Positieve uitlokking van ethisch hacken

Een onderzoek naar responsible-disclosurebeleid*

Karel Harms

1 Inleiding

De digitalisering van de maatschappij is in volle gang. Van steeds groter belang hierbij is cyberveiligheid. Een van de manieren waarop de overheid probeert bij te dragen aan de cyberveiligheid in Nederland, is door het uitdragen van een beleid van *responsible disclosure*. Responsible disclosure wordt door het Nationaal Cyber Security Centrum (onderdeel van het Ministerie van Veiligheid en Justitie, hierna: NCSC) omschreven als het 'binnen de ICT-wereld (...) op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure'.[1] Met een ICT-kwetsbaarheid wordt in deze context gedoeld op een veiligheidsrisico in een systeem, waarvan misbruik gemaakt zou kunnen worden. Te denken valt hierbij aan een programmeerfout in een systeem, die het mogelijk maakt dat van buitenaf toegang verkregen kan worden tot dat systeem, om zo bijvoorbeeld persoonsgegevens in te zien. Melders van kwetsbaarheden zijn doorgaans ethisch hackers: hackers die willen bijdragen aan de veiligheid van een systeem, en dus geen misbruik van kwetsbaarheden willen maken.

Door het uitdragen van een beleid van responsible disclosure is de overheid een weg ingeslagen naar een positieve, proactieve en constructieve bejegening van hackers. Dit is een unieke ontwikkeling in de benadering van feiten die in principe strafbaar zijn. Hacken, in het strafrecht aangeduid als computervredebreuk, is een misdrijf tegen de openbare orde en is als zodanig strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht (Sr). In deze bijdrage maak ik een conceptuele analyse van het verschijnsel responsible disclosure, zoals dat door de overheid aangemoedigd wordt. Responsible disclosure beschouw ik daarbij als een vorm van *positieve uitlokking*. Onder positieve uitlokking versta ik *het aanzetten tot gewenst gedrag dat formeel gezien strafbaar kan zijn*. In dit artikel wordt gesteld dat de implementatie van responsible disclosure, als vorm van positieve uitlokking, een wenselijke ontwikkeling is en in lijn is met de uitgangspunten die binnen het strafrecht gehanteerd worden. Deze opvatting is gebaseerd op drie elementen: (1) responsible disclosure is intrinsiek wenselijk; (2) omdat responsible

* Ik dank Anne Ruth Mackor, Jeroen ten Voorde en de anonieme reviewer hartelijk voor hun opbouwende kritiek.

1 Nationaal Cyber Security Centrum, *Leidraad om te komen tot een praktijk van Responsible Disclosure* (Den Haag: NCSC, 2013), 5. Te downloaden via: www.ncsc.nl/actueel/Responsible+Disclosure+Leidraad (geraadpleegd 25 september 2017).

doi: 10.5553/NJLP/221307132017046002006

disclosure intrinsiek wenselijk is, bestaan er in beginsel geen bewaren tegen positieve uitlokking; (3) er moet voor gewaakt worden dat positieve uitlokking omslaat in *negatieve uitlokking*. Dit laatste zou een ernstige schending van de belangen van een ethisch hacker opleveren. Onder negatieve uitlokking versta ik *het aanzetten tot onwenselijk gedrag dat tevens strafbaar is*.

In de volgende paragraaf wordt onderzocht hoe responsible-disclosurebeleid in Nederland vorm heeft gekregen en wordt op de verhouding tussen computervredebreuk en responsible disclosure ingegaan. Ook wordt de jurisprudentie ten aanzien van ethisch hacken behandeld en wordt de houding van het Openbaar Ministerie (OM) ten aanzien van responsible disclosure onderzocht (par. 2). Vervolgens wordt in paragraaf 3 het responsible-disclosurebeleid vergeleken met het Nederlandse beleid ten aanzien van softdrugs, omdat beide vormen van beleid een gedoogelement lijken te bevatten.[2] Aan de hand van deze vergelijking wordt gepoogd het beleid te duiden. Hier wordt duidelijk waarom responsible disclosure intrinsiek wenselijk is. In paragraaf 4 worden de begrippen positieve en negatieve uitlokking verder uitgewerkt en wordt onderzocht in hoeverre de waarborgen die gelden ten aanzien van het inzetten van lokmiddelen in het kader van de opsporing van toepassing zijn in het geval van responsible disclosure. Hier zal blijken dat positieve uitlokking in beginsel wenselijk is, maar dat positieve uitlokking niet mag omslaan in negatieve uitlokking. Afgesloten wordt met een conclusie (par. 5).

2 Responsible-disclosurebeleid en strafrecht: een kort overzicht

In 2013 publiceerde het NCSC, onderdeel van het ministerie van Veiligheid en Justitie, de *Leidraad om te komen tot een praktijk van Responsible Disclosure* (hierna: de Leidraad). In de Leidraad wordt uitgegaan van 'organisaties' en 'melders'. Kort gezegd komt het beleid van de overheid erop neer dat organisaties die openstaan voor responsible-disclosuremeldingen, worden aangemoedigd om hun eigen responsible-disclosurebeleid te ontwikkelen en te publiceren.[3] De door het NCSC gepubliceerde Leidraad kan hierbij als voorbeeld dienen, maar heeft geen juridische gelding. De concrete invulling van het beleid wordt aan de organisatie overgelaten, maar een aantal elementen is in ieder responsible-disclosurebeleid terug te vinden. In het door een organisatie gepubliceerde beleid is vastgelegd wat partijen over en weer van elkaar kunnen verwachten. De organisatie stelt bijvoorbeeld vast hoe gereageerd wordt op een melding en of er een beloning wordt uit-

2 Het Nederlandse gedoogbeleid ten aanzien van softdrugs heeft ook niet-strafrechtelijke elementen, maar die blijven in het kader van deze bijdrage buiten beschouwing.

3 Zie ter illustratie het responsible-disclosurebeleid van bijv. de ING (www.ing.nl/de-ing/veilig-bankieren/fraude-melden/meldpunt-kwetsbaarheden/index.html) of de Gamma (www.gamma.nl/klantenservice/veiligheid-privacy/responsible-disclosure). De Nederlandse overheid voert ten aanzien van haar eigen systemen overigens ook een responsible-disclosurebeleid, zie daarvoor bijv. www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en-antwoord/responsible-disclosure (links geraadpleegd 1 oktober 2017).

geloofd aan de melder.[4] Ook bevat responsible-disclosurebeleid de garantie dat de organisatie geen aangifte zal doen tegen een melder wanneer deze zich aan de voorwaarden van het gepubliceerde beleid houdt.[5]

Naast de organisatie die een responsible-disclosurebeleid voert, heeft ook de melder van een kwetsbaarheid verantwoordelijkheden. Zo wordt verwacht dat de melding zo snel mogelijk en op discrete wijze gedaan wordt. Ook mag de melder niet 'op onevenredige wijze handelen'.[6] In de Leidraad wordt een lijst opgesomd van handelingen die als onevenredig worden aangemerkt. Daarbij kan blijkens de Leidraad gedacht worden aan het meerdere keren binnengaan van een systeem, informatie van het systeem kopiëren of downloaden, of wijzigingen in het systeem aanbrengen.

Responsible disclosure en computervredebreuk

Computervredebreuk is strafbaar gesteld in artikel 138ab Sr. Strafbaar is het opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk of een deel daarvan.[7] Het verband met responsible disclosure is vanzelfsprekend. Om een ICT-kwetsbaarheid aan te tonen zal een hacker (vrijwel) altijd een systeem moeten binnendringen. Er is doorgaans immers pas sprake van een veiligheidsrisico wanneer buitenstaanders op enigerlei wijze toegang tot een systeem kunnen krijgen. Uit artikel 138ab lid 1 Sr blijkt dat binnengedrongen kan worden op ten minste vier manieren. Binnendringen kan gebeuren door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel of door het aannemen van een valse hoedanigheid. Bij het aantonen van beveiligingsrisico's in ICT-systemen zal doorgaans sprake zijn van het op enige wijze doorbreken van een beveiliging (dit is het daadwerkelijke hacken).[8]

Van computerbreuk is sprake wanneer dit opzettelijk en wederrechtelijk plaatsvindt. Van opzet zal altijd sprake zijn in het geval van een ethisch hacker die op zoek gaat naar kwetsbaarheden. Aan dit bestanddeel zal dan ook verder geen aandacht besteed worden. Het bestanddeel wederrechtelijkheid wordt hierna behandeld.

Ethisch hacken in jurisprudentie

Jurisprudentie ten aanzien van ethisch hacken is schaars. In twee zaken heeft de rechtbank zich uitgelaten over ethisch hacken. Beide zaken zagen op feiten die zich afspeelden voordat de Leidraad geïntroduceerd werd in 2013. De Rechtbank

4 In Nederland wordt doorgaans niet beloond met grote bedragen. Ethisch hacken in Nederland is geen lucratieve bezigheid, zoals dat wel het geval is in de VS, waar vaak grote beloningen (zogeheten Bug Bounties) uitgeloofd worden voor het melden van kwetsbaarheden.

5 Dit is een belangrijke voorwaarde voor melders. De garantie dat er geen aangifte gedaan wordt maakt het aantrekkelijk om kwetsbaarheden te melden.

6 Leidraad, 8.

7 Hierbij kan gedacht worden aan een bedrijfsnetwerk of een computer binnen dat netwerk.

8 Er bestaat echter een zekere overlap tussen de verschillende vormen van binnendringen. Het binnendringen met een gekraakt wachtwoord bevat elementen van zowel het doorbreken van een beveiliging als het gebruiken van een valse sleutel.

doi: 10.5553/NJLP/221307132017046002006

Oost-Brabant legde aan Tweede Kamerlid Henk Krol een geldboete op wegens het plegen van computervredebreuk. Krol had persoonsgegevens ingezien doordat hij was binnengedrongen in de server van een gegevensbeheerder. Volgens de rechtbank is 'elke inbreuk op een geautomatiseerd werk zonder toestemming van de rechthebbende strafbaar', behoudens het geval 'er onder zeer bijzondere omstandigheden hogere belangen zijn die een dergelijke inbreuk in volle omvang kunnen rechtvaardigen'.[9] De rechtbank overweegt voorts 'dat het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens een wezenlijk maatschappelijk belang kan dienen'. Hoewel Krol in beginsel handelde in het algemeen belang, acht de rechtbank diens handelen toch wederrechtelijk. Omdat Krol onder andere meerdere keren in de server is binnengedrongen en meteen de media heeft ingeschakeld, voldoet zijn handelen niet aan de eisen van proportionaliteit en subsidiariteit.

In de Groene Hart Ziekenhuis-zaak werd door de Rechtbank Den Haag dezelfde redenering gevolgd als in de zaak van Krol. De rechtbank overweegt 'dat elke inbreuk op een geautomatiseerd werk zonder toestemming van de rechthebbende strafbaar is, tenzij hogere belangen een dergelijke inbreuk rechtvaardigen'.[10] De rechtbank overweegt daarna 'dat het aantonen van gebreken in de beveiliging van vertrouwelijke, medische gegevens en persoonsgegevens een wezenlijk maatschappelijk belang kan dienen' en dat 'dergelijk hacken op zichzelf bezien een belangrijke bijdrage [levert] aan de beveiliging van vertrouwelijke gegevens in de gezondheidszorg en de maatschappelijke discussie daarover'.[11] De rechtbank acht het handelen van de verdachte daarnaast in lijn met de eis van subsidiariteit. Omdat de verdachte meerdere keren is ingelogd, is het handelen volgens de rechtbank niet proportioneel. Om die reden ontvalt de wederrechtelijkheid niet aan het handelen.

Uit de feitenrechtspraak blijkt dus dat computervredebreuk zonder voorafgaande toestemming in beginsel strafbaar is, maar dat het algemeen belang ervoor kan zorgen dat de wederrechtelijkheid ontvalt aan ethisch hacken. Falot en Schermer wijzen ook op de verhouding tussen het algemeen belang en de wederrechtelijkheid in het kader van responsible disclosure:

> 'In het geval van responsible disclosure kan (...) rechtvaardiging worden gevonden in het feit dat de ethisch hacker bij het plegen van computervredebreuk het oogmerk had informatiesystemen veiliger te maken en daarmee handelde in zowel het belang van de eigenaar van het informatiesysteem, als in een breder maatschappelijk belang'.[12]

9 Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1157 (Krol-zaak).
10 Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611, r.o. 4.4.1 (GHZ-zaak).
11 Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611, r.o. 4.4.1 (GHZ-zaak).
12 N. Falot en B.W. Schermer, 'De strafrechtelijke positie van de Nederlandse ethisch hacker,' *Computerrecht* 45 (2016).

Openbaar Ministerie

Kenmerkend voor de Nederlandse strafrechtpleging is het opportuniteitsbeginsel, vastgelegd in artikel 167 van het Wetboek van Strafvordering (Sv). Op grond van en ontleend aan het algemeen belang kan het OM van vervolging afzien. In maart 2013 heeft het OM een beleidsbrief gepubliceerd waarin uiteengezet wordt aan de hand van welke criteria officieren van justitie moeten beoordelen of er al dan niet sprake is van responsible disclosure.[13] In de beleidsbrief worden drie voorwaarden genoemd waaraan voldaan moet zijn wil er sprake zijn van een ethische hack.[14] Deze voorwaarden sluiten vrij nauw aan bij de voorwaarden die in de eerder behandelde feitenrechtspraak gehanteerd worden. Uit de eerste voorwaarde blijkt dat er sprake moet zijn van een 'zwaarwegend algemeen belang'. Het bijdragen aan de veiligheid van computersystemen is in dit geval aan te merken als een dergelijk algemeen belang. Ook moet een handeling proportioneel zijn. Hier wordt in de beleidsbrief verwezen naar de eerdergenoemde opsomming van handelingen die als onevenredig aangemerkt moeten worden. In het kader van responsible disclosure lijken voor het OM de termen proportioneel en evenredig dus inwisselbaar. Ten slotte moet een handeling voldoen aan het beginsel van subsidiariteit. Hierbij is de vraag of de hacker anders had kunnen en moeten handelen. Het niet direct melden van een aangetroffen kwetsbaarheid, bijvoorbeeld om sporen uit te wissen, wordt gezien als niet-subsidiair. Wanneer aan één of meer van deze drie eisen niet voldaan is, kan niet gesproken worden van een ethische hack, aldus de beleidsbrief. Ook blijkt uit de beleidsbrief dat er alleen sprake kan zijn van responsible disclosure wanneer de organisatie waarbij een kwetsbaarheid is aangetroffen, een responsible-disclosurebeleid gepubliceerd heeft.[15]

De beleidsbrief is in beginsel intern en kan dus niet gelijkgesteld worden met officieel vervolgingsbeleid van het OM. Hoewel de beleidsbrief zeker niet zonder betekenis is, biedt zij geen harde garanties ten aanzien van de rechtspositie van de ethisch hacker. Het OM heeft sinds het publiceren van de beleidsbrief geen vervolging ingesteld tegen ethisch hackers. Dit lijkt te suggereren dat het OM *de facto* terughoudend is met het vervolgen van ethisch hackers. Falot en Schermer concluderen dan ook dat responsible disclosure in Nederland 'een (informele) plek [heeft] verworven in het strafproces die de positie van de ethisch hacker verheldert en versterkt'.[16] Daarmee is 'het risico op strafrechtelijke vervolging en veroordeling voor Nederlandse ethisch hackers binnen Nederland tot op zekere hoogte beperkt'.[17]

13 Openbaar Ministerie, 'Beleidsbrief Responsible Disclosure 18 maart 2013.' Te downloaden via: www.om.nl/actueel/nieuwsberichten/@32028/beleid-ethische/(geraadpleegd 2 oktober 2017).
14 'Beleidsbrief Responsible Disclosure,' 3.
15 'Beleidsbrief Responsible Disclosure,' 2.
16 Falot en Schermer, 'Strafrechtelijke positie.'
17 Falot en Schermer, 'Strafrechtelijke positie.'

Netherlands Journal of Legal Philosophy 2017 (46) 2
doi: 10.5553/NJLP/221307132017046002006

3 Responsible disclosure: een gedoogbeleid?

Er zijn overeenkomsten tussen het Nederlandse responsible-disclosurebeleid en het Nederlandse gedoogbeleid ten aanzien van softdrugs. Het beleid van responsible disclosure wordt soms zelfs expliciet een gedoogbeleid genoemd.[18] Hacken is in beginsel een strafbaar feit. Er bestaat, zoals hiervoor duidelijk werd, echter OM-beleid op grond waarvan hacken – onder bepaalde voorwaarden – niet vervolgd wordt. Hetzelfde principe geldt waar het bijvoorbeeld gaat om softdrugs. Coffeeshops die 'onder strenge voorwaarden wiet en hasj verkopen', hebben niet voor vervolging door het OM te vrezen.[19] Dit geldt ook voor personen die 'kleine hoeveelheden softdrugs bezitten'.[20]

Softdrugs worden in Nederland gedoogd omdat zij volgens de overheid 'minder schadelijk (...) voor de gezondheid dan harddrugs' zijn.[21] Softdrugs vormen daarom in mindere mate dan harddrugs een gevaar voor de volksgezondheid.[22] De gedachte achter het gedoogbeleid is dan ook, dat wanneer mensen zonder problemen softdrugs kunnen gebruiken, de kans dat zij harddrugs gebruiken kleiner wordt.[23] Ten aanzien van softdrugs hanteert de overheid een beleid van beheersen in plaats van bestrijden. Op dit punt lijkt het gedoogbeleid op het beleid van responsible disclosure. Het toestaan van het gebruik van softdrugs is wenselijker dan het verbieden ervan, net zoals het toestaan van ethisch hacken tot een wenselijker situatie leidt dan wanneer dit niet toegestaan zou zijn.

Er is echter een belangrijk verschil tussen het gedogen van softdrugs en responsible disclosure. In het geval van softdrugs is er geen sprake van actieve aanmoediging van overheidswege. Het blijft bij gedogen. Dit is niet het geval bij responsible disclosure. Ethisch hacken wordt door de Nederlandse overheid *actief* – zij het binnen bepaalde grenzen – aangemoedigd. Dit is op meerdere manieren zichtbaar. Ten eerste hanteert de overheid ten aanzien van haar eigen systemen een

18 D. Tokmetzis, 'Deze hackers ruimen het internet voor ons op,' *De Correspondent* (2016), https://decorrespondent.nl/3977/Deze-hackers-ruimen-het-internet-voor-ons-op/302896703516-45ec3eda (geraadpleegd 13 september 2017).

19 Rijksoverheid, 'Gedoogbeleid softdrugs en coffeeshops,' www.rijksoverheid.nl/onderwerpen/drugs/inhoud/gedoogbeleid-softdrugs-en-coffeeshops (geraadpleegd 13 september 2017).

20 Rijksoverheid, 'Gedoogbeleid softdrugs en coffeeshops.' Het gaat dan om maximaal vijf gram cannabis of vijf hennepplanten per persoon.

21 Rijksoverheid, 'Gedoogbeleid softdrugs en coffeeshops,'

22 Naast de volksgezondheid is er een ander belang dat gediend is met het gedogen van softdrugs. Overlast, die vaak gepaard gaat met het de verkoop van softdrugs, wordt hierdoor enigszins binnen de perken gehouden, zie bijv. *Kamerstukken II* 2003/04, 24077, 125. Omdat dit niet genoemd wordt als primair belang dat gediend is met het gedoogbeleid, zal ik het hier verder buiten beschouwing laten.

23 J. Brouwer en J. Schilder, 'Over de grenzen van gedogen. Het failliet van de B en de I in het coffeeshopbeleid,' *NJB* 44/45 (2012): 2530.

beleid van responsible disclosure. Daarnaast zet de overheid zich in voor met het creëren van bewustzijn inzake cybersecurity en responsible disclosure.[24]

Waarom wordt ethisch hacken aangemoedigd en het gebruik van softdrugs niet? In de manier waarop softdrugs gedoogd worden is een consequentialistische redenering te ontwaren. Het volledig uitbannen van softdrugs zou de voorkeur hebben, omdat de volksgezondheid daarbij gebaat is. Dit is echter 'realistisch' noch 'haalbaar'.[25] In de optiek van de overheid heeft daarom het gedogen van softdrugs de voorkeur. Wanneer het gedogen van softdrugs ervoor zorgt dat gebruikers niet overgaan op schadelijker harddrugs, is het beleid te rechtvaardigen. Het beleid draagt dan bij aan de volksgezondheid en dat levert voor de maatschappij het best mogelijke resultaat op. Het gebruik van softdrugs is met andere woorden *relatief* wenselijk: het is slechts wenselijk in verhouding tot het alternatief – het gebruik van harddrugs.[26] Het gaat hier om een pragmatisch, niet een principieel argument.

Ethisch hacken is naast in relatieve, ook in absolute zin wenselijk. Relatief is ethisch hacken wenselijk omdat het tot een betere situatie leidt dan voorheen. Een ICT-kwetsbaarheid wordt opgelost, en daarmee is de cyberveiligheid van Nederland gediend – hoe klein die bijdrage ook is. Tot zover bestaat er geen groot verschil met het gedogen van softdrugs. Zoals gesteld werd is ethisch hacken echter ook in absolute zin wenselijk. Het intrinsiek wenselijke van het doen van responsible-disclosuremeldingen komt tot uiting in de bereidheid van een ethisch hacker om bij te dragen aan een algemeen belang van de samenleving. De ethisch hacker toont zich dienstbaar door de collectieve cyberveiligheid van de maatschappij te vergroten. Uit het actief uitdragen van responsible disclosure blijkt dat bij de overheid, in ieder geval onder voorwaarden, geen principieel bezwaar bestaat tegen ethisch hacken, terwijl een dergelijk principieel bezwaar wel bestaat ten aanzien van het gebruik van softdrugs. De intrinsieke wenselijkheid van ethisch hacken kan, zoals in de vorige paragraaf bleek, ook uit de feitenrechtspraak afgeleid worden.

4 Positieve uitlokking vs. negatieve uitlokking

Positieve uitlokking werd eerder omschreven als het aanzetten tot gewenst gedrag dat formeel gezien strafbaar kan zijn. Het tegenovergestelde van positieve uitlokking is negatieve uitlokking: het aanzetten tot onwenselijk gedrag dat

24 Het NCSC heeft bijv. uitgebreid gesproken over responsible disclosure met verschillende partijen in de ICT-wereld op het congres NCSC ONE 2015. Zie NCSC, 'NCSC presenteert best practice guide Responsible Disclosure in aanloop naar de Global Conference on Cyberspace' (2015), www.ncsc.nl/actueel/nieuwsberichten/ncsc-presenteert-best-practice-guide-responsible-disclosure-in-aanloop-naar-de-global-conference-on-cyberspace.html (geraadpleegd op 4 oktober 2017).

25 D. van der Gouwe, E. Ehrlich en M.W. van Laar, *Het drugsbeleid in Nederland* (Utrecht: Trimbos-instituut, 2009), 3.

26 Ik ga hier kortheidshalve voorbij aan de vraag of softdrugs überhaupt als onwenselijk en schadelijk aangemerkt zouden moeten worden.

doi: 10.5553/NJLP/221307132017046002006

tevens strafbaar is. Hierna wordt eerst het begrip negatieve uitlokking toegelicht, waarna dieper wordt ingegaan op positieve uitlokking.

Negatieve uitlokking

De betekenis van het begrip negatieve uitlokking lijkt vrij vanzelfsprekend. Het gaat allereerst om *strafbaar* gedrag, zoals het stelen van een fiets.[27] Het is evident dat het hier gaat om *onwenselijk* gedrag. De maatschappij is niet gebaat bij fietsendiefstal. Er is dan ook geen sprake van een zwaarwegend algemeen belang op grond waarvan het onwenselijke karakter aan fietsendiefstal zou kunnen komen te ontvallen.

Het begrip *aanzetten tot* verdient bijzondere aandacht. Hiertoe wordt de jurisprudentie van de Hoge Raad onderzocht. In een tweetal arresten heeft de Hoge Raad criteria ontwikkeld aan de hand waarvan het inzetten van een lokmiddel getoetst kan worden. In het lokfiets-arrest heeft de Hoge Raad bepaald dat het inzetten van een lokfiets in beginsel geoorloofd is, ondanks het feit dat daarvoor geen wettelijke grondslag bestaat. De rechtmatigheid van het inzetten van een lokfiets moet beoordeeld worden aan de hand van het Tallon-criterium.[28] Dit criterium houdt in dat een verdachte niet gebracht mag worden 'tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht'.[29] De Hoge Raad acht niet van belang dat de lokfiets op het moment van plaatsen door de politie niet op slot stond.[30] Bij schending van het Tallon-criterium kan niet meer gesproken worden van een eerlijk proces, wat een ernstige inbreuk op de belangen van de verdachte oplevert.[31] De Nederlandse politie verwoordt het Tallon-criterium treffend en verrassend simpel: lokken mag, uitlokken niet.[32]

In het lokauto-arrest bevestigt de Hoge Raad de rechtsregels uit het lokfiets-arrest.[33] In deze zaak had de politie met toestemming van de officier van justitie een lokauto geplaatst op een locatie waar veel auto-inbraken plaatsvonden. De auto met buitenlands kenteken stond op slot en was voorzien van een in het zicht liggende mobiele telefoon en een (namaak)navigatiesysteem. Volgens de Hoge Raad is er sprake van een rechtmatig lokmiddel, omdat de verdachte 'niet is gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht'.[34]

27 Er zijn legio andere strafbare feiten te bedenken die door middel van het inzetten van een lokmiddel uitgelokt kunnen worden, maar ik beperk me hier gemakshalve tot fietsendiefstal.
28 HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817, *NJ* 2009/224 (lokfiets-arrest).
29 HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817, *NJ* 2009/224, r.o. 2.4.
30 A-G G. Knigge is het niet eens met de redenering. Volgens Knigge mag 'het lokmiddel de situatie ter plaatse niet wezenlijk' veranderen (zie conclusie, punt 17). Het feit dat de lokfiets niet afgesloten was, maakt volgens Knigge dat de politie de dief uitlokt, hetgeen onrechtmatig is.
31 Zie in het kader van een eerlijk proces en art. 6 EVRM ook twee uitspraken van het Europese Hof voor de Rechten van de Mens met betrekking tot uitlokking door opsporingsambtenaren: EHRM 9 juni 1998, *NJ* 2001/471 en EHRM 26 oktober 2006, nr. 596991/00.
32 Politie, 'Gebruikt de politie lokagenten?,' www.vraaghetdepolitie.nl/politie/politiewerk/gebruikt-de-politie-lokagenten-let-op-verhaal-als-bijlage.html (geraadpleegd 2 oktober 2017).
33 HR 6 oktober 2009, ECLI:NL:HR:2009:BI7084 (lokauto-arrest).
34 HR 6 oktober 2009, ECLI:NL:HR:2009:BI7084, r.o. 2.6.3.

doi: 10.5553/NJLP/221307132017046002006

Waar in het lokfiets-arrest alleen het Tallon-criterium van belang is bij de beoordeling van de rechtmatigheid van het inzetten van een lokmiddel, hecht de Hoge Raad bij deze beoordeling in het lokauto-arrest ook waarde aan de beginselen van proportionaliteit en subsidiariteit. De Hoge Raad acht deze beginselen in casu niet geschonden. Volgens Corstens hangen beide beginselen samen met het beginsel van redelijke en billijke belangenafweging. Opsporingsambtenaren moeten rekening houden met 'de in aanmerking komende belangen'.[35] Deze belangen moeten 'behoorlijk tegen elkaar afgewogen' worden.[36] Het wegen van deze belangen geschiedt aan de hand van de beginselen van proportionaliteit en subsidiariteit. Van subsidiariteit is sprake wanneer de opsporing geschiedt op een voor de betrokkene zo min mogelijk ingrijpende manier. Het optreden is proportioneel wanneer het in redelijke verhouding staat tot het met het optreden gewenste doel.

Geconcludeerd kan worden dat de opzet van de verdachte in de jurisprudentie een belangrijke rol speelt: het is opsporingsambtenaren niet toegestaan om de opzet van een verdachte te beïnvloeden. Er is dan sprake van negatieve uitlokking.[37] Het Tallon-criterium verbiedt immers het *aanzetten tot* strafbaar gedrag. De inzet van een lokmiddel moet daarnaast voldoen aan de eisen van proportionaliteit en subsidiariteit.

Positieve uitlokking

Allereerst is bij positieve uitlokking sprake van het aanzetten tot *gewenst* gedrag. Zoals in paragraaf 3 werd beargumenteerd, is ethisch hacken intrinsiek wenselijk. De maatschappij als geheel is erbij gebaat. Op grond hiervan kan gesteld worden dat positieve uitlokking in beginsel een goede ontwikkeling is. Er lijkt op het eerste gezicht immers niets mis met het aanzetten van individuen tot wenselijke handelingen. Hier is een nuancering op zijn plaats. De overheid ziet ethisch hacken in beginsel als intrinsiek wenselijk, maar verbindt daaraan wel bepaalde *voorwaarden*: responsible disclosure moet blijkens de beleidsbrief van het OM binnen bepaalde kaders plaatsvinden. Er is voor de overheid, met andere woorden, pas sprake van gewenst gedrag, wanneer een hacker zich aan deze voorwaarden houdt.

Bij positieve uitlokking wordt *aangezet tot* gewenst gedrag. Onder aanzetten tot versta ik het bewegen van individuen tot het ondernemen van bepaald gedrag.[38] Het gaat hier dus om meer dan louter gedogen, zoals het geval is bij softdrugs. Gesteld zou kunnen worden – om in de terminologie van het Tallon-criterium te blijven – dat in het geval van responsible disclosure de melder tot andere handelingen gebracht mag worden dan die waartoe zijn opzet reeds gericht was. Iemand die beschikt over de technische kennis om te hacken zou door een gepubliceerd

35 G.J.M. Corstens, *Het Nederlands strafprocesrecht* (Deventer: Kluwer, 2014), 58.

36 Corstens, *Nederlands strafprocesrecht*, 58.

37 Let op: het inzetten van een lokmiddel is dus niet per definitie een vorm van negatieve uitlokking. Van negatieve uitlokking is pas sprake wanneer het Tallon-criterium geschonden is.

38 Zowel de overheid als organisaties kunnen in dit kader aanzetten.

doi: 10.5553/NJLP/221307132017046002006

responsible-disclosurebeleid overgehaald kunnen worden om op zoek te gaan naar kwetsbaarheden.[39]

Ten slotte gaat het bij positieve uitlokking – in ieder geval wat betreft responsible disclosure – om gedrag dat formeel gezien strafbaar *kan* zijn. Ethisch hacken lijkt op basis van de beleidsbrief van het OM onder bepaalde voorwaarden toegestaan. Het OM zal dan in beginsel niet tot vervolging overgaan. Met de term 'kan' wordt geprobeerd duidelijk te maken dat er soms een dunne lijn bestaat tussen wat wel en wat niet als een ethische hack te gelden heeft.[40] Ook wordt hiermee uitdrukking gegeven aan het feit dat zowel de Leidraad als de beleidsbrief van het OM geen harde garanties bieden ten aanzien van de rechtspositie van de ethisch hacker.

Verhouding responsible disclosure en uitlokking in het kader van de opsporing

Uit de jurisprudentie van de Hoge Raad bleek hiervoor dat de belangen van de verdachte zwaar wegen. Het is de vraag in hoeverre de belangen van de melder van een kwetsbaarheid in het gedrang komen bij responsible disclosure en in hoeverre de waarborgen die bestaan ten aanzien van het inzetten van een lokmiddel, gelden (of moeten gelden) ten aanzien van responsible-disclosurebeleid. Mag in het geval van responsible disclosure in plaats van slechts gelokt, ook *uit*gelokt worden? Welke rol speelt het Tallon-criterium daarbij?

In de Leidraad worden ethisch hackers consequent aangeduid als melders. Melders zijn geen verdachten in de zin van artikel 27 lid 1 Sv. Er bestaat in beginsel geen redelijk vermoeden van schuld tegen de melder. In beginsel is het Tallon-criterium dus niet van toepassing op melders. Hier is echter een kanttekening te plaatsen. Essentieel is dat responsible-disclosurebeleid duidelijk is. Wanneer dat niet het geval is, kan iemand immers worden aangezet tot handelingen die – onbedoeld – strafbaar zijn. Een ethisch hacker zou in de veronderstelling kunnen verkeren dat hij binnen de kaders van het gepubliceerde responsible-disclosurebeleid blijft, terwijl het OM ten aanzien daarvan een andere opvatting heeft. Het OM kan dan een onderzoek starten, wat vervolgens tot vervolging kan leiden. Een goedbedoelende melder wordt op deze wijze alsnog een verdachte.[41] Dit levert als het ware met terugwerkende kracht negatieve uitlokking op. De intentie was immers niet om een melder uit te lokken tot strafbaar gedrag, maar dat is dan wel

39 Het achterliggende motief van een ethisch hacker om een responsible-disclosuremelding te doen is hier niet relevant, hieraan worden althans geen eisen gesteld. Van een melder wordt alleen verwacht dat hij zich houdt aan het gepubliceerde responsible-disclosurebeleid.

40 Ter illustratie: in 2011 kreeg een journalist toegang tot de Miljoenennota van 2012. Dit deed hij door in de URL het getal 2011 te veranderen in 2012. Technisch gezien zou deze kinderlijk simpele handeling computervredebreuk op kunnen leveren. Zie NOS, 'Alle begrotingsstukken openbaar,' 15 september 2011, http://nos.nl/artikel/273011-alle-begrotingsstukken-openbaar.html (geraadpleegd 2 oktober 2017).

41 Duidelijkheid is overigens ook belangrijk in verband met de effectiviteit van responsible disclosure. Doorgaans zullen ethisch hackers pas wanneer zij garanties hebben dat ze niet vervolgd worden en exact weten wat wel en niet geoorloofd is, bereid zijn responsible-disclosuremeldingen te doen.

het resultaat. Positieve uitlokking moet, met andere woorden, niet omslaan in negatieve uitlokking. Ook in het geval van responsible disclosure kan het Talloncriterium dus relevant zijn – en geschonden worden.[42]

Proportionaliteit en subsidiariteit

In het lokauto-arrest stelde de Hoge Raad dat de inzet van een lokmiddel moet voldoen aan de eisen van proportionaliteit en subsidiariteit. In de beleidsbrief van het OM ten aanzien van responsible disclosure komen de beginselen van proportionaliteit en subsidiariteit ook voor. Het gaat daar echter niet om criteria ten aanzien van het handelen van overheidsambten, maar om criteria ten aanzien van het handelen van de *melder*. Kan gesteld worden dat het overheidsbeleid ten aanzien van ethisch hacken voldoet aan de eisen van proportionaliteit en subsidiariteit? Zoals hiervoor duidelijk geworden is, wordt in de jurisprudentie aan de belangen van de verdachte veel waarde gehecht bij het inzetten van een lokmiddel. Die belangen worden geschaad wanneer de verdachte wordt bewogen tot een misdrijf op een manier die niet in verhouding staat tot het doel of die te zwaar is om dat doel te bereiken. Het is goed te verdedigen dat met het publiceren van de Leidraad door het NCSC en het openbaar maken van de beleidsbrief door het OM de overheid voldoet aan de eisen van proportionaliteit en subsidiariteit. Wanneer dit immers leidt tot het handelen van melders binnen de eisen van proportionaliteit en subsidiariteit, is er voor die melders in beginsel geen gevaar voor schending van hun belangen. Daarmee handelt de overheid indirect ook binnen de grenzen van beide eisen. Hierbij merk ik echter nogmaals op dat aan de Leidraad en de beleidsbrief geen harde garanties kunnen worden ontleend.

Eigen mening: een breder begrip van responsible disclosure?

De rechtspositie van de ethisch hacker is in Nederland sinds het introduceren van de Leidraad in 2013 duidelijk verbeterd, maar is nog niet optimaal. Nu bestaat de situatie waarin voor ethisch hackers op basis van de beleidsbrief duidelijk lijkt wat al dan niet geoorloofd is in het kader van responsible disclosure, maar tegelijkertijd kunnen hackers hieraan geen harde garanties ontlenen. Het intrinsiek wenselijke karakter van ethisch hacken brengt echter naar mijn mening met zich dat ethisch hacken mogelijk moet zijn binnen kaders van de proportionaliteit en de subsidiariteit, zonder dat het risico bestaat dat het OM tot vervolging overgaat. De kaders van de proportionaliteit en de subsidiariteit kunnen afgeleid worden uit de feitenrechtspraak, maar eventueel ook uit de Leidraad. Responsible disclosure moet mijn inziens ook mogelijk zijn in situaties waarin geen voorafgaande toestemming is gegeven door organisaties door middel van het publiceren van eigen responsible-disclosurebeleid. Ook hierbij is het maatschappelijk belang immers gediend. Uit de beleidsbrief van het OM blijkt dat de afwezigheid van een dergelijk beleid momenteel *per definitie* maakt dat er geen sprake kan zijn van responsible disclosure.[43] Dit kan een beletsel vormen voor de bereidwilligheid van

42 Sinds het introduceren van de Leidraad is het OM niet tot vervolging overgegaan van ethisch hackers. Dit neemt het theoretische risico van onduidelijkheid echter niet weg.

43 'Beleidsbrief Responsible Disclosure,' 2.

Netherlands Journal of Legal Philosophy 2017 (46) 2
doi: 10.5553/NJLP/221307132017046002006

ethisch hackers om kwetsbaarheden te melden en dat komt het algemeen belang niet ten goede.

5 Conclusie

Het constructief en positief benaderen van ethisch hackers door middel van het van overheidswege uitdragen van responsible disclosure is vanuit een strafrechtelijk perspectief een unieke ontwikkeling. Volgens mij kan er van een gunstige ontwikkeling gesproken worden. Ethisch hackers kunnen een waardevolle bijdrage leveren aan de cyberveiligheid in Nederland en dienen daarmee een publiek belang. Op dit punt verschilt responsible disclosure fundamenteel met het gedogen van softdrugs. Ethisch hacken is in tegenstelling tot softdrugsgebruik – in ieder geval in de optiek van de Nederlandse overheid – intrinsiek wenselijk. Melders van ICT-kwetsbaarheden worden niet gezien als verdachten en daarom zijn de waarborgen die gelden ten aanzien van verdachten, concreet het Talloncriterium, in beginsel niet relevant. Het Nederlandse responsible-disclosurebeleid voldoet daarbij in beginsel aan de eisen van proportionaliteit en subsidiariteit. Van essentieel belang hierbij is de duidelijkheid van responsible-disclosurebeleid. Het moet voor melders duidelijk zijn wat wel en wat niet geoorloofd is. Bij onduidelijkheid bestaat het risico dat melders onbedoeld een grens overschrijden en alsnog verdachte worden. In dat geval is er sprake van wat ik omschrijf als negatieve uitlokking. Zoals bleek is negatieve uitlokking naar de maatstaven van de Hoge Raad aan te merken als onrechtmatig omdat daarmee de belangen van de verdachte in het gedrang komen. Van een dergelijke schending kan in theorie ook bij responsible disclosure sprake zijn. Er moet daarom voor gewaakt worden dat positieve uitlokking omslaat in negatieve uitlokking.

De houding van het OM ten aanzien van responsible disclosure lijkt in de praktijk enige zekerheid te bieden voor ethisch hackers, maar doorslaggevende garanties zijn er op basis van de beleidsbrief niet. Daarom ben ik er voorstander van dat het vervolgingsbeleid van het OM vastgelegd wordt in officieel OM-beleid, waarop een ethisch hacker zich kan beroepen. Hierbij valt te denken aan een vervolgingsrichtlijn.[44] De eis van voorafgaande toestemming moet daarbij mijns inziens losgelaten worden: ethisch hacken binnen de grenzen van proportionaliteit en subsidiariteit is wenselijk en daarvoor moet toestemming geen vereiste zijn. De versteviging van de rechtspositie van ethisch hackers kan eraan bijdragen dat de bereidwilligheid van ethisch hackers om kwetsbaarheden te melden groeit, hetgeen de cyberveiligheid van Nederland ten goede komt.

44 Een andere, meer verstrekkende optie zou zijn het opnemen in de wet van een bijzondere strafuitsluitingsgrond ten aanzien van ethisch hacken.