Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 286

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 11 juli 2013

De vaste commissie voor Veiligheid en Justitie heeft op 29 mei 2013 overleg gevoerd met Minister Opstelten van Veiligheid en Justitie over:

- **de brief van de Minister van Veiligheid en Justitie d.d. 3 januari 2013 inzake het kader voor responsible disclosure (Kamerstuk 26 643, nr. 264);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 19 maart 2013 houdende de reactie op de berichtgeving van de NOS dat de overheid laks is geweest met betrekking tot het Pobelka-botnet (Kamerstuk 26 643, nr. 268);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 3 april 2013 inzake het onderzoek naar het Pobelka-botnet (Kamerstuk 26 643, nr. 272);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 14 mei 2013 met een reactie op het verzoek van de commissie over DDoS-aanvallen bij de Rijksoverheid (Kamerstuk 26 643, nr. 278).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Jadnanansing

De griffier van de vaste commissie voor Veiligheid en Justitie,
Nava

kst-26643-286
ISSN 0921 - 7371
's-Gravenhage 2013

Voorzitter: Jadnanansing
Griffier: Tielens-Tripels

Aanwezig zijn vijf leden der Kamer, te weten: Dijkhoff, Gesthuizen, Jadnanansing, Oosenbrug, Verhoeven

en Minister Opstelten van Veiligheid en Justitie, die vergezeld is van enkele ambtenaren van zijn Ministerie.

Aanvang 14.00 uur

De **voorzitter**: Hierbij open ik de vergadering over het onderwerp cybersecurity. Ik heet de Minister, zijn ambtenaren, de mensen op de tribune en natuurlijk mijn geachte collega's van harte welkom. Wij hebben voor de eerste termijn vijf minuten spreektijd en twee interrupties afgesproken. Ik geef meteen het woord aan de heer Dijkhoff van de VVD.

De heer **Dijkhoff** (VVD): Voorzitter, dank u wel. De SP-fractie heeft dit debat aangevraagd en daarom heb ik voor de woordvoerder van de SP een stoel gereserveerd. Misschien komt zij later nog. Er is steeds meer aandacht voor cybersecurity, helaas niet om leuke redenen. Het is wel goed om die aandacht te gebruiken om iedereen op zijn verantwoordelijkheden te wijzen. Ik ben blij dat de Minister de verantwoordelijkheid heeft genomen om wetsvoorstellen te presenteren die in consultatie zijn. Daarin gaat het echt om de bovenkant van het verhaal, namelijk het aanpakken van cybercriminelen, de mogelijkheden om deze lieden op een fatsoenlijke manier op te sporen en de bevoegdheden voor de politie die daarvoor nodig zijn. Ik zal daar inhoudelijk niet verder op ingaan, omdat wij daar nog uitgebreid over te spreken komen.
Ik wil even stilstaan bij wat ik «het midden» en «de bodem» zal noemen. Het midden is wat de politie eigenlijk al doet aan opsporing onder de bevoegdheden van de Politiewet. Je kunt je daarbij afvragen of dit niet wringt in het cyberdomein. Zijn de wettelijke kaders goed genoeg? Ik noem een concreet voorbeeld. Als je iemand op straat even in de gaten houdt, zie je wat hij op dat moment daar doet. Als je iemand online in de gaten houdt, kun je in één ogenblik terugzien wat die persoon jarenlang en op allerlei plaatsen heeft gedaan. Ergens ontstaat er dan een spanning met de opsporingsbevoegdheden in algemene zin en de zaken die je in die nieuwe werkelijkheid vindt. Later in het jaar zullen wij spreken over de mogelijkheid om een computer te doorzoeken. Die mogelijkheid kan er nu ook al zijn als je in huis bent. Dan vind je natuurlijk ook veel meer en van veel langer terug. Dan rijst de vraag of je met creatieve middelen wettelijke waarborgen zou moeten inbouwen vanwege de privacy. In het vuurwapenarrest staat bijvoorbeeld duidelijk dat het oké is als je ergens voor drugs binnengaat, maar daar wapens vindt. Als je echter voor iets wat nu speelt, ergens binnengaat en je vindt op de computer iets van twintig jaar geleden, is het de vraag of het allemaal binnen die bevoegdheden past. Misschien kan de Minister nu niet meteen hierop reageren, maar mijn fractie vraagt hier wel aandacht voor. Als wij later over de wetsvoorstellen spreken, moeten wij erop letten dat wij het midden ook goed inrichten.
Ik bespreek nu de bodem. Daarmee bedoel ik eigenlijk de gebruikers zelf: bedrijven en particulieren, die een eigen verantwoordelijkheid dragen voor het gebruik en het veilig houden van ons online verkeer. Op dat vlak is nog wel wat te doen. De Minister zet een bewustwordingsproces in. Mijn fractie steunt dit van harte. De vertaalslag is echter nog niet altijd voor iedereen duidelijk. De vertaalslag naar de verantwoordelijkheid van bedrijven is ook niet altijd duidelijk.
Ik las ergens de mooie vergelijking dat elke 37 seconden een fiets gejat wordt in dit land en dat ook elke 37 seconden een computer besmet raakt,

met alle risico's van dien. Ik kan mij goed voorstellen dat er een verantwoordelijkheid ligt bij de internetproviders. Nu zie je dat een aantal van hen die verantwoordelijkheid uit maatschappelijk oogpunt opneemt. Zij waarschuwen als zij zien dat er in hun netwerk een computer is die deel uitmaakt van een botnet. Als wij het daarbij laten en de Minister geen druk zou uitoefenen op die bedrijven, krijg je een soort valse concurrentie. Bedrijven die zich maatschappelijk verantwoord opstellen, hebben extra kosten. De bedrijven die dat niet doen, worden daardoor bevoordeeld. Ik ben van mening dat het goed is als een provider waarschuwt zodra hij ziet dat een computer deel uitmaakt van een botnet. Ik zou als klant graag gewaarschuwd worden. Ik zou namelijk niet weten of mijn computer besmet is. Uit het oogpunt van bredere veiligheid zou ik graag zien dat je een computer in quarantaine zet, als er geen verbetering volgt. Dan kan die computer wel naar een nieuwssite, maar bijvoorbeeld niet meer naar DigiD. Mocht die computer opgeroepen worden om in het kader van dat botnet een aanval te doen op een bank of op een overheidsinfrastructuur, dan wordt hij geblokkeerd net zolang totdat hij hersteld is. Dat zijn enkele creatieve ideeën voor oplossingen. Ik hoor graag of de Minister samen met de sector tot overleg hierover wil komen.

De heer **Verhoeven** (D66): Dit klinkt allemaal interessant, maar hoe verhoudt deze lijn van gedachten zich tot het feit dat de VVD zegt dat zij de meldplicht voor computerinbraken smaller en kleiner wil maken? De VVD wil er dus enerzijds voor zorgen dat er juist minder vaak meldingen komen en dat daar wat mee gebeurt, terwijl de heer Dijkhoff nu anderzijds zegt dat wij alles in het werk moeten stellen om mensen te waarschuwen voor meer computer- en cyberonveiligheid.

De heer **Dijkhoff** (VVD): Wij zijn voorstander van een meldplicht van security breaches. Daarom is mijn andere vraag aan de Minister wanneer dat wetsvoorstel concreet komt. Dat gaat echter om vitale sectoren. Als wij de oplossingen op het gebied van cybersecurity gaan inrichten, zou ik graag zien dat wij alle kansen grijpen om te laten zien dat het een gezamenlijk probleem is. In mijn ogen kom je verder als je dat onderkent dan wanneer de wetgever meteen plichten oplegt.
Ik noem een ander voorbeeld in dit verband. Ik stimuleer graag dat zo veel mogelijk meldingen bij het NCSC binnenkomen. Ik maak mij er echter zorgen over dat, als je dit verplicht stelt en de Wet openbaarheid bestuur ervoor zorgt dat die informatie, die niet altijd rooskleurig is voor een bedrijf, via een omweg alsnog op straat komt, mensen zich juist niet zullen melden. Ik wil dus stimuleren dat wij zo veel mogelijk weten. Een plicht is echter niet altijd het meest effectieve middel om dat te bereiken.

De heer **Verhoeven** (D66): De heer Dijkhoff geeft toe dat hij enerzijds zegt dat hij alles in het werk wil stellen om iedereen te waarschuwen zodra een provider ziet dat een computer onderdeel van een botnet is en om die computer dan aan te pakken, maar dat hij anderzijds van mening is dat een bedrijf een softwaregat of een cyberinbraak lang niet altijd hoeft te melden, behalve als het bij een vitale sector is. Volgens mijn gevoel is dat een beetje tegenstrijdig.

De heer **Dijkhoff** (VVD): Nee, dat is bekijken hoe je meeste effect bereikt in de praktijk. Dan leg je niet alleen een plicht op die op papier mooi klinkt. Ik wil bereiken dat er zo veel mogelijk zaken gemeld worden. Als de plicht er bijvoorbeeld toe leidt dat mensen denken dat het op straat komt te liggen terwijl zij dat niet willen, is die plicht in bepaalde gevallen dus niet effectief. Je moet een balans zoeken. Het is duidelijk dat het een plicht is als je in vitale sectoren opereert. Verder vind ik het vooral een gezamenlijke verantwoordelijkheid. Volgens mij delen wij het doel om zo veel mogelijk meldingen binnen te krijgen. In mijn ogen is er ook een deel in

relatie naar klanten toe. Als mijn besturingssysteem – ik let daar gelukkig zelf op – zodanig verouderd is dat het risico's met zich brengt en mijn provider dat merkt, zou ik het bijvoorbeeld op prijs stellen dat hij mij daarvan op de hoogte stelt. Er zijn ook bedrijven die nu al beginnen met automatische updates waar je niet onderuit kunt. Die worden verkocht als een service. Volgens mij zijn ze dat ook, maar ze brengen ook een beveiligingswinst met zich.

Mevrouw **Oosenbrug** (PvdA): Het verhaal wat mijn collega hier vertelt, klinkt heel aantrekkelijk. Het gekke is dat ik het idee had dat dit al in oprichting is onder de naam Abuse Information Exchange. Daar zitten zeven internetproviders achter en SIDN. Toenmalig Minister Verhagen heeft daar een bedrag van € 285.000 tegenaan gegooid. Ik had begrepen dat dit in het eerste kwartaal van 2013, dat nu net geëindigd is, zou worden uitgerold. Is dit voorstel een aanvulling daarop of is dit eigenlijk hetzelfde als Abuse Information Exchange?

De heer **Dijkhoff** (VVD): Dit is precies het punt. Blijkbaar ben ik daarop tekort ingegaan. Een aantal doet het al, maar de bad actors – hoe je ze heel bestraffend kunt noemen – onthouden zich daaraan. Zij maken dan geen kosten en onttrekken zich aan hun verantwoordelijkheid. Ik zou graag willen dat in goed overleg ervoor gezorgd wordt dat iedereen daaronder valt en dat er een soort brancheafspraken is of een stimulans op een andere manier, zodat meer mensen hieraan deelnemen. De invulling daarvan laat ik aan de Minister. Je ziet dat het inderdaad kan. Een aantal bedrijven doet het ook en dat heeft effect. Je wilt niet dat een aantal bedrijven concurrentievoordeel behaalt op onveiligheid.

De **voorzitter**: Meneer Dijkhoff, u vervolgt uw betoog. Ik wijs u erop dat u nog anderhalve minuut hebt.

De heer **Dijkhoff** (VVD): Ja, dank u. Ik heb nog twee concrete punten naar aanleiding van de stukken die voor vandaag zijn geagendeerd.
Ten eerste was er het hele verhaal rond het Pobelka-botnet waarbij wij op een gegeven moment informatie aangeleverd kregen en het maar de vraag was of wij die mochten zien en gebruiken. In mijn fractie leeft duidelijk het idee dat je, als je daardoor kunt zien waar er gevoelige informatie van de overheid wellicht blootgesteld is aan gevaar, dit zou moeten kunnen gebruiken. Zo'n uitspraak is niet voldoende om dit in de toekomst mogelijk te maken. Wat waren de juridische belemmeringen of terughoudendheden in dit geval? Was het overdreven voorzichtigheid of ligt er inderdaad een juridisch probleem? Hoe gaan wij dat dan oplossen?
Ten tweede is er de richtlijn over de «ethische hackers», om ze zo maar te noemen. Mijn fractie kan zich vinden in die richtlijn. Het lijkt mij goed dat mensen die goedwillend kwetsbaarheden blootleggen, daarvoor niet per se gestraft worden. Er moet wel altijd iemand zijn die beoordeelt of er inderdaad binnen de lijntjes of daarbuiten is gekleurd. Dit lijkt mij een aangewezen taak voor het OM. Als ik de stukken zo lees, lijkt het erop dat beide zijden echt moeten meewerken aan het systeem, dus ook de partijen bij wie de kwetsbaarheid geconstateerd wordt. Als een bedrijf de kop in het zand wil steken en niet meewerkt, maar de hacker wel zeer ethisch gehandeld heeft, vraag ik mij af of de logica van deze richtlijn er ook toe leidt dat het OM in zo'n geval via deze checklist niet snel of niet tot vervolging zal overgaan. Een bedrijf moet niet kunnen bepalen dat een ethische hacker een kwetsbaarheid bij dat bedrijf niet bloot mag leggen, omdat het bedrijf daar geen beleid op heeft.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Dit algemeen overleg heeft een vrij korte agenda, maar cybersecurity blijft natuurlijk een heikel onderwerp. De Minister heeft in het vorige algemeen overleg toegezegd

dat hij in het kader van responsible disclosure in gesprek zal gaan met het Openbaar Ministerie over het toepassen van de richtlijn bij de vervolging van aangiftes van hacken. Ik vroeg mij af of de Minister al iets kan melden over de voortgang daarvan. Ik vind dat de ethische hacker – wij spreken namelijk niet over de kwaadwillende hacker, maar over de beveiligingsexpert – te weinig beschermd is in responsible disclosure. Ik ga deze zomer naar een hackcongres in Nederland en zal daar via crowd sourcing – het klinkt allemaal heel interessant – bekijken of ik een initiatiefwetsvoorstel kan maken om de ethisch hacker te beschermen. Dit heeft wel te maken met het fenomeen «klokkenluiders», maar valt daar net buiten. In deze tijd zijn wij heel erg bezig met het beschermen van bedrijven. Een bedrijf wil bekijken wat er misgaat en waar de kwetsbaarheden zitten, ook al heeft het geen geld om constant beveiligingsexperts in te huren. Iemand die voor zijn hobby of beroep hackt, zou dit kunnen doen, maar dan wel goed beschermd. Wij zouden daar allemaal veel meer over moeten nadenken. Ik denk dat een initiatiefwetsvoorstel de beste weg hiervoor is en kondig dat bij dezen aan.
Ik kom nu op de meldplicht. In oktober 2011 is de motie-Hennis over de meldplicht voor bedrijven Kamerbreed aangenomen. Op zich zijn wij daar heel blij mee, maar het is de vraag hoe het nu staat met die richtlijn. Die is namelijk op een gegeven moment naar de Raad van State gestuurd, maar daarna hebben wij er volgens mij niets meer van gehoord. Hoe verloopt het nu verder met deze richtlijn?
Verder had ik schriftelijke vragen gesteld over de omgang met het Pobelka-virus. Bij het cybersecuritycentrum werken goede mensen. Het is allemaal goed geregeld, maar er wordt niet duidelijk regie gevoerd. Wat doen wij het met die regiefunctie? Kunnen wij ervoor zorgen dat er bij één partij – voor mij zou dat heel goed het cybersecuritycentrum kunnen zijn – gemeld wordt bij een zo grote uitbraak als die van het Pobelka-virus. Wij moeten inderdaad van de vrijblijvendheid van de meldplicht af. Zodra zoiets gebeurt, moeten bedrijven en wie dan ook doorkrijgen dat er iets serieus aan de hand is dat gemeld moet worden. Ik had laatst een gesprek met een bedrijf. Ik noem geen namen, want ik vind dat bedrijven dat zelf moeten doen. Dat bedrijf kreeg het advies om de hack lokaal te melden en is naar de politie gegaan. De politie zei dat die niet zo veel wist van internethacks en stelde voor dat het bedrijf die hack bij het cybersecuritycentrum zou melden. Het bedrijf belde toen het cybersecuritycentrum, maar daar zei men weer dat er eerst aangifte gedaan moest worden. Het was dus heel onduidelijk. Kan er daarom een duidelijkere richtlijn komen? Welke stappen moet je zetten zodra je constateert dat je aangevallen bent?

De heer **Verhoeven** (D66): De voorstellen waarmee de Minister gaat komen voor terughacken door de politie staan niet op de agenda, maar zijn wel nauw gerelateerd aan de onderwerpen van dit AO. Wat vindt de Partij van de Arbeid daarvan?

Mevrouw **Oosenbrug** (PvdA): Die voorstellen staan niet op de agenda maar mijn partij heeft daar wel een duidelijke mening over. Het belangrijkste is dat je bij het binnendringen van iemands pc dezelfde richtlijn moet volgen als wanneer je iemands huis binnenkomt. Net zoals een huiszoekingsbevel moet je ook een computerzoekingsbevel hebben. Je kunt niet zomaar in iemands computer inbreken. Het lijkt mij dat dit volgens dezelfde richtlijnen zal moeten gaan als het binnenvallen van een huis.

De heer **Verhoeven** (D66): Zodra er een bevestiging of een goedkeuring van de rechter-commissaris ligt, vindt de PvdA het dus prima dat dit gedaan wordt? Is dat voldoende waarborg volgens de Partij van de Arbeid? De impact van dat inkijken is natuurlijk wel veel groter, zoals de

heer Dijkhoff ook al zei. Je kunt namelijk jaren teruggaan en ziet veel meer dan hetgeen je zoekt.

Mevrouw **Oosenbrug** (PvdA): Je zult heel duidelijke afspraken moeten maken over een dergelijk «computerzoekbevel». Ik geef het maar een naam hoor, want ik zou niet weten hoe je dat moet noemen. Je zult moeten zeggen waar je gericht naar gaat zoeken. Het kan niet zo zijn dat je zegt te zoeken naar foto's, maar vervolgens iemands e-mail leest. Ik denk dat je daar heel duidelijk in moet zijn, net zoals bij een huiszoekingsbevel. Ik ben geen jurist, dus ik weet hier niet zo veel van. Je kunt daar volgens mij goede afspraken over maken. Ik ga niet over de invulling, maar dat is de lijn die de PvdA-fractie in dit verhaal gaat volgen.

De **voorzitter**: De heer Verhoeven heeft nu zijn twee interrupties verbruikt.

De heer **Bontes** (PVV): Voorzitter. Banken, ziekenhuizen, de energiebranche en de overheid zijn al meerdere keren doelwit geweest van cyberaanvallen. Ik ga even door op wat mijn collega van D66 zei: er moet wel iets tegen gebeuren. Terughacken is een zwaar middel. Dat realiseert mijn fractie zich ook. Je kunt dit echter niet allemaal ongemoeid laten. Je zult jezelf dus wel moeten wapenen hiertegen. Je moet bevoegdheden hebben zodat je in andere netwerken kunt binnendringen. Dit alles moet echter wel proportioneel zijn. Het moet in verhouding staan tot de privacy van betrokkenen. Dat is de vraag. Misschien kan de Minister al een doorkijk geven? Veel hangt namelijk af van zijn wetsvoorstel. Het gaat nu met name over het Pobelka-botnet. Hoe zou dit in de praktijk gaan? Hoe wordt vormgegeven aan het verstoringsmiddel? Kan de Minister het iets concreter maken? Stel dat er een bevoegdheid is om terug te hacken en er vindt een aanval plaats zoals de Pobelka-botnetaanval, hoe gaat dit dan in de praktijk? Kan de Minister dit, in aanloop naar die wetsvoorstellen, enigszins toelichten? Dat maakt het wat makkelijker.
Ik ga nu concreet in op de cyberaanval met Pobelka-botnet. De overheid is naar de mening van mijn fractie te laks geweest daarin. De NOS heeft daarover bericht naar aanleiding van eigen onderzoek en daar zit wat in. De overheid zou op de hoogte zijn geweest van de honderden gigabytes aan gevoelige data die zijn buitgemaakt bij duizenden of honderden Nederlandse bedrijven en overheidsinstellingen, maar zou daar slechts weinig of niets aan hebben gedaan. De Minister benadrukt in zijn reactie op dit bericht dat deze kwalificatie onjuist is. De overheid heeft volgens de Minister namelijk verschillende middelen ingezet om het botnet bestrijden. Deze uitspraak staat natuurlijk haaks op de berichtgeving. Hoewel de Minister in de regel wel duidelijkheid schept in dit soort zaken, zet ik hier toch mijn vraagtekens bij. Ik zal uitleggen waarom.
Kan de Minister verklaren waarom het Team High Tech Crime (THTC) van de politie pas ruim een maand nadat het bekend was geworden met het bestaan van de buitgemaakte dataset contact heeft gezocht met het Nationaal Cyber Security Centrum? Waarom vond dat pas na een maand plaats? Waarom is in de tussentijd geen nader onderzoek verricht door het THTC? Het klopt toch dat dit team met veel bravoure is opgericht. Dat team zou de cybercrime gaan bestrijden. Waarom is dat in dit geval niet gebeurd? Kan de Minister dat uitleggen?
Verder hebben wij een Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Kan de Minister uitleggen waarom de NCTV pas medio februari een gedegen onderzoek is gestart naar de inhoud van de dataset en de andere partijen, zoals het OM, en de politie en de AIVD er toen pas bij betrokken heeft, terwijl de NCTV al eind november 2012 bekend was met de inhoud van de dataset? Is het niet juist de rol van de NCTV om in het geval van digitale bedreigingen coördinerend op te treden?

Hoe staat het met de centrale rol van het NCSC op het gebied van cybersecurity? Is er inmiddels voldoende kennis en capaciteit om dit voldoende effectief te bestrijden?
De Minister geeft in zijn reactie aan dat verschillende bedrijven en overheden het doel zijn geworden van deze aanval. Kan de Minister daar wat concreter in worden, zonder direct namen van profit-organisaties te noemen? Ik kan mij namelijk voorstellen dat dit gevoelig ligt, maar kan de Minister iets meer duidelijkheid geven?
Dan kom ik de op de bezuinigingen bij de AIVD. Cyberaanvallen worden ook steeds vaker verricht door andere landen. Daar zijn voorbeelden van. Deze week werd bekend dat China onder meer de hand heeft weten te leggen op ontwerpen van de Joint Strike Fighter, de JSF, en van diverse raketsystemen alsmede gevechtshelikopters. China zou in een ware cyberoorlog met Amerika zijn. Kan de Minister 100% uitsluiten dat er in Nederland sprake was van een gerichte cyberaanval door een ander land, bijvoorbeeld China of Iran? Kan de Minister bovendien aangeven welke consequenties de bezuinigingen op de AIVD voor cybersecurity zullen hebben? Ik heb eerder deze week al een motie ingediend met betrekking tot die bezuinigingen, maar deze bezuinigingen hebben niet alleen gevolgen voor het opsporen van jihadisten en terroristen, maar ook voor cybersecurity. Ik wil graag een toelichting van de Minister wat voor consequenties die bezuinigingen op dit vlak kunnen hebben.
Ik ga nu in op de meldplicht. De PVV-fractie vindt dat bedrijven een eigen verantwoordelijkheid hebben om hun beveiliging en ICT op orde te hebben. De Minister benadrukt dit ook steeds in zijn brieven. Het mag alleen niet zo zijn dat dit kabinet zich geheel niet verantwoordelijk voelt, terwijl er keer op keer cyberaanvallen plaatsvinden. De PVV vraagt zich af of bedrijven moeten worden verplicht om cyberaanvallen te melden. Kan de Minister de laatste stand van zaken daarover geven? Mevrouw Hennis heeft inderdaad een motie ingediend, maar wij hebben daar maar weinig meer over gehoord. De consument heeft er volgens de PVV recht op om te weten welke bedrijven hun beveiliging niet op orde hebben. Hoe staat de Minister tegenover een bredere meldplicht bij cyberaanvallen? Welke bedrijven vallen nu al precies onder die meldplicht? Ook dat is nog niet geheel duidelijk. Is het niet zo dat met een meldplicht beter in beeld gebracht kan worden waar de kansen en kwetsbaarheden liggen? Verwacht de Minister dat cybercrime beter bestreden kan worden met een meldplicht? Zo nee, waarom niet?
Tot slot kom ik op de informatieplicht van de overheid. De verantwoordelijkheid van de overheid voor cybersecurity begint bij de voorlichting over cybercrime. De meeste computergebruikers zijn zich niet bewust van de risico's die dit met zich brengt. Ook weten veel gebruikers niet eens wat een botnet is en hoe zij zichzelf hiertegen kunnen beschermen, bijvoorbeeld door de virusscanners en anti-spyware op hun pc up-to-date te houden. Welke maatregelen neemt de Minister om bewustwording te creëren bij computergebruikers? De banken kunnen op voorhand eisen dat je goede antivirussoftware hebt, voor het geval je bankgegevens of rekeningen gehackt worden. Hoe ontwikkelt zich dit? Heel veel mensen weten dit niet. Zij zouden zich bewust moeten worden van dit soort zaken.

De heer **Oskam** (CDA): Voorzitter. Ik wil graag van de Minister weten hoe Nederland ervoor staat. Drie weken geleden was er een groot cybersymposium. Toen hebben diverse deskundigen verschillende mededelingen over Nederland gedaan. Er is gezegd dat Nederland klungelt met cyberaanvallen. Er wordt ook verwezen naar de ongelukken die de laatste tijd zijn gebeurd. Ik moet echter ook toegeven dat de directeur van het Europees Cyber Crime Centrum heeft gezegd dat het Nederlandse systeem om te reageren op cybercriminaliteit uitmuntend is. De waarheid zal ergens in het midden liggen. Daarom wil ik graag van de Minister weten hoe Nederland ervoor staat.

Wat er ook van zij, het CDA vindt dat er in Nederland, Europa en mondiaal nog wel een wereld te winnen is wat betreft de bestrijding van cybercrime en de vergroting van cybersecurity. Het is natuurlijk volop in beweging. Volgens de schatting van het UNICRI, het onderzoeksinstituut van de Verenigde Naties, zijn vorig jaar 556 miljoen mensen wereldwijd het slachtoffer geworden van een aanval van cybercrime. Van alle Europese bedrijven zou slechts 26% een ICT-beveiligingsplan hebben. Nederland ICT zegt dat de Nederlandse overheid zou moeten stimuleren dat iedere organisatie voor zichzelf een risicokaart maakt waarbij de risico's nadrukkelijk zijn meegenomen. Wat vindt de Minister van het idee van Nederland ICT?
In Nederland lijken de problemen alleen maar groter te worden: DDoS-aanvallen op banken, een aanval op de incheckservice van de KLM, het hacken van boardapparatuur van vliegtuigen en het onderscheppen van berichten tussen vliegtuigen en verkeerstorens. Verder zijn er cyberaanvallen op overheidswebsites in België. Ook worden jongeren het slachtoffer van cyberpestgedrag en het hacken van hun computer of smartphone. Het is de vraag wanneer de NS, de energie- of telecomsector aan de beurt komen.
De Minister geeft aan dat de samenwerking van publieke en private partijen met de ICT security community van het grootste belang is in het streven naar cybersecurity. Niettemin is er kritiek dat de cyberkennis momenteel voornamelijk nog bij het bedrijfsleven zit, zoals Fox-IT en TNO, dat met die kennis te weinig wordt gedaan en dat justitie in dit veld maar een heel kleine speler is. Vindt de Minister dit ook? Wat gaat hij eraan doen om de rol van zijn departement daarin te versterken?
Wat vindt de Minister van het pleidooi voor de vergroting van de cybersecuritykennis bij de universiteiten en voor een speciale opleiding en training voor internetingenieurs. Wij hebben begrepen dat er een speciale hoogleraar cybersecurity bij de TU Delft is of wordt aangesteld. Klopt dat? Wat gaat hij doen? Heeft die aanstelling ook te maken met de berichtgeving over TNO, namelijk dat men oefenruimtes gaat inrichten? Wat vindt de Minister van de suggestie – om even bij dat laatste aan te sluiten – van een cyberoefenomgeving die cyberaanvallen, informatielekken en hacks nabouwt om mogelijke incidenten stap voor stap te analyseren? In hoeverre zitten dergelijke suggesties al in de actualiteit van de Nationale Cyber Security Strategie? Welk tijdspad heeft de Minister uitgezet voor zijn kortetermijnactiepunten? Dit alles moet natuurlijk wel snel gebeuren.
Is er voldoende budget om dit alles te realiseren? Vorige week hadden wij met dezelfde Minister een AO over terrorisme. Toen is de financiële taakstelling van de AIVD aan de orde geweest. De AIVD geeft onder andere prioriteit aan cybersecurity, maar kan de AIVD dat waarmaken gegeven de financiële taakstelling? Wat is het budget van het NCSC? Beschikt het NCSC over voldoende menskracht en financiële middelen om de taken te kunnen uitvoeren? Diezelfde vraag geldt voor het Team High Tech Crime, de landelijke eenheid van de politie, en voor de informatiebeveiligingsdienst van de gemeenten. Graag horen wij van de Minister hoe het zit met de financiële middelen voor die instanties.
Ik kom nu op het Nationaal Dreigingsbeeld Georganiseerde Criminaliteit. Wij hebben daar vanochtend ook al over gesproken. In verband met cybersecurity werd gezegd dat er een toename is van de ernst en de omvang van high tech crime, zoals hacken, het opzetten van botnets – de collega's zeiden dit ook al – en de verspreiding van virussen. Dit alles krijgt terecht prioriteit. Binnen de aanpak van cyber crime zou moeten worden gewerkt aan het opwerpen van barrières. Daar spraken wij vanochtend ook over. Diezelfde vraag stel ik ook nu aan de Minister. Hoe zit dit bij de aanpak van cybersecurity? Wordt de bovenwereld daarbij betrokken? Welk deel heeft zij daarin? Wordt de digitale expertise binnen de politie uitgebreid? Die speelt immers ook een belangrijke rol.

De Nederlandse Vereniging van Banken is terecht van mening dat cyberaanvallen een zaak van nationale veiligheid zijn en dat banken, overheid en toezichthouders daarom samen met een communicatieprotocol moeten komen. Wat dat betreft is het een goede zaak dat de Minister twee wetsvoorstellen heeft aangekondigd betreffende de meldplicht voor de overheid en private bedrijven in verband met cyberincidenten en datalekken. Hoe wordt straks gecontroleerd of men zich aan dat protocol houdt? Hoe wordt een en ander gehandhaafd?
De Europese Commissie is recentelijk gekomen met een mededelingsstrategie inzake cyberbeveiliging van de Europese Unie. Zij schetst vijf strategische prioriteiten. Ik zal die nu niet opsommen, omdat iedereen die wel kent. Wij onderschrijven de maatregelen en de lijst van prioriteiten die in de mededeling wordt voorgesteld en zien deze strategie ook als een belangrijke stap om binnen de Europese Unie een meer gelijkwaardig niveau van cyberbeveiliging te realiseren. Wordt er volgens de Minister op dit moment binnen de Europese Unie voldoende gedaan aan de bestrijding van cybercrime? Niet alleen straatmuzikanten, zakkenrollers en skimmers komen uit Roemenië, maar volgens de directeur van het eerder genoemde Europese Cyber Crime Centrum komt ook veel online criminaliteit uit Roemenië en ook wel uit Bulgarije. Wat doen de overheden van die landen daaraan? Hoe worden deze landen door de EU aangesproken c.q. aangepakt?
Er zijn signalen dat er cyberaanvallen zijn die van of namens andere overheden afkomstig zijn. De heer Bontes zei dit ook al. De genoemde Europese mededeling streeft onder andere ook naar goede samenwerking met strategische landen zoals de VS, India en China. Wat vindt de Minister van de suggestie om te komen tot een internationaal non-proliferatieverdrag?
Ik informeer even naar de tijd. Hoe lang heb ik nog?

De **voorzitter**: U hebt helemaal geen tijd meer.

De heer **Oskam** (CDA): Ik wil ook niet om meer tijd vragen. Dan bewaar ik de rest voor de tweede termijn.

De heer **Verhoeven** (D66): Voorzitter. Ik wil eerst het woord geven aan mijn collega, mevrouw Gesthuizen. Zij heeft een logistieke spanning.

De **voorzitter**: Dat is prima.

Mevrouw **Gesthuizen** (SP): Voorzitter. Excuus voor mijn late binnenkomst. Ik moet zo even naar de regeling; vandaar.
Allereerst complimenteer ik de Minister en zijn ondersteuning met het duidelijke en overzichtelijke rapport Nadere analyse Pobelka-botnet. Ik meen dat er echter wel een bepaalde misvatting te lezen valt. Ik las namelijk de volgende zin: «Op basis van de diversiteit van getroffen systemen en buitgemaakte gegevens is er op dit moment geen reden om aan te nemen dat het botnet specifiek gericht was op specifieke overheden, sectoren of organisaties.» Ik kan mij eerlijk gezegd helemaal niet voorstellen dat dit nu op basis van dit gegeven uit te sluiten valt. Het lijkt mij namelijk dat je de inmenging van statelijke factoren helemaal niet kunt uitsluiten, want gericht zoeken kost heel veel tijd. Bovendien loop je dan wellicht allerlei interessante informatie mis. Kan de Minister toelichten waarom hij heeft gemeend dit zo op te moeten schrijven?
De Minister zegt dat het NCSC geen rechtsbasis had om de resterende inhoudelijke en mogelijk gevoelige gegevens in te zien en te verwerken. Dat lijkt mij wel zorgwekkend. Het NCSC is wederom uitsluitend adviserend. Betekent het «niet oppikken» derhalve «niet oppikken in het algemeen»? Mag ik daar een reactie op?

De Minister stelt: «Tevens stond niet vast hoe Digital Investigation deze informatie had verkregen». Ik vind dat een merkwaardig argument. Het NCSC had hier een onderzoek naar moeten aanvragen, al dan niet met met hulp van THTC. Wanneer komt er op juridisch vlak meer duidelijkheid of en hoe het NCSC op een zorgvuldige wijze kan omgaan met de informatie die het NCSC vanuit de ICT-community bereikt?
Dat brengt mij op mijn volgende punt. Ik ben laatst bij een expertmeeting geweest. Overal waar je komt, bij welke club met ICT-experts je ook je licht opsteekt, er wordt steeds gehamerd op samenwerking, publiek-private samenwerking, samenwerking met de hackerscommunity of met mensen die al dan niet toevallig lekken in de beveiliging tegenkomen. Steeds wordt daarop gehamerd. Ik spreek mijn zorg hierover uit, omdat ik van diverse bronnen begrijp dat er in de hackers community grote zorgen zijn over de leidraad voor responsible disclosure. Ik vraag mij dus ook af of en hoe intensief er overleg en samenwerking is geweest met die hackersgemeenschap bij het opstellen van deze richtlijn. Deze groep ontdekt namelijk vaak als eerste de kwetsbaarheden in ICT-systemen. De Minister stelt in zijn brief dat hij de komende tijd met zijn collega's binnen de rijksoverheid om tafel gaat zitten om het breed toepassen van responsible disclosure binnen de rijksoverheid te bevorderen. Ik vind dat erg belangrijk. Ik vraag mij wel af of de Ministeries, als gevolg van een krimpend ambtenarenapparaat, wel in staat zijn om capaciteit vrij te maken om de meldingen op een adequate manier te behandelen. Hoe ziet de Minister dit? Graag krijg ik dus een uitgebreid antwoord op de vraag hoe intensief het overleg met de hackers community is geweest.
Ik ga nu in op DDdoS-aanvallen. Ik stel voorop dat ik me grote zorgen maak over de – zeker in het verleden te constateren – lakse houding bij banken en met name over de zeer kritische geluiden van veel mensen die daar te maken hebben met ICT en veiligheid. De banken namen het onvoldoende serieus. De mensen in de board die de beslissingen daarover moeten nemen, hebben er onvoldoende verstand van. Verder zou men doen aan struisvogelpolitiek en de kop in het zand steken. Ook zou men inzetten op andere dingen in plaats van de veiligheid op één te zetten en tot prioriteit te maken. Ik maak mij daar grote zorgen over. Deelt de Minister die zorg?
Een interessante opmerking in de brief van de Minister is: «Duidelijk is dat geïnvesteerd moet worden in beveiliging van ICT en alternatieve kanalen en infrastructuren voor e-dienstverlening om de veiligheid van vitale en essentiële voorzieningen in de dienstverlening te kunnen waarborgen. De aangevallen organisaties zijn daar zelf verantwoordelijk voor.» Wij hebben het in dit verband ook over de bescherming van persoonsgegevens en bescherming van het bezit van mensen en hun veiligheid. Daarom rijst de vraag of de Minister enig idee heeft of er bij al deze organisaties voldoende middelen en kennis in huis zijn om dit daadwerkelijk te realiseren. Is het niet wat gemakkelijk van de Minister, gezien het feit dat het ook om vitale zaken gaat die van landsbelang zijn?
Voorzitter. Ik denk dat ik nog ongeveer 30 seconden heb en daarom maak ik een laatste opmerking. Ik ben helemaal niet blij met de antwoorden op mijn Kamervragen naar aanleiding van de detentieomstandigheden van een Nederlander in de Verenigde Staten en over het feit dat FBI-agenten meehacken met de Nederlandse politie. De Minister zou tijdens dit algemeen overleg moeten aangeven of er bij de High Tech Crime Unit dan wel de KLPD ook verbindingsofficieren of andersoortige buitenlandse ambtenaren of agenten actief zijn van bijvoorbeeld het Department of Homeland Security, US Immigration and Customs Enforcement, United States Secret Service, the National Security Agency of enige andere Amerikaanse of buitenlandse opsporings-, veiligheids- of inlichtingendienst.

De heer **Verhoeven** (D66): Voorzitter. Omdat mijn collega's al zo veel verstandige dingen hebben gezegd, kom ik direct tot de kern. Cybercrime is vaak het gevolg van een tekort aan cybersecurity. Het doel is steeds om de cybersecurity te vergroten. Dat hebben alle collega's al gezegd. D66 wil dit vooral doen door de digitale weerbaarheid te vergroten. Dit begint met thuis de digitale deur goed dicht te doen, door kennis van online experts te benutten, door een overheid die de systemen niet onnodig kwetsbaar maakt en tijdig in actie komt als dat nodig is en door incidenten met elkaar te delen en te melden. Dat zijn belangrijke basisdingen.
Ik ga op een aantal punten in, allereerst op Pobelka. De Minister kondigt in zijn brief over de Pobelka- en de DDoS-aanvallen drie dingen aan. De eerste actielijn van de Minister is een geïntensiveerde aanpak van botnets. De Minister zegt dat er bij het Pobelka-probleem adequaat is gehandeld. Er zat echter maanden tussen de eerste kennis van het Team High Tech Crime en de acties van het NCSC. Kan de Minister uitleggen wat er adequaat is aan die wachttijd?

De **voorzitter**: Excuses dat ik u midden in uw speech onderbreek. Ik ga nu zelf naar de regeling van werkzaamheden. De heer Dijkhoff zal mij even vervangen. Excuses hiervoor.

Voorzitter: Dijkhoff

De heer **Verhoeven** (D66): Dat is geen punt, voorzitter, zolang u ook maar even uw stopwatch stopt.
Toen het NCSC uiteindelijk die informatie had, besloot het om via IP-adressen en de providers de getroffen computers in te seinen dat er ingebroken was. Ook al kwam deze oplossing rijkelijk laat, het was wel een elegante oplossing, die geen enkele extra bevoegdheid vereiste. Wil de Minister de geïntensiveerde aanpak van botnets op deze manier gaan inrichten? Maakt hij hiervoor voldoende capaciteit vrij bij het NCSC of creëert hij die?
De tweede actielijn van de Minister is het juridisch instrumentarium actualiseren en uitbreiden, de «inbreekpolitie van de Minister» zullen wij dat maar kortheidshalve noemen. Natuurlijk is het goed dat er een wetvoorstel computercriminaliteit III komt. Dat schept duidelijkheid over de mogelijkheden die de politie wel en niet heeft in het digitale domein. De inhoud van dat wetsvoorstel gaat echter ver, terwijl de onderbouwing mager en de omlijning vaag is. Daardoor vinden wij de invulling risicovol. Zo is het heimelijk binnendringen door de «inbreekpolitie» in computers gewoon iets heel ingrijpends. Ik ben blij met wat de woordvoerder van de PvdA heeft gezegd. Zij trekt de vergelijking met de huiszoeking, want daarbij weet je dat er op dat moment wordt ingebroken in je persoonlijke domein. Bij computers moet je dit in ieder geval ook doen. Heimelijk inbreken is van een grote vergaandheid. Wij vinden het nut dus nog onvoldoende onderbouwd. Wij vinden het bovendien buitenproportioneel, temeer omdat de Minister misschien wel een dubbel belang toekent door softwaregaten door de politie in stand te laten. Als het NCSC de opdracht heeft om die te dichten, kan de politie het belang hebben om die gaten juist open te houden, want anders kan zij niet heimelijk inbreken. Verder gaat de Minister volgens ons met de plannen voorbij aan de internationale verdragen, met alle gevolgen voor wederkerigheid.
Het decryptiebevel vinden wij ook zeer problematisch, in die zin dat het op gespannen voet staat met het nemo-teneturbeginsel, het niet hoeven meewerken aan je eigen veroordeling.
Dit waren kort een paar punten over de wetsvoorstellen die nog naar de Kamer komen. Zij zijn echter zo dicht aan het onderwerp gerelateerd, dat ik ze wel even wilde noemen. Graag krijg ik van de Minister een reactie op hoofdlijnen.

De derde actielijn van de Minister is het op- en uitbouwen van een nationaal detectie- en responsnetwerk. Gaat de Minister het internet, al dan niet in cruciale sectoren, monitoren met bijvoorbeeld deep packet inspection? De benadering van D66 is enigszins anders dan die van de Minister. Dat moge duidelijk zijn. Mijn fractie wil namelijk problemen voorkomen en waar er problemen ontstaan, kiezen voor proportionele maatregelen. Dat is onze opstelling in een notendop. Zo kun je bijvoorbeeld DDoS-aanvallen reduceren door minder computers tot botnet te laten worden. Zoals ik in het begin al zei, vereist dit basisveiligheid bij gebruikers. Dat is een vorm van je fiets op slot zetten, dus programma's via scanners en firewalls up-to-date houden. De overheid heeft in dezen ook een belang, want hoe meer besmette computers er zijn, hoe meer botnet-aanvallen. Hoe gaan wij dit aanpakken? De huidige overheidscampagnes op dit gebied volstaan namelijk niet.
De overheid en het bedrijfsleven moeten bovendien goed voorbereid zijn. Collega's hebben daar ook al veel over gezegd. Volgens de Minister zijn er pas na de recente overlast allerlei maatregelen genomen. De Minister schrijft over extra capaciteit, filters en een dienst voor aanvullende scheiding van benaderingen. Waarom zijn deze maatregelen niet eerder getroffen? Het is natuurlijk niet heel verrassend dat de websites van DigiD of de rijksoverheid doelwit kunnen zijn. In aanvulling op de inbreng van mijn collega van de SP die nu even bij de regeling is, deel ik mee dat er morgen een gesprek met de banken is over het online betalingsverkeer. Hoe goed hebben de banken de afgelopen tijd geanticipeerd op deze toch wel voor de hand liggende optie? DDoS-aanvallen zijn niet iets van de laatste jaren. Die vinden al minstens tien tot vijftien jaar plaats.
Tot slot kom ik op responsible disclosure, het gebruikmaken van de kennis van hackers. De leidraad is er op verzoek van D66 gekomen. Wij zijn daar blij mee. Er zitten twee open eindjes aan. Ten eerste houdt het OM alle ruimte om alsnog te vervolgen. Ten tweede houdt de partij met het lek alle ruimte om het probleem geheim te houden. Kan de Minister op deze twee open of losse eindjes ingaan? Verder sluit ik mij aan bij de vragen van collega Gesthuizen over de betrokkenheid van de hackers community bij de totstandkoming van de leidraad.

De **voorzitter**: Dit was de eerste termijn van de Kamer. De Minister heeft even tijd nodig voor de beantwoording. Ik schors de vergadering voor tien minuten.

Schorsing: 14.45 uur tot 14.55 uur.

De **voorzitter**: Ik verzoek iedereen om weer plaats te nemen. Voordat ik de Minister het woord geef voor zijn beantwoording in eerste termijn, maak ik graag de afspraak dat er twee interrupties per Kamerlid worden toegestaan. Ik geef het woord aan de Minister voor de beantwoording.

Minister **Opstelten**: Voorzitter. Ik dank de geachte afgevaardigden voor hun heel constructieve benadering van dit belangrijke onderwerp. Tegen de heer Verhoeven zeg ik dat mijn lijn in de eerste plaats is om dit alles te voorkomen. Daar zijn wij continu mee bezig. Vervolgens is mijn lijn om altijd proportioneel op te treden en niet anders. Dat ben ik trouwens mijn hele leven gewend en dat wil ik ook voortzetten.
De afgelopen maanden is er heel veel gebeurd op het terrein van cybersecurity, in ons land en internationaal. Wij zijn daar inderdaad voortdurend bij betrokken. Er is zowel sprake geweest van incidenten als van structurele stappen om de digitale veiligheid verder te verhogen. Het gaat namelijk heel snel.
Ik geef een paar illustraties van gebeurtenissen in de cyberwereld. Het nationaal centrum heeft tot en met april reeds 638 beveiligingsadviezen gegeven. Cybersecurity en het internet zijn per definitie grensover-

schrijdend. Daarom ben ik blij dat er in Europees verband goede stappen zijn gezet met een Europese cybersecuritystrategie. De onderhandelingen over de bijbehorende richtlijn zijn momenteel gaande. Ik heb in het AO over de strategie van 24 april reeds toegezegd dat ik de Kamer blijvend zal informeren over dit proces. Ook op nationaal vlak hebben wij beleidsmatige stappen gezet. Je kunt zeggen dat wij met het publiceren van de leidraad om te komen tot de praktijk van responsible disclosure wereldwijd tot de koplopers behoren. Dank voor de support daarbij. Er zijn natuurlijk nog open eindjes. Sommigen van u spraken al daarover. Ik kom er zo dadelijk nog op terug. We zijn de eerste overheid die deze stap heeft gezet. Juist om de kennis over de kwetsbaarheden van de ICT-community te gebruiken, is dit belangrijk. Ondertussen zijn er steeds meer publieke en private partijen die daadwerkelijk een eigen beleid voor responsible disclosure opstellen. Op de website van het NCSC is een overzicht te vinden van grote organisaties die een dergelijk beleid hebben gepubliceerd. Wat betreft een structurele aanpak moeten we over de gehele linie actie blijven ondernemen, dus awareness, detectie en response. Ook opsporing en vervolging horen erbij, als sluitstuk.
Op al deze vlakken is actie ondernomen. Ter verhoging van de awareness houden wij in het najaar opnieuw de campagne Alert Online. Ook wordt er gewerkt aan de op- en uitbouw van een nationaal detectie- en responsnetwerk, om bijvoorbeeld uitbraken van malware zo snel mogelijk te detecteren en van een gepaste respons te voorzien. Verder wordt er ten behoeve van de opsporing gewerkt aan een wetsvoorstel dat de opsporingsbevoegdheden aanpast aan de ontwikkelingen in het digitale domein. Een aantal leden heeft daar in de consultatiefase al iets over gezegd. Dit wetsvoorstel is recent in consultatie gebracht. De inbreng in de consultatieronde zullen wij met zorg bekijken. Daarna zal het wetsontwerp uiteraard zo snel mogelijk naar de Kamer gezonden worden via de route Ministerraad, Raad van State, Ministerraad, Tweede Kamer. Op dat moment kan het hier nader besproken worden. We hebben al een keer in een algemeen overleg over de uitgangspunten van het voorstel gesproken, aan de hand van een brief. We hebben zwaar gediscussieerd met iedereen. Ik ben blij dat ondanks accentverschillen iedereen wel vindt dat er iets moet gebeuren. Dat is belangrijk. Dat is dus een stap verder dan we destijds hadden geconcludeerd.
Ook op het vlak van onderzoek hebben we resultaten geboekt. Ik ben blij dat in samenwerking met AgentschapNL en NWO de financiering van de eerste ruim twintig onderzoeksvoorstellen inmiddels is gehonoreerd. Dit zijn innovatieve voorstellen, die bijdragen aan het veilig maken van de digitale bronnen.
Deze structurele stappen nemen niet weg dat wij in de eerste helft van 2013 ook een aantal incidenten hebben gezien. Incidenten zijn niet altijd te vermijden. Ze verrassen ons natuurlijk ook; je wordt ermee geconfronteerd. Incidenten zullen helaas blijven plaatsvinden. Het is van belang om ze van een gepaste respons te kunnen blijven voorzien. Dit vereist voortdurend scherp onderzoek en voortdurende reflectie op je eigen optreden.
Ten eerste hebben we te maken gehad met het Pobelka-botnet. Ik heb de Kamer daarover bij brief geïnformeerd. Ik kom er zo dadelijk nog op terug. Inmiddels is de casus afgerond. Op basis van de gegevens zijn na een zeer grote inspanning iets meer dan 200 partijen gericht geïnformeerd over mogelijke besmetting, zodat zij aanvullende acties ter bescherming kunnen treffen.
Daarnaast zijn we vanaf april geconfronteerd met meerdere DDoS-aanvallen. Ik noem het een «digitale file»; het zijn in feite aanvallen aan de voordeur waardoor een site tijdelijk onbereikbaar wordt. Zoals vaker gezegd, zijn dit nadrukkelijk geen digitale inbraken ofwel hacks. Deze digitale verkeersopstoppingen zijn niet zomaar onder controle te krijgen. Het is desalniettemin van groot belang om actie te ondernemen,

zodat websites bij aanvallen snel weer in de lucht zijn. Hieraan zal door de verantwoordelijke partijen dan ook aandacht worden besteed. Naar aanleiding van de aanval op partijen in de bancaire sector heb ik de Kamer met mijn collega Dijsselbloem op 16 april geïnformeerd over de door de overheid en de bancaire sector getroffen acties. Ik ben blij met de aangekondigde acties van de banken en met de toezegging van de bancaire sector om een liaison in het Nationaal Cyber Security Centrum te plaatsen. Toen de banken, gewoon in een weekend, geconfronteerd werden met deze aanvallen, hebben zij direct op het hoogste niveau, met mij, contact gezocht. We hebben op dat moment daadwerkelijk de dingen gedaan die noodzakelijk waren.
Daarnaast was er sprake van DDos-aanvallen op de rijksoverheid. Op 14 mei heb ik samen met de verantwoordelijke Ministers de Kamer geïnformeerd over de acties die zijn ondernomen naar aanleiding van deze aanvallen. Zoals eerder gezegd, gaan de ontwikkelingen ontzettend snel. Het is dan ook van belang om deze bij te houden. In dat kader gaan we dit jaar nog de Nationale Cyber Security Strategie actualiseren en aanscherpen. Na het zomerreces zal ik die aan de Kamer zenden. Er is sprake van nauwe publiekprivate samenwerking. Het buitenland kijkt soms met verbazing, maar ook met een zekere jaloezie, toe hoe bij ons, vanuit verschillende verantwoordelijkheden, de private sector, de wetenschap en de overheid samen aan boord zitten om zo de kennis met elkaar vast te houden, elkaar te versterken en vanuit die weg verder te gaan. Dat is in het buitenland niet overal mogelijk
De heer Dijkhoff sprak over nieuwe wetgeving en nieuwe ontwikkelingen, gewoon meedenken en stilstaan bij de wettelijke mogelijkheden en bevoegdheden die je hebt. Het is goed om discussie te voeren. Het is goed dat de heer Dijkhoff er in alle scherpte aandacht voor vraagt. De bevoegdheid wordt in het kader van bepaald onderzoek en matching uitgevoerd. Dit gebeurt natuurlijk door de machtiging van de rechter-commissaris. Er zit een balans in. Dit punt zal in de verdere behandeling aan de orde komen. Er is een spanning in de opsporingsbevoegdheid in algemene zin. Graag voldoe ik aan het verzoek. We nemen het gewoon mee.
Onze ambities betreffende kwaliteit en wat we willen bereiken, moeten het hoogste niveau hebben, Champions League, internationaal. Daar spelen we dan ook. Wij zijn een leading voice op dit terrein. Dat is niet iets om trots op te zijn maar gewoon normaal, gezien onze sterke digitale samenleving en ons digitale bedrijfsleven, de economie die er staat en onze visie daarop. Dat is natuurlijk belangrijk. We moeten echter ook de basis hebben. Ook het middenkader moeten we erin meenemen. Ik zie de discussie met de Kamer over de wetgeving graag tegemoet. Het zijn de punten die we aan de orde hebben als we met de Nationale Cyber Security Strategie komen. We komen ook met het nieuwe assessment. Daarin komen we met aanvullingen en aanscherpingen van wat we qua wetgeving nodig hebben. Zo gaat het altijd. Als je zegt «dit is je assessment», betekent dat ook «dat moet je aanpakken». We hebben daar de vorige keer onze juridische basis tegenaan gezet: welke wetten moeten we aanpakken. Daar hoort dit nadrukkelijk bij.
De heer Bontes vraagt of ik al kan aangeven hoe het verstoringsmiddel in de nieuwe wetgeving eruit gaat zien. Nadat bij de bedrijven is gezocht naar gegevens op hun netwerk, zal de politie een online doorzoeking kunnen doen, nadat hiervoor de goedkeuring is gegeven door de rechter-commissaris. De politie kan dan servers, computers en netwerken doorzoeken die in verband kunnen worden gebracht met de aanval. Als dat resultaat heeft, zal zo veel mogelijk geprobeerd worden om, samen met andere landen dan wel zelfstandig, het gebruikte computersysteem uit te schakelen en voor onderzoek veilig te stellen om zo de daders op te sporen. Dat gebeurt in de wetgeving die ik in consultatie heb gebracht. Dit is aan de orde bij zware misdrijven. In feite is het nu nodig dat je die

wetgeving hebt. Ik hoop daarom ook dat de Kamer dit wetsvoorstel snel wil behandelen als het is ingediend.
Er zijn vragen gesteld over het Pobelka-incident. De brief is op zichzelf helder. September 2012 heeft Digital Investigation de beschikking gekregen over de gegevens die op een centrale server van het Pobelka-botnet stonden. Het betrof een omvangrijk dataset van 750 GB, geschat wordt 120 miljoen A4'tjes. Het is maar dat u het weet, het maakt op mij nog steeds indruk... Op 16 oktober 2012 leverde Digital Investigation de dataset aan bij het Team High Tech Crime van de politie. Mogelijk was er sprake van een relatie met het Dorifelvirus. Over Dorifel liep reeds een strafrechtelijk onderzoek. De dataset bleek later bij de politie onleesbaar te zijn. Op 20 november 2012 kwam in een gesprek tussen Digital Investigation en het Team High Tech Crime van de politie naar voren dat er geen sprake was van een relatie met het Dorifelvirus. Hierop is door de politie geen nieuw exemplaar van de dataset aangevraagd. Op 26 november 2012 is door het Team High Tech Crime naar het NCSC verwezen. Op 8 december 2012 heeft het NCSC op grond van de voor hem geldende taken en bevoegdheden slechts een gedeelte van de dataset in ontvangst genomen. Het NCSC was en is namelijk niet bevoegd om mogelijk gevoelige data binnen de dataset in te zien.
Er is gevraagd waarom het NCSC pas medio februari een onderzoek is gestart. Ik denk dat dit op basis van mijn voorgaande relaas duidelijk moge zijn, maar ik wil het wel samenvatten. Naar aanleiding van de uitzending van het NOS journaal van 14 februari jl. zijn delen van de dataset in de openbaarheid gekomen. Daarmee is het risico van misbruik groter geworden. Daarnaast is door een aantal partijen de suggestie gewekt dat hierbij mogelijk grote belangen geschaad zouden zijn. Daarom was het van belang om de dataset in een brede context te analyseren, om zo de potentiële impact van de gegevens in de dataset in te kunnen schatten. Het gaat om een omvangrijke dataset, 120 miljoen A4'tjes, en het vergt enige tijd om die te analyseren. Ik heb de Kamer destijds toegezegd dat de eerste resultaten van dit onderzoek in de tweede helft van maart bekend zouden zijn. Dat is ook het geval geweest. Zoals mevrouw Gesthuizen al aangaf, heb ik de resultaten toen aan de Kamer toegezonden.
Mevrouw Oosenbrug ziet weinig regie wat betreft Pobelka. Het NCSC is op het gebied van de cybersecurity hét centrale punt in Nederland en daarmee de spin in het web. Daarover mag geen verschil van mening bestaan; dat is zo en dat wordt ook door iedereen zo gezien. Om organisaties buiten de eigen achterban van de rijksoverheid en de vitale sectoren te kunnen bedienen wanneer dat nodig is, werkt het NCSC samen met schakel- en partnerorganisaties. Niet alleen kunnen langs deze weg verschillende sectoren binnen de eigen verantwoordelijkheid zelfstandig hun digitale weerbaarheid vergroten, ook wordt hiermee de uitrol van een effectief landelijk netwerk van sectorale informatiebeveiligingsorganisaties gestimuleerd. De regie is er dus. Het NCSC heeft alle partijen bij elkaar gebracht bij het Pobelka-onderzoek. Dat is dankzij het centrum gebeurd.

De heer **Bontes** (PVV): Ik heb twee korte vragen. De eerste heeft betrekking op de tijdlijn. De Minister legde zojuist uit aan wie wat is afgeleverd en wie bij het onderzoek is betrokken. Er gingen echter wel een paar maanden overheen. Kan de Minister uitleggen waarom het, op het oog, zo lang duurt? Je zou zeggen dat in dit soort gevallen iedere seconde telt.
Mijn tweede vraag heeft betrekking op de dataset die is afgeleverd. Deze was deels niet leesbaar. Is dat gebrek aan techniek dan wel gebrek aan knowhow? Of is het niet goed op de schijf gezet door degene die het verzameld heeft? Wat is de reden van de gedeeltelijke onleesbaarheid?

Minister **Opstelten**: De heer Bontes vraagt naar het tijdsbeeld. Ik heb uitgelegd dat het eerst in handen van de politie was. Het betreft gevoelige informatie. Het is daarom juist dat het bij de politie terechtkwam. Vervolgens is het op het NOS journaal verschenen. Toen heeft het NCSC de regie gepakt. Op die manier is het gebeurd. Het was niet meer en niet minder dan de taak om zo veel mogelijk adressen te informeren over het punt dat dit plaatsvond. Dat is een krachtsinspanning geweest. Het is in tweehonderd gevallen gebeurd en dat is een knappe prestatie. Zo is het dus in de kern goed afgerond. Politie en OM doen het onderzoek en dat loopt nog.
De heer Bontes vraagt ook welke bedrijven zijn geraakt. Op basis van organisatienamen en domeinnamen die gebruikt worden door organisaties en op basis van veelgebruikte trefwoorden die in de dataset zijn gevonden, worden partijen binnen de doelgroep van de rijksoverheid en de vitale sectoren actief geïnformeerd door het NCSC. Het betreft 20 organisaties in vitale sectoren, 35 ziekenhuizen, 20 rijksoverheden en gelieerde instellingen en daaronder 30 lokale overheden.

De heer **Bontes** (PVV): Ik begrijp natuurlijk dat het veel werk is om een paar honderd bedrijven te informeren, maar ik wil graag van de Minister weten of hij tevreden is over de snelheid waarmee dat proces is verlopen. Of ziet hij aanleiding om dat proces verder te stroomlijnen en te bezien of het kan worden versneld?

Minister **Opstelten**: Laat ik duidelijk zijn: het centrum heeft geen politie- of OM-verantwoordelijkheid. Gelukkig niet, dat zal ook nooit gebeuren. De informatie is eerst terechtgekomen in de politieorganisatie, bij het speciale team dat daarvoor is opgericht. Daar heeft het centrum als zodanig geen rol in te spelen, want dan gaat het gewoon om onderzoek van politie en OM. Dat loopt door. Los daarvan is in het NOS journaal informatie naarbuiten gekomen. Daardoor is het een publieke zaak geworden. Dat had helemaal niet moeten gebeuren. Daarmee ontstond er een situatie waarin het NCSC moest acteren en dat heeft het ook gedaan. Ik heb in mijn brief al geschreven dat we voortdurend bekijken hoe het beter kan. In de kern moet het natuurlijk sneller. Dat hebben we al gezegd. Het NCSC moet zich ontwikkelen in zijn rol. Het is allemaal al aangekondigd. Het centrum wordt door iedereen geaccepteerd; niemand twijfelt eraan. We komen met een versterking van de positie van het centrum. Ik zal daarover nog een brief schrijven die een en ander duidelijk maakt. Laat er geen misverstand over bestaan: dit is een situatie die leidt tot reflectie, onderzoek, kritisch voor de spiegel staan en de maatregelen nemen die geboden zijn.
Voorzitter. De heer Dijkhoff heeft gevraagd naar juridische belemmeringen in het licht van Pobelka. Hij kan zich voorstellen dat het van belang is om op zorgvuldige wijze met mogelijk gevoelige gegevens om te gaan. Het gaat immers om persoonsgegevens, zoals IP-adressen, en om anderszins gevoelige gegevens. Het NCSC heeft in eerste instantie alleen de voor de respons noodzakelijke gegevens in ontvangst genomen. Daarna is overgegaan tot het uitvoeren van analyses voor de samenwerkende partijen. Daarbij zijn de gegevens in ontvangst genomen door de politie en aan het NCSC voor onderzoek ter beschikking gesteld. Dit is gebeurd op grond van artikel 19 van de Politiewet. Daarmee ontstond een wettelijke basis voor het verder bekijken van de data. In mijn brief van april heb ik aangekondigd dat ik de positie van het NCSC nader zal bekijken omdat ik absoluut niet wil dat er wordt opgetreden op basis van een niet-legale positie. Vanuit mijn positie kan dat ook niet. Er moet duidelijkheid zijn.
De heer Dijkhoff heeft ook gevraagd of ik in overleg ga met de internetserviceproviders. Ik vind dat de isp's een verantwoordelijkheid hebben jegens hun klanten. Laten we dat duidelijk vaststellen. Een belangrijk

gesubsidieerd initiatief, Abuse Information Exchange, is door de Minister van EZ genomen. In dit initiatief werken internetserviceproviders samen. Er wordt informatie uitgewisseld en samengewerkt op het punt van botnetbesmettingen. Op die manier worden besmette computers sneller opgemerkt en kunnen klanten beter en sneller worden geholpen. Ook ten aanzien van het informeren van klanten ben ik van mening dat isp's hun rol moeten nemen. Ik zal er via het centrum nog met hen overleg over voeren.
Mevrouw Gesthuizen vroeg waarom het NCSC geen onderzoek heeft gevraagd naar de gangen van Digital Investigation. Het centrum is geen verlengstuk van de opsporing. Laat dat duidelijk zijn. Dat moet ook niet. Het stuurt de opsporing dus ook niet aan.

De **voorzitter**: Ik gebruik de bel die nu luid klinkt om het voorzitterschap weer terug te geven aan mevrouw Jadnanansing.

Voorzitter: Jadnanansing

Minister **Opstelten**: Zoals ik al antwoordde op vragen van de heer Bontes: toen de informatie legaal was verkregen, heeft het centrum zijn coördinerende rol opgepakt.
Dan kom ik op het uitsluiten van de statelijke actoren bij Pobelka. Het botnet was er, net als de meeste botnets, op gericht om financiële transacties tijdens het internetbankieren te manipuleren en er op die manier voor te zorgen dat het geld uiteindelijk bij criminelen terechtkwam. Getroffen systemen en buitgemaakte gegevens zijn dermate divers dat er geen reden is om aan te nemen dat het botnet specifiek was gericht op specifieke overheden, sectoren, of organisaties. Uit een analyse van de AIVD is gebleken dat er geen sprake is van spionageactiviteiten. Uit een analyse van de MIVD zijn geen activiteiten gebleken die duiden op digitale spionage jegens het Ministerie van Defensie, de defensie-industrie of ten aanzien van een onderwerp met een militaire relevantie in het algemeen. Ik kom te spreken over het thema responsible disclosure.

De **voorzitter**: U hebt eerst een interruptie van de heer Verhoeven.

De heer **Verhoeven** (D66): Ik heb nog een vraag over Pobelka. De Minister heeft er een heleboel over gezegd en dat begrijp ik ook allemaal wel. Kan hij echter uitleggen hoe extra bevoegdheden of nieuwe bevoegdheden – die hij natuurlijk graag wil toekennen aan de verschillende spelers in de opsporingsketen – ervoor hadden kunnen zorgen dat het proces beter was verlopen? Volgens mij is er namelijk helemaal geen nieuwe bevoegdheid nodig om ervoor te zorgen dat bij een volgend botnet een en ander veel sneller wordt opgepakt door de verschillende betrokkenen bij de overheid.

Minister **Opstelten**: Politie en justitie nog bezig met het onderzoek. Dat wil ik even afwachten. Ik denk dat daar de bevoegdheden zijn. Het moet duidelijk zijn wat de bevoegdheid is van het NCSC om op het juiste moment de belangrijke providers te kunnen informeren, om IP-adressen te kunnen informeren en om met gezag dingen aan hen te kunnen vragen die nodig zijn als er sprake is van een situatie waarbij de nationale veiligheid in het geding is, bijvoorbeeld omdat het economisch verkeer kan worden verstoord. Dan moet er opgetreden kunnen worden als er partijen zijn die het niet doen. Het gaat hierbij om de proportionaliteit die ik tot nu toe voortdurend heb laten zien. In dergelijke gevallen moet er een centrum zijn dat een hoge kwaliteit heeft en in hoge mate wordt gesteund door Kamer en kabinet, dat op basis daarvan gezag ontwikkelt en dat een legale positie heeft. Een ander heel belangrijk punt in dezen betreft de verwerking van persoonsgegevens. Daar gaat het in de kern om. Het centrum moet altijd een legale positie hebben. Immers, met het in

ontvangst nemen van gevoelige data op eigen titel moet je heel secuur en juist omgaan, dat zal de heer Verhoeven volledig met mij eens zijn. Wat dat betreft reken ik op zijn steun, zodat de situatie goed verankerd is. Wij gaan daar verder aan werken.

De heer **Verhoeven** (D66): Het is altijd goed als de Minister rekent op onze steun, maar ik hoop dat hij zich niet te vroeg rijk rekent.

Minister **Opstelten**: Maar ik kan het proberen.

De heer **Verhoeven** (D66): Ja, dat is zo.

Minister **Opstelten**: Dan is dat alvast binnen.

De heer **Verhoeven** (D66): Laten we vaststellen dat dit een heel dappere poging was.

Minister **Opstelten**: Ik dank u zeer.

De heer **Verhoeven** (D66): Mijn vervolgvraag is van een andere orde. De Minister gaat in op de bevoegdheid van het NCSC richting de internetserviceproviders. Dat kan inderdaad een voorbeeld zijn van een bevoegdheid waar je in deze context over kunt praten. Ik doelde echter meer op de nieuwe bevoegdheden die de Minister, met enige bombarie en verwijzend naar DDos-aanvallen, zei nodig te hebben. Hij zei dat we echt nieuwe bevoegdheden nodig hebben om DDos aanvallen te keren. Maar ik denk dat Pobelka juist een voorbeeld was van een botnetaanval waarbij vooral heel veel misging in de coördinatie, bij het doorgeven van informatie en in de snelheid van de reacties. Er zijn geen nieuwe bevoegdheden voor nodig om het te versnellen. Daar zit de kern van mijn vraag. We hebben daar echt een goed antwoord van de Minister op nodig.

Minister **Opstelten**: Ik denk dat ik een heel goed antwoord heb gegeven, maar ik wil het nog wel een keer zeggen. Bij gevoelige informatie gaat om persoonsgegevens waarvan het niet de bedoeling is dat iedereen in Nederland en in de rest van de wereld die allemaal kent. In zo'n geval moet er iemand zijn die dat kan beschermen als daar in proportionaliteit aanleiding toe is. Daar gaat het om. Dat is in de kern de taak van het centrum. Daar ga ik mee werken. We zullen daar voorstellen over doen. De vragen die zijn gesteld over het NCSC zijn positief maar er wordt wel gevraagd of het niet sneller kan. Is er voldoende capaciteit en kwaliteit? Ik kom er nog op terug, maar het antwoord is: in de kern. Is er budget aanwezig? Ja, dat is aanwezig. Als ik deze dingen zeg, moet ik ze immers ook kunnen waarmaken met de middelen die we beschikbaar hebben. Dat is de prioriteitstelling binnen de beperkte mogelijkheden.
Ik kom te spreken over responsible disclosure. Zoals ik al eerder zei, juich ik de samenwerking met de ICT-community toe. Bij het uitwerken van het Kader voor Responsible Disclosure is dan ook met diverse partijen en potentiële melders gesproken. Hackers zijn in de kern, als zij kwade bedoelingen hebben, natuurlijk inbrekers. Er moet dus een scheiding worden gemaakt tussen hackers die te goeder trouw zijn en hackers die dat niet zijn. Dit heb ik altijd al gezegd en herhaal ik vandaag. Hackers dienen binnen de juridische kaders te vallen. Hierbij moet opgemerkt worden dat er binnen de overheid al ervaring is opgedaan met het werken met hackmethodes. Ik had twee jaar geleden niet kunnen vermoeden dat ik die nu ook een beetje zou kunnen hanteren. Ik heb het zien gebeuren, zo snel gaan die ontwikkelingen, ook bij mijzelf. Ik zie blikken van herkenning bij u allen, dus ik hoop dat u, als die methode wilt hanteren, dat te goeder trouw doet.

Informatie en kennis van hackers worden al door het NCSC gebruikt en zullen verder worden gebruikt. Als u daar op bezoek komt – een aantal van u heeft dat al gedaan – zult u daar ook in meegenomen worden; u bent gewaarschuwd. Een voorbeelden van verantwoord hacken is de praktijk van responsible disclosure, waarbij de hacker wacht met openbaarmaking van een beveiligingslek totdat dat lek is gedicht. Het centrum heeft reeds een rol als intermediair vervuld, om kennis van hackers bij bedrijven te adresseren. Het verkennen van de rol van hackers bij het op verantwoorde wijze inventariseren van kwetsbaarheden en het voorgenomen gebruik van de input van hackers, wordt het volgende beeld van Cyber Security Nederland. Een vraag daarbij is of ze bij de assessments een vraag naar hun inbreng en impulsen hanteren. Ook bij de totstandkoming van de leidraad is gesproken met diverse mensen uit de hackers community, inclusief welwillende hackers. Dat is heel goed, heel nodig en heel belangrijk.
Mevrouw Gesthuizen en de heer Verhoeven vragen hoe ik aankijk tegen strafrecht en responsible disclosure. Hier hebben we in een eerder AO al over gesproken. Indien er sprake is van computervredebreuk is het de afweging van de desbetreffende organisatie om al dan niet aangifte te doen. Het kan beleid van een organisatie zijn om onder bepaalde voorwaarden geen aangifte te doen. Vervolgens is het aan het OM om al dan niet te vervolgen. Het uiteindelijke oordeel is aan de rechter. Er zijn overigens geen gevallen bekend waarin het OM is overgegaan tot vervolging terwijl het betreffende bedrijf en de melder op basis van responsible disclosure met elkaar overeen waren gekomen dat er geen aangifte zou plaatsvinden. Ik ga er dus van uit dat dit de lijn is van het OM. In mijn brief van 3 januari jl. heb ik de Kamer laten weten dat ik met het OM in gesprek ga over de wijze van omgaan met responsible disclosure. Inmiddels heeft het OM deze handschoen opgepakt en de leidraad intern uitgedragen. Uitgangspunt van het OM zijn de volgende vragen. Was het handelen van de verdachte noodzakelijk binnen een democratische samenleving? Heeft de verdachte proportioneel gehandeld? Heeft de verdachte subsidiair gehandeld? Wanneer aan deze punten is voldaan, wordt het door het OM niet opportuun geacht om strafrechtelijk onderzoek te doen en vervolging in te stellen.
De heer Dijkhoff heeft nog gevraagd ...

De **voorzitter**: De heer Dijkhoff heeft eerst nog een vraag voor u.

De heer **Dijkhoff** (VVD): Ik hoop maar dat die niet dat onderdeel betreft. Kan de Minister bevestigen dat de richtlijn van het OM, die de Minister zojuist opsomde, ook geldt voor een ethische hacker, zonder dat het bedrijf met hem heeft gewerkt of zonder dat het bedrijf aan die richtlijn heeft voldaan? Is het zo dat als een bedrijf de kop in het zand steekt en niet mee werkt aan responsible disclosure, maar de ethisch hacker wel ethisch handelt volgens de richtlijn van het OM, het OM het ook dan niet opportuun acht om te vervolgen?

Minister **Opstelten**: Dat kan natuurlijk. Op zichzelf is het logisch dat dan ook aan deze drie criteria wordt voldaan. Maar als er grote maatschappelijke misstanden zijn ontstaan en veroorzaakt door deze hacker, ook al is het heel ethisch, dan zal daar toch naar gekeken kunnen worden. Ik kan dat niet uitsluiten.

De heer **Dijkhoff** (VVD): Dan begrijp ik dat er altijd een toets moet zijn. Daar ben ik ook voor. Je kunt niet zeggen dat we niet meer naar de zaak kijken als iemand zichzelf ethisch vindt. De richtlijn gaat echter uit van twee partijen die samen zeggen: je mag hacken. Wat nou als een bedrijf echt de kop in het zand steekt maar de hacker wel volgens de uitgangspunten van het OM, dus subsidiair, proportioneel en dergelijke, heeft

gehandeld? Zegt het OM dan ook: eigen richtlijn, niet opportuun om te vervolgen?

Minister **Opstelten**: Natuurlijk zal het OM die drie criteria van de richtlijn volgen. Maar er kan wel een afweging zijn. Ik zeg dat maar even voor alle duidelijkheid. Een ethisch hacker is echter een ethisch hacker.

Mevrouw **Oosenbrug** (PvdA): Ik wil daar een verduidelijkende vraag over stellen. Wat ik hoor is hetzelfde als waar ik me zorgen over maak: de vrijblijvendheid. Een bedrijf kan kiezen om zelf iemand te vragen om eens naar de systemen te kijken. Als een ethisch hacker vervolgens een kwetsbaarheid tegenkomt in de software of in het systeem en dat bedrijf is chagrijnig omdat die kwetsbaarheid is ontdekt, kan het dan besluiten om alsnog die ethisch hacker te vervolgen, die verder helemaal niets stuk maakt maar alleen het probleem aantoont? Kan hij in een dergelijk geval alsnog vervolgd worden ook al vindt het OM eigenlijk van niet? Ik ben echt op zoek naar bescherming voor de ethisch hacker. In de richtlijn lijkt het namelijk alsof de bedrijven heel erg beschermd zijn en de ethisch hackers helemaal niet.

Minister **Opstelten**: Nee, ze zijn allebei beschermd als ze maar met elkaar verstandige beslissingen nemen. Gelukkig is de samenleving zo ingericht. De ethisch hacker is niet altijd beschermd; ik herhaal het maar even, dan wordt het duidelijk. Er wordt bij de afweging gekeken naar drie uitgangspunten. Ten eerste. Was het handelen van de verdachte noodzakelijk binnen een democratische samenleving? Ten tweede. Heeft de verdachte bij zijn handelen proportioneel gehandeld? Dit zal altijd gelden, voor iedereen. Ten derde. Heeft de verdachte subsidiair gehandeld? Dit zijn de heel logische afwegingspunten van een magistratelijk opererend OM. Daar zit de bescherming dus in, rechtstatelijk.
Dan kom ik nog bij de heer Dijkhoff, die wil weten of de logica van deze leidraad ook wordt toegepast als bedrijven geen eigen beleid hebben. Ik herhaal het nog even, want dit is een punt waar je telkens heel goed over moet nadenken: ook dan kunnen partijen toch met elkaar in gesprek. Het NCSC treedt dan op als intermediair. Het OM heeft inmiddels bij de parketten aandacht gevraagd voor de leidraad. Het betreft een interne afweging. Het centrum kan er dus een intermediaire rol in spelen.
Mevrouw Gesthuizen vroeg of de rijksdienst genoeg capaciteit heeft. Ik heb daar al op geantwoord, maar ik wil het, nu zij er weer is, nog wel een keer zeggen. Ik heb geen aanwijzingen om te veronderstellen dat er onvoldoende capaciteit beschikbaar is. Ik ben in gesprek met mijn collega's om de responsible disclosure verder in te richten. Allereerst moeten wij natuurlijk in zijn algemeenheid over de capaciteit zeggen dat we twee jaar geleden niet wisten dat we nu zo veel capaciteit hiervoor zouden inzetten. Ten tweede wisten we ook niet dat we zo veel kwaliteit daarvoor zouden inzetten en ontwikkelen bij het OM, de politie, de overheid, de ondersteunende diensten, en bij het centrum. Dat wisten we toen niet, maar dat is nu wel het geval. We wisten ook niet dat er zo'n internationale situatie zou ontstaan, ondanks het Verdrag van de Raad van Europa dat er natuurlijk al jarenlang is. Dit gaat dus verder. Het is een kwestie van prioriteit binnen de aanwezige marges. Ik ben ervan overtuigd dat we de capaciteit beschikbaar zullen hebben en dat we niet zullen nalaten binnen te halen wat extra nodig is. Daar zijn ook goede afspraken over binnen het kabinet en met andere partners, ook binnen mijn departement.

Mevrouw **Gesthuizen** (SP): Nog even over die richtlijn. Er is kritiek. Ik begrijp dat de Minister zegt dat er uitvoerig overleg is geweest met de hackersgemeenschap alvorens de richtlijn werd opgesteld. Toch zijn er kritische geluiden te horen. Ik vraag de Minister in hoeverre er is voorzien

in een evaluatiemoment. Een van de critici is de journalist Brenno de Winter. Hij heeft de ov-chipkaart gehackt. Daarvoor zou hij in eerste instantie vervolgd worden. Hij haalt dit aan als voorbeeld van het feit dat het OM soms zelf onafhankelijk een eigen onderzoek start. Dan geldt die hele richtlijn niet meer. Ook in dat licht wil ik graag een evaluatiemoment afspreken waarop we dat alles in perspectief kunnen zetten en kunnen bezien in welke gevallen het goed heeft gefunctioneerd en in welke gevallen er op een wat ongelukkige manier is geopereerd.

Minister **Opstelten**: Ik heb natuurlijk al een paar dingen daarover gezegd, maar niet over de evaluatie. De hele wereld komt naar ons kijken omdat wij de eerste overheid zijn die een richtlijn heeft ontwikkeld. Ik denk dat een evaluatie vanzelfsprekend is, maar niet meteen. Men moet even de kans krijgen om de richtlijn verder te ontwikkelen. Het OM heeft er al op gereageerd, zoals ik zojuist uitvoerig heb bericht. Ik zou zeggen dat we een jaar of twee de kans moeten krijgen om het te ontwikkelen. Laten we nou verstandig zijn en niet iedereen die ermee bezig is, lastigvallen met allerlei onderzoeksvragen. De mensen die het doen, krijgen van mij nu de rust en volstrekt de ruimte als professionals om dit verder te ontwikkelen en te kijken hoe het gaat. Zullen we zeggen vanaf 1 januari 2014 twee jaar? Dan heeft men tweeënhalf jaar.

De **voorzitter**: Iedereen wil nu het woord, maar mevrouw Gesthuizen heeft het.

Mevrouw **Gesthuizen** (SP): Ik zat meer te denken vanaf 1 januari 2013. Laten we zeggen, twee jaar, zoals de Minister suggereert. Dan is het echter wel prettig om tussentijds, laten we zeggen na een jaar of anderhalf, een brief te krijgen met eventuele lichtpunten dan wel dieptepunten, zodat de Kamer wel op de hoogte is en een beetje de vinger aan de pols kan houden.

Minister **Opstelten**: Ja. Dat is monitoring, geen evaluatie. We kunnen gewoon per jaar monitoren. Dat lijkt mij een goede afspraak.
Dan kom ik bij de heer Bontes die, net als anderen, heeft gevraagd naar de uitvoering van de motie-Hennis-Plasschaert over een security breach notification. Het wetsvoorstel heeft betrekking op de invoering van een meldplicht bij het Nationaal Cyber Security Centrum (NCSC) voor bedrijven in de vitale sectoren, de financiële sector en de overheid, van inbreuken op de veiligheid of integriteit van de informatiesystemen waardoor de continuïteit van de dienstverlening wordt of kan worden onderbroken en maatschappelijke ontwrichting ontstaat of dreigt te ontstaan. In de lijn met mijn brief van 6 juli 2012 worden hierbij als vitale sectoren aangemerkt: drinkwater, gas, elektriciteit, telecom, keren en beheren van oppervlaktewater, transport en de mainports Schiphol en Rotterdam. De meldplicht geldt voor incidenten waardoor beschikbaarheid of betrouwbaarheid van een vitaal product of vitale dienst in belangrijke mate wordt of kan worden ... Hier is een onderbreking in mijn op zich tot nu toe heldere betoog. De zin is niet afgemaakt, maar ik zou daar een punt zetten.

(hilariteit)

Inmiddels wordt de laatste hand gelegd aan het wetsvoorstel. Het zal naar verwachting nog de komende maand ter consultatie worden aangeboden. Dat is snel.
Nu is mij duidelijk hoe het betoog moest worden vervolgd: ... wordt of kan worden onderbroken. Melding dient ingevolge het wetsvoorstel onverwijld bij het centrum te geschieden. Het wetsvoorstel zal meer in het bijzonder onder meer regelen wat de melding aan het centrum precies

moet omvatten en ingaan op de vertrouwelijke omgang met de melding. Dat is natuurlijk essentieel, want anders werkt het niet. Door deze meldplicht wordt het centrum beter in de gelegenheid gesteld om hulp te verlenen bij het zo snel mogelijk herstellen van de beschikbaarheid of betrouwbaarheid van getroffen vitale voorzieningen. Het wetsvoorstel bevindt zich op dit moment in de afrondende fase. De rest heb ik u al verteld.
De vraag is gesteld of er voldoende kennis is bij bedrijven om cybersecurity te herkennen en aan te pakken. Zeker, er is veel kennis en het is van belang om die nog verder te verbeteren. Onze mensen en mensen van het nationaal centrum treden ook op bij allerlei sessies met het bedrijfsleven om die kennis naar buiten te brengen. Awareness is natuurlijk heel belangrijk. Dit loopt allemaal via het nationaal centrum met campagnes, factsheets en presentaties. Tot en met april zijn meer dan 600 adviezen verstrekt. Er is een goede benadering via de brancheorganisaties, maar ook met organisaties als MKB Nederland en VNO-NCW.
Mevrouw Oosenburg heeft gevraagd naar de richtlijn. Op de website van de NCTV en het nationaal centrum is de Handreiking Cybercrime te vinden. Dit is een richtsnoer voor burgers en bedrijven hoe cybercrime kan worden herkend en welke stappen zij kunnen zetten, inclusief het doen van aangifte.
De heer Oskam vraagt wat ik vind van het idee van een ICT-risicokaart. Die is onderdeel van ons beleid. Wij zetten in op assets, threats and controls. Door middel van het CSBN wordt de dreiging inzichtelijk gemaakt. Daarnaast wordt inzicht geboden in kwetsbare plekken opdat maatregelen kunnen worden getroffen. Samen met private partijen werken wij aan tools om inzichtelijk te krijgen waar de zwakke plekken zijn.
Daarnaast is gevraagd naar de centrale rol van de NCTV en is de vraag gesteld of er voldoende capaciteit in huis is. Het nationaal centrum maakt onderdeel uit van de NCTV. Daarmee zijn meteen de structuur en de bevoegdheden aangegeven. De baas van het nationaal centrum is de nationaal coördinator. Het nationaal centrum is natuurlijk het centrale punt. De capaciteit wordt verder op- en uitgebouwd. In 2014 zal het nationaal centrum verder groeien.
Ook is gevraagd of er voldoende capaciteit en budget zijn voor het nationaal centrum maar ook voor het Team High Tech Crime Politie en de Informatiebeveiligingsdienst gemeenten. Ja, en wij breiden voortdurend uit. Voor de beveiligingsdienst bij de gemeenten is 2 miljoen per jaar uit het Gemeentefonds beschikbaar. Voor het Team High Tech Crime zal in 2013 nog eens een uitbreiding van 33 fte worden gerealiseerd. Het nationaal centrum krijgt in 2014 een versterking van 4 miljoen voor uitbreiding. Ik loop nu vooruit op Prinsjesdag. Het totale jaarbudget van het centrum is vanaf 2015 15 miljoen. Dit geeft natuurlijk niet aan hoeveel het kabinet op dit terrein uitgeeft.
De heer Bontes heeft gevraagd welke maatregelen ik neem om de bewustwording te vergroten. Ik heb al gesproken over Alert Online dat awarenessinitiatieven moet initiëren en samen brengen. Ik heb echter niet de illusie dat met een cybersecuritytiendaagse of een cybersecurityweek, hoe breed ingezet ook, Nederland opeens digitaal veilig is. Wij moeten doorgaan en samenwerken aan bewustzijn, kennis en gedrag om de maatschappij vaardig, veilig en secuur gebruik te kunnen laten maken van de digitale omgeving.
Ik ben het eens met de heer Verhoeven dat ieder in de eerste plaats verantwoordelijk is voor zijn eigen veiligheid en voor zijn eigen computer en digitale omgeving. Ik ben blij met de stappen die zijn gezet in het kader van Alert Online en de samenwerking die hierin gestalte heeft gekregen. Deze samenwerking voor cyberbewustzijn willen wij graag voortzetten met hopelijk nog meer bedrijven en organisaties die zich in 2013 willen aansluiten bij Alert Online.

De heer Oskam vraagt naar onze mening over speciale cybersecurityopleidingen. Opleiden is natuurlijk van cruciaal belang. Ik ben blij met het initiatief van de Cyber Security Academy. Onderwijs vormde al onderdeel van de cybersecuritystrategie. Het nationaal centrum werkt mee aan het opleidingsprogramma.
De heer Verhoeven heeft gevraagd hoe wij ervoor zorgen dat er betere preventie komt, omdat de huidige campagnes niet volstaan. Dat ben ik met hem eens. Burgers kunnen zelf stappen ondernemen om hun eigen ICT veilig te maken. Dat is natuurlijk het uitgangspunt. Daarnaast zullen awareness en preventie nog actiever via een publiek-private campagne van Alert Online ter hand worden genomen. Dat is een heel goed middel. Daarnaast wordt gebruikgemaakt van waarschuwingsdienst.nl en NCSC.NL. Op digibewust.nl zijn adviezen beschikbaar voor burgers en bedrijven om op eenvoudige wijze beschermingsmaatregelen te nemen.
De heer Oskam vroeg wanneer de spoorsector aan de beurt komt na alle cyberaanvallen. Incidenten kunnen nergens worden uitgesloten. Daarom hebben structurele acties voor vitale sectoren prioriteit.
Dan tot slot de internationale wetgeving waar de heer Oskam naar heeft gevraagd. Hij vraagt of in EU-verband genoeg wordt gedaan aan cybersecurity. De vraag is natuurlijk wat genoeg is. Nederland acht het huidige internationale juridische raamwerk wel voldoende. Het Boedapest cybercrimeverdrag van de Raad van Europa biedt goede mogelijkheden voor de aanpak van cybercrime. Ik acht het internationaal humanitair recht ook van toepassing op cyberspace. Ik acht het wel van belang dat landen gezamenlijk tot gedragsnormen voor cyberspace komen. Dit staat ook expliciet in de EU-cyberstrategie genoemd.
Er is natuurlijk naast overleg in de gremia van de EU, Verenigde Naties en Raad van Europa ook veel bilateraal overleg. Wij hebben bijvoorbeeld op dit punt veel contact met de Amerikaanse autoriteiten. In Europa is er verder een voorhoede van een aantal landen – Duitsland, Verenigd Koninkrijk, Zweden, Frankrijk en Nederland – die de trom slaat. Zij moeten ervoor zorgen dat de rest meegaat, maar zij mogen zich niet laten leiden door de langzaamste in het partnership.

De heer **Bontes** (PVV): De Minister zegt dat de wetgeving en de mogelijkheden op nationaal niveau toereikend zijn om dit het hoofd te kunnen bieden. De Europese Commissie is toch weer met allerlei dingen bezig, onder andere met een meldplicht voor bedrijven. Kan de Minister op de rem trappen bij de Commissie en haar vragen daarmee te stoppen, omdat wij het zelf aan kunnen?

Minister **Opstelten**: Als dat nodig is, zullen wij dat doen als er sprake is van een nationale bevoegdheid en een nationaal belang. Dit is heel precies werk en wij zullen goed volgen hoe dit loopt. Ik geef nu prioriteit aan onze activiteiten die ik zojuist heb genoemd. Ik vind wel dat wij internationaal moeten gaan werken. Wat nu op Europees niveau gebeurt, zal uitsluitend worden getoetst aan ons traject. Men komt nu met maatregelen die aansluiten bij ons traject; dan is het prettig dat je in de voorhoede zit. Wij kunnen daar alleen maar voordeel bij hebben. Dit komt naar de Kamer als er concrete voorstellen zijn. Het zal dan in een algemeen overleg over de JBZ Raad worden besproken. Alles zal keurig inzichtelijk worden gemaakt. Vertrekpunt is waar wij mee bezig zijn en Europa moet zich daarbij aansluiten. Dat lijkt mij ook verstandig voor de Europese dimensie.

De heer **Bontes** (PVV): De Europese bemoeienis is een belangrijk punt voor mijn fractie. Op tal van terreinen hebben wij al last gehad van wet op de remmende voorsprong, niet alleen met de digitale agenda, maar ook met de gaswetgeving. Ik vraag de Minister toch om Europa op dit gebied zo veel mogelijk buiten de deur te houden. Ik vraag hem duidelijk te

maken dat wij dit op nationaal niveau regelen, want in Brussel gaat men gewoon door.

Minister **Opstelten**: De Kamer krijgt het allemaal te zien. De heer Bontes kan zijn ogen niet sluiten voor het feit dat de digitale werkelijkheid niet ophoudt bij de landsgrenzen. Wij moeten daar dus ook voor openstaan met het oog op het nationaal belang. Ik zie nog geen digitale douanes.

De heer **Bontes** (PVV): Dat onderscheid maak ik nu juist. Je kunt samenwerken met andere landen en organisaties, maar dat is iets anders dan de Commissie de bevoegdheden geven om het op Europees niveau te regelen. Dat zijn echt twee werelden.

Minister **Opstelten**: Dat is iets anders. Wij zitten natuurlijk veel meer op de samenwerking, maar ik sluit niets uit, want als je iets uitsluit, doe je niet mee. Wij doen hier nadrukkelijk mee. Het signaal dat wij dit moeten volgen, is helder. De Europese ontwikkeling sluit aan bij onze eigen strategie en versterkt die.
De heer Bontes heeft nog gesproken over digitale spionage. Ik ken de berichtgeving uiteraard. Digitale spionage is absoluut een punt van zorg, ook in Nederland. Ik zet daar nog een streep onder. Het nationaal centrum waarschuwt partijen voor kwetsbaarheden en adviseert over te nemen maatregelen. Daarnaast is er de Kwetsbaarheidsanalyse spionage. Met deze toolkit worden bedrijven in vitale sectoren daarover geïnformeerd.

De heer **Verhoeven** (D66): Ik had al eerder een vraag willen stellen, maar de Minister gaat door als rustig stromend water en is soms lastig te onderbreken. Mijn vraag heeft betrekking op de meldplicht. Het kabinet wil die beperken tot vitale sectoren, want dat zijn blijkbaar de enige plekken waar inbraken van een dusdanig belang zijn dat het goed is om zaken te melden. Ik zou het omdraaien. Overal waar digitaal wordt ingebroken, is blijkbaar iets te halen. Dus waarom zou je tevoren een categorie uitsluiten als je veel beter kunt afgaan op de plaatsen waar wordt ingebroken? Waarom wordt niet gevraagd om altijd melding te doen als er wordt ingebroken? Als er fysiek wordt ingebroken, wordt er toch ook altijd een melding gemaakt? Dat blijft toch niet alleen beperkt tot banken of telecombedrijven? Dat moet iedereen doen. Waarom zou je vooraf sectoren uitsluiten terwijl je bedrijven niet met meer administratieve lasten of problemen opzadelt, omdat zij alleen hoeven te melden als er een inbraak is?

Minister **Opstelten**: Wij hebben hierover destijds een uitvoerig debat gevoerd. Het was een scherp inhoudelijk debat en toen is goed besproken wat wel en wat niet moet gebeuren. Het gaat natuurlijk om het effect. Toen is Kamerbreed de motie-Hennis-Plasschaert over de breach notification aangenomen. Je moet het zo doen dat mensen zich melden als het er toe doet. Daar hebben we een draagvlak voor gevonden bij het bedrijfsleven en dat wordt nu vertaald in de wet. Ik raad de leden aan die wet af te wachten. Ik ben er zelf heel positief over. Wij vervullen daarmee een voorhoederol, omdat wij niet de gemakkelijke weg kiezen: iedereen moet melden, dus niemand meldt zich. Het gaat het om het strategische niveau, het niveau waarop nationale items en de nationale veiligheid in de kern worden geraakt. Daar moet je kunnen optreden.
Verder kan er een melding worden gemaakt als er wordt ingebroken, dat kan nu al. De meldplicht kan in de toekomst eventueel worden uitgebreid. Het gaat om dringende zaken die echt impact hebben, ter voorkoming van maatschappelijke ontwrichting. Daarop hebben wij onze prioriteit en focus gericht. Het was een knappe motie. Dit was geen initiatief van de regering, maar wij hebben besloten dit in tempo in te brengen. Laten wij ons daarop richten en kijken hoe zich dit ontwikkelt.

Ik begrijp het punt van de heer Verhoeven heel goed. Als er wordt ingebroken, moet betrokkene natuurlijk naar de politie.

De heer **Verhoeven** (D66): Ik ben blij, maar ook niet geheel verrast dat de Minister zo content is met het wetsvoorstel van zijn Ministerie en met de motie die destijds is ingediend door de VVD-fractie. Alle complimenten daarvoor. Als wij toch nog gaan kijken naar verbetermogelijkheden en het wetsvoorstel moeten afwachten, dan wijs ik nog op het voorbeeld van Duitsland. Daar is een eenvoudig formulier voor de melding ontwikkeld. Ik neem aan dat de mensen van het Ministerie hiermee bekend zijn. Daar is inspiratie te halen. Nu steeds wordt geschermd met termen als «lastendruk» en moeilijk wordt gekeken als ook andere niet vitale bedrijven worden genoemd – dat is toch een beetje een VVD-reflex – is het misschien goed om te kijken of wij ook een simpel en snel formulier kunnen ontwerpen en dat breder inzetten.

Minister **Opstelten**: Ik dank de heer Verhoeven voor deze suggestie; wij nemen die mee. Als het niet bekend is, zullen wij daar in onze contacten met de Duitsers naar vragen.
De heer Oskam heeft gevraagd wat ik vind van de gedachte van een cyber non-proliferatieverdrag. Het is belangrijk dat internationaal wordt samengewerkt en dat afspraken worden gemaakt om de cyberdreiging in de wereld tegen te gaan. Daarvoor participeert Nederland in verschillende gremia op Europees en internationaal niveau. Wij hebben overleg op het niveau van de Raad van Europa, maar nog niet op het niveau van de Verenigde Naties. Dat zou er uiteindelijk van kunnen komen, maar het is bekend dat dit wel enige tijd in beslag neemt. Je moet op de gremia inzetten, maar ook bilateraal te werk gaan. Met de Verenigde Staten hebben wij een verdrag afgesproken. Wij zullen over en weer onze kennis inzetten, ervaringen delen en dat soort zaken.
Er is gesproken over de effecten van de bezuinigingen van de AIVD op de cybersecurity. De AIVD investeert in cyber. De dienst doet ongelooflijk actief mee en is zichtbaar op dat terrein. Dat is heel belangrijk, net als de MIVD heel belangrijk is. Ik ga niet in de schoenen staan van Minister Plasterk. Dat is al eerder besproken tijdens een algemeen overleg en ik laat dit aan hem. Ik bevestig echter dat de AIVD enorm actief is en veel professionaliteit heeft op dit terrein. Wij hebben daar veel aan. Cyber blijft prioriteit houden bij de AIVD.
Dan tot slot een vraag van mevrouw Gesthuizen. Zij heeft gevraagd of er liaisons van de Amerikaanse autoriteiten zijn bij het Team High Tech Crime. Er is één liaison van de US Secret Service en één van de FBI. Zij verrichten geen handelingen, maar versterken en bevorderen de internationale samenwerking en de uitwisseling van gedachten, kennis enzovoort.

De **voorzitter**: Ik dank de Minister voor de uitvoerige beantwoording. Er is nog gelegenheid voor een tweede termijn met een spreektijd van twee minuten en de mogelijkheid van één interruptie. Ik wijs erop dat de heer Oskam nu naar een andere vergadering moet.

De heer **Dijkhoff** (VVD): Voorzitter. Ik ben tevreden dat de Minister de stelling omarmt dat service providers een eigen verantwoordelijkheid hebben. Hij verwijst terecht naar het door het Ministerie van Economische Zaken gesubsidieerde project. Mijn punt is dat ik gaandeweg van het idee af wil dat een paar voortrekkers verantwoordelijkheid nemen en maatregelen ontwikkelen en dat het daarbij blijft. Op een gegeven moment moet er een einde komen aan een gesubsidieerd project. Die subsidie is nodig om het concurrentienadeel op te heffen dat die voortrekkers hebben doordat zij wel investeren in maatregelen als het waarschuwen van gebruikers die besmet zijn en het eventueel in quarantaine stellen daarvan

ter beveiliging van ons allen. In plaats van het opheffen van dat nadeel van mensen die hun verantwoordelijkheid nemen, moet iedereen standaard zijn eigen verantwoordelijkheid nemen. Ziet de Minister ook in dat het probleem inmiddels zo groot is, dat het, nu duidelijk is hoe het moet, tijd wordt om met alle partijen in de sector het gesprek aan te gaan om ervoor te zorgen dat zij dat allemaal goed doen? Dan ontstaat er een level playing field gecombineerd met verantwoordelijkheid en veiligheid.
Ik vraag ook nog aandacht voor het ethisch hacken. Het is mij nog niet duidelijk hoe het precies zit. Het hangt een beetje af van het antwoord dat wij kiezen. Laat ik voor alle duidelijkheid zeggen hoe ik het zie en ik hoop dat de Minister dan antwoordt dat hij het ook zo ziet. Natuurlijk verdient het de voorkeur dat een bedrijf en een hacker overleg plegen en samen de richtlijn aflopen en volgen. Het OM kan dan nog een check doen op grond van de eigen criteria, maar het zal er daarbij vanuit gaan dat het waarschijnlijk wel goed zit nu er overleg is gevoerd en overeenstemming is bereikt. Dan zijn er nog situaties waarin de hacker ethisch opereert maar bij het bedrijf een gesloten deur vindt. De handleiding in de brochure kan dan niet worden gevolgd doordat het bedrijf de kop in het zand steekt. Dan zou het OM ook op basis van de criteria die de Minister noemde – is dit nodig in de democratische rechtstaat en heeft de hacker de subsidiariteit en proportionaliteit in acht genomen – moeten beoordelen of het wel of niet tot vervolging overgaat. Het zou ook in dergelijke gevallen tot de conclusie moeten komen dat het niet opportuun is om tot vervolging over te gaan als de hacker die de misstand aankaart, voldoet aan de checklist van ethiek.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Allereerst dank aan de Minister voor zijn uitgebreide beantwoording. Ik meen in zijn antwoorden een toezegging te horen voor een brief over de positie van het Nationaal Cyber Security Centrum als spin in het web en over de vraag hoe het centrum meer body kan krijgen. Ik ben daar erg blij mee.
Wij verschillen nog wel van mening over responsible diclosure. Ik verwacht echter dat wij er wel achter zullen komen dat het handig is dat een hacker die iets ontdekt dat niet tevoren is afgesproken, goed beveiligd is. Ik zal op dit thema doorgaan.

De heer **Bontes** (PVV): Voorzitter. Ik dank de Minister voor de beantwoording van de vragen. De Minister heeft niet het lakse beeld kunnen wegnemen dat in de media is geschetst van de aanpak van het Pobelkabotnet. Wij wachten af of het de volgende keer beter gaat. De Minister heeft immers gezegd dat bij dit soort aanvallen voortdurend wordt gezocht naar verbeteringen van de aanpak.
Verder kijk ik uit naar de wetsvoorstellen van de Minister om deze misstanden te bestrijden.

De heer **Verhoeven** (D66): Voorzitter. Ik dank de Minister voor de antwoorden. Hij zegt dat de ontwikkelingen snel gaan. Ik wil hem complimenteren met het feit dat de ontwikkelingen de afgelopen twee jaar bij hem ook zo snel zijn gegaan. Dat is knap. Er is veel aandacht voor het onderwerp en er wordt langs veel verschillende lijnen gehandeld.
Voor ons is het kernpunt de relatie tussen de bestaande mogelijkheden en de nieuwe bevoegdheden. Wat kun je binnen de huidige kaders, worden die optimaal gebruikt, zijn er genoeg kennis en capaciteit om de mogelijkheden te gebruiken of moet er bij iedere nieuwe dreiging, groot of klein, direct naar grote middelen worden gegrepen en om nieuwe bevoegdheden worden gevraagd onder het mom dat de politie anders achter de feiten aanloopt? Mijn fractie kijkt daar heel kritisch naar en zal dat in de toekomst ook blijven doen.

Een verder punt van zorg is de vraag hoe dit praktisch zal uitpakken. Hoe kun je dit in kaders zetten en hoe kun je dit definiëren? Hoe zorg je voor dusdanig strakke kaders dat de invulling niet uit de hand loopt?
Waarom is er gekeken naar een mogelijke relatie met het Dorifelvirus bij het doorsturen van de Pobelka-dataset? Is dat om technische redenen gedaan of uit oogpunt van capaciteit?
Tot slot nog een opmerking over de responsible disclosure. Ik vind de intentie van de Minister en de manier waarop dit is opgezet goed, maar aan de kant van de bedrijven is inderdaad nog wel sprake van enige vrijblijvendheid. Als zij dingen niet zo prettig vinden om te horen, kunnen zij daar op hun manier mee omgaan. Ik ben het ermee eens dat je als je een interne richtlijn maakt zoals het OM dat doet, je daaraan moet houden. Dit moet dan echter wel worden geborgd en daarom ben ik blij met de toezegging voor een evaluatie na anderhalf jaar in plaats van de mogelijkheid tot creatief boekhouden na twee en een half jaar. Ik hoop dat wij dit scherp kunnen doen.

Mevrouw **Gesthuizen** (SP): Voorzitter. Ik dank de Minister voor zijn beantwoording. Ik heb helaas door de lange duur van de regeling van werkzaamheden een groot deel van het antwoord gemist. Ik heb via mijn medewerker echter het nodige gehoord.
Het is mij nog niet duidelijk of de Minister de mening deelt dat in de financiële sector te laat is gereageerd en dat men te laat in actie is gekomen. Is er sprake van verwijtbaarheid of een lakse houding? Het is goed mogelijk dat hierover in de toekomst wordt geprocedeerd. Het is dan aan de rechter, maar ik hoor nu graag van de Minister wat zijn oordeel is over het optreden van de banken.
Ik heb begrepen dat de Minister heeft gezegd dat is onderzocht of er statelijke actoren betrokken zijn geweest bij het stelen van zo veel gegevens. Ik herhaal dat de getroffen systemen en buitgemaakte gegevens dermate divers zijn dat er geen reden is te veronderstellen dat het botnet gericht was op specifieke overheidssectoren en organisaties. Op welke manier is onderzocht en vast komen te staan dat er geen statelijke actoren actief waren? Volgens mij heeft de Kamer dat inzicht nog niet gekregen. Ik heb mij laten informeren over de manier waarop wordt gewerkt door bijvoorbeeld de Chinezen of de Amerikanen bij de identificatie van de IP-adressen van belangrijke instellingen en bedrijven in belangrijke landen. De IP-adressen en poortnummers worden volcontinu en volautomatisch gescand. Op het moment dat nieuwe zero ID's van andere kwetsbaarheden in het systeem bekend worden en worden geregistreerd, worden die benut, wordt de systemen binnengedrongen en wordt alles leeg getrokken. Vervolgens worden die data opgeslagen, verzameld, geanalyseerd, gecategoriseerd en geprioriteerd. Ik wil de Minister best geloven, maar dan wil ik heel precies weten op welke wijze hij nu echt kan uitsluiten dat hier sprake is van statelijke actoren. Kan de Kamer daarover nadrukkelijk worden geïnformeerd?

Minister **Opstelten**: Voorzitter. Ik begin bij de twee vragen van de heer Dijkhoff. Ik begrijp zijn opmerking over de afhankelijkheid van een gesubsidieerd traject. Het gaat hier natuurlijk om verschillende burgers en bedrijven en om de relatie tussen bedrijven en de overheid. De vernieuwde cyberstrategie is een mooi moment om hierover te spreken. In het najaar kom ik uitgebreider terug op de rollen van burgers, bedrijven en overheid. Een ieder zal meer moeten doen. Ook de basisbeveiliging moet op orde zijn en eventuele verplichtingen daartoe zullen dan ook aan de orde komen. Ik kijk naar dergelijke nieuwe initiatieven. Ik vraag de heer Dijkhoff daar nog even op te wachten. De lijn die hij kiest, is terecht; er moet een level playing field zijn. Wij zullen dit nadrukkelijk bekijken en meenemen in onze strategie.

In antwoord op de opmerkingen over het ethisch hacken en de responsible disclosure het volgende. Het OM beslist zelf. Ik breng de interne richtlijn van het OM ter informatie aan de Kamer. Ik ben natuurlijk verantwoordelijk voor het OM, maar dit bepaalt het OM zelf. Ik neem aan dat de criteria uit de leidraad worden meegenomen om de proportionaliteit te beoordelen, ook als er geen beleid is. Jurisprudentie zal dit moeten bevestigen. Overigens is er nooit tot vervolging overgegaan als partijen akkoord waren. De vraag is natuurlijk ingegeven door de mogelijkheid dat partijen geen akkoord kunnen bereiken. Ik zal aan het OM overbrengen dat de Kamer ervan uitgaat dat ook in die situatie de interne richtlijn wordt gehanteerd.
Mevrouw Oosenbrug sprak over de toezegging voor een brief over de grondslag van het centrum. Die brief komt waarschijnlijk voor het reces bij de Kamer.
Ik kan aan de heer Verhoeven meegeven dat de twee punten die hij noemt, ook mijn vertrekpunt zijn. Je kunt natuurlijk voor een verschillende invulling kiezen. Daarom is het goed om elkaar scherp in de gaten te blijven houden. Ik vraag voortdurend wat met het bestaande instrumentarium kan worden bereikt opdat zo min mogelijk voor nieuw instrumentarium moet worden gekozen. Als er nieuw juridisch instrumentarium nodig is, moet keihard en onomstreden zijn dat dat noodzakelijk is om een bepaald doel te bereiken.
De organisaties moeten lean and mean zijn en over grote kwaliteiten beschikken om hun werk te doen. De taken moeten scherp en SMART zijn geformuleerd. Ik hoop dat wij elkaar daarin kunnen vinden.

De heer **Verhoeven** (D66): Ik was nog één vraag vergeten. Zal de Minister het internet monitoren met deep packet inspection?

Minister **Opstelten**: Het antwoord op die vraag is ja. Dit hoort bij het detectienetwerk.
Er is gevraagd naar de relatie met het Dorifelvirus. De eerste gedachte was aan een link met het lopend onderzoek. Toen dit niet het geval bleek te zijn, is nieuw onderzoek gestart.
De afspraak is dat er na twee jaar een evaluatie zal komen. Twee jaar is twee jaar en geen anderhalf of twee en een half jaar. Wij zullen dit jaarlijks monitoren. De Kamer wordt hierover geïnformeerd in de voortgangsrapportage over de Nationale Cyber Security Strategie. Dat is een mooi natuurlijk moment.
Ik ben al ingegaan op de opmerking van mevrouw Gesthuizen over het uitsluiten van statelijke actoren bij Pobelka, maar ik doe dit graag nog een keer. Het botnet was er – net als de meeste botnets – op gericht om financiële transacties tijdens het internetbankieren te manipuleren en er op die manier voor te zorgen dat het geld uiteindelijk bij criminelen terechtkomt. De getroffen systemen en buitgemaakte gegevens zijn dermate divers dat er geen reden is om aan te nemen dat het botnet was gericht op specifieke overheden, sectoren of organisaties. Uit de analyse van de AIVD is gebleken dat er geen sprake is van spionageactiviteiten. Uit een analyse van de MIVD zijn geen activiteiten gebleken die duiden op digitale spionage jegens het Ministerie van Defensie, de defensie-industrie of onderwerpen met een militaire relevantie in het algemeen.

Mevrouw **Gesthuizen** (SP): Als de Minister zegt dat er geen reden is om aan te nemen dat er statelijke actoren mee gemoeid zouden kunnen zijn, is dat iets anders dan dat hij dat volledig uitsluit. Nu begrijp ik dat de onderzoeken van de AIVD en de MIVD mogelijk geheel of gedeeltelijk vertrouwelijk zijn. Ik breng dit punt zo nadrukkelijk onder de aandacht omdat ik mij zorgen maak. Het zou naar mijn mening een onverstandige insteek zijn om het feit dat op deze manier gegevens zijn verzameld, als mogelijk belangrijkste punt te nemen voor de stelling dat er geen sprake

is van betrokkenheid van statelijke actoren. Naar mijn mening is er voldoende bekend over de manier waarop spionageactiviteiten heden ten dage plaatsvinden. Als dit zo is, zou ik mij erg veel zorgen maken over de informatiepositie van onze diensten in dezen. Daarom vraag ik nadrukkelijk hoe een en ander is onderzocht.

Minister **Opstelten**: Dat weet de Kamer natuurlijk als geen ander. Ik kan hier de conclusies van het onderzoek van de AIVD en de MIVD weergeven. Men heeft het goed en breed bekeken en dat heeft tot deze conclusies geleid. Het is altijd goed om heel gericht vragen te stellen, ook in relatie tot de diensten. Ik kan het natuurlijk nooit 100% uitsluiten – dat kan niemand in deze wereld – en garanderen kan ik het ook niet, maar dit is de beste informatie die wij hebben. Ik vertrouw daarop. In het cybersecuritybeeld dat ik voor het reces aan de Kamer stuur, zal hieraan specifiek aandacht worden besteed.

Mevrouw **Gesthuizen** (SP): Zou de Minister dit nog iets nader kunnen toelichten? Ontvangt de Kamer voor het reces informatie over een dreigingsbeeld?

Minister **Opstelten**: Nee, de Kamer ontvangt het Cyber Security Beeld Nederland-3 voor de zomer. Daarin wordt dit opgenomen.
Ik ben uitgebreid ingegaan op de positie van de banken. Ik ben van mening dat zij actief hebben geacteerd. Ik heb dit zo ervaren. Minister Dijsselbloem en ik hebben gesproken met de CEO's van de drie grote Nederlandse banken naar aanleiding van de laatste DDoS-acties bij de banken. In dat weekend hebben wij op topniveau zaken gedaan met elkaar en geacteerd. Minister Dijsselbloem en ik hebben de Kamer daarover geïnformeerd. De banken hebben nu een vaste liaison afgevaardigd naar het nationaal centrum. Dat is een stap. Dat wil zeggen dat zij daar niet alleen één meneer neerzetten, maar dat zij ook hun informatie beschikbaar stellen. Het is terecht dat zij dit doen, maar dit neemt niet weg dat dit een stap is die wijst op vertrouwen en goede samenwerking. Dit zijn goede ontwikkelingen.

De **voorzitter**: Hiermee is een einde gekomen aan de tweede termijn van de Minister.
Ik heb vier toezeggingen genoteerd.
- De Minister zegt toe over twee jaar een evaluatie aan de Kamer te sturen en de Kamer jaarlijks op de hoogte te stellen in de monitoringrapportage.
- De Kamer ontvangt voor het zomerreces een brief over de versterking van het Nationaal Cyber Security Centrum.
- In het najaar stuurt de Minister de Kamer een brief over de vernieuwde cyberstrategie waarin de rol van de verschillende actoren wordt meegenomen.
- De Kamer ontvangt voor de zomer een brief met informatie over het Cyber Security Beeld Nederland-3.

Ik dank de Minister, zijn ambtenaren, de mensen op de publieke tribune en uiteraard mijn collega's. Ik sluit de vergadering.

Sluiting 16.28 uur.