BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M .
E
W https://www.bof.nl

Ivo Opstelten
Minister van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Betreft
Reactie op consultatie Wetsvoorstel Computercriminaliteit III

Amsterdam
28 juni 2013

Geachte Minister Opstelten,

Met deze brief gaan wij in op uw uitnodiging om te reageren op het Wetsvoorstel Computercriminaliteit III.[1] Dit voorstel wil de politie en justitie de bevoegdheid geven om op afstand in te breken op een geautomatiseerd werk[2], spyware te installeren en het werk over te nemen, daarop rond te kijken en gegevens te verwijderen – in zowel binnen- als buitenland (het 'hackvoorstel'). Daarnaast wordt een verbetering voorgesteld van de bevoegdheid om informatie ontoegankelijk te maken, wordt een decryptiebevel en een strafbaarstelling van heling van gegevens geïntroduceerd.

Zoals wij hierna zal toelichten zijn deze voorstellen voor Bits of Freedom onacceptabel. Ten aanzien van het hackvoorstel en het decryptiebevel geldt dat onze bezwaren, zowel afzonderlijk als tezamen genomen, zo fundamenteel van aard zijn, dat deze voorstellen in hun geheel moeten worden afgewezen. Voor de bezwaren tegen de overige voorstellen geldt dat zij zodanig zijn dat de voorstellen op essentiële onderdelen moeten worden herzien. Wij zullen dit hierna toelichten en verzoeken u dringend onze overwegingen bij uw beleidskeuzes te betrekken.

Met vriendelijke groet,

1 Voorstel tot Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), 2 mei 2013.
2 Zie voor de definitie van 'geautomatiseerd werk' paragraaf 1.1.3 onder (i). In dit stuk wordt een geautomatiseerd werk ook wel aangeduid met 'computer'.

Inhoudsopgave

1	**De hackbevoegdheid**		3
1.1	De hackbevoegdheid is een onbegrensd opsporingsmiddel		3
1.1.1	*Het middel is niet beperkt tot verdachten*		3
1.1.2	*Het middel kan bij te veel misdrijven worden ingezet*		3
1.1.3	*Ook per misdrijf zijn de mogelijkheden eindeloos*		5
1.1.4	*Het middel is technisch onbeperkt*		7
1.1.5	*Tussenconclusie*		8
1.2	De hackbevoegdheid is in strijd met fundamentele rechten		9
1.2.1	*Inbreuk op privacy*		9
1.2.2	*Noodzaak, proportionaliteit en effectiviteit niet aangetoond*		10
1.2.3	*Tussenconclusie*		12
1.3	De hackbevoegdheid is in strijd met het volkenrecht		12
1.3.1	*Het soevereiniteitsbeginsel*		12
1.3.2	*Internationale verdragen*		13
1.3.3	*Tussenconclusie*		14
1.4	De hackbevoegdheid creëert onaanvaardbare cybersecurityrisico's		15
1.4.1	*Kwetsbaarheden in software*		15
1.4.2	*Spyware moeilijk binnen de perken te houden*		15
1.4.3	*De detectie van overheidsspyware door antivirus-software*		17
1.4.4	*Tussenconclusie*		18
1.5	Conclusie		18
2	**De bevoegdheid om informatie ontoegankelijk te maken**		18
3	**Het decryptiebevel**		19
3.1	Het decryptiebevel is in strijd met fundamentele rechten		19
3.2	Het decryptiebevel is niet noodzakelijk		21
3.3	Het decryptiebevel is niet effectief		21
3.4	Het decryptiebevel leidt tot misbruik		22
3.5	Conclusie		23
4	**Heling van gegevens**		23
4.1	'Niet-openbaarheid' onjuist aanknopingspunt voor strafbaarheid		23
4.2	Het voorstel heeft 'chilling effect'		24
4.3	Noodzaak van het voorstel onvoldoende onderbouwd		24
4.4	Conclusie		25

1 De hackbevoegdheid

De hackbevoegdheid kent grote bezwaren: het is een onbegrensd opsporingsmiddel (paragraaf 1.1), de bevoegdheid is in strijd met fundamentele rechten (paragraaf 1.2), de bevoegdheid is in strijd met het volkenrecht (paragraaf 1.3) en creëert onaanvaardbare cybersecurityrisico's (paragraaf 1.4).

1.1 De hackbevoegdheid is een onbegrensd opsporingsmiddel

De onthullingen over het Amerikaanse spionagesysteem PRISM laten zien dat de onbegrensde toegang van de overheid tot ons online leven diep ingrijpt op de fundamentele rechten op privacy en vrijheid van meningsuiting van onschuldige burgers wereldwijd. Het is daarom zaak om de bevoegdheden van de overheid tot het hoogst noodzakelijke te beperken en ervoor te zorgen dat de macht van de overheid scherp wordt gecontroleerd. De hackbevoegdheid schiet hierin op cruciale punten te kort.

1.1.1 Het middel is niet beperkt tot verdachten

Juist niet-verdachten zullen het slachtoffer worden van acties van een hackende overheid. Criminelen werken immers bijna nooit vanaf hun eigen computer, maar vooral vanaf de computers van onschuldige burgers, en soms zelfs via een keten van computers.[3] Net zoals een bankovervaller in de meeste gevallen zijn eigen auto niet als vluchtauto gebruikt, maar een gestolen auto, gebruiken criminelen op internet ook niet-eigen middelen. Bovendien kunnen ze gebruik maken van anonimiseringsdiensten, proxies en Virtuele Private Netwerken die de ware identiteit verbergen. Als de politie alleen naar het IP-adres van de vermeende dader kijkt en vervolgens de computer gaat hacken waar de aanval vandaan komt of lijkt te komen, zullen ze dan ook vaak niet de computer van de crimineel zelf treffen, maar die van een onschuldige internetgebruiker of een van een bedrijf dat bijvoorbeeld anonimiseringsdiensten aanbiedt. De politie vangt dus geen criminelen, maar maakt wel inbreuk op het grondrecht op privacy en creëert bovendien het aanzienlijke risico dat de gehackte computer offline gaan of dat er gegevens beschadigd raken.[4] Burgers en bedrijven worden dan de dupe van een hack, die verder niets oplevert.

1.1.2 Het middel kan bij te veel misdrijven worden ingezet

In de eerste plaats zou de hackbevoegdheid kunnen worden ingezet bij verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat een ernstige inbreuk op de rechtsorde oplevert. Dat bestrijkt niet alleen "ernstige vormen van computercriminaliteit" maar ook andere en minder ernstige

3 Zie ook de Toelichting, p. 17.
4 Bijvoorbeeld "Terughacken politie kan bedrijfsleven verstoren", Nu.nl, 5 mei 2013. Zie: http://nutech.nl/cybercrime/3415045/terughacken-politie-kan-bedrijfsleven-verstoren.html.

misdrijven[5], zoals lichte vormen van mishandeling[6], drugsdelicten[7], woningkraak[8], majesteitsschennis[9] of handelen in strijd met openbaar gezag[10]. Deze delicten hebben vaak geen enkele connectie met computercriminaliteit, zodat de inzet van de hackbevoegdheid niet kan worden gerechtvaardigd.[11]

Het cumulatieve vereiste dat voor de inzet van de hackbevoegdheid ook sprake moet zijn van "een ernstige inbreuk op de rechtsorde", maakt dit niet anders. Deze maatstaf is afhankelijk van de omstandigheden van het geval en geeft dus weinig houvast. Bovendien blijkt uit de jurisprudentie dat deze eis in de praktijk een wassen neus is: bij de diefstal van een telefoon in een brandweerkazerne [12] of de diefstal van enkele computers is al sprake van een ernstige inbreuk op de rechtsorde.[13]

Verder geldt dat de gevallen waarin de hackbevoegdheid mag worden toegepast niet beperkter zijn dan de gevallen waarin minder ingrijpende opsporingsmethoden, zoals de telefoon- en internettap, mogen worden toegepast.[14] Dat is gek, want hacken is een stuk ingrijpender (paragraaf 1.2.1). Bovendien wordt een van die andere opsporingsmethoden, de aftapbevoegdheid, in de praktijk zeer vaak en voor een breed scala aan delicten ingezet. De politie doet dat bovendien onzorgvuldig en ineffectief – zo blijkt uit de minimale informatie die de overheid hierover publiceert.[15] Nu de veel ingrijpendere hackbevoegdheid in dezelfde gevallen mag worden toegepast ligt het in de lijn der verwachting dat ook dit middel breed zal worden toegepast.

In de tweede plaats creëert het wetsvoorstel de mogelijkheid om de hackbevoegdheid niet alleen in te zetten als opsporingsmiddel, maar ook als 'verstoringsmiddel' – om bijvoorbeeld botnets te bestrijden.[16] Een dergelijk middel heeft hele andere doelen en toepassingen dan een hackbevoegdheid. Zij zou worden ingezet in specifieke situaties waarin sprake is van bepaalde acute aanvallen op personen of infrastructuur in Nederland.[17] Dit is dus géén opsporingsmiddel. Door de 'verstoringsbevoegdheid' en opsporingsbevoegdheid op één hoop te gooien, is het doel van de hackbevoegdheid onvoldoende afgebakend en dus de wijze waarop deze kan worden ingezet.

---

5 Artikel 125 ja Sv Wijzigingsvoorstel en de Toelichting, p. 5 en 12.
6 Artikel 67, lid 1 Sv, juncto 300, lid 1, Sr.
7 Artikel 67, lid 1 Sv, juncto artikel 11, lid 2, Opiumwet.
8 Artikel 67, lid 1 Sv, juncto artikel 138a Sr.
9 Artikel 67, lid 1 Sv, juncto artikel 111 Sr.
10 Artikel 67, lid 1 Sv, juncto artikel 177 Sr.
11 "Ronald Prins: terughacken enige weg om dader op te sporen", NOS Radio 1, donderdag 2 mei 2013. Zie: http://nos.nl/audio/502368-ronald-prins-terughacken-enige-weg-om-dader-op-te-sporen.html.html.
12 HR 21 november 2006, LJN AY9673.
13 Hof Den Bosch, 31 januari 2002, LJN9433.
14 Artikel 126m Sv.
15 O.a. "Het gebruik van de telefoon- en internettap in de opsporing", Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Veiligheid en Justitie, mei 2012.
16 Toelichting, p. 12 en 43.
17 Zie o.a. Bart Jacobs, "Policeware", Nederlands Juristenblad, 9 november 2012, afl. 39, p. 2764.

1.1.3 Ook per misdrijf zijn de mogelijkheden eindeloos

De inzet van de hackbevoegdheid is ook op de volgende manieren te ruim:

(i) Inbreken mag op eindeloos veel plekken

In de eerste plaats wordt in artikel 80sexies Sr voorgesteld om het begrip 'geautomatiseerd werk' te verruimen, zodat dit begrip ook de router omvat.[18] De voorgestelde definitie strekt echter veel verder. Het begrip 'geautomatiseerd werk' wordt namelijk uitgebreid met álle computerachtige apparaten die in verbinding staan met een netwerk – en dus niet alleen met routers.[19] Deze definitie omvat computers, servers, modems en routers; apparaten die iedereen thuis heeft staan om het internet op te gaan. Maar ook de smartphone en tablet zoals de iPad – die iedereen overal met zich meedraagt – vallen eronder. Bovendien omvat deze definitie álle andere technische apparaten die in verbinding staan met een netwerk, zoals de SCADA-systemen die worden gebruikt bij industriële productiesystemen, navigatiesystemen, televisies, een digitaal fototoestel met wifi-compatibiliteit, een smart-meter, maar ook een pacemaker of gehoorapparaat en in de toekomst ook Google Glass. De mogelijkheden zijn onbeperkt.

In de tweede plaats vereist artikel 125ja Sv dat het geautomatiseerde werk of de daarmee in verbinding staande gegevensdrager door de verdachte 'in gebruik' is. Volgens de Toelichting bij het wetsvoorstel betekent dit "dat op grond van feiten of omstandigheden aannemelijk dient te zijn dat de verdachte gebruik maakt van het geautomatiseerde werk of de gegevensdrager."[20] Waartoe 'in gebruik' beperkt blijft, is echter onduidelijk. Zo duidt het criterium niet op eigendom noch op individueel gebruik. Dit is problematisch omdat een computer, het netwerk of de server waarmee de computer in verbinding staat, kan worden gebruikt door een groot aantal gebruikers. De Toelichting erkent dit ook door te zeggen dat niet is vereist dat de verdachte de enige gebruiker is.[21] Hiervan is bijvoorbeeld sprake als een computer is gehackt door een kwaadwillende (paragraaf 1.1.1). De computer van onschuldige burgers of bedrijven wordt dan door gebruikt om strafbare feiten te plegen, zonder hun medeweten. Het voorstel lijkt het daarmee mogelijk te maken om computers te hacken die onderdeel zijn van een botnet.[22] Dat zou betekenen dat als 100.000 computers geïnfecteerd zijn, de politie op elk van die computers mag inbreken. Dat is onacceptabel.

Bovendien omvat 'in gebruik' ook het gebruik door de verdachte van de servers

18 Toelichting, p. 69-70.
19 "[H]et [is] dan ook wenselijk om de router onder de definitie van geautomatiseerd werk te brengen." Toelichting, p. 70.
20 *Ibid*, p. 75.
21 *Ibid*.
22 *Ibid*, p. 17.

van aanbieders van cloudcomputingdiensten, bijvoorbeeld Hotmail en Google.[23] De politie mag deze servers namelijk – heimelijk – hacken, zonder dat de verdachte of de aanbieder daarbij is betrokken.[24] Dat betekent dat de politie zo een server vanaf de computer van de verdachte kan benaderen[25], maar ook dat de politie direct op de server van de aanbieder zou kunnen inbreken.[26] Dit heeft grote gevolgen. Als de server van Gmail wordt gehackt om de gegevens van één persoon te verkrijgen, dan betekent dit namelijk dat de hele server wordt gehackt. De politie krijgt dan niet alleen toegang tot de gegevens van de verdachte, maar ook tot de gegevens van alle andere – onschuldige – burgers en bedrijven die gebruik maken van Gmail. Met de grote toename in het gebruik en aanbod van cloudcomputingdiensten, zou dit probleem in de toekomst alleen maar groter worden.

Ten derde is de hackbevoegdheid grenzeloos: zij is niet beperkt tot Nederland, maar kan ook buiten onze landsgrenzen worden ingezet.[27] In welke gevallen dat zou zijn toegestaan, wordt open gelaten.

(ii) Ná inbreken zijn ontelbare handelingen mogelijk

De verschillende handelingen die de politie kan uitvoeren, nadat is ingebroken, zijn ontelbaar. Een kleine selectie op basis van de Toelichting:

> "Nadat de politie op het geautomatiseerd werk heeft ingebroken kan zij een keylogger installeren die de aanslagen op het toetsenbord vastlegt, of een richtmicrofoon, met behulp waarvan op grote afstand vertrouwelijke informatie kan worden afgeluisterd en opgenomen.[28] Ook kan worden gedacht aan het op afstand aanzetten van een microfoon van een computer, zodat bijvoorbeeld VOIP-gesprekken kunnen worden afgeluisterd die worden gevoerd met de betreffende computer.[29] Door heimelijk toegang te verkrijgen tot een smartphone, kan de politie via de GPS-locatie nagaan waar de smartphone zich bevindt."[30]

Maar er is nog een heel scala aan andere mogelijkheden: zo is het denkbaar dat de camera op afstand wordt ingeschakeld, dat via afstand online-bankingdiensten worden bekeken en zo inzicht wordt verkregen in iemands financiële gedrag, dat live wordt meegekeken op het beeldscherm, dat iemands emailcorrespondentie en privé-foto's wordt bekeken etc. Dit betekent dat de hackbevoegdheid een onbeperkt palet aan opsporingsmethoden creëert.

Bovendien kunnen met de hackbevoegdheid ook reeds bestaande

23 *Ibid*, p. 9.
24 *Ibid*, p. 10.
25 *Ibid*, p. 15.
26 *Ibid*, p. 10.
27 *Ibid*, p. 34-35.
28 *Ibid*, p. 19.
29 *Ibid*.
30 *Ibid*, p. 20.

opsporingsmethodes worden 'vervangen', zoals het aftappen van communicatie. Dit heeft als risico dat de hackbevoegdheid te lichtvaardig en gemakshalve zou kunnen worden ingezet om verschillende vliegen in één klap te slaan. Volgens de Toelichting is dit ook de bedoeling:

> "Daarnaast kan worden verwacht dat de inzet van onderzoek in een geautomatiseerd werk mogelijk ook andere vormen van politie-inzet kan vervangen en daarmee middelen kunnen worden bespaard."[31]

Dit is het ultieme voorbeeld van 'function creep': het gebruik van een middel voor een ander doel dan waarvoor het oorspronkelijk is bedoeld. Dat is in bijna elk geval onacceptabel, maar zeker in het geval van zo'n ingrijpende bevoegdheid als de hackbevoegdheid. Het maakt ook duidelijk dat de proportionaliteits- en subsidiairiteitstoets bij de toepassing in de praktijk een wassen neus is: het argument dat er een minder inbreukmakend opsporingsmiddel is, is niet doorslaggevend, nu door het gebruik van de hackbevoegdheid op middelen kan worden bespaard.

(iii) Rondkijken mag te lang

Volgens de Toelichting is de minst vergaande bevoegdheid rond het onderzoek in een geautomatiseerd werk het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerd werk of de gebruiker (ook wel aangeduid met 'virtuele plaatsopneming').[32] In dit geval kan het overnemen van gegevens – anders dan de huidige doorzoeking ter vastlegging van gegevens – echter ook betrekking hebben op gegevens die ná het tijdstip van afgifte van het bevel worden verwerkt.[33] Dit is problematisch. Anders dan bijvoorbeeld een huiszoeking is een 'virtuele plaatsopneming' geen momentopname, maar gebonden aan een termijn van vier weken, die telkens met een periode van vier weken kan worden verlengd.[34] Deze termijn creëert voor de politie de mogelijkheid om op de computer, waarop zij heeft ingebroken, rond te blijven hangen in de hoop dat op een later moment nog gegevens worden verwerkt. Ook deze termijn is dus onvoldoende begrensd.

1.1.4 Het middel is technisch onbeperkt

De Toelichting maakt een scherp onderscheid tussen verschillende onderzoekshandelingen.[35] Dit impliceert dat er ook in de praktijk een scheiding kan worden gemaakt tussen bijvoorbeeld de bevoegdheid om rond te kijken in een geautomatiseerd werk of de bevoegdheid om gegevens over te nemen. Zo'n onderscheid bestaat echter niet. Voor het installeren van software op een computer zijn zogenoemde admin of root gebruikersrechten nodig, waarmee

31 *Ibid*, p. 68.
32 *Ibid*, p. 14-15.
33 *Ibid*, p. 75.
34 Artikel 125 ja, lid 3, Sv Wijzigingsvoorstel.
35 Toelichting, p. 14.

men totale controle over die computer krijgt. Bij het verkrijgen van een root/admin-status is dan ook technisch alles mogelijk: lezen én schrijven, en dus aanbrengen van wijzigingen op de computer.[36] De Toelichting probeert deze onbeperkte toegangsrechten te begrenzen door een functiescheiding aan te brengen tussen opsporingsambtenaren die de software plaatsen en opsporingsambtenaren die het onderzoek uitvoeren. Daarnaast wordt vereist dat voor elke bevoegdheid een afzonderlijk bevel wordt afgegeven en dat de software steeds wordt gebruikt binnen de grenzen van die bevoegdheid: "andere functionaliteiten [dan waarvoor het bevel is afgegeven] worden niet ingeschakeld en geïnstalleerd in het geautomatiseerde werk."[37]

In de praktijk blijken die technische beperkingen echter niet goed te implementeren: zo mocht de politie in Duitsland slechts software gebruiken die een beperkte functionaliteit had. Duitse security-onderzoekers van de CCC toonden echter aan dat deze software op afstand makkelijk kon worden uitgebreid.[38] Naar aanleiding daarvan heeft de Duitse overheid de software teruggetrokken. Tegen deze achtergrond is onduidelijk hoe dit soort beperkingen in Nederland technisch zullen worden geëffectueerd en of de technische risico's überhaupt afdoende kunnen worden ondervangen.

Het voorstel geeft aan verschillende technische risico's te willen ondervangen door het vaststellen van nadere regels over de inzet van het middel en de controle daarop en door nadere technische eisen te stellen aan de software die wordt gebruikt om het onderzoek te verrichten.[39] Daarnaast moeten deze regels de integriteit van het vergaarde bewijsmateriaal garanderen.[40] Deze regels zijn dus duidelijk geen bijzaken. Sterker nog: omdat de hackbevoegdheid in juridische en technische zin vrijwel onbegrensd is, zijn deze nadere regels de belangrijkste beperkingen die aan deze opsporingsmethode worden gesteld. Het is dan ook onacceptabel dat – zoals wordt voorgesteld – deze regels in lagere wetgeving worden geregeld en dat dit pas gebeurt nádat het wetsvoorstel is aangenomen. Immers, daarmee worden de regels onttrokken aan parlementaire controle en blijft de precieze reikwijdte ongewis.

1.1.5 Tussenconclusie

Gezien bovenstaande is er sprake van een dermate ruime bevoegdheden ten aanzien van een dermate grote groep personen en misdrijven dat de hackbevoegdheid een carte blanche voor de opsporingsdiensten creëert. Zo een bevoegdheid is per definitie disproportioneel.

---

36 Bart Jacobs, "Policeware", Nederlands Juristenblad, 9 november 2012, afl. 39, p. 2762.
37 Toelichting, p. 80.
38 Zie CCC, "Chaos Computer Club analyzes government malware", 10 augustus 2011, te vinden op http://ccc.de/en/updates/2011/staatstrojaner.
39 Toelichting, p. 19, 24 en 79-80. Dit zou worden uitgewerkt in respectievelijk een Algemene Maatregel van Bestuur (AMvB) en het Besluit technische hulpmiddelen.
40 Toelichting, p. 28.

1.2 De hackbevoegdheid is in strijd met fundamentele rechten

Niet alleen is de bevoegdheid onbegrensd: de hackbevoegdheid voldoet ook niet aan de vereisten van noodzakelijkheid, proportionaliteit en effectiviteit, die gelden voor maatregelen die een sterke inbreuk maken op fundamentele rechten.

1.2.1 Het recht op privacy

De hackbevoegdheid leidt tot een ernstige inperking van het grondrecht op privacy.[41] Dit geldt niet alleen voor verdachten. Het voorstel raakt namelijk ook een grote groep mensen die géén verdachte is (paragraaf 1.1.1). Bovendien hebben de voorgestelde bevoegdheden veel grotere gevolgen voor de privacy van betrokkenen dan de huidige bevoegdheden. Bij het aftappen van telefoongesprekken of het plaatsen van afluisterapparatuur geldt al dat niet alleen de verdachte, maar ook al die personen waarmee de verdachte via die lijn of in die woning communiceert wordt afgeluisterd. Maar de privacy-implicaties bij het doorzoeken van computers zijn echter nog eens tien keer groter: alle mailtjes, alle foto's en alle berichten op sociale media die een verdachte met anderen heeft uitgewisseld, komen in het vizier van de opsporing. Dit geldt niet alleen voor de periode waarin er wordt afgetapt, maar ook voor alle data die eerder al zijn uitgewisseld en/of opgeslagen. Een inkijk in iemands computer vertelt je dan ook veel meer over die persoon dan dat je ooit in zijn huis kan vinden.[42]

Daarnaast leidt de hackbevoegdheid tot een inperking van het recht op vertrouwelijkheid en integriteit van eigen computersystemen. Dit grondrecht werd voor het eerst erkend in Duitsland, tegen de achtergrond van de introductie van een hackbevoegdheid aldaar. Het Duitse Constitutionele Hof (BVerfG) gaf uitgebreide redenen waarom de inzet van de hackbevoegdheid met het hiervoor genoemde recht conflicteerde.[43]

> In het leven van burgers nemen IT-systemen een centrale plek in en het toenemende gebruik daarvan brengt voor burgers gevaren met zich mee. Zo meende het Hof dat door het verzamelen en onderzoeken van gegevens profielvorming mogelijk was en het gevaar bestond dat derden systemen zouden misbruiken. Het Hof overwoog verder dat IT-systemen zodanig ingewikkeld waren geworden dat de burger zich niet of in beperkte mate zich tegen deze gevaren kon beschermen. In dit verband merkte het Hof op dat de burger erop mag vertrouwen dat de Staat de verwachtingen met betrekking tot de integriteit en vertrouwelijkheid van IT-systemen respecteert. Bovendien

41 Artikel 10 Grondwet en artikel 8 EVRM.
42 Ronald Prins, "Cybersecurity in Nederlands op de agenda", 28 november 2012. Zie: http://blog.fox-it.com/2012/11/28/cyber-security-in-nederland-op-de-agenda/.
43 BVerfG, 1 BvR 370/07, 27 februari 2008. Zie: www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

vond het Hof dat beveiligingsmaatregelen die de burger neemt om zichzelf te beschermen, zoals encryptie, omzeild kunnen door het gebruik van overheidsspyware. Dit verhoogde naar zijn oordeel de zwaarte van de inbreuk op de fundamentele rechten van het individu.

In de Toelichting wordt het recht op vertrouwelijkheid en integriteit van eigen computersystemen ook voor Nederland erkend.[44]

Uit het voorgaande volgt dat de hackbevoegdheid mogelijk ook grote gevolgen voor mensen met een beschermd beroep, zoals advocaten en journalisten. Ook zij komen daarom tegen de hackbevoegdheid in verzet.[45]

1.2.2 Noodzaak, proportionaliteit en effectiviteit niet aangetoond

Onze Grondwet, het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (het 'EVRM'), het Handvest van de Grondrechten van de Europese Unie en het Internationaal Verdrag inzake burgerrechten en politieke rechten (het 'IVBPR') vereisen dat maatregelen die fundamentele rechten – zoals het recht op privacy en het recht op vertrouwelijkheid en integriteit van computersystemen – beperken, noodzakelijk in een democratische samenleving zijn en dat deze proportioneel en effectief zijn.[46] Dit moet voorafgaand aan de invoering van die maatregelen zijn aangetoond, zoals ook de motie Franken stelt.[47] Het hackvoorstel voldoet niet aan deze vereisten.

Ten aanzien van de noodzaak van de hackbevoegdheid stelt de Toelichting dat bestaande opsporingsbevoegdheden "in toenemende mate tekort [schieten] om aan wezenlijke problemen en gebleken knelpunten op het gebied van cybercriminaliteit tegemoet te komen."[48] Bij drie van die knelpunten wordt uitgebreid stilgestaan: de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en cloudcomputerdiensten.[49] Ondanks alle woorden die aan deze knelpunten worden besteedt, wordt uit het wetsvoorstel echter niet duidelijk hoe een hackbevoegdheid deze problemen zal oplossen en of een dergelijke oplossing noodzakelijk en proportioneel is. Uit paragraaf 1.1 blijkt juist dat de hackbevoegdheid een disproportioneel middel is. Daarnaast kán van een noodzaak tot nieuwe bevoegdheden geen sprake zijn: de huidige bevoegdheden worden namelijk niet optimaal benut. Er is namelijk een tekort

44 Toelichting, p. 39.
45 Zie de reactie op de consultatie van het wetsvoorstel computercriminaliteit III van de Nederlandse Uitgeversbond (NUV), de Nederlandse Vereniging van Journalisten (NVJ), het Nederlands Genootschap van Hoofdredacteuren (NGvH) en het Persvrijheidfonds (PVF) van 21 juni 2013. Zie: *Verfassungsbeschwerde*, B. Winsemann, 27 januari 2009. Zie ook: *Zusammenfassung der wesentlichen verfassungsrechtlichen Beanstandungen*, RAV, 9 mei 2011.
46 Artikel 10 Grondwet, artikel 8 EVRM en artikel 17 IVBPR.
47 Motie Franken, (Eerste Kamer 2010–2011, nr 31 051, D).
48 Toelichting, p. 6.
49 *Ibid*, p. 6-12.

aan kennis en capaciteit om computercriminaliteit effectief te bestrijden. Dit blijkt uit de media-berichten[50]:

> "Nu vallen kleinere zaken tussen wal en schip doordat de Nationale Recherche onvoldoende capaciteit heeft. In 2010 jaar werd in Haarlem het criminele Bredolabnetwerk opgerold, dat maar liefst 143 servers besloeg. Prins: „Wij hadden al gewaarschuwd toen het netwerk nog maar twee servers groot was. De politie kwam pas in actie toen er een klacht van de FBI kwam: weten jullie wel wat er in Haarlem staat te draaien?""[51]

Dit blijkt uit de praktijk:

> Uit een recent rapport van antivirus en beveiligingsbedrijf McAfee blijkt dat er meer dan honderd command & control-servers in Nederland staan.[52] De politie kan die servers uit de lucht halen, achterhalen wie de servers heeft gehuurd en de verbinding van de servers laten blokkeren. Echter, uit de observaties in dit rapport kan worden afgeleid dat de politie deze servers gewoon laat draaien, waarschijnlijk omdat de politie voor het uitschakelen daarvan de benodigde kennis en capaciteit mist.[53]

En dit wordt ook bevestigd door de overheid.[54]

> Zo blijkt uit een onderzoek over de effectiviteit van aftappen dat een gebrek aan kennis en capaciteit ervoor zorgt dat bepaalde middelen, zoals de internettap, onvoldoende worden ingezet.[55]

Een hackbevoegdheid is duidelijk niet de oplossing voor dit probleem.

Bovendien is de hackbevoegdheid ook anderszins geen effectief middel om computercriminaliteit te bestrijden. Een crimineel zal zijn sporen immers vaak verhullen door gebruik van een keten van andere computers (paragraaf 1.1.1). Hacken heeft dan vrijwel geen zin. Verder biedt een hackbevoegdheid ook bij het bestrijden van botnets weinig soelaas.[56] Het uitschakelen van botnets is

---

50 O.a. Wouter Stol, Tijdschrift voor de Politie, waarnaar wordt verwezen in "Cybercrime kennis politie schiet tekort", Security.nl, 13 januari 2011. Zie: https://www.security.nl/artikel/35813/%22Cybercrime_kennis_politie_schiet_tekort%22.html. Zie verder: "Matige aanpak cybercrime: bloed gaat voor bytes", Dagblad van het Noorden, 30 juni 2012; en "Te weinig kennis en aansturing bij politie over aanpak cybercrime", Volkskrant, 29 juni 2012.

51 "Wanted: soldaten tegen cybercrime", NRC Handelsblad, 11 juni 2012. Zie: http://content.nrccarriere.nl/2012/06/wanted-soldaten-tegen-cybercrime/.

52 "Botnet Control Servers Span the Globe", McAfee Labs, 23 januari 2013. Zie: http://blogs.mcafee.com/mcafee-labs/botnet-control-servers-span-the-globe.

53 Een ander praktijkvoorbeeld kan worden afgeleid uit de Pobelka-zaak. Zie onze brief aan de vaste Commissie voor Veiligheid en Justitie van de Tweede Kamer met commentaar op overheidsoptreden rondom Pobelka en het hackvoorstel van 23 mei 2013, zoals gepubliceerd op: https://www.bof.nl/2013/05/30/opstelten-bevestigt-inzet-dpi-bij-controleren-communicatie-vitale-sectoren/.

54 Brief van de Minister van Veiligheid en Justitie over de bestrijding van georganiseerde criminaliteit (TK 2012-2013, nr. 79), 13 maart, 2013.

55 "Het gebruik van de telefoon- en internettap in de opsporing", Wetenschappelijk Onderzoek- en Documentatiecentrum, Ministerie van Veiligheid en Justitie, mei 2012, p. 158.

56 Toelichting, p. 12, 17, 34 en 43.

namelijk zeer lastig. Om dit te bemoeilijken proberen criminelen de locatie van de hoofdserver onder meer te verbergen en gebruiken ze gedecentraliseerde communicatiemethoden om het botnet aan te sturen als de hoofdserver wordt uitgeschakeld.[57] Er zijn wel methoden om deze gedecentraliseerde botnets te infiltreren, maar dit is vrij lastig en bovendien blijkt uit onderzoek dat de makers achter deze P2P-botnets steeds beter worden in het voorkomen van uitschakeling.[58] Botnets die werden uitgeschakeld kwamen dan ook vaak na enige tijd weer terug, bijvoorbeeld doordat er toch een manier werd gevonden om de besmette computers te bereiken en het adres van een nieuwe hoofdserver door te geven. Bovendien kunnen de criminelen altijd weer opnieuw beginnen. De onderliggende oorzaak van botnets is namelijk dat computers niet goed beveiligd worden. Een nieuw botnet is dus zo'weer opgezet. De hackbevoegdheid pakt dit probleem niet aan.

1.2.3 Tussenconclusie

Tegen deze achtergrond en zonder nadere uitleg, die in de Toelichting ontbreekt, is onduidelijk hoe de nieuwe hackbevoegdheid een noodzakelijk en proportioneel middel is en hoe deze effectief kan bijdragen aan het bestrijden van computercriminaliteit. De inbreuk op ons grondrecht op privacy en het grondrecht op de vertrouwelijkheid en integriteit van computersystemen is dus niet gerechtvaardigd.

1.3 De hackbevoegdheid is in strijd met het volkenrecht

Volgens de Toelichting kan de hackbevoegdheid – "binnen de grenzen van het volkenrecht en internationale recht" – ook buiten Nederland worden ingezet, zonder in overleg te treden met de belanghebbende staat.[59] Hoe dit binnen de genoemde grenzen past, is echter volstrekt onduidelijk.

1.3.1 Het soevereiniteitsbeginsel

Als Nederland op eigen houtje gaat hacken in het buitenland dan leidt dat tot een schending van de soevereiniteit van het land waar zij op inbreekt. D it kan ertoe leiden dat ook andere landen het met dit rechtsbeginsel niet zo nauw nemen, in het bijzonder in relatie tot Nederland. Dat kan leiden tot inbraken op computers in Nederland vanuit andere landen om zeer uiteenlopende redenen zoals godslastering, haatzaaien en inbreuken op auteursrechten. Burgers, dissidenten in het bijzonder, worden daar het slachtoffer van.

---

57 In het geval van een P2P-botnet zijn het bijvoorbeeld de 'peers', oftewel de besmette computers in het botnet zelf, die de instructies aan elkaar doorgeven. Er is dus geen centrale 'stem' meer, maar groepjes besmette computers die met elkaar praten en de 'boodschap' (bijvoorbeeld een website aanvallen) aan elkaar doorgeven.

58 Zie bijvoorbeeld "P2P-botnets veel groter dan gedacht", Security.nl, 31 mei 2013, waarin wordt verwezen naar: C. Rossow et al., "SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets", 2013, zie: http://www.christian-rossow.de/publications/p2pwned-ieee2013.pdf.

59 Toelichting, p. 34-35.

Er is dan veel verzet vanuit de internationale gemeenschap, zoals dit statement van de bekende Bahreinse blogster Amira Al Hussaini illustreert:

> "Arab-style dictatorship comes to mind when reading about the new draft law under consideration in the Netherlands. [...] As a Bahraini blogger, I felt I was reading a draconian law from my own country or that of a neighbouring country, many of which have internet freedom rankings and human rights records which are a shame to humanity. Activists in Bahrain have recently complained about their computers infected by FinSpy, a product sold by British company Gamma International, which allowed not only spying on material on the infected computers, but also remotely turned on cameras and microphones on the computers and mobile phones being spied on. This is a stark invasion of privacy and goes against human decency. This nightmarish scenario is what makes me weary of any law which aims to monitor, spy and hack into people's computers under the disguise of fighting cybercrime as there are certainly other means of fighting crime.
>
> As digital natives, we aspire to have the freedoms and responsibilities other "free" people around the world are entitled and bond to. Seeing the "West" descend to this alarming level of enshrining surveillance into a law is a serious concern. What would dictatorships around the world do when a country like Holland rubberstamps such a law?"[60]

Ook een brede internationale coalitie van meer dan 40 internationale experts op het gebied van digitale burgerrechten, heeft haar zorgen geuit. In een brief van 30 november 2012 roept de coalitie op het voorstel in te trekken gezien de grote risico's van het voorstel voor cybersecurity en de bescherming van mensenrechten wereldwijd.[61]

1.3.2 Internationale verdragen

De hackbevoegdheid is ook in strijd met internationale verdragen. In de eerste plaats gaat dit om het EVRM en het IVBPR (paragraaf 1.2.2). Daarnaast is de bevoegdheid in strijd met Cybercrime Verdrag van de Raad van Europa. Artikel 32 van dit verdrag voorziet in twee mogelijkheden voor grensoverschrijdende toegang tot gegevens.[62] Omdat verdragspartijen het over aanvullende mogelijkheden niet eens konden worden, is voor het overige het accent op 'wederzijdse bijstand' gelegd.[63] De verhouding tussen het grensoverschrijdend

60 Ontvangen in een email die met toestemming van Amira Al Hussaini is overgenomen.
61 Zie: https://www.bof.nl/2012/12/04/persbericht-internationaal-verzet-tegen-hackplannen-opstelten/.
62 "Dit betreft in de eerste plaats de toegang tot openbare gegevens (uit open bronnen) die zijn opgeslagen, ongeacht de locatie van de gegevens (artikel 32, onderdeel a, van het Cybercrime Verdrag). Dit betreft in de tweede plaats de toegang, door middel van een netwerkzoeking, tot opgeslagen gegevens in een andere verdragspartij, met de rechtmatige en vrijwillige instemming van de persoon die gerechtigd is de gegevens via het computersysteem aan de partij te verstrekken (artikel 32, onderdeel b, van het Cybercrime Verdrag)." Toelichting, p. 35.
63 *Ibid.*

vastleggen van gegevens en rechtsmacht is binnen de Raad wel onderwerp van voortdurend gesprek.[64] Daaruit komt naar voren dat grensoverschrijdend opereren, zoals met de hackbevoegdheid wordt beoogd, geen grondslag vindt in artikel 32 van het verdrag en dat betrokken partijen ook zeer terughoudend zijn om het verdrag op dit punt uit te breiden.[65] Zoals de Toelichting zelf benadrukt, is volgens de Raad van Europa "de effectiviteit van artikel 32 van het verdrag juist gebaat bij een meer eenduidige uitleg van de in die bepaling neergelegde begrippen."[66] De eigenrichting die de Nederlandse overheid zich met de hackbevoegdheid zou toe-eigenen, is dus op drie manieren in strijd met het verdrag: het is in strijd met artikel 32, het is in strijd met de pogingen van de Raad om tot een meer eenduidige uitleg van het verdrag te komen en het is in strijd met het uitgangspunt van 'wederzijdse bijstand'.

In reactie op dit laatste punt werpt de Toelichting tegen dat internationale samenwerking op het gebied van computercriminaliteit (door middel van rechtshulp) twee problemen kent: afhankelijkheid van andere landen en vertraging van de procedure.[67] Er wordt echter niet onderzocht of internationale samenwerking kan worden verbeterd. Dit verdient dan ook de nodige aandacht voordat van de introductie van nieuwe bevoegdheden sprake kan zijn.

Dit geldt eens te meer nu door eigenhandig optreden van Nederland elke vorm van internationale samenwerking onder druk komt te staan en de reputatie van Nederland op diverse beleidsvlakken wordt ondergraven. Bijvoorbeeld: Minister Timmermans van Buitenlandse Zaken heeft aangegeven dat hij op het bij de wereldwijde bevordering van internetvrijheid de komende jaren "een leidende rol" voor Nederland ziet weggelegd.[68] Uit de statement van Amira Al Hussaini (paragraaf 1.3.1) blijkt echter dat Nederland bij de inzet van de hackbevoegdheid in deze rol niet geloofwaardig en dus onsuccesvol zal zijn. De repercussies van de inzet van de hackbevoegdheid zullen dus groot zijn.

1.3.3 Tussenconclusie

De hackbevoegdheid is in strijd met het soevereiniteitsbeginsel en verschillende internationale verdragen. De belofte van het wetsvoorstel, dat bij de inzet van de hackbevoegdheid de regels van het internationale volkenrecht zullen worden gerespecteerd, wordt dan ook niet nageleefd. Bovendien zal de inzet van de hackbevoegdheid de internationale positie van Nederland ondergraven.

---

64 *Ibid*, p. 36.
65 "Trans border access and jurisdiction: What are the options?, Report of the Trans border Group", Aangenomen op 6 december 2012, hoofdstuk 7. Zie: www.coe.int/TCY.
66 Toelichting, p. 36.
67 *Ibid*, p. 35.
68 "Opening Ceremony van de Freedom Online conferentie ter Tunis", 19 juni 2013. Zie: http://www.rijksoverheid.nl/regering/bewindspersonen/frans-timmermans/toespraken/2013/06/17/opening-ceremony-van-de-freedom-online-conferentie-te-tunis.html.

1.4 De hackbevoegdheid creëert onaanvaardbare cybersecurityrisico's

De hackbevoegdheid creëert verschillende veiligheidsrisico's en maakt Nederland daarom niet veiliger, maar juist onveiliger.

1.4.1 Kwetsbaarheden in software

Als de politie op computers moet kunnen inbreken, heeft ze er belang bij dat die systemen kwetsbaar blijven.[69] De politie kan immers slechts inbreken bij systemen die onvoldoende beveiligd zijn. Dit geeft de overheid een perverse prikkel om informatie over kwetsbaarheden (zogenaamde 'exploits') voor zichzelf te houden, in plaats van deze te delen met Nederlandse internetgebruikers. Zij kunnen hun eigen informatiesystemen hierdoor minder goed beschermen.

> Dat de geheimhouding van exploits, nadelige gevolgen heeft voor de veiligheid van een land en haar onderdanen, wordt onderschreven Howard Schmidt en Richard Clarke, voormalige adviseurs op het gebied van cybersecurity van de Amerikaanse president.[70] "Het is een beetje naïef om te denken dat jij als enige in de wereld kennis hebt van een bepaalde exploit", zegt Schmidt. "Als je als overheid ervoor kiest om een exploit geheim te houden, dan moet je er ook op rekenen dat die exploit door anderen wordt gebruikt om jou aan te vallen."[71]

De inzet van een hackbevoegdheid zal dus leiden tot minder veiligheid, op individueel maar ook op nationaal niveau, zoals blijkt uit voorgaand citaat. Dit zal leiden tot verlies van vertrouwen in de informatiemaatschappij. De hackbevoegdheid staat daarmee lijnrecht tegenover alle investeringen van de overheid in cybersecurity over de afgelopen jaren en heeft bovendien nadelige gevolgen voor de economische positie van Nederland.

1.4.2 Spyware moeilijk binnen de perken te houden

Bovendien is spyware moeilijk binnen de perken te houden. In Duitsland hebben ze dat al ervaren. Uit onderzoek van de hackersvereniging Chaos Computer Club ('CCC') bleek dat heimelijk door de Duitse politie geïnstalleerde afluistersoftware (ontwikkeld door het Duitse bedrijf Digitask[72], dat ook spyware aan de Nederlandse overheid heeft verkocht[73]) makkelijk – via het internet – te hacken was.[74] Dit betekent dat niet alleen de politie gebruik kon maken van deze software om op computers rond te kijken, maar dat ook kwaadwillenden dat

---

69 Bart Jacobs, "Policeware", Nederlands Juristenblad, 9 november 2012, afl. 39, p. 2763-2764.
70 "Special Report: U.S. cyberwar strategy stokes fear of blowback", Reuters, 10 mei 2013.
71 *Ibid.*
72 "Choas Computer Club analyses new German government spyware", ccc.de, 26 oktober 2011. Zie: http://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner.
73 "Nederlandse politie gebruikt spionagesoftware", Tweakers.nl, 13 december 2011. Zie: http://tweakers.net/nieuws/78722/nederlandse-politie-gebruikt-spionagesoftware.html.
74 "Choas Computer Club analyses government malware", ccc.de, 8 oktober 2011. Zie: http://www.ccc.de/en/updates/2011/staatstrojaner.

konden doen omdat de overheidsspyware zélf te hacken was.

> "The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet."[75]

Dit misbruik werd onder andere mogelijk gemaakt door diverse kwetsbaarheden in de software, zoals slechte encryptie en gebrekkige authenticatie-methoden. Hierdoor was het – zelfs voor middelmatige bekwame – aanvallers mogelijk om het geïnfecteerde systeem over te nemen, verbinding te maken met de politie en misbruik te maken van overheidsspyware, om bijvoorbeeld belastende informatie te uploaden. Via deze weg was het zelfs mogelijk om de systemen van de politie aan te vallen.[76]

Naast het risico van misbruik van overheidsspyware door criminelen, concludeerde de CCC dat deze software ook zeer vatbaar was voor misbruik door de politie zelf. Zo bleek dat spyware die bedoeld was om alleen Skype gesprekken af te luisteren, in de praktijk ook kon worden ingezet voor het op afstand aanzetten van de camera. De functionaliteiten van de software gingen dus veel verder dan was toegestaan. Sterker nog, in plaats van functionaliteiten te beperken waren er juist bewust opties voor uitbreiding open gelaten.

> "The analysis concludes, that the trojan's developers never even tried to put in technical safeguards to make sure the malware can exclusively be used for wiretapping internet telephony, as set forth by the constitution court. On the contrary, the design included functionality to clandestinely add more components over the network right from the start, making it a bridge-head to further infiltrate the computer."[77]

Naar aanleiding van de ontdekkingen van de CCC heeft de Duitse overheid besloten om het gebruik van de hackbevoegdheid te stoppen totdat er veilige software beschikbaar is.[78] De eisen van het Duitse Constitutionele Hof gelden daarbij als uitgangspunt.[79]

Vooralsnog is de Duitse overheid er nog niet in geslaagd die veilige software ook daadwerkelijk te ontwikkelen of aan te trekken.[80] Dat geldt overigens ook voor Frankrijk.[81] Wel heeft de Duitse overheid recent voor veel geld de spyware

75 *Ibid.*
76 *Ibid.*
77 *Ibid.*
78 Zie o.a. Netzpolitik, "Secret government document reveals German federal police plans to use gamma FinFisher spyware", 16 januari 2013, https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/.
79 BVerfG, 1 BvR 370/07, 27 februari 2008. Zie: www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.
80 "Duitse Hof tegen inzet politie-spyware", Security.nl, 18 december 2012. Zie: https://www.security.nl/artikel/44389/1/Duitse_Hof_tegen_inzet_politie-spyware.html
81 "LOPPSI : aucun mouchard informatique utilisable en France?", Numerama.com, 11 maart 2013. Zie: http://www.numerama.com/magazine/25351-loppsi-aucun-mouchard-informatique-

FinFisher van het Britse bedrijf Gamma International ingekocht.[82] Deze spyware is berucht omdat zij door totalitaire regimes wordt ingezet tegen mensenrechten-activisten en politieke dissidenten.[83] Los van de vraag of deze software voldoet aan de strenge eisen van het Duitse Constitutionele Hof, zou het eventuele gebruik van deze spyware door de Duitse overheid dus ook allerhande ethische vragen oproepen.

De ervaringen in Duitsland leren ons dus dat overheidsspyware moeilijk binnen de perken te houden is en dat 'veilige' overheidsspyware vooralsnog niet voor handen is. Deze risico's worden door het wetsvoorstel op geen enkele manier ondervangen. In tegendeel: de regels die deze risico's moeten ondervangen zijn weggeschreven in lagere wetgeving en vooralsnog onbekend (zie paragraaf 1.1.4).

1.4.3 De detectie van overheidsspyware door antivirus-software

Ook meer praktische problemen hebben gevolgen voor onze cybersecurity. Burgers en bedrijven krijgen van de overheid regelmatig het advies zich goed te beveiligen en actuele antivirus-software te gebruiken.[84] Maar als deze software overheidsspyware op een computer aantreft, zal dit in principe aan de gebruiker worden gemeld, zodat deze spyware kan worden verwijderd. De vraag is dus of de overheid van antivirus-bedrijven zal verwachten of hen ertoe zal verplichten dat ze overheidsspyware niet detecteren, melden of verwijderen, met het gevolg dat gebruikers extra kwetsbaar zijn.[85] Hun vertrouwen in antivirus-software zal daardoor afnemen en daarmee het gebruik ervan. Daar komt bij dat overheidsspyware, in het bijzonder wanneer die niet gedetecteerd wordt door de virusscanner, een dankbaar doelwit is voor criminelen.[86] Criminelen zullen dus spyware gaan ontwikkelen die niet van overheidsspyware te onderscheiden is, of inbreken op de spyware die door de politie wordt gebruikt en deze overnemen en misbruiken voor het plegen van strafbare feiten. Kortom, de cybersecurity van burgers, bedrijven en de overheid komt door de inzet van overheidssoftware in een negatieve spiraal terecht. In de aanloop naar het wetsvoorstel is toegezegd dat het wetsvoorstel aan voornoemde vragen tegemoet zou komen.[87] Dit is niet gebeurd en deze belofte moet dus alsnog gestand worden gedaan. Ook andere vragen moeten daarbij worden betrokken:

---

utilisable-en-france.html.

82 "De Duitse politie koopt FinFisher-spyware", Webwereld.nl, 17 januari 2013. Zie: http://webwereld.nl/beveiliging/59022-duitse-politie-koopt-finfisher-spyware.

83 "You Only Click Twice: FinFisher's Global Proliferation", Citizenlab.org, 13 maart 2013. Zie: https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

84 Bart Jacobs, Policeware, Nederlands Juristenblad, afl. 39, p. 2764.

85 *Ibid.*

86 Zie in dit verband ook de vele berichten over de populariteit van politievirussen. Bijvoorbeeld: "400.000 computers gegijzeld door politievirus", Security.nl, 16 januari 2013. Zie: https://www.security.nl/artikel/44742/1/400.000_computers_gegijzeld_door_politievirus.html.

87 Antwoord van minister Opstelten (Veiligheid en Justitie) op vragen van het lid Berndsen-Jansen (D66), 11 december 2012 (TK 2012–2013, Aanhangsel 751), antwoord 4.

De Toelichting geeft aan dat het van groot belang is dat spyware, wanneer deze wordt herkend, niet te herleiden is tot de politie.[88] Maar stel dat bedrijven op burgers die spyware detecteren (zonder die te kunnen herleiden) en verhinderen dat deze hun systeem betreedt? Of als iemand merkt dat zijn systeem trager draait en zijn systemen her-installeert of een nieuwe computer aanschaft? Is dit dan een belemmering van het opsporingsonderzoek en wat zullen de gevolgen daarvan zijn?

En andersom? Als de politie op computers inbreekt kunnen die computers – al dan niet opzettelijk – offline gaan en kunnen er gegevens beschadigd raken of worden vernietigd. Wat als je bedrijf offline is vanwege een hackactie van de politie en je daardoor schade lijdt? Is de overheid dan aansprakelijk?[89] Dergelijke hackacties kunnen bovendien levensgevaarlijke gevolgen hebben, bijvoorbeeld als hierdoor de vitale systemen van een bedrijf verstoord raken.[90] Hoe denkt de overheid daarmee om te gaan?

1.4.4 Tussenconclusie

Een hackbevoegdheid creëert diverse veiligheidsrisico's die door het wetsvoorstel niet of onvoldoende worden erkend en ondervangen. Dit zal Nederland niet veiliger, maar juist onveiliger maken.

1.5 Conclusie

De voorgestelde hackbevoegdheid is onbegrensd. De maatregel vormt een ernstige inperking van de grondrechten van onschuldige en verdachte burgers wereldwijd, terwijl de noodzaak, proportionaliteit en effectiviteit van de maatregel niet is aangetoond. Bovendien heeft de maatregel grote internationale implicaties. De hackbevoegdheid is in strijd met internationaal recht en zal tegenreacties van andere landen uitlokken: burgers wereldwijd, maar Nederlandse burgers in het bijzonder, worden daar het slachtoffer van. Tot slot heeft de hackbevoegdheid gevaarlijke gevolgen voor onze cybersecurity: de inzet van deze techniek maakt Nederland onveiliger. Om deze redenen, afzonderlijk en tezamen genomen, moet het voorstel worden ingetrokken.

2 De bevoegdheid om informatie ontoegankelijk te maken

Het voorgestelde artikel 54a Sr in combinatie met het voorgestelde artikel 125p Sv bepaalt dat een aanbieder door de officier van justitie kan worden bevolen om gegevens ontoegankelijk te maken. Dit bevel kan worden gegeven na voorafgaande schriftelijke machtiging van de rechter-commissaris.

88 Toelichting, p. 80.
89 "Terughacken politie kan bedrijfsleven verstoren", NU.nl, 5 mei 2013. Zie: http://nutech.nl/internet/3415045/terughacken-politie-kan-bedrijfsleven-verstoren.html.
90 Brenno de Winter, 'Terughackende politie: de duivel uitdrijven met beezelbub', HP/De Tijd, 13 mei 2013. Zie: http://www.hpdetijd.nl/2013-05-13/terughackende-politie-de-duivel-uitdrijven-met-beelzebub/.

Hoewel dit een verbetering is ten opzichte van het wetsvoorstel dat eerder ter consultatie is aangeboden, doet deze bepaling onvoldoende recht aan het grondrecht op vrijheid van meningsuiting. De rechter-commissaris wordt immers niet verplicht om de aanbieder of de verdachte te horen; hij zou op basis van zijn eigen indruk moeten bepalen of een bevel in strijd is met het grondrecht op vrijheid van meningsuiting.

Om hieraan tegemoet te komen, zou daarom een paragraaf moeten worden toegevoegd aan lid 4 van artikel 125p Sv, met de strekking dat de rechter-commissaris de aanbieder in de gelegenheid stelt te worden gehoord. Als dit door de spoedeisendheid van de zaak niet mogelijk is, zou de rechter-commissaris de aanbieder zo snel als mogelijk na verstrekking van de machtiging moeten horen. De rechter-commissaris zou in dat geval, nadat hij de aanbieder heeft gehoord, alsnog de machtiging en daarmee de grondslag van het bevel moeten kunnen intrekken.

3 Het decryptiebevel

Het wetsvoorstel omvat ook een decryptiebevel, waartegen de volgende bezwaren bestaan: het decryptiebevel is in strijd met de grondrechten van verdachten en niet-verdachten (paragraaf 3.1), niet noodzakelijk (paragraaf 3.2), niet effectief (paragraaf 3.3) en leidt tot misbruik (paragraaf 3.4).

3.1 Het decryptiebevel is in strijd met fundamentele rechten

Een verplichting een wachtwoord te verstrekken is in strijd met het grondrecht van de verdachte om niet mee te hoeven werken aan zijn eigen veroordeling, het nemo tenetur-beginsel, en het recht dat iemand onschuldig is tot het tegendeel is bewezen. Met het decryptiebevel kan iemand worden gedwongen om mee te werken aan zijn eigen veroordeling: iemand kan tot drie jaar worden opgesloten omdat hij een wachtwoord niet afgeeft.[91] Daarmee komt het beginsel dat iemand onschuldig is tot het tegendeel is bewezen onder druk te staan: iemand wordt in zekere zin schuldig geacht aan het primaire delict, tenzij hij – door afgifte van de decryptiesleutel – het tegendeel kan bewijzen . Dit steekt des te meer nu in het wetsvoorstel geen waarborgen tegen misbruik zijn ingebouwd.

Daarnaast komen de grondrechten op privacy en op communicatievrijheid door een decryptieplicht onder druk te staan. Dat het grondrecht op privacy wordt ingeperkt als een decryptiebevel wordt afgegeven is evident – daarmee wordt de verdachte immers verplicht om gegevens die voorheen slechts voor hem toegankelijk waren ook toegankelijk te maken voor anderen.

Maar een decryptiebevel zal ook gevolgen hebben voor de privacy en vrijheid van meningsuiting van niet-verdachten. Doordat het versleutelen van bestanden in

91 Artikel 125k Wijzigingsvoorstel.

sommige gevallen strafbaar wordt, wordt encryptie mogelijk minder gebruikt. Het bredere maatschappelijke belang dat van encryptie komt hierdoor onder druk te staan. Dat belang heeft zich als volgt ontwikkeld:

> In de jaren negentig is de verspreiding van encryptietechnologie onderwerp geweest van een uitgebreid debat. Na de introductie van het versleutelprogramma PGP stelden de Verenigde Staten zich op het standpunt dat verspreiding naar het buitenland in strijd zou zijn met exportbeperkingen. Deze strijd is uiteindelijk, mede onder druk van economische belangen van bedrijven zoals banken, beslecht in het voordeel van de brede beschikbaarheid van encryptietechnologie.[92] Dat was een verstandige keuze: de maatschappij kan eenvoudigweg niet zonder goede versleutelingstechnologie.
>
> Inmiddels wordt versleutelingstechnologie dan ook steeds meer gebruikt. Vrijwel alle besturingssystemen, waaronder Mac OS, Linux, Android en Windows bieden sterke encryptietechnologie zodat alle bestanden op een laptop goed zijn beschermd. Daarnaast wordt SSL-technologie gebruikt om communicatie via het internet te beveiligen (dit is communicatie via HTTPS). Er zijn plugins beschikbaar om email te versleutelen (PGP) en om bestanden te versleutelen, bijvoorbeeld op USB-sticks (TrueCrypt). Deze versleuteling gebeurt vaak zonder dat de gebruiker daar veel voor hoeft te doen, en soms zelfs zonder dat de gebruiker daarvan op de hoogte is. Dat is wenselijk – het betekent dat encryptietechnologie zo gebruiksvriendelijk is geworden dat de toepassing hiervan zich onttrekt aan het oog van de gebruiker.

Kortom: encryptie is een belangrijke ontwikkeling die leidt tot meer cybersecurity. Door versleuteling van harde schijven kan worden voorkomen dat derden toegang krijgen tot de bestanden op apparatuur als die bijvoorbeeld wordt gestolen. Door het versleutelen van communicatie kan worden voorkomen dat derden, bijvoorbeeld via een openbaar wifi-netwerk, verkeer kunnen afluisteren en op die manier toegang kunnen krijgen tot bankgegevens. Het is dan ook niet voor niets dat de telefoon van Rutte wordt beveiligd door Fox-IT.[93] Maar ook mensenrechten-activisten maken gebruik van encryptie om zichzelf te beschermen tegen autoritaire regimes. Encryptie heeft een belangrijke maatschappelijke functie in het faciliteren van beschermde communicatie. Deze functie wordt door een decryptiebevel doorkruist. De boodschap is immers dat het versleutelen van bestanden in sommige gevallen strafbaar is, met als onwenselijke gevolg dat het versleutelen van bestanden maatschappelijk minder geaccepteerd wordt.

92 S. Levy, *Crypto*, Penguin: 2001.
93 Buitenhof, 21 oktober 2012. Zie: http://programma.vpro.nl/buitenhof/afleveringen/buitenhof-21-oktober-klaas-knot---cybercriminaliteit.html.

3.2 Het decryptiebevel is niet noodzakelijk

Inperkingen op grondrechten zoals het grondrecht op privacy en vrijheid van meningsuiting, moeten noodzakelijk zijn in een democratische samenleving. Gezien de gevolgen voor de grondrechten van verdachten en niet-verdachten, moeten aan dit criterium strenge eisen worden gesteld. Het decryptiebevel voldoet hier niet aan. Er is namelijk geen enkel bewijs dat het decryptiebevel nodig is. Bits of Freedom heeft hierover een aantal Wob-verzoeken naar de politie gestuurd, waarin we hebben gevraagd of de politie kan aangeven welke zaken zijn gestrand doordat bestanden waren versleuteld en zij geen toegang konden krijgen tot die bestanden. De resultaten zijn ontluisterend: het is volstrekt onduidelijk of, en in welke gevallen versleuteling in de weg stond aan het oplossen van een zaak. In een antwoord van 6 januari 2012 op één Wob-verzoek antwoordde het Landelijk Parket: [94]

> "Het Landelijk Parket houdt geen centrale administratie bij van het aantal gevallen waarin in strafrechtelijke onderzoeken versleutelde informatie werd aangetroffen, noch van de methodes die in die gevallen zijn gebruikt om die versleuteling ongedaan te maken, de tijd die daarmee is gemoeid en de resultaten van dergelijke ontsleutelpogingen. Er bestaan geen documenten waaruit informatie als door u gewenst reeds is vervat."

Ook het KLPD geeft dit aan:[95]

> "Onderzoek binnen de Landelijke Eenheid heeft geleerd dat er geen documenten bestaan die aan uw verzoek voldoen. Dit heeft te maken met het feit dat er geen afzonderlijke registratie wordt bijgehouden of en zo ja op welke wijze er sprake is van encryptie van informatie op (digitale) gegevensdragers."

Bij gebrek aan bewijs dat zaken door encryptie niet konden worden opgelost moet ervan worden uitgegaan dat deze maatregel niet nodig is. Dit geldt nog sterker gelet op het zwaarwegende maatschappelijk belang van brede toepassing van encryptie.

3.3 Het decryptiebevel is niet effectief

Het decryptiebevel is bovendien niet effectief. Mensenrechtenactivisten hebben de afgelopen jaren software ontwikkeld die afhankelijk van het wachtwoord dat wordt verstrekt verschillende delen van een schijf ontsleutelt. De reden hiervoor is dat dissidenten, onder meer via marteling of dreiging met gevangenisstraf, gedwongen kunnen worden om een wachtwoord af te geven. Zij kunnen dan ervoor kiezen om de sleutel te geven tot bepaalde bestanden die niet leiden tot marteling (de bestanden opgeslagen in het zogenoemde non-hidden volume). In

94 Zie: https://www.bof.nl/live/wp-content/uploads/20120106-beslissing_Redacted.pdf.
95 Zie: https://www.bof.nl/2013/03/26/wij-lossen-liever-echte-problemen-op/.

het 'hidden volume' zijn echter nog meer bestanden versleuteld, maar de autoriteiten kunnen het bestaan hiervan niet bewijzen.[96]

Slimme criminelen zullen dan ook incriminerende bestanden opslaan in het hidden volume, terwijl zij het wachtwoord verstrekken tot het non-hidden volume en daarmee wel voldoen aan het decryptiebevel. In een rapport waar de ook Toelichting naar verwijst, wordt dan ook gewaarschuwd dat juist bij berekenende misdadigers het decryptiebevel niet zal werken:

> "Vanuit beleidsoogpunt moet de wetgever zich echter wel realiseren dat de ontsleutelplicht vermoedelijk weinig effectief zal zijn bij zware en berekenende misdadigers en dat vooral de kleinere of mindere slimme misdadigers zullen gaan meewerken (of bestraft kunnen worden voor decryptieweigering)."[97]

Ook is de vraag of de keuze van de minister – strafbaarstelling – in dit geval leidt tot het gewenste doel. In het geval van afbeeldingen van seksueel kindermisbruik zijn de belangrijkste doelen die de regering noemt het in kaart brengen van slachtoffers, het waarschuwen van betrokkenen en het voorkomen van verdere verspreiding. Deze doelen kunnen beter bereikt worden door een zekere vorm van immuniteit te verlenen aan verdachten die bestanden op verzoek van de politie ontsleutelen, want de prikkel om die bestanden te ontsleutelen is dan immers veel groter. In het geval van terrorisme zullen de motieven van de verdachte waarschijnlijk juist van dien aard zijn dat een decryptiebevel geen zin heeft: als een verdachte bereid is om te sterven voor een hoger doel, zal hij een straf voor het niet voldoen aan een decryptiebevel ook accepteren. De decryptieplicht richt zich echter tevergeefs juist op die kleine groep doorgewinterde criminelen en extremisten.

3.4 Het decryptiebevel leidt tot misbruik

Het is tegelijkertijd duidelijk dat politie en justitie met het decryptiebevel een krachtig wapen in handen krijgen dat makkelijk misbruikt kan worden: ze kunnen dreigen met een decryptiebevel, ook in het geval dat iemand onschuldig is en goede redenen heeft om zijn wachtwoord niet met politie of justitie te delen. Gelet op brede toepassing van encryptie, kunnen politie en justitie dat in theorie tegen een groot deel van de bevolking inzetten (als iemand verdacht wordt van een de "primaire" delicten). Dat het aantal "primaire" delicten in het kader waarvan zo een decryptiebevel mag worden ingezet – op dit moment – beperkt is, is minder relevant: deze maatregel creëert immers een strafbaarheid die losstaat van deze primaire delicten, en daarmee kan in theorie worden gedreigd bij iedereen die zijn bestanden versleutelt en verdachte is van een primair delict.

96 Zie: http://www.truecrypt.org/hiddenvolume.
97 B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel*, p.104.

3.5 Conclusie

Nu het voorliggende decryptiebevel een stevige inperking vormt op de grondrechten van verdachten en niet-verdachten terwijl de noodzaak hiervoor niet is aangetoond, de maatregel niet effectief is en bovendien makkelijk misbruikt kan worden, moet ook dit voorstel worden ingetrokken.

4 Heling van gegevens

Verder kleven aan de voorgestelde strafbaarstelling van heling van gegevens bezwaren: er wordt een onjuist aanknopingspunt voor strafbaarheid gehanteerd (paragraaf 4.1), het voorstel heeft een 'chilling effect' (paragraaf 4.2) en de noodzaak van het voorstel is onvoldoende onderbouwd (paragraaf 4.3).

4.1 'Niet-openbaarheid' onjuist aanknopingspunt voor strafbaarheid

Het wetsvoorstel wil het strafbaar stellen om niet-openbare gegevens die door middel van een geautomatiseerd werk zijn opgeslagen wederrechtelijk met een technisch hulpmiddel over te nemen.[98] Daarnaast wordt voorgesteld om het verwerven of voorhanden hebben van deze gegevens onder omstandigheden strafbaar te stellen. Verder zou het onder omstandigheden strafbaar worden om deze gegevens aan een ander bekend te maken.[99] Er is een uitzondering op de strafbaarheid van degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang bekendmaking van gegevens vereiste.[100]

De gevolgen van deze strafbepalingen voor de vrijheid van meningsuiting zijn moeilijk te overzien en deels onwenselijk. Het verbod is zeer breed, waarbij met name de reikwijdte van de term 'niet-openbare gegevens' in de praktijk tot problemen zal leiden. Het is voorstelbaar dat het overnemen, verwerven, voor handen hebben of bekendmaken van gegevens in bepaalde gevallen onwenselijk is. Dat bepaalde gegevens 'niet-openbaar' zijn, is echter geen goede maatstaf voor de onwenselijkheid van gedragingen ten aanzien van die gegevens. Sterker nog: strafbaarstelling van gedragingen ten aanzien van een zo brede categorie informatie breekt met het uitgangspunt dat informatie vrij moet kunnen worden uitgewisseld, tenzij die uitwisseling wegens een zwaarwegend belang beperkt moet worden. Zelfs binnen het auteursrecht is het uitgangspunt dat informatie mag worden overgenomen, tenzij deze beschermd is. De reikwijdte van deze bepaling is dan ook niet te overzien en er zijn ieder geval twee situaties waarin deze bepaling onwenselijk is, zoals hieronder wordt toegelicht.

98 Artikel 138c Sr Wijzigingsvoorstel.
99 Artikel 139f Sr Wijzigingsvoorstel.
100 *Ibid*, lid 2.

4.2 Voorstel heeft 'chilling effect'

Het voorstel heeft een 'chilling effect' op mensen die een belangrijke functie vervullen in onze democratische samenleving. In de eerste plaats zijn dit journalisten en klokkenluiders. Mede naar aanleiding van de bezwaren van Bits of Freedom en anderen in een eerdere consultatie, is een uitzondering van de strafbaarheid van de bekendmaking van gegevens 'in het algemeen belang' opgenomen.[101] Deze uitzondering lijkt zich echter niet uit te strekken tot het overnemen, verwerven of voorhanden hebben van deze gegevens. Doordat die uitzondering zo een beperkte reikwijdte heeft, blijven klokkenluiders die bepaalde gegevens hebben overgenomen strafbaar, ook als de journalist die vervolgens de gegevens publiceert niet strafbaar is op grond van deze uitzondering. Ook voor de journalist die mogelijk wél van deze uitzondering gebruik kan maken geldt dat deze bepaling een belemmerend effect heeft. Die journalisten zullen immers moeten bewijzen dat zij kunnen profiteren van deze uitzondering.

De reikwijdte van deze bepaling belemmert ook security-onderzoekers. Zo is denkbaar dat informatie die is verkregen door het in eigen laboratorium *reverse engineeren* van apparatuur, zoals de OV-chipkaart of informatie uit een telefoon, ook moet worden aangemerkt als niet-openbare gegevens. Dit soort onderzoek naar de beveiliging van apparaten wordt dan op zich strafbaar, zeker als dit in strijd is met algemene voorwaarden of andere contractuele bepalingen van de leverancier. Op de security-onderzoeker rust vervolgens de plicht om te bewijzen dat zijn gedragingen geen wederrechtelijk karakter hadden. Dat heeft in de praktijk een sterk 'chilling effect' op security-onderzoekers, en is daarmee slecht voor informatiebeveiliging.

4.3 Noodzaak van voorstel onvoldoende onderbouwd

Nu duidelijk is dat het wetsvoorstel in de praktijk een 'chilling effect' heeft op de vrijheid van meningsuiting zal deze maatregel slechts toelaatbaar zijn als die noodzakelijk is in een democratische samenleving. Deze noodzakelijkheid is in de Toelichting onvoldoende onderbouwd. Er wordt vooral gesteld dat het overnemen van gegevens over personen en die gegevens op het internet zetten verwerpelijk is en dat daar strafrechtelijk tegen moet kunnen worden opgetreden.[102] Niet al deze gegevens zijn per definitie beschermenswaardig, en zelfs áls dat het geval zou zijn, dan is het wetsvoorstel onvoldoende toegespitst op deze situatie: het wetsvoorstel strekt zich immers uit tot alle niet-openbare gegevens. Daarbij komt dat een eiser nu al via civiele handhaving maatregelen kan nemen om publicatie te beëindigen. Bovendien is het goed denkbaar dat reeds bestaande strafbepalingen in voorkomende gevallen uitkomst kunnen

101 *Ibid.* Zie ook de Toelichting, p. 67.
102 Toelichting, p. 63 e.v.

bieden.

4.4 Conclusie

Het strafbaar stellen van het overnemen van 'niet-openbare gegevens' leidt tot een zeer breed verbod, dat een 'chilling effect' heeft op de vrijheid van meningsuiting van mensen die een belangrijke functie vervullen in onze democratische samenleving, zoals journalisten, klokkenluiders en security-onderzoekers. Een dergelijke inperking vereiste noodzakelijkheid ontbreekt, zodat dit voorstel moet worden ingetrokken.

* * *