Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 265

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 15 januari 2013

De vaste commissie voor Veiligheid en Justitie heeft op 6 december 2012 overleg gevoerd met minister Opstelten van Veiligheid en Justitie over:

- **de brief van de minister van Veiligheid en Justitie d.d. 6 juli 2012 inzake de voortgang Nationale Cyber Security Strategie (26 643, nr. 24);**
- **de brief van de minister van Veiligheid en Justitie d.d. 6 juli 2012 inzake Cyber Security Beeld Nederland-2 (26 643, nr. 245);**
- **de brief van de minister van Veiligheid en Justitie d.d. 6 juli 2012 inzake meldplicht (security breach notification) en interventiemogelijkheden (26 643, nr. 247);**
- **de brief van de minister van Veiligheid en Justitie d.d. 1 oktober 2012 inzake kwetsbaarheid in Internet Explorer (26 643, nr. 255);**
- **de brief van de minister van Veiligheid en Justitie d.d. 9 juli 2012 inzake de evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis door de Inspectie Veiligheid & Justitie (26 643, nr. 250);**
- **de brief van de minister van Veiligheid en Justitie d.d. 14 augustus 2012 inzake het Dorifelvirus bij (overheids)instellingen (26 643, nr. 251);**
- **de brief van de minister van Veiligheid en Justitie d.d. 21 september 2012 houdende het verslag van een schriftelijk overleg over de brief inzake het Dorifelvirus bij (overheids)instellingen (26 643, nr. 253);**
- **de brief van de minister van Veiligheid en Justitie d.d. 15 oktober 2012 inzake wetgeving bestrijding cybercrime (28 684, nr. 363);**
- **de brief van de minister van Veiligheid en Justitie d.d. 12 november 2012 inzake crisisbeheersing in het digitale domein (26 643, nr. 258);**
- **de brief van de minister van Veiligheid en Justitie 19 november 2012 inzake het bilateraal verdrag voor onderzoek en technologie op het gebied van binnenlandse en civiele veiligheid (26 643, nr. 259).**

kst-26643-265
ISSN 0921 - 7371
's-Gravenhage 2013

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

Voorzitter: Elias
Griffier: Nava

Aanwezig zijn zeven leden der Kamer, te weten: Bontes, Dijkhoff, Elias, Gesthuizen, Oosenbrug, Oskam en Verhoeven,

en minister Opstelten van Veiligheid en Justitie, die vergezeld is van enkele ambtenaren van zijn ministerie.

Aanvang 16.00 uur

De **voorzitter**: Ik heet de bewindsman en zijn gevolg van harte welkom, evenals iedereen op de publieke tribune en degenen die ons anderszins, via moderne middelen, volgen. Welkom ook aan de collegaleden. Dit AO staat gepland van 16.00 uur tot 19.00 uur. Dat wil niet zeggen dat het niet eerder zou kunnen zijn afgelopen, maar in ieder geval mag het niet later. Als voorzitter moet ik tot mijn spijt vanaf ongeveer 16.45 uur verstek laten gaan om aanwezig te kunnen zijn bij een plenair debat. Mevrouw Gesthuizen is zo vriendelijk om dan de voorzittershamer over te nemen. Ik ga ervan uit dat zij dan ook al in eerste termijn zal hebben gesproken. De spreektijd is vijf minuten per spreker. Dat is een indicatie. Ik zal niet zeuren over tien seconden meer of minder. Uiteraard zijn interrupties toegestaan, maar laten we daarbij de klok een beetje in de gaten houden.

Mevrouw **Gesthuizen** (SP): Voorzitter. In dit digitale tijdperk kan ik bijna niet over de stapel stukken heenkijken die ik toch maar allemaal heb uitgeprint voor dit algemeen overleg. Er staat heel wat op de agenda, en dat is maar goed ook.
De minister verdient een compliment. Toen we ons ongeveer anderhalf jaar geleden in de DigiNotar-crisis bevonden, had ik stellig minder de indruk dat wij het in Nederland een beetje in de vingers kregen om iets te doen op het gebied van ICT en veiligheid. Ik heb me daarover ook in de bijna anderhalf jaar daarna nog ernstig zorgen gemaakt. Nu heb ik echter meer de indruk dat we de dreigingen zeer serieus nemen, dat we serieus bezig zijn om zaken op te tuigen en dat we waarde toekennen aan diegenen die er echt verstand van hebben en ons voor bepaalde zaken waarschuwen. Ik ben ongeveer twee weken geleden bij het NCSC op werkbezoek geweest, zoals de minister ook al weet, want ik heb dat gemeld bij de begrotingsbehandeling van Veiligheid en Justitie vorige week. Ik was zeer onder de indruk van het werk dat daar wordt gedaan. Daar zitten in ieder geval mensen die er echt verstand van hebben. Ik heb maar één kritische vraag over het NCSC. In de tijd van de DigiNotar-crisis heb ik steeds gepleit voor het instellen van een digitale brandweer. Is het NCSC op dit moment in staat om die rol van digitale brandweer te vervullen, ongeacht of het NCSC zelf dat zo zou noemen?
Ik wil nog wel de aandacht vestigen op een aantal andere zaken. Er wordt nogal wat opgezet aan clubs, overleggen, agenda's en allerlei actie-plannen. Soms krijg ik de indruk dat er, terecht, heel veel aandacht wordt gevraagd voor de mate waarin betrokkenen verstand hebben van crisisbeheersing. Dat is natuurlijk ontzettend belangrijk, maar zijn er bij dit soort processen ook voldoende mensen betrokken die echt verstand hebben van de technische zaken? Er wordt steeds gezegd, zoals ook in een vandaag verschenen interview met de heer Jacobs en door de experts die we hier hebben gehoord naar aanleiding van de DigiNotar-zaak, dat bestuurders te weinig luisteren naar de mensen die echt verstand hebben van de techniek. Dat was anderhalf jaar geleden zeker ook mijn indruk. Heeft de minister de indruk dat dit aan het veranderen is? Gaat dat snel genoeg?
Ik ga nu in op een aantal losse zaken die hier vandaag ter bespreking voorliggen. Mij is in het kader van het DigiNotar-onderzoek ter ore

gekomen dat het bestaan van een lek al een halfjaar voor de inbraak bekend was bij de overheid, althans dat daarvoor gewaarschuwd was. Er is toen niet ingegrepen, omdat de inschatting was dat het geen zaak was die de rijksoverheid zou raken. Is dat zo? Zo ja, waarom is dat dan niet meteen bij het bekend worden daarvan aan de Kamer gemeld?
In de stukken die we hebben gekregen, wordt gemeld dat het Nationaal Crisisplan ICT in de loop van 2012 wordt geactualiseerd. Is dat reeds gebeurd? Voorts wordt aangegeven dat er wordt gewerkt aan het opstellen van een agenda en dat er gesprekken zijn gevoerd met ICT-Office, Netelcom en het CIO Platform Nederland. Deze agenda wordt nu met publieke en private partijen uitgewerkt in het dit jaar gestarte programma Digivaardig & Digiveilig. Wanneer is dit allemaal klaar?
De minister meldt ook dat de EU naar verwachting nog dit jaar een EU-cyberstrategie zal presenteren. Is al bekend wat de richting van die strategie zal zijn? Kan de minister ons ook daarover informeren?
Ik kom nu op het misschien wel belangrijkste punt dat we vandaag moeten bespreken. Ik zie dat ik daarvoor nog maar een minuut de tijd heb. Het gaat over de «hackbrief» oftewel «decryptiebrief» die de minister ons heeft gestuurd. Ik noemde zojuist al even de wetenschapper Bart Jacobs, maar ook anderen hebben kritisch gereageerd op de plannen van de minister. De minister is jurist, dus hij heeft vast ook het artikel Policeware in het NJB gelezen. Jacobs legt daarin heel precies de vinger op een aantal zaken. Hij waarschuwt onder andere voor het overnemen van een computer. Het is mij overigens nog niet helemaal duidelijk wanneer iemand dusdanig verdacht is dat zijn computer daadwerkelijk door de politie mag worden gehackt of wanneer daarop software mag worden achtergelaten. Jacobs zegt: als de computer van iemand op die manier wordt overgenomen, dan ontkom je er niet aan dat je tegelijkertijd ook aan het schrijven bent. Dat is ook mijn voornaamste zorg bij alle plannen die de minister heeft gelanceerd voor het hacken van computers van verdachten. Het internationale aspect noem ik straks nog even heel kort. Hoe kijkt de minister tegen dit punt aan? Ik ga ervan uit dat hij het artikel van deze wetenschapper heeft gelezen. Kan hij in den brede reageren op de kritiekpunten die Jacobs daarin aandraagt?
Niet alleen Jacobs maar ook Bits of Freedom heeft op nog een ander punt kritiek. Die komt op het volgende neer. Het kan Nederland duur komen te staan als we, op de manier zoals de minister nu van plan lijkt te zijn, zonder toestemming van de desbetreffende autoriteiten gaan infiltreren in systemen die niet op Nederlands grondgebied staan en daarmee de internationale normen overschrijden. Wat is daarop de reactie van de minister?

De heer **Oskam** (CDA): Voorzitter. Ook wij hebben een aantal kritische vragen aan de minister. De minister wil politie en justitie de bevoegdheid geven om in te breken in computers teneinde daarop spionagesoftware te installeren. Verder moet de politie op afstand informatie uit computers en digitale netwerken kunnen kopiëren, vernietigen of ontoegankelijk maken. De politie moet ook netwerken en servers in het buitenland kunnen doorzoeken.
Als onduidelijk is aan wie een verzoek om rechtshulp in zo'n geval moet worden gedaan, dan moet het maar zonder zo'n verzoek, zo zei de minister. Dat is nogal wat. Gelukkig beseft de minister dat zelf ook. Hij schrijft dat dit soort bevoegdheden strikt ingekaderd moet worden en dat er alleen ruimte voor is bij speciale misdrijven van een zekere ernst. Het CDA heeft daar vragen bij. De regel dat je om rechtshulp vraagt voordat je op vreemd grondgebied iets gaat doen, bijvoorbeeld opsporingshandelingen verrichten, is er natuurlijk niet voor niets. Een dergelijke regel is wederkerig. De Nederlandse justitie verricht niet zomaar een huiszoeking in Frankrijk en de Franse undercoveragent kan niet zomaar, zonder toestemming en instemming van de minister, in Nederland aan het werk.

Wat zijn de gevolgen als we die wederkerigheid opzeggen of aan onze laars lappen? Krijgen we dan ook de Chinese inlichtingendienst in Nederland over de vloer, die dan in computers gaat neuzen?
Als ik de minister goed begrijp, is het eigenlijk al bestaande praktijk dat justitie in computers neust zonder te weten waar de server staat. Zo heeft de politie al eens afbeeldingen van kinderporno vernietigd en ontoegankelijk gemaakt zonder de exacte locatie van de server te kennen.
Misschien maakt dit voorbeeld wel duidelijk dat de voorstellen van de minister gewoon nodig zijn. Als we digitale misdrijven willen bestrijden, en dat willen we, dan moeten politie en justitie voldoende armslag, voldoende bevoegdheden hebben. Bij moderne misdaad horen moderne opsporingsbevoegdheden. We hebben wel wat aarzelingen. Het leven van de moderne mens speelt zich voor een groot deel af in de digitale wereld, maar ik lees in de brief van de minister weinig over de zorgen betreffende de onlineprivacy. De minister schrijft over een voorafgaande machtiging van de rechter-commissaris, maar waar moet deze precies aan toetsen? Hoe gaat de minister waarborgen dat de rechter-commissaris heel nauwkeurig kijkt naar de noodzaak, proportionaliteit en effectiviteit? Ik wijs erop dat Nederland bovenaan staat in het lijstje van landen die veel telefoons aftappen.
Ik wijs verder op de motie (31 051, letter D) van mijn partijgenoot Franken in de Eerste Kamer, een motie die daar Kamerbreed is aangenomen. In de motie wordt de regering verzocht om privacybeperkende voorstellen te toetsen aan vijf strenge criteria. Waarom heeft de minister in zijn brief met geen woord over deze motie gerept? Is hij van plan om deze motie te hanteren bij de ontwikkeling van zijn plannen? Hij schrijft dat hij zijn voorstellen nu wil gaan uitwerken, maar hij heeft het met geen woord over burgerrechten of privacyorganisaties, zoals het CBP, het College bescherming persoonsgegevens. Mag ik aannemen dat de minister ook dit soort organisaties zal raadplegen? Is hij bereid om een stevig privacy impact assessment uit te voeren?
Ik kom nu op een vraag over de kennis die nodig is voor het bestrijden van cybercrime. Mijn collega Gesthuizen refereerde al aan wat de heer Jacobs, hoogleraar aan de Radboud Universiteit, heeft aangegeven. Hij wees erop dat bij plaatsing en gebruik van policeware de rechter-commissaris de broncode daarvan zou moeten kunnen terugkijken en begrijpen. De rechter-commissaris zou er bovendien van overtuigd moeten zijn dat precies die broncode en geen andere bij de infiltratie wordt gebruikt. Ook wijst Jacobs erop dat het plaatsen van policesoftware op een computer zeer specifieke kennis vereist. Hoe gaat de minister zorgen voor de nodige kunde op dit terrein?
Jacobs schrijft ook dat met policeware iemands identiteit volledig kan worden overgenomen. Hij wijst op het risico dat verdachten die worden blootgesteld aan de nieuwe opsporingsmiddelen, zullen beweren dat eventuele belastende informatie door de politie zelf is gecreëerd en op de computer is geplaatst. Ook hierop krijg ik graag een reactie van de minister.
Omdat cybercrime zich niet aan grenzen houdt, is ook internationale samenwerking essentieel. Hoe verloopt de samenwerking met andere landen? Hoe gaan die de digitale dreiging te lijf? Kan de minister meer zeggen over het Europese verband waarin hij opereert? Doen we aan onderzoek, kennisopbouw en uitwisseling van best practices?
Ik rond af. Ik vraag aandacht voor de website www.alertonline.nl. Deze website van de Nationaal Coördinator Terrorismebestrijding en Veiligheid is gelanceerd om burgers en bedrijfsleven attent te maken op cybersecurity. De site ziet er buitengewoon knullig uit, moet ik zeggen. Ja, lach maar, maar ook het CDA gebruikt tegenwoordig ferme taal.

De **voorzitter**: Dat woordje «tegenwoordig» glipte er even uit.

De heer **Oskam** (CDA): Precies. U houdt me wel scherp, voorzitter. De site is ouderwets. Ik heb me laten informeren door een kenner. Men heeft op cio-gebied grove steken laten vallen. Qua vindbaarheid is het niet goed geregeld. De site is niet schaalbaar voor smartphones en andere mobiele apparaten, terwijl de helft van het internetbezoek tegenwoordig daarmee plaatsvindt. Daar zou dus iets aan moeten gebeuren. De site maakt gebruik van iframes, wat al jaren not done schijnt te zijn. Verder is door het ontwerp de tekst slecht leesbaar. Met dit soort sites gaan we de cyber security war in ieder geval niet winnen. Kan de minister daar nog eens naar laten kijken?

Mevrouw **Oosenbrug** (PvdA): Voorzitter. «Teach your childeren well», zongen Crosby, Stills, Nash & Young al in de jaren zeventig. Juist in deze tijd, waarin communicatie steeds meer via digitale wegen loopt, lijkt dit thema urgenter dan ooit. Vandaag hebben we het onder andere over cybersecurity. Hoe richt je een veilige digitale omgeving in voor jong en oud? Hoe ga je om met alle kansen die het internet biedt? Ik denk dat je er zo vroeg mogelijk mee moet beginnen. Leer kinderen hoe ze moeten omgaan met het internet en hoe ze informatie kunnen vinden, maar wees daarnaast niet te angstig om hen ook op de gevaren te wijzen. Voorbeelden van misbruik zijn er helaas ook. Ook jongeren doen soms dingen op internet die strafbaar zijn, zonder dat ze dat doorhebben. De technische kennis is er wel, maar de ethische kennis niet. De samenleving wordt steeds afhankelijker van informatietechnologie. Naast alle kansen die het internet biedt, neemt het aantal bedreigingen ook toe. Een van de kenmerken van communicatienetwerken is dat ze zich niets aantrekken van grenzen, terwijl ons rechtssysteem nog wel grotendeels is gebaseerd op nationale autonomie. Computercriminelen maken daarvan handig gebruik. Ze plaatsen hun systemen in landen waarmee moeilijk tot samenwerking te komen is, of ze weten te versluieren waar het systeem zich fysiek bevindt. De samenleving roept om het aanpakken van creditcardfraudeurs, verspreiders van kinderporno en de eindeloze reeks spamberichten. Diezelfde samenleving maakt zich daarnaast uiteraard ook zorgen over de inbreuk op de privacy, de vrijheid op het internet en de wens om gegevens anoniem of versleuteld te kunnen blijven versturen. De minister stelt in zijn brief voor om van afstand een computer binnen te dringen, te hacken dus, al dan niet met behulp van software die op afstand op de computer wordt geïnstalleerd. Waaraan moet ik denken? Gaat het dan om een virus of om malware? En wie is verantwoordelijk als deze software voor andere kwetsbaarheden zorgt op de gehackte computer? In NRC Handelsblad van vandaag lees ik dat ik niet de enige ben die zich deze dingen afvraagt. Ook de adviseurs en experts van de minister delen mijn zorg. Ik krijg hierop graag een reactie van de minister. Ik begrijp de behoefte van politie en justitie om over meer digitale wettelijke mogelijkheden te beschikken, maar het doel moet wel in verhouding blijven staan tot de middelen. Nederland is qua aantal telefoontaps koploper, maar de effectiviteit ervan is nog steeds niet gebleken. Welke garantie kan de minister mij geven dat hetzelfde patroon niet ontstaat bij de computertaps? Ik krijg graag een uitgebreidere toelichting van de minister, waarin nut en noodzaak worden onderbouwd. In Nederland is veel expertise aanwezig binnen de wereld van hackers en beveiligingsexperts. Een aantal van deze specialisten gaat zelf op zoek naar veiligheidslekken, meldt deze bij de instantie en geeft haar de tijd om de kwetsbaarheid te verhelpen voordat de openbaarheid wordt gezocht. Bedrijven die cyberaanvallen melden, moeten ervan uit kunnen gaan dat de gegevens die ze verstrekken, vertrouwelijk worden behandeld. Wel vind ik het belangrijk dat burgers worden geïnformeerd als hun informatie mogelijk is gestolen. Ik vraag de minister om aandacht voor dit punt. Gezien de berichtgeving over de diverse hacks in ziekenhuisdossiers maak ik me zorgen over de beveiliging van patiëntendossiers enerzijds en de

positie van hackers anderzijds. Ethische hackers zijn een van de antwoorden op de vraag hoe om te gaan met cybersecurity, maar dan moet wel duidelijk zijn waar de grens ligt tussen het zoeken naar kwetsbaarheden en het daadwerkelijk inbreken op een systeem. Is er inmiddels een kader geformuleerd, zoals eerder toegezegd door de minister?
Ik sluit af met het pleidooi om als overheid het goede voorbeeld te geven en ethische hackers in te schakelen om overheidssystemen veilig te maken en veilig te houden. Anders gezegd: teach your children well.

De **voorzitter**: Ik ben nog maar heel kort ondervoorzitter, dus ik weet niet zeker of ik iets heb gemist. Was dit uw eerste inbreng in een AO?

Mevrouw **Oosenbrug** (PvdA): Ja.

De **voorzitter**: Dan feliciteer ik u daar van harte mee.

De heer **Verhoeven** (D66): Mag ik een vraag stellen?

De **voorzitter**: Ja, dat mag.

De heer **Verhoeven** (D66): Mevrouw Oosenbrug van de PvdA zegt dat ze twijfelt over de balans tussen het probleem en de oplossing die de minister nu kiest. Ze stelt daarover een aantal vragen en geeft daarover een aantal overwegingen. Ik ben benieuwd naar de antwoorden van de minister. Ik ben echter ook benieuwd naar het antwoord van de PvdA zelf. Gaan deze plannen niet heel ver?

Mevrouw **Oosenbrug** (PvdA): Bedoelt u de plannen van de minister?

De heer **Verhoeven** (D66): Ja.

Mevrouw **Oosenbrug** (PvdA): Ik ben daar in mijn inbreng heel duidelijk over geweest. Eerst wil ik weten wat nut en noodzaak van dit verhaal zijn. Aan de ene kant wil de maatschappij dat kinderporno wordt aangepakt, dat creditcardfraudeurs worden aangepakt en dat spam stopt. Aan de andere kant wil diezelfde gemeenschap niets inleveren qua vrijheid. Ik vraag me af waar de balans is. Ik ben op zoek naar die balans.

De heer **Verhoeven** (D66): Moet die balans volledig komen uit de antwoorden van de minister of heeft de PvdA daar zelf ook een opvatting over naar aanleiding van de brief van de minister? Hoever mag het van mevrouw Oosenbrug gaan? Ik ben daar wel benieuwd naar.

Mevrouw **Oosenbrug** (PvdA): Daar zijn wij naar op zoek. Ik ben benieuwd naar de antwoorden van de minister, sowieso op een aantal punten. De vraag is bijvoorbeeld hoe het technisch haalbaar is. Dat is al een probleem. En ís het wel mogelijk? Een andere vraag is of je maatschappelijk draagvlak kunt vinden. Ook de PvdA is daarnaar op zoek.

De **voorzitter**: In zijn algemeenheid zou ik, als uw voorzitter, willen zeggen dat een algemeen overleg er ook toe strekt om de oordeelsvorming te scherpen. Daar moet je niet met alleen maar een afgerond standpunt ingaan. De een kan dat al wel hebben en de ander kan dat ontwikkelen. Ik vind het dus niet zo'n probleem.

De heer **Verhoeven** (D66): Dank voor deze suggestie over het voeren van een debat. Ik zal die zeer ter harte nemen. Ik ben er ook dankbaar voor. Toch zijn er wel plannen denkbaar, zeker van dit kabinet, waarover ik vrij

vooringenomen ben. Ik zal in mijn bijdrage straks bekijken hoe vooringenomen ik vandaag ben.

De **voorzitter**: Ieder zijn eigen smaak.

De heer **Dijkhoff** (VVD): Voorzitter. Cybersecurity is van groot belang. Het Nationaal Crisisplan ICT dat we hebben mogen ontvangen, geeft dat treffend aan. De samenleving is steeds afhankelijker van ICT. Er zijn eigenlijk geen werkbare alternatieven meer. Als de ICT-netwerken platliggen, ligt heel Nederland plat. We hebben ook een nieuwe versie van het Cyber Security Beeld Nederland gekregen. Dat is een breder beeld. Dank daarvoor. Het is nuttig om als basis te gebruiken bij de vraag waar we aan moeten werken. Dat is veel. Kort samengevat: digitale spionage en cybercrime zijn het grootste probleem en overheid, burger en bedrijven zijn het kwetsbaarst. Oftewel, iedereen is kwetsbaar op zowat alles. Dat is niet alleen een zaak van de overheid. Het vraagt ook bewustzijn van iedere Nederlander. Ik kom hierop later nog terug. Het is alsof we wel onze fiets op slot zetten, maar al onze privégegevens op de computer nog erg open laten voor iedereen die er kwaad mee wil.
Het Nationaal Cyber Security Centrum loopt. Het ziet er goed uit. Dat is een cruciale factor. We zijn er echter nog niet. De VVD wil het goede begin een goed vervolg geven, allereerst met het voorstel van een meldplicht. Ik verwacht dat het wetsvoorstel snel komt. Het was aangekondigd voor dit kalenderjaar. Heeft de minister al zicht op het moment waarop het naar de Kamer komt? Ik wil het echter breder trekken dan alleen de meldplicht voor vitale sectoren. De private sector valt daar niet onder. Dat lijkt me verstandig, omdat het vaak om bedrijfsgevoelige informatie gaat. Samenwerking met de private sector, breder dan alleen de vitale sectoren, is echter wel cruciaal, omdat daar veel informatie is die ook van belang is voor een goed cybersecuritybeeld. Hoe ziet de minister intensivering van die samenwerking voor zich? Enerzijds moeten bedrijven erop kunnen vertrouwen dat hun vuile was niet op straat ligt en dat de bedrijfsgevoelige informatie vertrouwelijk blijft. Anderzijds moeten we goed omgaan met die kennis, zodat we die kunnen gebruiken om Nederland veiliger te maken.
De minister heeft het ook over een Europese meldplicht. Wat moet ik daaronder verstaan? Het is prima om op abstract niveau de informatie en de ervaringen te delen met andere landen, zodat we daardoor sterker worden. Storingen in Nederlandse vitale belangen hoeven echter niet meteen een-op-een heel Europa rond te gaan.
Dit is allemaal wel achterafgepraat, na een storing, die dan gemeld is. Maar hoe voorkomen we het? Hoe sporen we het op? Bij terrorisme hebben we dreigingsbeelden. Gaan we daar ook naartoe bij cybersecurity? Wordt daar door het centrum aan gewerkt? Leren we ook van wat we tegenkomen en vangen? Bij virussen en hacks is sprake van een doorontwikkeling. Is er nu voldoende capaciteit en kunde voorhanden om ontwikkelingspatronen te doorgronden en zo ook de preventie te kunnen steunen? Preventie is immers altijd beter dan achteraf iets fiksen.
Bij ouderwetse rampen is de dreiging duidelijk en zijn mensen zich heel bewust van het gevaar. Dat kwam niet in alle gevallen vanzelf. Er was naar ik meen een tijd dat voor een ramp met een kerncentrale de waarschuwing gold om met de handen boven het hoofd onder het bureau te kruipen. Ook daarvoor is er een lang proces van voorlichting geweest en heeft men geprobeerd de impact zichtbaar te maken door simulaties en rampenoefeningen. Is dit ook het plan voor cybersecurity? Dat zou dan niet alleen bij betrokken instanties, technisch vanachter het bureau, moeten gebeuren, maar ook wat levendiger, met burgers en bedrijven, zodat zichtbaar wordt wat de gevolgen kunnen zijn en iedereen voelt

welke verantwoordelijkheid hij zelf draagt. Aangezien netwerken zich niet aan grenzen houden, is de vraag of dit niet ook samen met andere landen kan.
De heer Oskam zei het al: de nieuwe misdaad vereist nieuwe manieren van opsporing en dus moeten politie en recherche met de tijd mee kunnen gaan. De VVD is erg blij met de High Tech Crime Unit, maar die vormt wel een voorhoede. Bewustzijn en kennis van alles wat er online gebeurt, is van belang voor het hele politieapparaat. Criminaliteit online is geen tijdelijk fenomeen en evenmin een aparte tak. Als de samenleving steeds meer permanent online is, dan zal de criminaliteit dat ook worden. Als de techniek ons hele leven makkelijker maakt, dan zal ze dat helaas ook voor criminelen doen. Hoe is het met de balans? Is er genoeg kennis bij de politie in den brede? Hebben we nu genoeg cyberrechercheurs? Heeft de minister voor ogen om een deel van de 150 miljoen intensivering hiervoor in te zetten? Ook niet onbelangrijk is de vraag hoe de samenwerking met andere ministeries is, vooral met Economische Zaken en met Defensie. Lukt het om goede medewerking te krijgen of is er nog sprake van verkokering?
Er is voorgesteld om de opsporingsbevoegdheden te verruimen. De VVD staat in principe welwillend tegenover middelen die helpen in de bestrijding van criminaliteit, offline en online. Het is wel van belang dat er genoeg waarborgen zijn voor personen die niets kwaads doen, en dat de middelen effectief zijn in de praktijk. De door de minister ingediende wetsvoorstellen gaan over verruiming van de opsporingsbevoegdheden. Dat is niet gek, want de desbetreffende artikelen uit het Wetboek van Strafvordering zijn wel aan modernisering toe. Ze zijn nog net niet met de ganzenveer geschreven, maar ik heb ook niet de indruk dat er al veel onlinekennis was toen die wet werd gemaakt. De VVD is niet van plan om de politie toestemming te geven om zomaar in een computer een dagboek te lezen, maar wil ook niet accepteren dat een terrorist of crimineel de politie lachend aankijkt, terwijl elke minuut van zwijgen de kans verkleint dat hij zijn verdiende straf krijgt.
De voorstellen zijn fraai omschreven. Daarover is veel gezegd. Er is echter wel een vraagteken bij de effectiviteit in het geval van grensoverschrijding. Als eerste reactie zou je kunnen zeggen: als de politie een verwerpelijke of gevaarlijke daad opspoort, ongeacht waar het is, zorg er dan voor dat je de dader niet kwijtraakt. Er is echter een keerzijde: andere landen zouden dat ook kunnen doen. We hebben ons in het verleden zorgen gemaakt over wat de Amerikanen op basis van de Patriot Act met gegevens in Nederland zouden kunnen. Wat gaan wij zeggen als wij ons die bevoegdheid toe-eigenen en Iran vervolgens de computer van een e-boekverkoper wipet omdat Rushdie in het assortiment zit?

De **voorzitter**: Kunt u afronden?

De heer **Dijkhoff** (VVD): Dat zal ik proberen.

De **voorzitter**: Nee, u moet het doen. U bent al flink over uw tijd heen.

De heer **Dijkhoff** (VVD): If you can't beat them, join them. Dat is voor de VVD echt een laatste redmiddel. Ziet de minister nog mogelijkheden in het op andere terreinen samenwerken met andere landen? Over het decryptiebevel kan ik misschien nog wat zeggen als een collega daarover een interruptie pleegt.

De **voorzitter**: Hier is geen kruid tegen gewassen.

De heer **Bontes** (PVV): De heer Dijkhoff maakte een paar kritische opmerkingen, met name over het risico dat andere landen terughacken, maar ook over het plaatsen van spyware in computers. Waar staat de VVD

wat dat betreft, zoals de plannen er nu voorliggen? Kan de heer Dijkhoff daarmee instemmen?

De heer **Dijkhoff** (VVD): Er liggen geen wetsvoorstellen voor, dus daar valt niet mee in te stemmen. Op basis van de plannen kan ik het volgende zeggen. Ik ben er niet op tegen dat de politie dat doet. Als je iemand opspoort en achtervolgt, dan mag je ook te hard rijden. We moeten dus niet roomser zijn dan de paus. We moeten ook niet met het woord «privacy» de hele discussie doodslaan. Het is meer: wat u niet wilt dat u geschiedt, doe dat ook een ander niet. Ik maak me wel een beetje zorgen. Als we ons deze bevoegdheid toe-eigenen, wat uiteindelijk misschien kan als er geen goede internationale afspraken te maken zijn, dan hebben we geen poot meer om op te staan als andere landen het bij ons doen. Als we bijvoorbeeld zouden lezen dat Iran zich morgen de bevoegdheid toe-eigent om onwelgevallige teksten in Nederland te wipen, dan zou de PVV vooraan staan om daarop kritiek te leveren.

De **voorzitter**: De heer Bontes wil daarop nog wel iets terugzeggen, denk ik.

De heer **Bontes** (PVV): We zitten inderdaad niet in de plenaire zaal om over wetsvoorstellen te stemmen. Ik merk wel dat de heer Dijkhoff kritisch is op de lijn. Mag de minister van de heer Dijkhoff deze lijn uitwerken?

De heer **Dijkhoff** (VVD): Natuurlijk mag de minister deze lijn uitwerken. Daarom ben ik ook blij dat we nu alvast wat kanttekeningen kunnen meegeven. Het zou mooi zijn als we ook kunnen zien hoe dit internationaal zit, hoe andere landen ertegen aankijken. Iedereen worstelt hiermee. Bij de Patriot Act hebben we ook de omgekeerde situatie meegemaakt. We vonden toen dat de Amerikanen wat te vrijpostig waren. Als iedereen ermee worstelt, wil ook iedereen graag een oplossing, internationaal gezien. Dat heeft natuurlijk wel de voorkeur.

Mevrouw **Gesthuizen** (SP): Ik wil aan de VVD-fractie best iets vragen over decryptie, maar dan wel op mijn eigen manier. Omdat het verplicht meewerken aan het ontsleutelen van je eigen gegevens zeker geen wondermiddel is – de minister zelf geeft dat ook toe – suggereert een aantal mensen dat het ook een optie zou zijn om een computer voordien te hacken en op die manier zo veel mogelijk wachtwoorden van iemand te verzamelen. Dan zouden op die manier versleutelde gegevens ontsleuteld en leesbaar worden. Hoe denkt de VVD-fractie daarover?

De heer **Dijkhoff** (VVD): Dat kan alleen bespreekbaar zijn als er voldoende waarborgen zijn. De minister geeft dat ook aan: je doet het niet bij alle overtredingen of misdrijven, alleen bij selecte, heel zware zaken en dan moet er ook nog een toetsing door de rechter-commissaris zijn. Ik vraag me wat dat betreft af of de rechter-commissaris in Nederland ondanks het hoge niveau van de rechterlijke macht genoeg kennis en kunde heeft. Ik vond het Britse model interessant. Daarin zit een aparte toezichtstak, die meer echte expertise op dit vlak heeft. Je moet je dit middel niet bij voorbaat ontzeggen.

Mevrouw **Gesthuizen** (SP): Dat is interessant. Pleit de VVD-fractie nu ook voor gespecialiseerde rechtbanken?

De heer **Dijkhoff** (VVD): Nee, dat niet meteen. De VVD vraagt zich in eerste instantie af of onze rechters-commissarissen op dat terrein voldoende toegerust zijn. Daar zou dus ook nog een mogelijkheid kunnen

liggen. Je kunt van mensen echter ook niet verwachten dat ze alles weten. Ik wil graag van de minister horen of hij brood ziet in enige taakspecialisatie.

De **voorzitter**: Ik schors de vergadering uit humanitaire overwegingen voor enkele minuten.

De vergadering wordt enkele ogenblikken geschorst.

De **voorzitter**: De heer Dijkhoff was klaar, althans door zijn tijd heen. We gaan nu dus naar de heer Bontes.

De heer **Bontes** (PVV): Voorzitter. Cybercrime is een groot probleem. Dat probleem wordt alleen maar groter naarmate je afhankelijker wordt van de digitale infrastructuur. Er moet dus wat gebeuren. Dat is een ding dat zeker is. Ik noem een paar voorbeelden. Bendes halen vanuit Oekraïne Nederlandse bankrekeningen leeg. Grote bedrijven als Sony en ook het beveiligingsbedrijf RSA – van dat bedrijf hebben wij een token om in te loggen, dus ook onze eigen kwetsbaarheid heeft daarmee te maken – kunnen het slachtoffer van hacks worden of zijn dat al geworden. Ook de Nederlandse overheid is slachtoffer geworden, namelijk van het Dorifelvirus. Je moet cybercrime dus keihard aanpakken.
Aan de andere kant is er een flinterdunne scheidslijn tussen het vechten tegen cybercrime en de privacy. Je moet daarbij precies de goede balans zien te vinden. Je kunt de privacy niet zomaar overboord gooien. Evenmin moeten andere landen de mogelijkheid krijgen om in te breken in Nederlandse computers. Hieruit blijkt weer dat de scheidslijn dun is. Je wilt mogelijk wel actie ondernemen in andere landen, zoals in Oekraïne, waar de servers voor de verspreiding van het Dorifelvirus stonden, maar je wilt ook geen tegenaanval krijgen. Je moet dus een bepaalde balans zoeken.
De minister komt met een ontsleutelplicht voor verdachten en een terughackrecht voor opsporingsdiensten. Dat zijn de twee hoofdlijnen. Het belangrijkste agendapunt van vandaag is echter het plan van de minister om opsporingsdiensten de mogelijkheid te geven om computers van criminelen te hacken. De minister wil de politie de bevoegdheid geven om spyware te plaatsen op computers van verdachten en deze computers op afstand te doorzoeken – daar komt het in de praktijk op neer – ongeacht het land waar die computers zich bevinden. Deze plannen zijn door verschillende internationale organisaties slecht ontvangen. Bits of Freedom heeft er kritiek op, maar ook de eigen adviesraad van de minister, de Cyber Security Raad, heeft recentelijk kritiek geuit.
Ik heb een paar vragen aan de minister. Kan de minister de proportionaliteit en de effectiviteit van de voorgestelde bevoegdheden aantonen? Bij effectiviteit moet je ook de volgende vraag stellen. Als je spyware plaatst, krijg je dan niet in no time antivirusprogramma's, antispyware, waarmee die spyware meteen weer kan worden verwijderd? Word je dus niet binnen een paar dagen weer ingehaald door de techniek? Samenvattend: kan het effectief en staat het gebruikte middel in verhouding tot het doel? Waarom breidt de minister de kennis en capaciteit op het gebied van cybercrime niet verder uit in plaats van het aantal bevoegdheden te laten toenemen? Nu ligt het zwaartepunt bij de bevoegdheden, maar je kunt dat ook leggen bij kennis en knowhow.
Hoe beoordeelt de minister de waarschuwing van verschillende internationale organisaties dat andere landen het voorbeeld van Nederland zullen volgen? Dan zou bijvoorbeeld Iran, een land dat fel tegen homoseksualiteit is, alle aan homoseksualiteit gerelateerde content hier in Nederland kunnen gaan vernietigen of onbruikbaar maken. Dat risico loop je. Hoe kijkt de minister daartegen aan?

Een ander voorstel van de minister is het strafbaar stellen van de heling van digitale gegevens. De minister wil het voorhanden hebben van gegevens die zijn verkregen door hacking, strafbaar stellen. De PVV vraagt zich echter af hoe groot het risico is dat gehackte gegevens bij nietsvermoedende burgers terechtkomen. Worden onschuldige burgers daar niet het slachtoffer van?
Onlangs is er een conceptversie van een Europees plan over het tegengaan van cybercrime en terrorisme op het internet uitgelekt. Het moet voor de politie mogelijk worden om providers te gelasten bepaalde inhoud al dan niet tijdelijk van het internet te verwijderen. Nu moet de rechter zich nog over een dergelijk verzoek buigen. Dat komt dan te vervallen. Met dit plan is dat niet meer nodig. Hoe kijkt de minister tegen dit plan aan? Ik begrijp dat Nederland de voortrekker van dit plan is. De minister heeft daar dus een rol in. Kan hij een toelichting geven? Tevens is naar buiten gekomen dat werkgevers legaal de computers van hun werknemers moeten kunnen bekijken. Dat zijn heel zware dingen, die een grote inbreuk op de privacy vormen. Ik krijg graag een reactie op dat zorgwekkende plan dat is uitgelekt.
Vorige week stond op NU.nl dat een halfjaar voor de inbraak bij DigiNotar de overheid al was gewaarschuwd voor een lek. De overheid zou niet hebben ingegrepen omdat werd ingeschat dat het geen zaak was voor de rijksoverheid aangezien het de rijksoverheid niet zou schaden. Klopt dat? Hoe verhoudt dat zich tot de meldplicht? Het werd toen wel gemeld, maar het werd niet serieus opgepakt. Dat moet wel in verhouding tot elkaar blijven staan. Ik krijg hierop graag een reactie.

De heer **Verhoeven** (D66): Voorzitter. Een aantal woordvoerders heeft het al gezegd: internet groeit, wordt steeds belangrijker en geeft steeds meer gemak, maar daardoor stijgt ook de kwetsbaarheid. Dat laatste hebben we het afgelopen jaar gezien met de incidenten rond KPN, DigiNotar, enz. We willen dus graag meer veiligheid en daarom willen we de cybersecurity beter organiseren. Daarin heeft de overheid een rol. We moeten er daarbij echter wel op letten dat de balans niet doorslaat naar het ingrijpen op de privacy, naar een veel te grote macht bij de overheid over informatie van burgers en naar het creëren van schijnveiligheid. Maak dus een goede belangenafweging, want 100% veilig kan geen doel zijn. 100% veilig kan niet. Hooguit is het doel: veel vertrouwen van de burger in ICT.
Het is daarom eerst nodig om te analyseren hoe erg het is als iets onveilig is, wie wat moet doen om die acceptabele balans te vinden, dus welke rol voor wie is weggelegd, en wat specifiek de rol van de overheid is. En hoe grijp je in als er iets mis is? Met die analyse moet je beginnen. Ik heb een beetje het gevoel – dat wordt door het Cyber Security Beeld Nederland bevestigd – dat het volgende beeld wordt geschetst: er is een probleem, dus we moeten meteen maar actie ondernemen om het aan te pakken. Maar de zojuist genoemde afweging wordt niet gemaakt. Het Cyber Security Beeld Nederland, dat bij de stukken zat, is als een soort van total body scan die je tegenwoordig kunt laten maken. Het is een soort opname, een soort garantie tot aan de deur. Maar is de foto wel goed genomen? Is hij scherp? Staat iedereen erop? Dat blijft altijd de vraag. En kun je daar dan wel beleid op baseren, zeker beleid dat zover gaat als de minister nu voorstelt?
De rol van de overheid is daarbij ook cruciaal, want die koppelt zelf ook steeds meer systemen aan elkaar. Ook daardoor wordt de kwetsbaarheid vergroot. Immers, als er één vat lek is, dan is er bij communicerende vaten gelijk een probleem bij alle vaten. De integratie van databases kan op zich best wel praktisch zijn, maar ze maakt ons wel kwetsbaar. Kan dat bij het volgende Cyber Security Beeld Nederland worden meegenomen? Kan daarbij dan ook worden ingegaan op de zorgsector? Is het sowieso niet beter om een en ander veel kleinschaliger in te richten en ervoor te zorgen dat niet alles op één beveiliging leunt, zoals bij DigiNotar het geval

was? Kan het voornemen tot meer kleinschalig inrichten worden meegenomen in de Baseline Informatiebeveiliging Rijksdienst (BIR), de meetlat waarlangs alle ICT-projecten van de ministeries worden gelegd? Dan krijgen we wat meer security and privacy by design.
Het kabinet kiest vrij direct voor twee grote maatregelen: het NCSC verder optuigen en zorgen voor een vergaande computerinbraakwetgeving. De NCSS en het NCSC zijn veelbelovend qua ambitie. Mijn collega's hebben dat ook gezegd. Het lijkt echter ook wel veel op een kerstboom. Dat past misschien goed bij deze tijd, maar het is niet functioneel. In de brief van de minister staan enorm veel afkortingen. Ik zou bijna zeggen: zo kennen we de minister niet. Ik lees in alle stukken vooral veel adviserende en coördinerende rollen. Maar wie gaat nu wat doen? Wie gaat het uitvoeren? Dat is niet duidelijk. Heeft de rijksoverheid zelf de capaciteit om dingen te doen of moet onze private politie Fox-IT het uitzoeken? Met die partij is overigens niets mis, maar als zij er een keer niet is, wie doet het dan? Hebben we voldoende eigen capaciteit om een crisis op te lossen?
Ik kom, tot slot, op de hackende politieagenten. De minister stelt voor dat de politie zelf op afstand moet kunnen inbreken, hier en in het buitenland. Die bevoegdheden zullen niet alleen gelden voor cybercrime maar ook voor het aanpakken van «gewone» zware misdaad. Dat vind ik cruciaal. In mijn ogen is zware criminaliteit nu zoiets als het nieuwe terrorisme van dit decennium aan het worden. Ze fungeert als een soort blinde rechtvaardiging voor het aan de politie en de overheid geven van vergaande nieuwe bevoegdheden die wel de internetvrijheid van alle burgers raken. Ik ben wat stelliger dan de PvdA, de VVD en de PVV zojuist, voor mij. Zij spreken alle hun zorgen uit en zoeken de balans, maar ik vind dat de balans in deze plannen is doorgeschoten. Het op afstand binnendringen, doorzoeken en ontoegankelijk maken is niet alleen een forse inbreuk op de privacy, maar ook een grote controlemacht en een grote concentratie van macht en bevoegdheden bij de overheid. De bevoegdheid om zelf binnen te dringen zou de overheid ook nog een prikkel kunnen geven om bepaalde lekken niet te melden, omdat ze zelf naar binnen kan, wat het doel van de minister is.
Hoelang heb ik nog, voorzitter?

De **voorzitter**: U hebt nog één minuut spreektijd.

De heer **Verhoeven** (D66): Ah, dat gaat goed. Dank!

Mevrouw **Gesthuizen** (SP): Ik zal een uitgebreide vraag aan u stellen, mijnheer Verhoeven. Ik begrijp uit de woorden van de D66-fractie dat zij zich erg veel zorgen maakt. Een aantal van die zorgen deel ik. De opsomming van zaken waarover D66 zich zorgen maakt, is echter zo lang dat ik niet goed begrijp tegen welke punten van de brief D66 nu echt fundamentele bezwaren heeft. Wat gaat D66 nou gewoon te ver? Is dat de reikwijdte of is dat het feit dat men computers van potentiële verdachten binnendringt?

De heer **Verhoeven** (D66): Indringen in computers van verdachten gaat ons al te ver. Zonder een verzoek om rechtshulp meteen actie ondernemen, dus het ontlopen van internationale afspraken, gaat ons ook te ver. Mijn collega zegt het prettig te vinden als wij dat in de Oekraïne kunnen doen, maar het eng te vinden als de Oekraïne dat bij ons doet. Die wederkerigheid zien wij wel. Als wij niet willen dat een ander het doet, doen wij het liever ook zelf niet. Dat de politie niet alleen op afstand inbreekt in de computer van een verdachte van cybercrime, maar ook van een verdachte van andere criminele activiteiten, vinden wij te ver gaan.

Mevrouw **Gesthuizen** (SP): Ik begrijp het even niet zo goed. De heer Verhoeven vindt het gewoon te ver gaan, dus ook als iemand wordt verdacht van welke misdrijven dan ook?

De heer **Verhoeven** (D66): Je kunt nooit perfect afbakenen wanneer iemand voldoende verdacht is om zover te gaan. Je bevindt je daarbij op een glijdende schaal. Je onderwerpt een veel te brede groep mensen aan een vergaande bevoegdheid van de overheid. Natuurlijk zijn er gevallen waarbij je het liefst in de computer zou willen inbreken, maar er zullen ook heel veel gevallen zijn waarbij in computers wordt ingebroken terwijl dat helemaal niet terecht is gelet op de mate van verdenking. Het is een aanpak die niet in balans is met het probleem. Die balans slaat door. Veel helderder kan ik het overigens niet zeggen, mevrouw Gesthuizen. Als u nu weer gaat zeggen dat u het niet begrijpt, dan is dat zo.

De **voorzitter**: Laatste keer, mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP): Ik wil het wel graag scherp krijgen. Alle politieke partijen zien zich natuurlijk voor dit dilemma geplaatst. Ik wil heel graag van de fractie van D66 horen of zij in alle gevallen vindt dat het binnendringen in computers door de overheid per definitie niet kan, ongeacht het misdrijf. Ik wil dat graag weten.

De heer **Verhoeven** (D66): «In alle gevallen» raakt precies het probleem. De minister confronteert ons nu met dit probleem, want als ik zeg «nee, het moet in sommige gevallen wel kunnen», dan gaat de minister lekker glijden op de glijbaan.

De heer **Dijkhoff** (VVD): Ik moet de heer Verhoeven complimenteren. In een eerdere interruptie zei hij dat hij vooringenomen was, en dat maakt hij in ieder geval waar. Als het om kinderporno gaat, mag in de retoriek van de heer Verhoeven in een keer alles. Dat is net als bij mij als het om privacy gaat: dan mag in een keer niks. Daar zit natuurlijk wel iets in, maar waarom zoekt de heer Verhoeven zelf niet mee naar de balans? Hij spreekt over veel te grote groepen, maar wij bepalen bij de uitwerking toch zelf wie wel en wie niet onder groepen vallen? Waarom neemt de heer Verhoeven zo'n andere houding aan bij de beveiliging in het online-domein? Het hele strafrecht offline bevat immers dit soort dilemma's, keuzes en afwegingen: wie mag je in welke gevallen met een waarborg van de onafhankelijke rechter wel onderwerpen aan bepaalde opsporingsmethoden?

De heer **Verhoeven** (D66): Ik denk dat ik een heel goede bijdrage aan dit debat heb geleverd door...

De **voorzitter**: Dat bepalen de mensen die meeluisteren.

De heer **Verhoeven** (D66): Ik denk dat ik een heel nuttige bijdrage heb geleverd, ook in het licht van de vraag van de heer Dijkhoff. Ik zeg namelijk duidelijk dat de tendens van de plannen van de minister, de manier waarop een en ander wordt ingericht en de waarborgen die de minister best wil geven, naar mijn mening niet voldoende veiligheid bieden om de problemen die ik zie, te voorkomen. Daar begin ik. Ik begin niet met te zeggen dat ik een aantal zorgen heb en met voor te stellen om samen op zoek te gaan naar de balans. Het startschot van de minister vind ik een stevig beginbod. Ik bied dan liever even wat tegenwicht. Dan zeg ik tegen de minister: even wat voorzichtig zijn. Zoals het nu is opgeschreven, gaat het mij te ver.

De heer **Dijkhoff** (VVD): Ik ben blij dat ik die vraag heb gesteld, want ik proef nu bij collega Verhoeven toch alweer iets meer ruimte voor het zoeken naar een balans in de uitwerking. Dan zijn we in ieder geval niet overal blind tegen. Het biedt hoop voor de toekomst.

De **voorzitter**: Wat is de vraag? Een interruptie mondt in de regel uit in een vraag.

De heer **Verhoeven** (D66): Nee, dat hoeft niet.

De heer **Dijkhoff** (VVD): Als de voorzitter daaraan hecht, vraag ik de heer Verhoeven of hij mijn hoop gerechtvaardigd vindt.

De heer **Verhoeven** (D66): D66 is een progressieve partij in het redelijke midden. Anders dan sommige andere partijen die hier aanwezig zijn, zal D66 nooit met een blinde waas voor ogen direct zeggen: tegen!. Dat is niet onze stijl. Wij zullen altijd meedenken met de minister. Als men met mij wil praten over voorstellen die moeten uitmonden in wetgeving, inclusief deze brief van de minister, en als men mij vraagt of ik daar een goed gevoel bij heb, dan zeg ik «nee, daar heb ik geen goed gevoel bij». Het leek mij goed om dat eens naar voren te brengen, en dat heb ik zojuist gedaan. Het zou echter heel raar zijn als we nu stoppen met denken. Ik ga er wel van uit dat de minister de zorgen van mijn collega's en onze zorgen serieus neemt en geen versie 2.0 voorstelt waarin niets is veranderd. Daar zal ik de minister weer op controleren.

De **voorzitter**: U had nog iets te betogen, zei u, maar dat is wellicht met dit antwoord op de interrupties al gebeurd.

De heer **Verhoeven** (D66): Dat is ijdele hoop, voorzitter, want ik heb nog een aantal scherpe vragen.

De **voorzitter**: Daar hebt u nog precies één minuut voor.

De heer **Verhoeven** (D66): Dank u wel. Uitgerekend vandaag ontving de Kamer de antwoorden op de vragen van mijn fractiegenoot Berndsen. Die namen mijn zorgen echter niet weg. Dat heb ik ook duidelijk gemaakt. Waarom heeft de minister cybercrime en zware misdaad op één hoop gegooid? Hoe gaat de politie spyware verspreiden? Gaat de politie lekken verzwijgen om zo toegang te kunnen krijgen of te houden tot bepaalde computers die openstaan? Willen we echt kunnen inbreken in computers in andere landen zonder dat daaraan een verzoek om rechtshulp is voorafgegaan? En mogen andere landen dat dan ook?
Ik sluit mij voorts aan bij de vraag van het CDA of de rechter-commissaris genoeg kennis heeft om een dreiging te kunnen beoordelen. Of moeten wij daarvoor op een private partij vertrouwen die wellicht meer expertise heeft, maar die er misschien ook een ander belang bij heeft? Anders dan in de antwoorden van de minister op de vragen van D66 staat, is een dergelijke hack niet hetzelfde als een gewone huiszoeking. In een computer kunnen meer mensen meer zien dan bij een huiszoeking. Een computer is niet hetzelfde als een huis.
De minister noemt strikte argumenten en voorwaarden, maar als je hiermee begint, begeef je je op een glijdende schaal, de afgeleide van een glijbaan. Dan is er gewoon geen weg meer terug. Dat hebben wij voorheen ook vaker gezien bij terrorisme. Wij willen gewoon duidelijkheid over de bevoegdheden van de politie op het gebied van cyberveiligheid, maar de aangekondigde voorstellen gaan ons veel te ver.

De **voorzitter**: Hiermee zijn we gekomen aan het eind van de eerste termijn van de Kamer. Ik schors de vergadering opdat de minister zich kan voorbereiden op zijn antwoord.

Schorsing 16.51 tot 17.02 uur

Voorzitter: Gesthuizen

De **voorzitter**: De eerdere voorzitter van dit overleg moest de plenaire vergadering bijwonen. Ik zit daarom het vervolg van het algemeen overleg voor. Hier en daar zal ik echter ook zelf een interruptie plaatsen.
Ik geef het woord aan de minister voor zijn antwoord in eerste termijn.

Minister **Opstelten**: Mevrouw de voorzitter. Ik dank de geachte afgevaardigden voor hun bijdrage. In het regeerakkoord is duidelijk vermeld welke prioritaire punten wij zullen voorstellen. De dossiers zijn al samen met de Kamer in de vorige samenstelling intensief doorgenomen. De brieven zijn niet voor niets geschreven. Vooral de brieven die hier veel aan de orde komen, zijn op verzoek van de Kamer verstuurd. Ik ben de Kamer dan ook dankbaar voor de constructieve benadering van dit belangrijke onderwerp.
Een veilige, open en betrouwbare cyberinfrastructuur is essentieel om onze samenleving draaiende te houden en de economie te laten groeien. Nederland is een internationaal internetknooppunt en heeft een van de hoogste gebruikersdichtheden van het internet ter wereld. De steeds groter wordende afhankelijkheid van de cyberinfrastructuur maakt ons echter ook kwetsbaar. Recente incidenten zoals de DigiNotar-crisis, de KPN-hack en het Citadel/Dorifel-virus onderstrepen dit. Dit vergt een overheid die daar adequaat op in weet te spelen. Dat staat vandaag op de agenda.
Op 15 oktober heb ik de Kamer een brief gestuurd waarin naar mijn mening noodzakelijke nieuwe wetgeving wordt aangekondigd. Daarmee wil ik ook het debat daarover openen. De Kamer heeft daar ook om gevraagd. Deze wetgeving is bedoeld om de strijd tegen de vele ernstige vormen van cybercrime in het voordeel van de samenleving en haar opsporingsinstanties te doen kantelen. De digitalisering van de samenleving heeft tot gevolg dat ICT, waaronder internet, bij vele strafbare feiten een wezenlijke rol is gaan spelen. Het internet wordt door criminelen gebruikt voor de voorbereiding, de uitvoering en de afloop van diverse delicten, als communicatiemiddel en als informatiebron. Het is ook een marktplaats voor de aankoop en verkoop van illegale goederen, niet strafbare hulpmiddelen en grondstoffen, voor het aanbieden en afnemen van diensten en voor het rekruteren van slachtoffers en medeplegers. Het wordt gebruikt om het plegen van misdrijven af te schermen en om illegaal vermogen wit te wassen. Het kenmerk is dat deze vormen van criminaliteit veelal niet gebonden zijn aan landsgrenzen en veel in de anonimiteit plaatsvinden.
De huidige bevoegdheden stammen bijna allemaal uit de tijd waarin computers niet bestonden of niet aan het internet waren verbonden. De politie en het Openbaar Ministerie zijn daardoor onvoldoende in staat om op te sporen en te vervolgen. De Kamer heeft mij uitgedaagd om te bekijken of het instrumentarium wel voldoende is. Ik ben mij ervan bewust dat ik vergaande en ingrijpende voorstellen heb gelanceerd. Laat ik dat vooropstellen, ook tegenover de heer Verhoeven, die op dit vlak in feite het verst ging. Natuurlijk is over deze voorstellen niet het laatste woord gezegd, maar zij komen voort uit de problemen die dagelijks bij de opsporing worden ervaren.
Op mijn departement wordt samen met belangrijke vertegenwoordigers uit het veld hard gewerkt aan deze nieuwe wetgeving. Het is mijn bedoeling om de conceptwetgeving in het eerste kwartaal van 2013 in

consultatie te geven. Natuurlijk zal ik bij de voorbereiding daarvan goed luisteren naar wat in de Kamer wordt gezegd. De rest van het traject zal ik binnen de mogelijkheden doorlopen om deze voor de opsporing belangrijke wetgeving tot stand te brengen. Ik hoop daarbij op de steun en constructieve bijdrage van de Kamer. Verder zal ik goed gaan kijken naar de vele commentaren, waaronder de brief van Bits of Freedom. Het is wel eens anders geweest met Bits of Freedom, maar nu is er een constructief overleg met Bits of Freedom over de strategie. Er wordt goed samengewerkt. Op de laatste brief, waar een prachtige zilveren strik omheen zat en die mij in persoon is overhandigd, heb ik gezegd dat er nog wel verschillen zijn, maar dat ik wel bereid ben om er goed naar te kijken. Ik denk dat wat dat betreft de sfeer is veranderd. Ik weet niet of ik een volgend jaar voor de award die zij een keer per jaar in de aanbieding hebben ... Ik heb hem twee jaar geleden gekregen, maar vorig jaar niet.

De **voorzitter**: Misschien kan de minister toelichten wat het voor een award is. Wellicht is dat niet bij iedereen bekend.

Minister **Opstelten**: Ik weet niet meer precies hoe die award heet. In de geschiedenis van Bits of Freedom was het een award voor degene die er naar hun mening niet al te veel van had gemaakt. Twee jaar geleden vond ik dat niet erg, maar het klimaat is veranderd, ook bij Bits of Freedom. Zij hebben ook in de gaten dat er iets moet gebeuren. Of wij er op dit onderwerp uit komen, is echter de vraag. Het zou weleens kunnen van niet, maar het is wel goed om daar scherp met elkaar face to face over te spreken. Dat klimaat hebben we wel bereikt. Dat heb ik met de mevrouw die mij de brief heeft aangeboden, allemaal afgesproken. Ik zie dat ze hier aanwezig is.
Verder wordt op dit moment samen met belangrijke partners gewerkt aan de verdere verdieping van de Nationale Cyber Security Strategie. Daar is ook om gevraagd. Hierbij staat de hele keten centraal: awareness, het verhogen van de weerbaarheid, de mogelijkheid om te detecteren, vroegtijdig alerteren, adequate respons en crisisbeheersing, opsporing en vervolging. Zo zal de focus door middel van actieplannen worden vergroot en zal de internationale dimensie verder worden uitgewerkt. Op 23 november jongstleden heb ik de bijdrage van Bits of Freedom over het cybersecuritybeleid van de toekomst gelezen. Het is alsof ik het erom doe, maar dat is niet zo. Ik juich deze evenwichtige bijdrage toe. Het is weleens anders geweest. Samen met Bits of Freedom wordt bekeken hoe deze bijdrage kan worden gebruikt bij de verdere uitwerking van de Nationale Cyber Security Strategie. Daarnaast draagt Nederland actief bij aan de inspanningen van de EU. Ik maak mij in EU-verband in het bijzonder sterk voor een gecoördineerde aanpak van de Europese Cyber Security Strategie. Ook heeft Nederland binnen de EU een netwerk van vertrouwde partners opgebouwd. Binnen dit netwerk worden informatie en ervaringen gedeeld en ontwikkelt men samen nieuwe initiatieven. Het gaat hierbij om Frankrijk, het Verenigd Koninkrijk, Duitsland en Zweden.
Ik heb mijn antwoord in een paar blokjes ingedeeld.
Ik ga eerst in op de kennis, waar veel naar is gevraagd. Onder meer is gevraagd of het Nationaal Cyber Security Centrum (NCSC) in staat is om de rol van digitale brandweer te vervullen. Ten tijde van de ICT-crisis speelt het NCSC een ondersteunende rol bij de crisisrespons. Een voorbeeld daarvan is de DigiNotar-crisis. De Kamer heeft het rapport van de Onderzoeksraad Voor Veiligheid (OVV) daarover gelezen. Indien nodig wordt ook op locatie ondersteuning verleend. Ook samen met anderen wordt gewerkt aan oplossingen voor virussen. Het NCSC groeit nog. De komende tijd zullen hiervoor nog extra mensen worden aangenomen.
De heer Verhoeven vraagt of er voldoende capaciteit is om een crisis op te lossen. Organisaties zijn zelf verantwoordelijk voor de respons. Dat moet de heer Verhoeven aanspreken. Het Nationaal Cyber Security Centrum

speelt een ondersteunende rol bij de ICT-incidenten. Ik heb ze genoemd. Om krachtiger te kunnen reageren, zal in 2014 een nationaal detectie- en responsnetwerk worden opgericht dat 24 uur per dag bereikbaar zal zijn. Daardoor kunnen aanvallen eerder en beter worden gesignaleerd en bestreden.
Mevrouw Gesthuizen vraagt of het crisisplan in 2012 wordt geactualiseerd. Het crisisplan wordt voortdurend geactualiseerd. De meest recente versie is op 12 november naar de Kamer verzonden. Indien nodig zal het weer worden geüpdatet in 2013.
De heer Dijkhoff en anderen vroegen of de politie voldoende kennis heeft op het gebied van cybercrime. Ik blijf erbij dat de politie mee moet gaan met de ontwikkeling in de samenleving. Dat houdt in dat iedere agent op basisniveau kennis moet hebben van cybercrime. Dat is nu nog niet het geval. Ontvreemding of oplichting komt bijvoorbeeld steeds vaker in een digitale vorm voor. Daarom besteedt de Politieacademie hier nadrukkelijk aandacht aan in het dit jaar gestarte nieuwe curriculum van de initiële politieopleiding. Daarnaast heeft de Politieacademie in het postinitiële onderwijs een opleiding ingericht die zich specifiek richt op de aanpak van cybercrime. Ook is er de handleiding Alledaags politiewerk in een gedigitaliseerde wereld, die ook via het PolitieKennisNet beschikbaar is voor iedere medewerker. Voorts zet ik in op het binnenhalen van hoger opgeleiden, op hbo-plusniveau, voor specifieke thema's in de opsporing, waaronder de aanpak van cybercrime. Voor de gecompliceerde hightech-crime is in een apart team binnen de politie voorzien. Dit team behoort tot de top van de wereld op het gebied van opsporing op het internet. Dat mag ik echt zeggen. Dit team is in 2012 onder de landelijke prioriteit met 33 fte uitgebreid. In 2013 gebeurt dit nog een keer. Het Team High Tech Crime (THTC) van het KLPD is straks de landelijke eenheid binnen de nationale politie en heeft tevens als doelstelling om de kennis en kunde binnen de regiokorpsen – we hebben straks regionale eenheden en één korps – te versterken. Ik ben van mening dat met bovenstaande maatregelen zowel de kwaliteit (het kennisniveau en de kennisdeling) als de kwantiteit (de uitbreiding van beschikbare capaciteit) van het Team High Tech Crime, van de agenten die zich met de aanpak van cybercrime bezighouden, wordt versterkt. Het is echter nooit voldoende. Dat zeg ik ook. Het is niet geëindigd, absoluut niet. De 105 miljoen euro waarnaar de heer Dijkhoff vroeg, zal daarbij zeker nog kunnen helpen.

De heer **Verhoeven** (D66): De minister zegt in een tussenzin dat het nooit voldoende zal zijn. Dat is een verkapt antwoord. Er zal dus ook nooit een balans zijn; we zullen nooit ver genoeg gaan in het bestrijden van cybercrime. Kan de minister nog eens ingaan op het feit dat het nooit genoeg zal zijn? Er kan immers best een moment zijn dat het wel genoeg is.

Minister **Opstelten**: Die opmerking van de heer Verhoeven verrast mij. Ik neem aan dat hij het met mij eens is dat we een heel dynamische en zichzelf ontwikkelende samenleving hebben. Dit onderwerp is daar een voorbeeld van. Als ik zou zeggen dat die 33 fte voor de komende vier jaar genoeg zijn, dan zou ik niet op deze plek thuishoren. Dan hoor ik daar niet te zitten, want dan heb ik niet begrepen in welke samenleving wij leven. Natuurlijk is dit een ontwikkeling waarbij ik nog niet weet waar we uiteindelijk uitkomen. Ik heb wel een gevoel daarvoor; daarom is het ook een prioriteit. De Kamer en de regering moeten deze ontwikkeling gewoon op de voet volgen en elkaar daarbij scherp houden. Zo is mijn opmerking bedoeld.
Mevrouw Oosenbrug heeft gevraag naar mijn inzet op het gebied van de ethische hackers. Binnen de overheid heeft men ervaring met het werken met hackmethodes. Ik heb het aan den lijve ondervonden, en ik heb het ook zelf gedaan. Dat beken ik nu even, maar het was wel binnen de regels

van het spel. Voorbeelden hiervan zijn natuurlijk de operaties, de penetratietesten binnen de PKI-overheid. Verder worden de kennis en ervaring van de ICT community gebruikt bij het Cyber Security Beeld Nederland-3. Wij werken daar dus aan. Ethisch hacken gebeurt natuurlijk binnen het raamwerk dat de wet biedt.
De heer Dijkhoff vroeg of wij leren van incidenten. Ik kan hem toezeggen dat er in 2013 een analysecel komt die de aard en vorm van virussen onderzoekt en samen met de industrie zorgt voor een adequate oplossing en aanpak.
Hij vroeg verder hoe wij binnen het Nationaal Cyber Security Centrum publiekprivate samenwerking (pps) en kennis kunnen intensiveren. Ik kan toezeggen dat de publiekprivate ICT Response Board (IRB) er in 2014 met alle vitale sectoren zal zijn. Dit betekent een verdubbeling naar 60 cyberexperts. Gelukkig hebben we vanaf het begin de visie gehad om op publiekprivate samenwerking te koersen. We hebben een klein land. We moeten kennis bundelen en niet iedereen met z'n eigen aparte crisiscentrum laten werken. Natuurlijk moet een en ander wel plaatsvinden binnen de strakke verantwoordelijkheden die de overheid heeft en die de overheid niet kan delen met het bedrijfsleven. Ik denk daarbij bijvoorbeeld aan kwesties die zich voordoen op het vlak van de nationale veiligheid.
Mij is gevraagd hoe ik aankijk tegen de kritiek van de heer Jacobs, lid van de Cyber Security Raad. Ik ben blij met zijn opmerkingen en zijn artikel. Daarom zit hij ook in deze Raad. Hij is een expert. Mijn antwoorden op de vragen van mevrouw Berndsen heb ik vanmiddag naar de Kamer gestuurd. Daarbij is ook ingegaan op het artikel van de heer Jacobs. Ik snap dat deze antwoorden wellicht nog niet door alle leden zijn ingezien. Daarin wordt wel precies mijn standpunt weergegeven. Ik wil de leden daarnaar verwijzen. Alle kritiekpunten en suggesties worden gewoon in het wetgevingstraject meegenomen. Het zou niet goed zijn als je op verzoek van de Kamer wel een opening biedt, maar vervolgens niet verdergaat. Dan staat de wereld stil. Dan zou ik in het land met mededogen worden aangekeken. Ik kijk dan ook scherp naar de zorgen die professor Jacobs uit.
Over het binnentreden in een pc en schrijven op die pc wil ik het volgende zeggen. Het heimelijk binnentreden in een pc door de politie zal met de grootst mogelijke zorg en waarborgen worden omkleed. Ik onderstreep dat; ik heb het ook in de brief gezegd. Ik ben natuurlijk niet gek. De rechter-commissaris zal steeds de belangen afwegen en zal daarvoor toestemming moeten geven. De politie zal iedere handeling die zij verricht in het kader van de opsporing vastleggen, opdat zij later controleerbaar en verifieerbaar is. Ik ben nu aan het uitzoeken hoe dit technisch precies in elkaar steekt. Ik kan daar nu dus nog geen nadere toelichting op geven.

De **voorzitter**: De heer Bontes heeft een vraag op dit punt.

Minister **Opstelten**: Ik ga nu over tot het beantwoorden van de vragen van de heer Bontes.

De **voorzitter**: De heer Bontes wil toch nu zijn vraag stellen.

De heer **Bontes** (PVV): De minister zegt dat hij blij is met het kritisch vermogen van de heer Jacobs. De heer Jacobs zegt echter dat «kinderporno als argument wordt misbruikt om absurde bevoegdheden te introduceren». Dat gaat wel iets verder dan kritiek. Hij zegt eigenlijk dat de minister volledig verkeerd bezig is omdat hij absurde bevoegdheden introduceert. Wil de minister daarop reageren anders dan «ik ben blij met het kritisch vermogen van de heer Jacobs»?

Minister **Opstelten**: Ik ben er blij mee dat de heer Jacobs in de Cyber Security Raad zit, maar op dat punt ben ik het niet met hem eens. De

rechter-commissaris moet altijd toestemming geven. Het is alleen bedoeld voor de zware misdrijven. Dat heb ik gezegd en dat is ook de inzet van de brief. Misschien kom ik daar nog scherper op terug door dit bij het wetsontwerp in consultatie preciezer aan te geven. Alles wordt gelogd. De politie dringt zeer gericht binnen. Het middel staat dus in verhouding tot het doel en kan continu worden aangepast aan de specifieke casus. Dat is dus de balans.
Ik wil ook nog ingaan op de effectiviteit. Daarbij wil ik de volgende punten noemen. Mevrouw Oosenbrug heeft daar ook over gesproken.

De **voorzitter**: De heer Bontes heeft toch nog een vraag.

De heer **Bontes** (PVV): Wat gebeurt er nu met deze kritiek? Heeft iemand in de denktank van de minister nu zo'n zware kritiek dat er toch een ander beleid komt en de bevoegdheden worden afgezwakt?

Minister **Opstelten**: Nee. Daar gaan we over spreken. Professor Jacobs is een autoriteit op dit terrein, maar misschien minder op het terrein van het strafrecht. Hij doet toch een tegenzet in het debat. Het voorstel voor nieuwe wetgeving is natuurlijk wel belangrijk voor de bestrijding van kinderpornografie. Laat ik dat ook zeggen.
Het verhaal van encryptie en decryptie is een initiatief uit het Verenigd Koninkrijk. Ik herinner mij dat mevrouw Van Toorenburg mij in een debat over kinderpornografie heeft verzocht om daar alsjeblieft naar te kijken omdat het een groot succes zou zijn. Na grote aarzeling heb ik gezegd dat we ernaar gingen kijken. De Kamer heeft mijn brief gelezen: we hebben er een heel onderzoek naar laten doen. Ik kom tot de conclusie dat je dat zou moeten doen. Door te luisteren scherpen wij elkaar in het debat aan. Waarom zou je hier niet mee verder gaan? Zo is het ook bij dit. De producenten van kinderpornografie zijn vaak zeer bedreven in het gebruik van het internet. Door de wereldwijde jacht die op hen wordt gemaakt, zijn zij zelf steeds zwaardere middelen gaan gebruiken. Ik denk hierbij aan versleuteling, maar ook aan het gebruik van de TOR-netwerken. Kinderporno is een onderwerp dat grote maatschappelijke onrust veroorzaakt en prominent wordt uitgemeten in de media. Wij zijn het er in deze Kamer allemaal met elkaar over eens dat wij daarop scherp moeten inzetten. Er gebeurt natuurlijk veel meer op het internet in relatie tot criminaliteit. Het internet wordt op een aantal manieren door criminelen gebruikt; in mijn inleiding heb ik ze al genoemd.
Dan ga ik nu in op de effectiviteit. De politie beschikt over software waarmee zij zeer gericht en specifiek kan ingrijpen. Deze is juist veel effectiever dan de huidige analoge methode, waarbij je in een huis moet inbreken en apparaatjes op te computer moet plaatsen. Sommige misdaden zijn niet op een andere manier op te lossen dan door in computers in te breken.
Mij is verder gevraagd hoe ik aankijk tegen de kritiek inzake het grensoverschrijdend hacken. Ik begrijp dat men bezorgd is dat andere landen als reactie op ons wetsvoorstel actie zullen ondernemen. Dat is een breed gedragen punt. Deze relatie is volgens mij niet zonder meer causaal. Het is wel een bericht waarover veel wordt gedebatteerd. De landen waar wij het over hebben, zullen immers gewoon tot actie overgaan en dat niet laten afhangen van onze cybercrimewetgeving. Nederland loopt nu voorop en zal altijd voorop blijven lopen. Bij de internationale samenwerking zullen wij altijd de route van de rechtshulp bewandelen indien dat redelijkerwijs mogelijk is. De afgelopen dagen is in Straatsburg in het kader van het cybercrimeverdrag – het is bekend dat het daar allemaal begonnen is – overeenstemming bereikt over het vergroten van de mogelijkheden om zonder specifiek rechtshulpverzoek in het buitenland op te treden. 38 verdragspartijen zijn het hierover eens. Dit steunt Nederland in zijn streven om ook de grens over te gaan met zijn onderzoeken.

De heer Bontes vroeg nog of burgers niet de dupe worden van de strafbaarstelling van heling. Nu zijn ieder geval veel burgers slachtoffer van heling op het internet. Ik verwacht dat, als iemand voor een dergelijke zaak voor de rechter wordt gebracht, goed zal worden afgewogen of er sprake is van strafbaarheid.
De heer Oskam vraagt naar de motie van professor Franken. Daar heeft de heer Oskam een punt. De motie-Franken is overgenomen door het kabinet. Ik zal zorg dragen voor de privacy impact assessments, die nodig zijn voordat de wetgeving in consultatie gaat. De uitvoering van deze motie zal dus ook een criterium zijn voordat de wetgeving in consultatie gaat. In de memorie van toelichting zal worden vermeld aan de hand van welke criteria en op basis van welke conclusies dit wordt gedaan.
De heer Oskam vraagt verder hoe ik omga met de proportionaliteit. Dat zal niet anders zijn dan nu het geval is bij de huidige bijzondere opsporingsmethodes van de politie. Ik hoop dat de heer Oskam mij inmiddels wel kent. Hierbij zal extra worden gezorgd voor logging: het vastleggen van alle stappen die de politie uitvoert. Dat is precies werken. Per procesverbaal komen de gegevens ter beschikking van alle procespartijen, zodat zij in het dossier aanwezig zijn.
Mevrouw Oosenbrug heeft gevraagd om welke software of malware het gaat. Het kunnen verschillende soorten software zijn, variërend van keyloggers tot systemen die hele computers kunnen overnemen. Wij zullen dit uitgebreid in de memorie van toelichting vermelden. De heer Bontes vraagt waarom de capaciteit niet wordt uitgebreid. Beide zijn aan de orde. Je hebt niet zo veel aan extra capaciteit als de mensen niet worden voorzien van de goede bevoegdheden. De mensen die wij nu aantrekken, schreeuwen om deze maatregelen. Wij moeten dat natuurlijk goed in balans brengen. In de komende jaren zal de politie bij alle zaken waarin het internet een rol speelt, kwalitatief en kwantitatief worden versterkt.

De **voorzitter**: Ik begrijp dat u overgaat naar een nieuw blokje. Ik wil u ook zelf nog een vraag stellen.

Minister **Opstelten**: Ik ga nu in op het blokje internationaal.

De **voorzitter**: Dan vraag ik aan de Kamerleden of zij mij willen toestaan om als woordvoerder een interruptie te plegen.
De minister heeft net gezegd dat in ieder geval wordt gedacht aan of wordt gewerkt met secure logging. Is de minister zich er wel van bewust dat in het artikel van de zojuist al veel genoemde mijnheer Jacobs wordt gesuggereerd dat het nog volstrekt onduidelijk is hoe dat zou moeten plaatsvinden?
Er is nog een andere expert, die hier op de tribune zit, en dat is de heer Prins. Hij heeft gezegd dat, als de politie gaat hacken, «de hack zelf volledig moet worden opgeslagen door de computer(s) van de hackende diender te tappen». Kan de minister daarop reageren?

Minister **Opstelten**: Dat is een goede interventie, mevrouw Gesthuizen. Ik ben u dankbaar, terwijl ik de bron, de heer Prins, aankijk. Het antwoord daarop is «ja». Dat is duidelijk het uitgangspunt.
Op de eerste vraag antwoord ik dat wij ervoor zullen zorgen dat dit wordt uitgezocht. Ik ken de kritiek van professor Jacobs natuurlijk. We gaan daarover ook met hem in gesprek. We zullen bezien of wij hem kunnen overtuigen. Wellicht kan hij ons op een aantal punten wijzen, zodat wij een en ander kunnen verbeteren. Hij heeft ons nog niet overtuigd van zijn gelijk. Daar houd ik het vooralsnog bij. Wij willen dat debat wel voeren. Daarom zijn wij hem ook erkentelijk voor zijn opmerkingen. Wij nemen die mee bij de voorbereiding van het wetsontwerp.

De **voorzitter**: Als de politie software installeert, gebeurt dat dus met een functionaliteit die ervoor zorgt dat alles wat die software doet, wordt geregistreerd, zodat dit vervolgens aan de verdachte en diens advocaat kan worden voorgelegd?

Minister **Opstelten**: Jazeker, dat is absoluut de bedoeling. Dat zei ik ook in het laatste punt van mijn betoog over het vorige thema. Dat moet worden vastgelegd. Ik zei het al in antwoord op de vraag van de heer Oskam. Dit moet gewoon duidelijk in het dossier worden opgenomen en bekend worden bij de andere procespartijen. Zo leven wij in deze rechtsstaat en dat wil ik ook zo houden. Die moet ik tenslotte ook bewaken. De Kamer kan er verzekerd van zijn dat ik dat doe.
Mevrouw Gesthuizen heeft onder andere gevraagd wanneer de EU-strategie zal verschijnen. Het tempo is hoog. Ik zie het zorgelijke gezicht van de heer Verhoeven; hij vraagt zich af of wij dit wel allemaal moeten doen. De strategie verschijnt eind januari van het komende jaar. Zij is nog alleen op hoofdlijnen bekend. Hierbij zal aandacht worden besteed aan algemene waarden zoals internetvrijheid, het opbouwen van de capaciteiten in de EU-landen, het bestrijden van cybercrime en internationale aspecten en afspraken. Ik kan wel zeggen dat de kopgroep in de EU bestaat uit de vijf landen die ik heb genoemd. Nederland speelt daar wel een belangrijke rol bij.
De heer Dijkhoff vraagt hoe men denkt over de EU-meldplicht. De Europese Commissie zal naar verwachting in de eerste helft van 2013 een Europese cybersecuritystrategie uitbrengen. Gezien het grensoverschrijdende karakter van dreigingen en het gegeven dat sectoren veelal in een breder internationaal verband actief zijn, is het van belang dat hierover op Europees niveau afspraken worden gemaakt. Op deze wijze kan in Europa een level playing field worden gehandhaafd. Nederland zal zich inzetten voor en actief bijdragen aan het aansluiten van de Nederlandse meldplicht op de inspanningen van de EU voor een Europese security breach notification.
Wat betreft internationale samenwerking, vroeg de heer Oskam of ik aan best practices doe. Ja, er is veel samenwerking met andere landen. Dat heb ik al gezegd. Wij wisselen daarbij ook best practices uit. Europol gaat dat de komende tijd voor zijn rekening nemen. Door het Nationaal Cyber Security Centrum wordt met ongeveer 30 andere landen heel actief internationaal samengewerkt.
Ik heb nog een aantal losse vragen. Mevrouw Gesthuizen vroeg of er eerder informatie bekend was over de kwetsbaarheden van DigiNotar. Enkele anderen hebben daar ook vragen over gesteld. In eerste instantie is de Kamer geïnformeerd over de crisisbestrijding bij DigiNotar en de door de overheid ondernomen acties. Daarna is de Kamer geïnformeerd over de door het kabinet ondernomen acties in het kader van de verbetering van de PKIoverheid. Ook heeft de Kamer het rapport ontvangen van Fox-IT waarin de kwetsbaarheid in versie 4.8 als oorzaak van de hack wordt genoemd. Dit betreft dus niet de kwetsbaarheid in versie 5, waarop het Nationaal Cyber Security Centrum door Fox-IT werd geattendeerd. De kwetsbaarheid in versie 4.8 was al sinds 2008 publiekelijk bekend en is gemeld door de leverancier van de software. Het voorzien van informatie over updates en over de eigen producten geeft invulling aan de eigen verantwoordelijkheid van de leverancier van die producten. Kennisnemen hiervan en hiernaar handelen past binnen de verantwoordelijkheid voor de veiligheid van informatiesystemen die eigenaars van deze systemen zelf hebben. DigiNotar had hierop dus kunnen en moeten acteren. Zoals geschetst, bestaat er geen directe relatie tussen de melding over de kwetsbaarheid en de hack bij DigiNotar.

De heer **Bontes** (PVV): Feit is dat het al een halfjaar voor de inbraak bekend was. Kan de minister daar nog op ingaan?

Minister **Opstelten**: GOVCERT.NL, de voorganger van het Nationaal Cyber Security Centrum die onder verantwoordelijkheid van de minister van BZK viel, heeft wel degelijk iets met deze melding gedaan. De dienstverlening van GOVCERT.NL bestond op dat moment, in de toenmalige verhoudingen en verantwoordelijkheden, uit het ondersteunen van overheidsorganisaties die via een deelnemersmodel bij GOVCERT.NL waren aangesloten voor het voorkomen en afhandelen van ICT-veiligheidsincidenten. Conform dit mandaat en de daarbij behorende procedures is naar aanleiding van de melding van 13 januari 2011 beoordeeld of het desbetreffende lek ook voorkwam in software die door de deelnemers van GOVCERT.NL werd gebruikt. Dit bleek niet het geval te zijn. Daarmee is correct geacteerd op de bij GOVCERT.NL binnengekomen melding. Met de overgang naar het Nationaal Cyber Security Centrum heeft deze organisatie een bredere taak gekregen. Nu zou ook contact worden opgenomen met het bedrijf. Daarnaast worden adviezen nu gepubliceerd op de website van het NCSC, waarmee de informatie breed wordt verspreid.

De heer **Bontes** (PVV): Het is mij toch nog niet helemaal duidelijk. Is er nu een inschattingsfout gemaakt door te stellen dat het de rijksoverheid niet zou gaan schaden? Op dat punt wil ik graag een toelichting. Het heeft immers de rijksoverheid wel geschaad, terwijl de inschatting was dat het de rijksoverheid niet zou schaden.

Minister **Opstelten**: Ik ben hier erg precies in. De informatie toen was niet op de rijksoverheid gericht, maar op het particuliere bedrijf DigiNotar. Binnen zijn taak en mandaat voelde GOVCERT.NL geen verplichting om daar nadere melding over te doen. Het is heel goed nagelopen. Ik heb het bericht op NU.nl ook gelezen. Dan krijgt natuurlijk direct een aantal mensen een telefoontje met de vraag hoe het zit. Anders had ik het ook anders gezegd. Ik vind dat ik de mensen van GOVCERT.NL onrecht zou doen door dit anders te zeggen. Zo is het precies gelopen. Nu zou het anders lopen. Dat heb ik ook gezegd. Het NCSC heeft een bredere verantwoordelijkheid en een bredere taak. Nu kan ik daarop worden aangesproken.
Ik kom nu op een opmerking van de heer Oskam. Ik was nog zo tevreden over het opstarten van de campagne Alert online samen met de CEO van de Rabobank. Ik zal hem nog eens vragen wat hij van die website www.alertonline.nl vond. Alert online is geslaagd in zijn opzet om initiatieven op het gebied van cybersecurityawareness te initiëren en samen te brengen, uiteraard met een passende website. De website is een tijdelijke site ten behoeve van de campagne. Ik begrijp dat de heer Oskam hem niet erg modern vond. Dat was nieuws voor mij. Die kritiek had ik nog niet ontvangen, maar ik zal haar wel serieus nemen. Wij gaan de site opnieuw bekijken. Het is natuurlijk ook nooit klaar, zo zeg ik ook tegen de heer Verhoeven. Wij moeten ermee doorgaan.

De heer **Verhoeven** (D66): Er staan op campagnewebsites wel eens vaker gekke dingen, ook bij de VVD. Het is wel zaak om het nu structureel goed te regelen. Het moet dan wel echt gaan gebeuren. Je kunt niet een website hebben waarmee je iets wilt bereiken waar die site zelf totaal niet aan voldoet.

Minister **Opstelten**: Daar ben ik het totaal mee eens. Het feit dat de heer Oskam dit noemt, neem is zo serieus dat ik er even alle troepen op zet. Overigens valt over smaak niet te twisten.
Mevrouw Oosenbrug vroeg naar het kader voor responsible disclosure. Het was destijds een initiatief van de D66-fractie in het debat over DigiNotar, voor zover ik mij herinner. Eind 2012 kom ik met een kader responsible disclosure. Het is nu 6 december, dus dat kan ik met een

gerust hart zeggen. Het betreft een afspraak tussen een partij en een melder over de wijze van melding, de wijze van openbaarmaking, termijnen en verdere afspraken. Er is over het kader gesproken en dat is nog dit jaar beschikbaar.
De heer Dijkhoff vroeg wanneer het wetsvoorstel over de meldplicht komt. Het wetsvoorstel gaat in januari 2013 in consultatie en wordt daarna aan de Tweede Kamer gezonden, uiteraard nadat er advies is ingewonnen bij de Raad van State.
De heer Bontes stelde een vraag over het Europese project Clean IT. Clean IT is een Europees project met drie doelen, namelijk het starten van een publiek-private dialoog over het gebruik van internet door terroristen en de wijze waarop dit kan worden tegengegaan, het komen tot gezamenlijke uitgangspunten hierover en het identificeren van best practices op dit terrein. De implementatie van initiatieven valt niet onder dit project. Initiatieven moeten in overeenstemming zijn met nationale en Europese wet- en regelgeving en met de grondrechten zoals de vrije toegang tot internet, vrijheid van vergadering, vrijheid van meningsuiting, privacy en databescherming. De heer Bontes vroeg ook nog hoe het project Clean IT zich verhoudt tot de fundamentele rechten. Ik meen dat Clean IT die respecteert, zoals ik net zei. Het doel van Clean IT is om de dialoog aan te gaan en een balans te vinden tussen beide perspectieven. Het is dus een belangrijk project.
De heer Verhoeven vroeg of de zorg kan worden meegenomen in het Cyber Security Beeld Nederland-3. In het Cyber Security Beeld Nederland wordt ingegaan op kwetsbaarheden. Ik deel zijn zorgen omtrent de gezondheidszorg. Ook die kwetsbaarheden worden indien relevant – ze zijn relevant – meegenomen in het Cyber Security Beeld Nederland.
De heer Verhoeven vroeg of in de Baseline Informatiebeveiliging Rijksdienst (BIR) het principe van kleinschaligheid kan worden opgenomen. De verantwoordelijkheid voor het opstellen van de BIR ligt bij de minister voor Wonen en Rijksdienst. Ik zal deze vraag naar hem doorgeleiden.
De heer Dijkhoff vroeg naar de vertrouwelijkheid van meldingen. Ik deel zijn mening dat vertrouwelijkheid van groot belang is. Dat is ook onderwerp van gesprek met mensen van het bedrijfsleven, VNO-NCW cum suis. In mijn brief van 6 juli 2012 heb ik aangegeven dat het wetsvoorstel hierin zal voorzien.
Er werd gevraagd wanneer het programma Digivaardig & Digiveilig afgerond is. In dit programma werken overheid en bedrijfsleven intensief samen aan voorlichting aan en het bevorderen van bewustwording bij het midden- en kleinbedrijf, consumenten en de jeugd. Het huidige programma loopt formeel tot eind 2013. Awareness blijft cruciaal. Wij blijven ons daarvoor inzetten.

De **voorzitter**: Dank u wel, minister. Ik kijk even of er nog leden nu willen interrumperen.

De heer **Oskam** (CDA): Ik dank de minister voor zijn antwoorden, maar ik mis nog antwoorden op twee van mijn vragen. De eerste betrof de wederkerigheid van rechtshulpverzoeken. Wij begrijpen dat je snel moet handelen en dat je soms een verzoek om rechtshulp moet laten lopen. Het risico is echter dat andere landen dat ook gaan doen. Landen als Oekraïne en China zijn genoemd. Dat vinden wij natuurlijk vervelend. Hoe kijkt de minister daarnaar?
Verder is er ook nog geen aandacht besteed aan de vragen over policeware. Professor Jacobs noemde het overnemen van de identiteit. Potentiële verdachten zouden kunnen zeggen dat de politie de informatie op internet heeft gezet en niet zijzelf.

Minister **Opstelten**: Ik dacht dat ik al over die wederkerigheid had gesproken, over de rechtshulp en de internationale verdragen. De conferentie in Straatsburg is hiervoor van belang, waar 30 landen met elkaar hierover hebben gesproken. Als er sprake is van een vermeende aanval, zijn natuurlijk al onze diensten beschikbaar om maatregelen te nemen om daarop in te spelen. De vraag was of als wij met wetgeving komen, andere landen dat ook doen. In internationaal verband en EU-verband is dat natuurlijk een kwestie van afstemmen. Zo moeten wij daar volgens mij naar kijken. Was dat de bedoeling van de vraag van de heer Oskam?

De heer **Oskam** (CDA): Zeker. Het moet echter niet alleen in Europees verband, maar ook wereldwijd en met landen waar wij wat minder vertrouwen in hebben.

Minister **Opstelten**: In een aantal affaires die aan de orde zijn geweest, kwam dat in beeld. Wij zullen daar altijd met man en macht naar kijken. Gelukkig zijn wij zo langzamerhand in staat om elkaar publiek-privaat te ondersteunen. Ik vind het erg prettig om te weten ondersteund te worden door de media, experts, de wetenschap, het bedrijfsleven en commerciële dienstverleners. Als wij iets laten liggen dan zal men ons daar bijvoorbeeld in de publiciteit aan herinneren. Zo is de countervailing power op dit dossier georganiseerd. Dat geeft mij als bewindspersoon het comfortabele gevoel dat wij met de goede dingen bezig zijn.
Met policeware wordt de identiteit niet overgenomen. Wat wordt gedaan, wordt gelogd. Policeware wordt bovendien alleen ingezet na toestemming van de rechter-commissaris. Daarmee zijn de rechtstatelijke waarborgen aangegeven.

De heer **Oskam** (CDA): Het is prima dat de identiteit niet wordt overgenomen. Professor Jacobs heeft echter ook gezegd dat de mogelijkheid bestaat dat zo'n verdachte zegt dat bepaalde zaken door de politie zijn geplaatst en niet door hem of haar zelf.

Minister **Opstelten**: Op dit punt ben ik uitvoerig ingegaan in de beantwoording van de schriftelijke vragen van mevrouw Berndsen. Die is al naar de Kamer toegestuurd.

De **voorzitter**: Voor de volledigheid merk ik op dat dit vragen zijn van een individueel lid en dat de beantwoording daarvan derhalve niet op de agenda van dit overleg staat.

Minister **Opstelten**: Voor het gemak – ik kijk naar de klok, al mag dat niet – verwijs ik ernaar omdat het daarin heel uitvoerig is aangegeven. Daarin ben ik er heel specifiek op ingegaan.

De heer **Oskam** (CDA): Dat klopt, maar die antwoorden zijn pas vandaag binnengekomen. Ik had vandaag drie algemeen overleggen, dus die heb ik nog niet goed kunnen lezen.

Minister **Opstelten**: Daar heb ik respect voor, maar dan kunt u het thuis nog eens rustig nalezen.

De heer **Verhoeven** (D66): Ik raad de heer Oskam aan om antwoorden op vragen van D66 altijd prioriteit te geven bij de voorbereiding van debatten.
Ik wil nog een van mijn vragen even extra onder de aandacht brengen, al is de minister op een heleboel punten reeds ingegaan. Mijn punt is het op één hoop gooien van allerlei vormen van criminaliteit, niet zijnde cybercriminaliteit, om deze bevoegdheid op los te laten. Kan de minister

zijn afwegingen op dit terrein nog één keer noemen? Ik vind dit een heel cruciaal punt en daar hebben wij het eigenlijk bijna niet over gehad.

Minister **Opstelten**: Ik heb gesproken over de effectiviteit van de voorstellen en gezegd waarom het nodig is. Het is een zware bevoegdheid, dus er moeten zware zorgvuldigheidseisen worden gehanteerd. Het gaat om specifieke misdrijven. Ik heb ook een duidelijke grens getrokken. Ik neem uiteraard wat is gezegd in dit debat mee in de voorbereiding van het wetsvoorstel. Dat wetsvoorstel gaat publiekelijk in consultatie. Iedereen kan dat volgen. Ik hoop dat ik hiermee de heer Verhoeven en de D66-fractie ervan heb kunnen overtuigen dat wij met een zorgvuldig proces bezig zijn. Daarin ben ik inderdaad de balans aan het zoeken, want dat moet gebeuren.

De heer **Verhoeven** (D66): Ik vraag de minister om daarbij ook de opmerking van de heer Takkenberg, de chef van de High Tech Crime Unit van het KLPD, mee te nemen. Hij heeft eerder gezegd dat bepaalde grote criminaliteit kan worden aangepakt door veel betere recherchetechnieken, opsporingstechnieken, te gebruiken. Dat kan in bepaalde gevallen om een extra bevoegdheid vragen – dat geef ik toe – maar soms kan het ook binnen de bestaande bevoegdheden. Ik wil graag dat heel zorgvuldig aan de knop wordt gedraaid. Wij moeten niet de knop van de bevoegdheden volledig opendraaien en vervolgens achteroverleunen waar het gaat om mogelijke verbeteringen binnen de bestaande bevoegdheden. Daar zit in de kern mijn zorg.

Minister **Opstelten**: Dat vind ik een goed punt. Als het anders kan, met moderne recherchetechnieken zonder extra bevoegdheden, gebeurt dat. Dan ga ik de Kamer niet lastigvallen met wetsvoorstellen. Ik heb ook andere dingen te doen, net als de Kamer. Dat is duidelijk. Het is echter ook mogelijk dat de heer Takkenberg zegt dat hij dringend behoefte heeft aan deze bevoegdheden, dat de meest moderne recherchetechnieken met zich meebrengen dat hij deze bevoegdheden nodig heeft. Is dan de fractie van D66 te overtuigen?

De heer **Verhoeven** (D66): Niet alleen door die uitspraak.

Minister **Opstelten**: Ik zal dit punt en die afweging meenemen in het wetsvoorstel. Ik zal in de memorie van toelichting ingaan op die afweging. Ik zal ingaan op de vraag waar politietechniek eindig is in haar mogelijkheden en waarom er een extra bevoegdheid nodig is.

De heer **Bontes** (PVV): Stel dat policeware op computers wordt geplaatst. Is het dan niet mogelijk dat razendsnel software of antivirusware wordt ontwikkeld die deze gelijk weer verwijdert? De minister heeft nog niet geantwoord op de vraag of je niet steeds wordt achterhaald door de techniek en, zo ja, of het dan wel zin heeft om het te doen.

Minister **Opstelten**: Dat is een heel algemene vraag. Zoals gezegd, is de mening van de opsporingsdiensten dat wij achterlopen. Dat is een internationale constatering. Ik kijk zelf ter voorbereiding van een debat als dit altijd even twee jaar terug: waar stonden wij toen en waar zijn wij nu? Je moet de sense of urgency voelen en erop inspelen. De ontwikkeling gaat door. Ik neem dat punt mee. Wij moeten proberen om niet achter de feiten aan te lopen. Wij moeten inzien wat nodig is om cybercriminaliteit aan te pakken. Ik verwacht niet dat dit op korte termijn allemaal zal gebeuren. De door de politie te gebruiken software zal up-to-date moeten zijn en zal moeten inspelen op de mogelijkheden die er zijn. Op dit moment hebben we het niet te pakken. Ik doe een beroep op iedereen om

mee te denken, kritisch en ook constructief. Wij zijn er namelijk op dit moment nog niet.

De **voorzitter**: Hiermee zijn wij gekomen aan het einde van de eerste termijn. Ik zie dat er behoefte bestaat aan een tweede termijn.

De heer **Oskam** (CDA): Voorzitter. Ik heb nog maar één vraag aan de minister. Ik kijk naar de rol van de rechter-commissaris. Toetsing wordt nu aan de rechter-commissaris opgehangen. Normaal gesproken krijgt de rechter-commissaris van de politie en van de officier van justitie concrete informatie over een strafbaar feit. Daaraan kan hij het verzoek om een machtiging toetsen. Stel dat de politie iemand verdenkt van het bezit van kinderporno, maar de vraag is of zij het concreet kan maken omdat zij niet tevoren in de computer heeft kunnen kijken. De politie wil dan inbreken in een of andere cloud. De rechter-commissaris, die niet weet waar die cloud zich bevindt, moet dan toetsen aan verdragen en toetsen of de verdenking inderdaad wel voldoende concreet is. Waar toetst die rechter-commissaris nu aan?

De **voorzitter**: Mevrouw Oosenbrug geeft aan dat zij geen behoefte heeft aan een tweede termijn.

De heer **Dijkhoff** (VVD): Voorzitter. Ik dank de minister voor zijn heldere antwoorden. Hij zal wel proeven dat de VVD-fractie welwillend staat tegenover de wetsvoorstellen over bevoegdheden die wij gaan ontvangen, maar dat zij wel vragen heeft. Ik zie uit naar de scherpe discussie om uiteindelijk als Kamer tot een gedegen, effectieve en juiste balans in de aanpak te komen. Ik heb nog enkele vragen.
Ik heb een vraag over de waarborg. De rechter-commissaris wordt iedere keer genoemd. Die is in Nederland een beetje de heilige graal voor de waarborg van rechten en privacy. Moeten wij het zo houden dat alle rechters-commissarissen overal capabel op moeten zijn en zijn? Wat is de visie van de minister op het Britse voorbeeld, waarin een commissie een specifieke taak heeft?
Een ander punt was soevereiniteit bij grensoverschrijdende opsporing. De minister heeft er gelijk dat het niet per se zo is dat als wij ons een bevoegdheid toe-eigenen, andere landen iets gaan doen in Nederland. Er is weliswaar geen causaal verband, maar wellicht wel een moreel of juridisch verband. Het is natuurlijk zo dat de kwaaien het toch wel doen. Dan worden wij, overigens heel terecht, boos en willen wij het aanpakken. Dan komen wij een beetje in de sfeer van cyberdefence en cyberwarfare en niet in die van cybersecurity en cybercrime, terwijl ik het daar toch in zou willen houden. «If you can't beat them, join them» vind ik vooral erg geschikt voor supermachten en ik vrees dat Nederland dat niet is. De staatssecretaris is gisteren naar een bijeenkomst met 47 landen geweest om een gezamenlijke aanpak van kinderporno af te spreken. Ook hierover wil ik zo veel mogelijk gezamenlijke afspraken met landen, over het onderling rechtshulpverzoeken doen of meer in generale zin.
Er was een discussie over de campagne Alert online en de website alertonline.nl. Ik heb het zelf eigenlijk meer gezien als een tijdelijke actie met een digitale flyer, waarvan mijn recensie is dat ik die kostenbewust vond. Dat is ook wat waard. Ik had er ook eerlijk gezegd niet zo'n probleem mee. Het bewustzijn is erg belangrijk. Zo'n website recenseren is één ding, maar als je even rondkijkt dan zijn er al snel tien websites te noemen die er ooit voor een campagne voor bewustzijn waren en daarna een tijdje weer minder actief waren. Er is ook wel sprake van overlap. Ik vind dit zo belangrijk dat ik de minister voor een volgend algemeen overleg over cybersecurity wil vragen hoe dit meer gecoördineerd kan. Als ieder individu in Nederland niet zelf aan zijn beveiliging denkt, wordt het een heel zware taak voor de overheid om alles te waarborgen. Ik

begrijp dat er meerdere ministeries bij betrokken zijn, maar ik zie toch een leidende rol hier.

De **voorzitter**: Gaat u afronden, mijnheer Dijkhoff?

De heer **Dijkhoff** (VVD): Mijn vraag is of wij voor het volgende algemeen overleg een coherenter beeld kunnen krijgen van de bewustwordingscampagnes.

De heer **Bontes** (PVV): Voorzitter. In mijn eerste termijn heb ik gezegd dat de scheidslijn tussen het vechten tegen cybercrime en de privacy van burgers flinterdun is. De minister heeft zijn uiterste best gedaan om alle vragen te beantwoorden. Hij heeft er ook wel een verhaal bij. Ik ben echter nog niet over de streep getrokken wat betreft de vraag of dit de goede weg is. Ik wijs ook op de kritiek uit zijn eigen denktank, de Cyber Security Raad. Ik vraag de minister om daar heel nadrukkelijk mee in gesprek te gaan, net als met andere organisaties zoals Bits of Freedom. Daarvoor moet ook de deur worden opengehouden. De minister heeft dat al toegezegd. Ik hoop dat dit trechtert naar een plan waar wij wel ja tegen kunnen zeggen. Op dit moment vind ik het nog te riskant om te zeggen: dit is de goede weg en het zit wel snor.

De heer **Verhoeven** (D66): Voorzitter. Dat geldt ook voor D66. Ik geef toe dat ik wat vooringenomen naar dit debat ben gekomen. Ik heb met veel interesse naar de minister geluisterd. Hij is serieus ingegaan op een aantal kritische vragen, waarvoor mijn dank. Ik zag een groot rood sein toen ik langs dit spoor moest en dacht: dat moeten wij maar niet doen. Ik zie nu nog lang geen groen sein. Dit is een mooie uitdaging voor de minister. Er is ook een uitgestoken hand van mij, en dus ook van de PVV, naar de minister. Verbeter het, maar doe dan ook echt iets met wat er is gezegd. Anders kan dit wat ons betreft niet doorgaan. Ik dank de minister voor zijn toezegging om in de memorie van toelichting in elk geval in te gaan op vragen als tot hoever je bij welke criminaliteit moet kunnen gaan en vooral wanneer er wel of niet een nieuwe bevoegdheid nodig is, wat een kwestie is van bevoegdheid versus nieuwe technieken.
Ik dank de minister ook voor de toezegging om mijn verzoek inzake een kleinschalige inrichting van de BIR door te geleiden naar de minister voor Wonen en Rijksdienst. Mijn vraag is om ook in te gaan op het afhankelijk zijn van één beveiligingssysteem.
Gaat de minister nu gewoon doordenderen op basis van: met elke stap die ik zet, kom ik wel weg? Of gaat hij echt de koers veranderen als wij stuiten op technische, juridische of ethische barrières? Durft hij dan ook zover te gaan om er geen politiek prestigeproject van te maken, maar echt te zeggen: als het te ver gaat, gaat het te ver en waar het te ver gaat, ga ik ervoor zorgen dat het kan op een manier die wel past binnen een aantal van de kaders? Dat is eigenlijk mijn hoofdvraag voor nu.

De **voorzitter**: Nu nog een korte inbreng van de SP-fractie, die ik zelf zal doen.
Ik dank de minister voor zijn beantwoording. Ik ben erg blij dat wij vandaag te horen hebben gekregen dat een aantal zaken goed op koers ligt en dat wij de komende tijd nog een heel aantal stukken, van actieplannen tot nieuwe wetsvoorstellen, tegemoet kunnen zien.
Ik wil nog één punt onder de aandacht brengen. In de rondetafelgesprekken die wij hebben gevoerd naar aanleiding van de crisis rond DigiNotar hebben wij van diverse mensen uit onder meer de hackercommunity te horen gekregen – dat hangt heel erg samen met de discussie die wij vandaag volgens mij vrij diep hebben gevoerd over de vraag hoever je moet gaan met de opsporingsbevoegdheden, met het hacken door de politie – dat wij wel een beetje ver doordenderen. Wij maken

onszelf enorm snel te afhankelijk van ICT. Dat geldt zowel voor de overheid als voor burgers, die gedeeltelijk gestimuleerd zijn door de overheid en het bedrijfsleven. De aanpak van kinderpornografie is iets anders. Als je een volgende stap zet, moet je je als overheid heel bewust zijn van die afhankelijkheid van ICT bij het bestrijden van gewone criminaliteit, zoals het stelen van bankgegevens via een botnet of ander malware of spionage. Als je spreekt met raadsheren of andere mensen die met de rechterlijke macht te maken hebben, kan het soms ook wel eens verstandig zijn om je te realiseren dat je af en toe een pas op de plaats moet maken. Als je dat niet doet en jezelf verder afhankelijk maakt van ICT, word je langzamerhand toch naar de door de heer Verhoeven het scherpst neergezette afgrond van het opofferen van grondrechten gedwongen. Daar moeten wij ons met zijn allen wel erg bewust van zijn.
Ik heb nog een heel korte tweede vraag. Ik heb van NU.nl begrepen dat er onrust is onder ethische hackers, zoals wij ze maar even moeten noemen, over het meldpunt. Er zijn signalen dat het op te richten meldpunt nu al wordt gewantrouwd, naar aanleiding van de zaak rond de hack bij het Groene Hart Ziekenhuis. Kan de minister daar kort op reageren?

Minister **Opstelten**: Voorzitter. Ik zal met de hoofdlijn beginnen, waar mevrouw Gesthuizen, de heer Verhoeven en de heer Bontes over spraken. Ik wil de commissie dankzeggen voor de constructieve wijze waarop het debat, naar mijn idee, is gevoerd. De leden zijn hier met verschillende invalshoeken naartoe gekomen, maar toch open. Ik ben mij ervan bewust dat nog niet iedereen het licht op groen heeft gezet. Daar is ook geen aanleiding voor. Wij zitten aan het begin van een discours, een dialoog daarover. Die wil ik ook in alle scherpte voeren. Ik wil er ook geen misverstand over laten bestaan dat het totaal niet aan de orde is dat inbreuk op grondrechten en andere rechtstatelijke elementen mogelijk wordt gemaakt. Het is altijd goed in het leven om af en toe een pas op de plaats te maken als dat verstandig is. Ik zal de eerste zijn die dat doet en zal dan ook uitleggen waarom ik dat doe. Van politiek prestige is wat dit onderwerp betreft totaal geen sprake. Wij moeten hier gewoon iets doen omdat er iets aan de hand is in de samenleving. Daarbij wordt naar de overheid gekeken om maatregelen te nemen die noodzakelijk zijn om criminaliteit te bestrijden, zoals wij dat anders ook doen, in een andere situatie dan wij normaal gewend waren. Zo zit ik erin en niet anders. Ik wil met een goed wetsvoorstel komen. Ik vind het plezierig dat er handen naar mij zijn uitgestoken. Ik zal proberen die handen aan te grijpen.
Ook de heer Oskam geeft er blijk van dat hij daarop koerst. Hij vraagt op grond waarvan de rechter-commissaris zijn afweging moet maken. Die moet telkens – daarom is dat een mooie functie – afwegen. Hij toetst aan de wet en aan de ernst van het feit. In deze situaties is dat ook aangegeven. Het is niet gemakkelijk de afweging te maken of er voldoende aanleiding is om die maatregelen te nemen. Ik kan daar nog veel specifieker op ingaan, maar ik denk dat dat voor dit debat niet nodig is. Wij zullen die vraag nog specifieker in het wetsvoorstel aan de orde stellen.
Er was een vraag over een causaal verband ten aanzien van opsporing. Internet is inderdaad internationaal. Daarover is in Straatsburg gesproken. Er wordt in de Brusselse arena heel veel over gesproken. De staatssecretaris is gisteren bij een bijeenkomst over kinderporno geweest. Het is heel goed dat hij daarheen is gegaan. Het is duidelijk dat er over dergelijke zaken goede, sterke en strakke afspraken zijn gemaakt. In internationaal verband afspraken maken is ook mijn inzet. Dat moeten wij goed in de gaten houden.
Er was een vraag over ethisch hacken en de visie van de Cyber Security Raad daarover. Dat onderwerp is diverse malen aan de orde geweest in de raad, evenals responsible disclosure. De raad hecht eraan om over deze onderwerpen een afgewogen inhoudelijke dialoog te voeren. Deze heeft

echter nog niet plaatsgevonden. De hoofdlijnen van de gewenste verstandige relatie tussen de overheid en het bedrijfsleven en ethische hackers wordt door de raad onderschreven. In de eerstvolgende vergadering zal de raad nadrukkelijk stilstaan bij dit onderwerp en een advies geven aan mij. Ik zal dat meenemen bij het opstellen van de maatregelen die wij moeten nemen.
Mevrouw Gesthuizen stelde dat er sprake is van onrust ten aanzien van het meldpunt. Ik heb er vertrouwen in dat het contact met responsible hackers zal blijven bestaan. Ik heb al benadrukt dat ik mij nadrukkelijk inzet om de kennis uit de ICT-community te gebruiken en er zorg voor te dragen dat deze kennis bij de juiste partijen belandt.
De heer Verhoeven vroeg of ik niet doordender. Ik dacht van niet, althans niet op dit onderwerp. Ik maak wel tempo. Wat mevrouw Gesthuizen zei, spreekt mij aan. Hier vindt natuurlijk voortdurend reflectie plaats. Na zo'n debat vindt reflectie plaats. Ik ga straks als deze vergadering afgelopen is opdracht geven om het wetsvoorstel in een paar weken conform de brief klaar te maken en op de site te zetten voor consultatie. Zo gaat het altijd na een debat. Ik kijk met mijn mensen wat de hoofdconclusies zijn, waar wij lessen moeten trekken, met wie wij nog moeten praten en welke relevante adviezen wij binnen hebben gekregen. Ik communiceer ook met mensen met wie ik het niet eens ben, ook als ik weet dat wij het misschien niet eens zullen worden. Ik wil met hen wel communiceren en het gesprek aangaan. Zo zitten wij erin.
Dit is een onderwerp waar ik nog wel vrij lang over zou kunnen spreken, maar de commissie biedt mij niet de kans doordat zij verder geen vragen heeft gesteld.

De **voorzitter**: Ik wil u best nog één interruptie geven, als woordvoerder van de SP-fractie. Heb ik goed begrepen dat de minister zegt dat het hem niet bekend is dat er op dit moment onrust is in de hackercommunity? Is hem niet bekend dat er vanuit diverse hackerspaces, zoals Frack, wordt gezegd dat zij niet weten of zij zich daar nog wel willen melden en dat zij gaan zoeken naar andere manieren om datgene waar zij zich zorgen over maken kenbaar te maken?

Minister **Opstelten**: Nee, anders zou ik dat niet zeggen. Nadat mevrouw Gesthuizen dat bij herhaling heeft gevraagd, heb ik natuurlijk weer rechts en links gekeken. Ik word daarin nog steeds bevestigd. Bij het opstellen van het kader voor responsible disclosure wordt nadrukkelijk het gesprek aangegaan met potentiële melders. Dit kader zal eraan bijdragen dat hackers makkelijker het gesprek kunnen aangaan met partijen waar zij een kwetsbaarheid aantreffen. Bij het opstellen van het Cyber Security Beeld Nederland-3 zal wederom de ICT-community worden benaderd voor het leveren van een bijdrage. Wij steken voortdurend de hand uit naar de hele ICT-community met de vraag om te reageren. Zo proberen wij het vertrouwen dat er is vast te houden. Dat is ook onze plicht en taak. Daar leren wij van. De kritiek en de angst hebben wij niet gevoeld. Die was bij ons niet bekend. Ik dank mevrouw Gesthuizen voor het signaal dat zij ons heeft gegeven.

De **voorzitter**: Het was ook openbaar te lezen. Ik zie dat de heef Dijkhoff nog een vraag heeft.

De heer **Dijkhoff** (VVD): Ik heb gevraagd of de rechters-commissarissen allemaal in staat zijn om over dit soort zaken te oordelen. Ook heb ik gevraagd naar het model van de Britse specifieke commissie. Ik kan mij voorstellen dat die bij de voorbereiding van het wetsvoorstel onder het kopje waarborgen nog apart worden behandeld, maar misschien kan het ook nu.

Minister **Opstelten**: Ik dacht dat ik het impliciet al had gezegd. Zelfs bij rechters-commissarissen komt het voor dat men middels ervaring en opleiding nog extra tools binnen moet krijgen. Wij gaan natuurlijk niet een wetsvoorstel entameren terwijl wij in de uitvoering de kwaliteit en de capaciteit niet in huis hebben. Die fout maak ik niet, daar kan de heer Dijkhoff van op aan. Dit punt, dat de heer Dijkhoff terecht bij herhaling opvoert, vind ik een heel zwaar punt. Het gaat om de vraag of de kwaliteit en de capaciteit in de hele keten aanwezig zijn. Die zullen aanwezig moeten zijn, want anders moet je het niet doen.

De **voorzitter**: Hiermee is een einde gekomen aan de beantwoording van de minister in tweede termijn en ook aan het gehele debat. Ik dank alle aanwezigen voor hun komst. De vergadering wordt dus drie kwartier eerder dan gepland gesloten.

Sluiting 18.16 uur.