terroristische CSV's (Boerman en Mooij, 2006: 86). Overigens zijn terroristische CSV's wel betrokken bij diverse criminele activiteiten, onder meer op het gebied van high-tech crime, om het terrorisme mee te financieren.

Ook hier kunnen we echter niet anders dan constateren dat er over georganiseerde high-tech crime op basis van deze literatuurstudie nog te weinig kan worden gezegd. De inventarisatie biedt een globaal overzicht van de criminele activiteiten (die soms gecombineerd met elkaar worden gepleegd), van het niveau van expertise dat daarvoor nodig is, van de inhuur van experts en dienstverleners, en van het grensoverschrijdende karakter van high-tech crime met zijn internationale connecties. Naar verwachting zal high-tech crime steeds meer het werkterrein worden van de georganiseerde misdaad waarbij telkens nieuwe trends en innovatieve technieken zullen worden toegepast. Specifieke kennis over daders en samenwerkingsverbanden ontbreekt echter in de literatuur, en aanvullend onderzoek (bijvoorbeeld dossieronderzoek) is nodig om de georganiseerde misdaad op het gebied van high-tech crime beter in kaart te brengen.

Wat zijn de lacunes in kennis over daders?

Op basis van deze literatuurinventarisatie kunnen we vaststellen dat er over daders en criminele samenwerkingsverbanden weinig specifieke kennis voorhanden is. In het overzicht zijn de bevindingen op het gebied van inzichten in daders geclassificeerd van 1 (zeer beperkte kennis) tot 4 (zeer goede kennis), met de geprioriteerde thema's van high-tech crime vetgedrukt. In de rijen (van links naar rechts) staat de kennispositie over individuele daders weergegeven, en in de kolommen (van boven naar beneden) de kennis over georganiseerde high-tech crime. Uit het overzicht is voor iedere verschijningsvorm van high-tech crime dus direct af te lezen wat er in de literatuur bekend is over individuele daders en HT-CSV's.

Overzicht: Daderkennis van high-tech crime in de literatuur

	Individuele daderkenmerken			
HT-CSV's	Zeer beperkt	Redelijk	Goed	Zeer goed
Zeer beperkt	**Dierenrechtenactivisme** **Extreem-rechts terrorisme** **Softwarepiraterij** **Identiteitsfraude** **Pharming (internetfraude)** **Witwassen** **Grooming** **Cyberterrorisme** **Hacking** **Novice hacker** **Petty thief hacker** **Old guard hacker** **Virus writer hacker** **Professional criminal hacker** **Information warrior hacker** **Political activist hacker** **Malware** **ICT-dienstverleners** Handel in geneesmiddelen Handel vuurwapens/ explosieven Mensenhandel Drugshandel Heling Illegale kansspelen Marktmanipulatie Spionage Spamming dDoS-aanval Defacing	**Rechts-radicalisme** **Islamistisch radicalisme** **Islamistisch terrorisme** **Cyperpunk hacker** **Internal hacker** Cyberstalkers Discriminatie	-	-
Redelijk	Afscherming Afpersing en chantage	**Kinderporno** **Voorschotfraude**	-	-
Goed	-	-	-	-
Zeer goed	-	-	-	-

Uit het overzicht blijkt dat er *redelijk* wat zicht is op daders van kinderporno en voorschotfraude (zowel in termen van individuele daders als van HT-CSV's), dat er van extreem-rechts en islamistisch radicale en terroristische stromingen *redelijk* zicht is op individuele daderkenmerken (maar niet van HT-CSV's), en dat van enkele hackervarianten (cyberpunk en internal hacker) en gedragsdelicten (cyberstalking en discriminatie) eveneens *redelijk* zicht is op individuele daderkenmerken maar niet van HT-CSV's.[3] Van een aantal technieken (afscherming, afpersing, pharming)

3 In geval van cyberstalking zijn samenwerkingsverbanden door de aard van het delict ook niet aan de orde.

is weliswaar enig zicht op HT-CSV's maar zijn juist de individuele daders erachter relatief onzichtbaar.

Voor geen van de verschijningsvormen wordt de kennis over daders en HT-CSV's als goed of zeer goed gekwalificeerd. Opvallend is dat van het gros van de verschijningsvormen er zeer beperkte kennis in de literatuur te vinden is over daderkenmerken (de cel linksboven in het overzicht is het meest gevuld). En voor veel van de verschijningsvormen die zijn aangemerkt als dreiging voor de Nederlandse samenleving (dierenrechtenactivisme, extreem-rechts terrorisme, softwarepiraterij, identiteitsfraude, pharming, witwassen, grooming, een aantal typen hackers, schrijvers van malware en ICT-dienstverleners)[4] kunnen we concluderen dat er dus sprake is van een gebrek aan kennis. Dit impliceert niet direct dat dergelijke kennis ook binnen de opsporingsdiensten ontbreekt: de huidige conclusies uit dit rapport zijn immers gebaseerd op basis van bestudering van veelal openbare literatuur.

Verwachtingen voor de toekomst

Toename van high-tech crime
De verwachting voor de komende jaren op het gebied van high-tech crime is dat zowel het aantal slachtoffers als de criminele winsten verder zullen toenemen. Daders wisselen snel van werkwijze en de trend van diversificatie (waarbij criminelen zich richten op meerdere activiteiten tegelijk) en taakspecialisatie (waarbij specifieke expertise wordt ingezet voor criminele deeltaken) zal zich verder voortzetten (NHTCC, aangehaald door KLPD/DNRI, 2007a: 36). De criminele activiteiten zullen naar verwachting ook meer afgestemd worden op specifiek doelwitten (zijnde een individu of organisatie), en vooral slachtoffers die de technische kennis van digitale communicatiestructuren nagenoeg ontberen (bijvoorbeeld ouderen) en zich onvoldoende hebben beveiligd zullen hiervan de dupe worden (NHTCC, 2006b: 10-11).

Het internet als plaats delict
De illegale handel op en via het internet zal door het toenemende gebruik van het internet (waarmee de afzetmarkten alleen maar groeien) en de geringe pakkans mogelijk verder gaan toenemen. Door de toenemende virtuele geldstromen is de verwachting bovendien dat internetfraude (en identiteitsdiefstal) de komende jaren de grootste aantallen slachtoffers en financiële schade zullen aanrichten (Taylor en anderen, 2006: 357-383). Ook in het V-NDB2006 wordt identiteitsfraude met behulp van phishing

4 Dat er kennis ontbreekt over daders van cyberterrorisme is evident gegeven dat dergelijke aanslagen nog niet gepleegd zijn.

als stormachtige ontwikkeling beschreven (Boerman en Mooij, 2006: 21, 30). De hoge ADSL-dichtheid, waarbij computers vrijwel permanent in verbinding staan met het internet, maken vooral Nederland een zeer aantrekkelijk werkterrein voor phishers. Het gaat hierbij niet alleen om cybercriminaliteit maar ook om varianten van computercriminaliteit zoals spamming (Ianelli en Hackworth, 2005). Phishing op internet geschiedt recentelijk deels via botnets (netwerken van door malware geïnfecteerde computers die vervolgens door derden vanaf externe locaties worden gecontroleerd). Botnets spelen ook bij vele andere verschijningsvormen een belangrijke rol en vormen dus een aanzienlijke bedreiging (Europol, 15 juni 2006). Doordat botnets kleinschaliger worden gemaakt en gericht wordt op specifieke doelgroepen, worden zij bovendien moeilijker te traceren.[5]

De opkomst van hackers als dienstverleners
Als belangrijkste ontwikkeling op het gebied van georganiseerde misdaad en high-tech crime moet worden aangemerkt de inzet van ICT-dienstverleners en -experts. Er zijn indicaties dat vooral criminele netwerken uit Oost-Europa en Rusland hackers inhuren die veelal afkomstig zijn uit West-Europa. Hackers hebben in de loop van de jaren ontdekt dat er met hun deskundigheid snel en veel geld te verdienen is. Daardoor zijn hackers ook in de belangstelling gekomen van CSV's en in sommige gevallen behoren ze er (waarschijnlijk) ook toe. Een aanzienlijk deel van de criminelen met belangstelling voor high-tech crime heeft bijvoorbeeld belang bij botnets, en dat geeft de hackers die over deze zombienetwerken kunnen beschikken een bijzondere positie. Hackers zijn daarmee geworden tot belangrijke 'facilitators' voor criminele groeperingen. Zij leveren op bestelling allerlei technische hulpmiddelen zoals backdoors (om toegang tot systemen te krijgen), Trojaanse paarden en bots (om computers extern mee te besturen) en volledige botnets (legers aan zombiecomputers die op afstand bestuurbaar zijn). Met name de multifunctionele toepassingen van *malware* en *botnets* zijn sterk bepalend voor de criminele markt van high-tech crime: zij worden op maat gemaakt en faciliteren diverse criminele activiteiten zoals dDoS-aanvallen, phishing, spamming, internetfraude en verspreiding van kinderporno. Vooral de rekrutering van jonge studenten (die worden benaderd op universiteiten, computerclubs of online forums), corruptie van hoogopgeleid ICT-personeel,[6] en infiltratie van criminelen in ICT-bedrijven of de e-commerce is reden tot bezorgdheid. Door een gebrek aan kennis over daders en de manier waarop criminele groeperingen ICT inzetten bij hun activiteiten doen er zich op dit terrein aanzienlijke problemen voor bij de opsporing en vervolging zodat

5 Doordat vele botnets tegelijkertijd actief kunnen zijn, hoeft de impact ervan namelijk niet minder te worden.
6 Er zijn al enkele jaren discussies gaande over de introductie van een beroepscode voor ICT'ers (Rogers, 2001: 132-133).

de beheersbaarheid van het fenomeen als zorgelijk wordt gekwalificeerd (NDB2004, KLPD, DNRI).

Jongeren als risicogroep
Vooral de jongere generatie en studenten met goed onderlegde ICT-kennis en -vaardigheden en verstand van het internet kunnen als risicogroep voor high-tech crime worden aangemerkt. Dit geldt in het bijzonder voor de mogelijkheid om betrokken te raken bij de georganiseerde misdaad en niet alleen voor criminele maar ook voor terroristische samenwerkingsverbanden (Europol, 2003; McAfee, 2006; Neve, 2007). Uit onderzoek is gebleken dat daders van computercriminaliteit (en sommige aanverwante vormen van cybercriminaliteit) steeds jonger zijn en steeds complexere activiteiten uitvoeren (Europol, 2003: 116). Los van de spanning en de uitdaging levert high-tech crime veel geld op. Hierdoor kunnen jongeren, die aanvankelijk getypeerd kunnen worden als een soort 'jeugdbende', in een criminele spiraal terechtkomen waaruit moeilijk meer te ontsnappen is.

Corruptie binnen bedrijven
Een ander fenomeen dat aandacht verdient zijn de kwetsbaarheden binnen bedrijven die ontstaan wanneer werknemers onzorgvuldig met veiligheidsmaatregelen omgaan of deze juist doelbewust blokkeren of ontregelen. Doordat kernprocessen bij bedrijven en overheden in toenemende mate aangestuurd worden door ICT is men aangewezen op experts die de vaardigheden en technieken beheersen om systemen te ontwikkelen, te beheren en te beveiligen. Vooral personen met een hoog niveau aan ICT-bevoegdheden (programmeurs, systeem- en gegevensbeheerders), met toegang tot gevoelige en vertrouwelijke gegevens (bijvoorbeeld klanten- en betalingsbestanden), en werkzaam bij bedrijven of organisaties die verantwoordelijk zijn voor de vitale infrastructuren en veiligheid (SCADA-systemen, opsporingsdiensten) vormen een risico. Het betreft niet alleen mensen die gevoelig kunnen zijn voor corruptie, maar bijvoorbeeld ook wraakzuchtige (ex-)werknemers (internal hackers en CITI's) die in potentie grote schade kunnen aanrichten. Bedrijven huren ook steeds vaker IT-consultants extern in om systemen of software te bouwen. Wanneer dit mensen zijn met criminele bedoelingen of wanneer criminelen als zelfstandige ondernemers ICT-diensten op de markt aanbieden, kan er sprake van een aanmerkelijk veiligheidsrisico.

Subculturen
Bij een deel van de sociale activiteiten die zich voorheen in 'het fysieke' afspeelden, wordt tegenwoordig gebruikgemaakt van ICT en digitale technologie. Virtuele gemeenschappen die bijvoorbeeld gebruikmaken van discussiefora kunnen in sommige gevallen als subculturen worden aangemerkt (hackers, wetenschappers, jeugdbendes, pedofielen). Er is binnen deze gemeenschappen sprake van een eigen identiteit, eigen normen,

waarden en interesses, en in sommige gevallen ook een eigen 'taal' (het gebruik van afkortingen en tekens). Dit geldt bijvoorbeeld voor jongeren met een radicaal (islamistisch of extreem-rechts) gedachtegoed, maar ook voor jongeren die tot het ondergrondse van de hackergemeenschap zijn gaan behoren. Wat volgens Turgeman-Goldschmidt (2005) aanvankelijk begint als vorm van entertainment kan makkelijk uitmonden en escaleren tot een crimineel verschijnsel. De steeds verdergaande verschuiving naar een digitale samenleving betekent ook dat gedragingen vaker zullen leiden tot uitspattingen en excessen op bijvoorbeeld het internet. Het verdient aandacht om een aantal verschijningsvormen van high-tech crime waar jongeren bij zijn betrokken (radicalisering en extremisme, softwarepiraterij, discriminatie, hacking) te evalueren in relatie tot subculturen en jeugdcriminaliteit. Expliciete aandacht daarbij is vereist op het gebied van sociaal-psychologische factoren en groepsprocessen die zich afspelen via het internet (bijvoorbeeld morele ontwikkeling, gezinsproblematiek, sociale beïnvloeding en subculturele groepsvorming) (zie ook NCTb, 2006b: 10; Yar, 2005b).