Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 312

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 21 mei 2014

De vaste commissie voor Veiligheid en Justitie en de vaste commissie voor Defensie hebben op 27 maart 2014 overleg gevoerd met Minister Opstelten van Veiligheid en Justitie over:

- **de brief van de Minister van Veiligheid en Justitie d.d. 3 juli 2013, houdende aanbieding van het Cyber Security Beeld Nederland – 3 (Kamerstuk 26 643, nr. 285);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 28 oktober 2013, houdende aanbieding van de Nationale Cyber Security Strategie 2 (Kamerstuk 26 643, nr. 291);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 12 december 2013 over de versterking van de positie van het Nationaal Cyber Security Centrum (NCSC) (Kamerstuk 26 643, nr. 297).**

Van dit overleg brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

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

De voorzitter van de vaste commissie voor Defensie,
Ten Broeke

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Doorn

kst-26643-312
ISSN 0921 - 7371
's-Gravenhage 2014

Voorzitter: Jadnanansing
Griffier: Tielens-Tripels

Aanwezig zijn zes leden der Kamer, te weten: Bontes, Gesthuizen, Jadnanansing, Oosenbrug, Van Oosten en Verhoeven,

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

Aanvang 14.36 uur.

De **voorzitter**: Goedemiddag. We hebben met elkaar een spreektijd van vijf minuten per woordvoerder afgesproken, met twee interrupties. Ik heet de mensen op de publieke tribune van harte welkom, evenals de Minister, zijn ambtenaren en mijn collega's.

De heer **Van Oosten** (VVD): Voorzitter. We hebben het vandaag over cybersecurity: een veilige digitale omgeving. Het is een omgeving waarin, net als in de fysieke wereld, wordt gewerkt, waarin je geld verdient en waarin contacten met de overheid worden onderhouden. Dan moeten we vaststellen dat in die digitale wereld ook boeven ronddwalen. Ze zijn niet op jacht naar je fiets, maar proberen je wachtwoord te bemachtigen om daarmee zonder toestemming informatie uit je computer te jatten. Daarmee is de tijd waarin je als een soort halve naïeveling op het internet kon rondstruinen, nu echt wel passé. Zoals iedereen zelf verantwoordelijk is om te zorgen voor een stevig fietsslot, zo mag ook van de computergebruiker een hogere beschermingsgraad worden verwacht. Met andere woorden: als internetgebruikers hebben wij allemaal de verantwoordelijkheid om te zorgen voor een goed antivirussysteem en een stevig cyberslot. Die verantwoordelijkheid kunnen we niet geheel afschuiven op de overheid of het bedrijfsleven. Daarin past een eigen rol.
Dit laat onverlet dat onze overheid wat mij betreft wel hard moet optreden tegen bedrijven die hun geld verdienen met het aanbieden van software die alleen een kwaadaardig doel dient, als business. De Minister schrijft er in zijn brief zelf ook over: «cybercrime-as-a-service», om maar bij de Engelstalige aanduiding van dit AO te blijven. Daarom vraag ik de Minister of er voldoende middelen en een wettelijke basis voorhanden zijn om dit soort criminaliteit bij de bron aan te pakken.
Ik heb ook een vraag over de beveiliging van de overheid zelf. Recentelijk vernamen we dat Windows XP ermee ophoudt. Hoeveel computers draaien daar nog op? En hoeveel draaien er op andere verouderde software? Moet niet actiever gebruik worden gemaakt van bijvoorbeeld versleuteling en toegangsbeveiliging bij overheidssystemen?
Hoe veilig is de communicatie van de overheid zelf? Klopt het dat op dit moment bijna alle e-mailcommunicatie tussen ambtenaren onderling en tussen ambtenaren en burgers onversleuteld wordt verstuurd? Wordt het geen tijd dat het NCSC – in de stukken kom je nogal wat afkortingen tegen – oftewel het Nationaal Cyber Security Centrum voor ambtenaren software en best practices op een rijtje zet om berichten versleuteld te kunnen versturen en dat burgers erop wordt gewezen hoe zij dat kunnen gaan doen? Op die manier zou de overheid eraan kunnen bijdragen dat we niet alleen beter worden beschermd tegen buitenlandse inlichtingendiensten maar bijvoorbeeld ook tegen criminelen die persoonlijke gegevens misbruiken voor fraude.
In hoeverre is de samenwerking tussen het NCSC en de andere diensten op orde? De AIVD is bijvoorbeeld verantwoordelijk voor de beveiligingsadviezen aan overheidsinstanties over communicatiemiddelen. Heeft het Nationaal Cyber Security Centrum de lead, om het zo maar uit te drukken, in de coördinatie van dit dossier, of is dat een andere overheidsdienst? En welke rol speelt dan de Cyber Security Raad? Strekt die zich ook uit tot

taken van defensie? Het is een flink aantal vragen, maar eigenlijk komen die erop neer dat ik wil voorkomen dat we in allerlei competentiedisputen terechtkomen. Wellicht kan de Minister dit verduidelijken.
Ik heb nog een paar kleine onderwerpen. Het eerste punt betreft de aanbestedingen. Het zou een goede zaak zijn als we het zo kunnen organiseren dat innovatieve clubs, organisaties met oog voor cybersecurity en nieuwe tools, in aanmerking kunnen komen voor ook overheidsopdrachten die betrekking hebben op de veiligheid van de vitale digitale infrastructuur. Kan de Minister dit punt oppakken, wellicht ook in overleg met de Minister van Economische Zaken?
Het tweede en laatste punt gaat over de cloud. Het zijn flink wat Engelse termen allemaal. We weten dat Amerikaanse wetgeving ver kan reiken als het gaat om het opvragen van data. Hebben we goed doorgrond welke risico's de Nederlandse overheid op dit punt loopt in het geval dat overheidsdiensten van die cloud gebruikmaken?

De heer **Bontes** (Bontes): Voorzitter. In de derde editie van het Cybersecuritybeeld Nederland wijst de Minister op burgers, bedrijven en overheden die regelmatig het slachtoffer zijn van botnets en ransomware. Het Nationaal Cyber Security Centrum – ik zal hierna de afkorting «NCSC» gebruiken – focust alleen op de vitale sectoren van Nederland, daarbij inbegrepen de rijksoverheid. Het is een belangrijke kabinetsdoelstelling om zo veel mogelijk 24/7 onlinedienstverlening te kunnen leveren. Tevens is er de kabinetsdoelstelling om dit te bereiken in 2017. Is de Minister het met mij eens dat voorzieningen van de overheid, zoals DigiD, ook binnen het vitale pakket zouden moeten vallen?
DigiD is vaak getroffen door ddos-aanvallen. Gelukkig was DigiD niet offline in de afgelopen periode waarin Nederlanders massaal hun belastingaangiftes indienden. Naar aanleiding van het Diginotar-debacle verneem ik graag van de Minister of PKIoverheid – zo heet die organisatie nu eenmaal; PKI staat voor Public Key Infrastructure – inmiddels ook een zeer kort lijntje heeft met het NCSC. En is de Minister voornemens om PKIoverheid «vitaal» te verklaren? Kan hij ten minste de Kamer bij brief informeren over vitale onderdelen bij de overheid die onder de scope van het NCSC vallen?
Dit brengt mij bij een ander belangrijk punt: Windows XP. Uit berichtgeving blijkt dat met name gemeenten te laat zullen zijn met de overstap naar een nieuw besturingssysteem. Ik ben erg benieuwd naar de wijze waarop de expertise van het NCSC als nationaal expertisecentrum en spin in het web, zoals de Minister vaak zegt, wordt ingezet.
Hoe zit het met de gewone burger? Hoe attendeert de Minister burgers op cybergevaren, los van de updates op de website waarschuwingsdienst.nl? Hoe ziet hij zijn rol? En wat wil hij nog meer doen? Behoort bijvoorbeeld een campagne tot de mogelijkheden?
Verder steun ik uiteraard de versterking van de positie van het NCSC. Op welke wijze werkt het NCSC samen met de Informatiebeveiligingsdienst voor gemeenten? De expertisefunctie en de rol van spin in het web is er niet voor waterschappen en provincies. Hoe zorgt de Minister ervoor dat alle partners in het openbaar bestuur zijn aangesloten bij de versterkte positie van het NCSC?
Tot slot – ik ben er al even op gekomen toen ik het had over DigiD – vraag ik waarom bepaalde onderdelen van de overheid niet «vitaal» worden verklaard. Ik denk aan DigiD, PKIoverheid, het GBA en het CBS. Deze instanties beschikken over zeer vertrouwelijke gegevens van burgers en bedrijven. Ik vraag aan de Minister om in samenspraak met zijn collega van Binnenlandse Zaken een lijst van essentiële overheidsonderdelen vast te stellen. Graag krijg ik een reactie op dit punt. Mijn laatste vraag is dus: een lijst van essentiële overheidsonderdelen op dit gebied.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Uit de Nationale Cyber Security Strategie 2 blijkt dat de omgang met dit onderwerp volwassen is geworden. We begonnen met een algemeen beleid om de alertheid bij burgers, bedrijven en overheid te vergroten, maar nu zetten we de stap vooruit naar de gerichtere aanpak van zwakke plekken in onze digitale veiligheid. In de afgelopen jaren hebben we kennis opgebouwd over de zwakke plekken en hebben we samenwerking tot stand gebracht tussen bedrijven en overheid, met het Nationaal Cyber Security Centrum als verbindend centrum. In de komende jaren kan op deze infrastructuur worden voortgebouwd, waarbij we onze kennis ook kunnen gaan delen met andere landen. Voor ons ligt de nadruk in de eerste plaats op een goed functionerende ICT in Nederland, maar tegelijk wordt waardevolle kennis opgebouwd, waarbij andere landen baat kunnen hebben.
In de afgelopen jaren hebben we meermaals aandacht gevraagd voor de versterking van de rol en de positie van het Nationaal Cyber Security Centrum – ik zal het «NCSC» noemen, want anders moet ik die lange naam steeds uitspreken – en de Minister werkt daar nu aan. Dat is een proces waarin we weloverwogen keuzes moeten maken. We willen immers dat het NCSC een gelijkwaardige partner is, waarmee partijen op een veilige manier gevoelige gegevens kunnen delen, en dat vitale sectoren verplicht zijn om inbreuk op hun datasystemen te melden aan het NCSC. Wat is de visie van de Minister op die gelijkwaardige rol? Hoever is het daar inmiddels mee gesteld? Wordt die rol, die eigenlijk door de wet is afgedwongen, op een goede en effectieve wijze vervuld? We willen ook graag weten hoe het zit met de wet op de meldplicht voor datalekken en de voorgenomen wet melding inbreuken elektronische informatiesystemen. Hoever staat het daarmee?
Hierop aansluitend wil ik toch nog maar weer eens de aandacht vragen voor de onafhankelijke beveiligingsexpert, in de volksmond ook wel «ethische hacker» genoemd. De Minister van BZK heeft besloten om binnenkort een «hackathon» over antifraude te organiseren, waarin hij zal laten zien dat het allemaal niet zo eng is als het lijkt. Heel vaak spreken we over hacken als iets dat heel eng is. Toch denk ik dat we die hackers, in samenwerking met het NCSC, moeten inschakelen. Natuurlijk, er zijn verschillende soorten hackers. Er zijn mensen die echt kwaad willen doen. Daar spraken mijn collega's al over. Ik wil echter de nadruk leggen op de mensen die het goed willen doen, op juist deze sociaal-maatschappelijk bewogen mensen die willen meehelpen. Nogmaals dus mijn uitgebreide oproep om dit nu eens te omarmen. Zorg er nu eens voor dat deze mensen worden ingeschakeld. Binnenlandse Zaken doet dit inmiddels. Ik zie graag hoe Veiligheid en Justitie hier inmiddels mee omgaat.
Het is goed om te zien dat de regering ambitieus is op de agenda voor cybersecurity. Er wordt veel gesproken over investeringen in cyberveiligheid door overheid en bedrijven, het vergroten van de capaciteit bij verschillende organen en meer opleiding op het gebied van veiligheid en ICT. Wat hier ontbreekt, zijn de geldbedragen. Maar deze agenda is natuurlijk meer dan alleen mooie woorden. Kan de Minister ook de financiële kant van zijn agenda verduidelijken? Wie investeert uiteindelijk, en hoeveel?
Ook ik heb nog een stukje over Windows XP, waarover mijn collega's ook al spraken. Ik heb er ook schriftelijke vragen over gesteld. We vragen namelijk ook veel aandacht voor de eigen verantwoordelijkheid van burgers om een bijdrage te leveren aan de digitale veiligheid. In de NCSS – het zijn allemaal afkortingen – oftewel de Nationale Cyber Security Strategie wordt dat mooi beschreven als «cyberhygiëne», die in zekere mate van de burgers mag worden verwacht. Een onderdeel daarvan is op dit moment het advies om Windows XP te vervangen omdat de ondersteuning door Microsoft afloopt. Maar goed, de vragen daarover zijn al gesteld. De overheid moet hierin natuurlijk wel het voortouw nemen en laten zien dat ze dit advies zelf ook ter harte neemt: ze moet ervoor zorgen

dat de systemen binnen de overheid die nu nog op Windows XP draaien, zo snel mogelijk worden vervangen.
Ik kom op de inzet van policeware, software waarmee de politie zich toegang kan verschaffen tot computers en andere systemen. Ik ga het er toch nog even over hebben. In technische en juridische kringen heb ik hierover veel gesproken. Er is daar veel discussie over deze verregaande bevoegdheden voor de overheid. De grootste twijfel over de mogelijke extra risico's betreft de onduidelijkheid over de systemen waarop de policeware kan worden ingezet. Bij het terughacken worden vraagtekens gezet. Hoe verhoudt dat zich tot het internationale recht? En wat zijn de mogelijke repercussies door andere landen? We herkennen deze problemen en willen graag van de regering weten welke voortgang er is geboekt met het betreffende wetsvoorstel inzake computercriminaliteit.

Mevrouw **Gesthuizen** (SP): Voorzitter. Eén bevinding uit het Cyber Security Beeld Nederland – 3 is dat de eindgebruiker een grote verantwoordelijkheid krijgt voor beveiliging, terwijl hij steeds meer wordt geconfronteerd met kwetsbaarheden in apparaten en diensten waarop hij maar beperkte invloed heeft of waarvan hij geen kennis heeft. Hoe ziet de Minister deze ontwikkeling? Op welke wijze kan de gebruiker hierop volgens hem meer grip krijgen?
Er staan zeker interessante zaken in de Nationale Cyber Security Strategie. Het is een heel belangrijk onderwerp. Ik heb er nog wel de nodige vragen over. Ik vind het speerpunt van het haalbaarheidsonderzoek voor een gescheiden netwerk voor de vitale infrastructuur erg interessant. Wanneer kunnen we dit onderzoek verwachten? Zijn er al andere landen waar een dergelijk systeem is geïmplementeerd? Zo ja, kan de Minister de ervaring in andere landen meenemen in zijn eigen onderzoek?
Ook het versterken van het Nationale Cyber Security Centrum kan ik zeker ondersteunen. Ik ben er al eens op werkbezoek geweest. In de commissie loopt nu een procedure om er nogmaals op werkbezoek te gaan. Volgens mij hebben we met elkaar afgesproken dat we zullen gaan. Dat is heel goed. Ik keek destijds mijn ogen uit. Ik kijk hierbij ook even naar de man aan de rechterzijde van de minister; hij heeft mij toen ontvangen. Hij zit nu nog bij het centrum. Ik begreep toen dat het erg lastig is om aan voldoende goed gekwalificeerd personeel te komen. Hoe staat het daar nu mee? Beschikt het centrum over voldoende mensen? Ook ben ik benieuwd hoe het staat met de capaciteit van de politie. Is er voldoende tijd, geld en mankracht beschikbaar om een eerlijke strijd te voeren tegen cybercriminaliteit?
Natuurlijk steunen we de Taskforce Cybersecurity Onderwijs. Voor de toekomst is het van groot belang om voldoende kundige mensen te hebben. Hoeveel personen is de Minister van plan jaarlijks op te leiden? Hoe groot is de behoefte aan goed gekwalificeerd personeel? Is deze taskforce voldoende uitgerust om voldoende mensen op te leiden?
Ik ben benieuwd of de Nationale Cyber Security Strategie volledig aansluit op de wensen en prioriteiten van de Europese Commissie. Zij benadrukt onder andere dat voor een optimale coördinatie op nationaal niveau alle betrokken ministeries moeten samenwerken. Is dit nu reeds het geval? Zo ja, welk ministerie is eindverantwoordelijk?
In de brief over de juridische verkenning betreffende de verwerking van gegevens door het NCSC schrijft de Minister dat hij in uitzonderlijke gevallen melding zal doen aan het verantwoordelijke ministerie als organisaties niet voldoende ondernemen bij cybergevaar. Blijft dit slechts informerend of heeft de Minister ook mogelijkheden om van organisaties te eisen dat ze direct actie ondernemen? Ik kan me zo voorstellen dat dit in een aantal gevallen zeer urgent is.
De Minister schrijft in zijn brief over de versterking van de positie van het NCSC dat hij het wenselijk acht dat ook de bevoegdheid tot het verwerken van andere gegevens, bijvoorbeeld door malware verkregen gegevens,

wordt voorzien van een concrete wettelijke basis. Valt de aanpak van botnets ook onder deze wettelijke basis? Er is immers bij veel organisaties nog onduidelijkheid over wat wel en wat niet mag bij de aanpak van botnets. Ik heb hier nog een aantal concrete vragen over. Wat is de botnetaanpak van het kabinet? Is het NCSC dé centrale plaats waar organisaties en mensen terechtkunnen als ze worden geconfronteerd met (de gevolgen van) botnets? Is er toezicht op de activiteiten bij de aanpak van botnets die gevolgen kunnen hebben voor a.) de privacy van burgers, b.) de integriteit en vertrouwelijkheid van de data van burgers en c.) de werking van computers en netwerken van burgers en bedrijven? Welke visie heeft het kabinet op de privacy bij de aanpak van botnets? Welke aansprakelijkheid geldt voor overheidsorganisaties, dus ook voor het NCSC en zijn partners, en private partijen als bij de aanpak van botnets iets mis zou gaan? Wie heeft formeel de leiding bij de (opsporings)onderzoeken naar botnets, en waarom? Is de Minister van mening dat de aanpak van botnets op dit moment voldoende is geformaliseerd? Zo ja, zijn de procedures dan voldoende duidelijk voor alle betrokken partijen, inclusief de aangevers? Is er voldoende toezicht? Zijn de veiligheidsmaatregelen afdoende? Is, tot slot, de privacy van de burger voldoende gegarandeerd?

De heer **Verhoeven** (D66): Voorzitter. Als een van de weinige landen is Nederland echt actief bezig met cybersecurity: er komt een Nationaal Cyber Security Centrum, jaarlijks komt er een Cyber Security Beeld en de Nationale Cyber Security Strategie wordt regelmatig geüpdatet. Daarmee lijkt de cyberverdediging van Nederland goed op orde. We zijn ons bewust van de dreigingen, we hebben een strategie die samenhangt met andere beleidsterreinen en we hebben een compleet centrum, waar alles samenkomt. «Lijkt», zeg ik, want ik maak me wel heel veel zorgen over de richting die de Minister inslaat. Dat is niet voor het eerst in dit soort debatten over cybersecurity. D66 staat voor vrijheden, voor een open internet en voor jezelf kunnen zijn. De Minister zegt in debatten altijd dat hij daar ook voor is, maar onder het mom van veiligheid doet hij nog weleens de verkeerde dingen. Op drie van die gebieden wil ik vanmiddag ingaan.
Allereerst ga ik in op het NCSS, op het monitoren. Laat ik het maar heel duidelijk zeggen: D66 wil geen cyberpolitiestaat, dus geen grootschalige monitoring van cruciale netwerken. D66 wil daarentegen eindelijk eens een fatsoenlijke meldplicht voor alle incidenten en enkel een internetkoppeling waar nodig. Ik noem een voorbeeld uit de niet-digitale wereld: als je met mensen afspreekt dat ze de politie bellen op het moment dat ze iets zien, hoef je ook niet overal camera's op te hangen. D66 wil daarom dus ook niet dat de Minister in de gaten houdt wie er allemaal internetbankieren bij de ING. Zorg er dus voor dat die meldplicht voor cyberinbraken er gewoon snel komt. Ik vraag de Minister concreet: waar blijft dat wetsvoorstel? Kan de Minister toezeggen dat met belangrijke meldingen daadwerkelijk iets gebeurt? Ik denk even aan de melding van het gevaarlijke, risicovolle computervirus waarop de ACM, de Autoriteit Consument & Markt, drie dagen bleef zitten voordat ze bekendmaakte dat het misschien weleens gevaarlijk was en communiceerde naar de mensen. Dat was niet snel en niet goed. Aanvullend vindt D66 dat je niet alles aan het internet moet willen koppelen. Het is een ontwikkeling dat alle apparaten aan het internet worden gekoppeld, maar waarom moeten sluizen eigenlijk worden gekoppeld aan het internet? Is dat wel wenselijk? En is het wel echt nodig? Dat iets kan, wil nog niet zeggen dat het ook direct goed is. Met een extra hek om een elektriciteitscentrale hoef je enkel camera's op je eigen terrein op te hangen en hoef je niet overal een heel stelsel van camera's te hebben. Kan de Minister ingaan op de kwetsbaarheden in de vitale sectoren en de noodzaak van koppeling aan het internet?

Het tweede punt betreft de bevoegdheden voor de diensten om te spioneren. D66 is altijd huiverig geweest, en heeft dat ook altijd gezegd, voor meer taken en meer bevoegdheden voor de veiligheidsdiensten op het gebied van cyberspionage. We willen vooral inzetten op meer bewustzijn, op meer «doe-het-zelfweerbaarheid» oftewel, om het iets concreter te maken, op goede firewalls, software die up-to-date is, maar bijvoorbeeld ook openbare broncodes en softwareaansprakelijkheid. Juist deze dingen laat de Minister echter liggen in zijn strategie. Hij heeft het over meer bevoegdheden en allerlei nieuwe mogelijkheden, maar hij laat de dingen liggen die heel praktisch en heel werkzaam zouden kunnen zijn. Dat is wel vaker gebeurd. Dat vind ik gewoon jammer. Welke mogelijkheden ziet de Minister voor versterking van de verantwoordelijkheid van de softwareleveranciers? De discussie begint op Europees niveau een klein beetje te spelen, maar wat is het standpunt van onze eigen minister? Kan hij reageren op de suggestie om meer te werken met openbare broncodes?
D66 vermoedt – dat vermoeden is zeer sterk, zo kan ik wel zeggen – dat bij het aanpakken van spionage het niet echt helpt als je eigen wetgeving gaat creëren om in andere landen in te breken in computers. Als je zelf gaat inbreken in andermans computers, dan neem je de remmingen bij andere landen om hetzelfde bij ons te doen, natuurlijk weg. Kan de Minister daarom toezeggen dat dit gedeelte uit zijn voorstel, waarover binnenkort zal worden gesproken, wordt gehaald? Het is het voorstel dat wij altijd het voorstel voor de inbreekpolitie of de hackpolitie noemen, maar in ieder geval is het het wetsvoorstel dat binnenkort naar de Kamer komt.

De heer **Van Oosten** (VVD): Ik hoorde de heer Verhoeven, volgens mij in het vorige blok, zeggen dat de Minister een aantal onderwerpen links laat liggen, met name als het om de praktische invulling gaat. Hij noemde daarbij firewalls et cetera. Maar waar blijft de eigen verantwoordelijkheid van de internetgebruiker zelf? Ik bracht in mijn inbreng, toen de heer Verhoeven nog net niet aanwezig was, naar voren dat het aan de internetgebruiker zelf is om te zorgen voor een stevig cyberslot, goede antivirussystemen et cetera.

De heer **Verhoeven** (D66): Ik denk dat dat waar is. Ik betreur dat ik dat deel van de inbreng van de VVD-woordvoerder heb gemist, maar ik kan dat straks nog nalezen. Het begint inderdaad met de eigen verantwoordelijkheid van de gebruikers van internet. Ik ben het op dit punt geheel eens met de heer Van Oosten. Daarbovenop moet je een aantal dingen doen om ervoor te zorgen dat degene die wil inbreken, wordt geremd. Het is en-en. Als internetgebruiker moet je zeker je verantwoordelijkheden nemen en zorgen voor virusscanners, firewalls, updates en al die zaken. Daar begint het inderdaad mee.

De heer **Van Oosten** (VVD): Dan zijn we het gelukkig eens. Ik was even bang dat de heer Verhoeven eropuit was om aan te geven dat die praktische zaken ook een overheidstaak zouden zijn. Dat begreep ik namelijk een beetje uit de bijdrage die ik hoorde. Ik begrijp dat ik dat dus niet geheel juist heb gezien.

De heer **Verhoeven** (D66): Als ik die indruk heb gewekt, dan is dat inderdaad niet handig geweest. Ik ben er echter een beetje bang voor dat de VVD het wel prima vindt dat allerlei bevoegdheden worden opgerekt zonder dat die praktische mogelijkheden, waarover wij het zo eens zijn, ten volle worden benut. Daarop spreek ik de Minister elke keer aan. Ik zeg hem: ga nu niet allemaal nieuwe dingen bedenken en nieuwe bevoegdheden geven als de bestaande mogelijkheden nog lang niet uitputtend zijn gebruikt. Ik hoop dat de Minister straks op een stevige en duidelijke

manier hierop zal reageren, want ik wil op dit punt toch een keer een duidelijke positiebepaling van het kabinet zien.
Voorzitter, als ik nog heel even mag ...

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

De heer **Verhoeven** (D66): Ik heb nog een minuut, en die wil ik benutten om mijn geschrokkenheid te laten doorschemeren over de ambitie om een parallel tweede internet op te zetten. Mijn fractie begrijpt en leest uit de stukken dat het slechts een haalbaarheidsonderzoek is. Tot mijn niet geringe verbazing was mevrouw Gesthuizen er volgens mij net heel enthousiast over. Een haalbaarheidsonderzoek in het algemeen moet wel kunnen, maar het streven om tot een tweede, een parallel internet te komen – we hebben het er toevallig in het AO Telecommunicatie hiervoor over gehad – vinden we echt onwenselijk. Dat zal ook weer op gespannen voet komen te staan met netneutraliteit, die juist weer zo belangrijk is om een open en vrij internet voor iedereen te waarborgen. Wij willen daarin geen gradaties, geen lagen, geen schillen en geen schijven hebben. Ik hoop dat de SP-woordvoerder hierover straks, in de tweede termijn, nog iets meer kan zeggen.
Ik kom op mijn laatste drie zinnen, voorzitter. Als een partij extra dienstverlening wil, dan kan ze altijd extra bandbreedte kopen of zelfs een eigen glasvezellijn aanleggen. Als je internet aanbiedt, dan biedt je het hele internet aan en niet een stukje. Graag krijg ik van de Minister de geruststelling dat hij dit onzalige plan intrekt.

De vergadering wordt van 15.01 uur tot 15.15 uur geschorst.

Minister **Opstelten**: Voorzitter. Ik dank de leden, de geachte afgevaardigden, voor hun bijdragen. Ik wil duidelijk stellen dat we de nodige stappen hebben gezet. Eigenlijk hebben alle woordvoerders dit ook gezegd. Het is goed en verheugend dat veel woordvoerders hebben laten weten dat ze belangstelling hebben voor een bezoek aan het Nationale Cyber Security Centrum. Dat is belangrijk. Ook de stappen die we internationaal zetten, zijn van belang.
Met de strategie zetten we gezamenlijk in op de volgende ambities, die ik hierbij nog eens neerzet: 1. Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het digitale domein; 2. Nederland pakt cybercrime aan; 3. Nederland investeert in veilige en privacybevorderende ICT-producten en -diensten; 4. Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het digitale domein; 5. Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen. We doen dit in een publiek-private samenwerking. Het buitenland kijkt hier buitengewoon jaloers naar en daarom krijgen we ook veel bezoekers. Zo'n samenwerking is in dit land ook geboden. Alles wat we nu zeggen, wordt gesteund door de private sector. Het is belangrijk om dat te weten. Verder betrekken we de universiteiten erbij als het gaat om de kennis. Het is dus een drieslag. We laten ons niet uit elkaar spelen.
Verder hebben we ten opzichte van de eerste Cyber Security Strategie een grote stap vooruit gezet wat betreft de internationale component. De vrijheid in het digitale domein is in onze strategie heel belangrijk. Ik zeg dit met name tegen de heer Verhoeven, aan wie dit volgens mij een beetje was ontgaan. Die vrijheid is ongelooflijk belangrijk in het digitale tijdperk. Verder is het economische belang groot. Dat geldt ook voor de security en het maatschappelijk belang daarvan. Tijdens het EU-voorzitterschap in 2016 zal cybersecurity een belangrijk speerpunt zijn. Ik opereer op dit front heel goed en schouder aan schouder met een aantal van mijn collega's. In 2015 zal Nederland gastland zijn van de grote cybersecurity summit. Ik benadruk nog eens de plaats van vrijheid en van het economische belang

in onze strategie en het feit dat Nederland de toegangspoort tot het digitale domein van Europa is en wil zijn. Daarvoor moeten we ook de waarborgen geven.
Ik kom op een aantal vragen die door de diverse leden zijn gesteld. De heer Van Oosten vroeg of het NCSC in de lead is op het punt van de cybersecurity, of het de coördinatie heeft bij de samenwerking met andere diensten. Deze vraag is gisteren in het AO Defensie ook gesteld. Ik kan uiteraard hetzelfde antwoorden. Het NCSC is als onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid coördinerend op het terrein van cybersecurity. Ik draag dus die coördinerende verantwoordelijkheid. Daarmee ben ik ook de spin in het web. Belangrijker: ook het NCSC is dat. De lead voor initiatief, coördinatie en aanpak van cyberproblemen in de vitale sectoren ligt dus inderdaad bij het centrum. Organisaties blijven zelf verantwoordelijk voor hun cybersecurity. Het is vanzelfsprekend dat ze dat zijn. Het is überhaupt het uitgangspunt bij veiligheid dat iedereen in de eerste plaats verantwoordelijk is voor zijn eigen veiligheid. Er wordt intensief met publieke en private partners, waaronder de AIVD en Defensie, samengewerkt. Die samenwerking is buitengewoon goed. Voorbeelden daarvan zijn de liaisons van de verschillende departementen bij het NCSC, het Nationaal Detectie Netwerk en het Nationaal Response Netwerk. Verder is in de afgelopen periode intensief samengewerkt in het kader van de NSS, waarbij cyber ook een buitengewoon belangrijk risicopunt was, maar het was goed voorbereid. Bij incidenten sluiten ze aan op de operationele coördinatie bij het NCSC. Als onderdeel van de strategie wordt gesproken over een versterkte samenwerking bij de analyse van fenomenen als botnets, waarop ik straks ook nog terugkom.
De heer Bontes en mevrouw Oosenbrug vroegen naar de stand van zaken betreffende de migratie van Windows XP. Het NCSC heeft conform zijn rol actief gewaarschuwd voor het einde van de ondersteuning van Windows XP. Veel organisaties hebben al gemigreerd, maar een flink aantal bedrijven is nog actief met de migratie. Dat geldt ook voor een deel van de overheid. De Minister voor Wonen en Rijksdienst, collega Blok, is namens de rijksoverheid in gesprek om gedurende de migratie extra veiligheidsmaatregelen te nemen. Zo verzekert hij zich van veiligheidsupdates. Hierover zijn ook reeds schriftelijke vragen gesteld door mevrouw Oosenbrug. Ik verwijs dan ook naar de beantwoording daarvan door de Minister.
De heer Bontes vroeg hoe UWV en andere belangrijke partners aan te sluiten op het NCSC. Om partners aan te sluiten, loopt het project Nationaal Response Netwerk als een van de drie hoofdpijlers voor 2014. UWV zal daarbij een van de partners zijn. UWV is aangesloten op de dagelijkse adviezen van het NCSC.

De heer **Bontes** (Bontes): Het is nog niet helemaal duidelijk wat bij de transitie van Windows XP precies de rol van het NCSC is. Wat doet het precies? Geeft het advies? Gebruikt het concreet zijn expertise in die situatie?

Minister **Opstelten**: Het uitgangspunt is dat wij waarschuwen, adviezen geven en expertise leveren. Wij zeggen: kijk daarnaar en neem je verantwoordelijkheid. De verantwoordelijkheid voor de hele rijksdienst ligt bij het departement van BZK, dat daarop wordt aangesproken en dat daarmee aan de slag gaat. Dat is de lijn. Zo is het ook in het bedrijfsleven. Zo is iedereen in beweging. We volgen dat natuurlijk. We geven telkens een signaal: er is iets aan de hand, doe iets. Als het goed is, is dat signaal niet nodig, omdat men al bezig is. Het kan ook samenlopen. Dat is de positie.
Ik kom bij mevrouw Gesthuizen, die vroeg wat de rol van het NCSC is bij botnets. Wordt er voldoende samengewerkt met de andere partners? Hoe

zit het met de privacy? Vanuit het centrum worden bij de aanpak van botnets publieke en private partners bij elkaar gebracht. Een centrale rol is er voor het private initiatief AbuseHUB. Dit wordt door het Ministerie van Economische Zaken ondersteund. Het NCSC werkt samen met AbuseHUB. Overigens is dit in ontwikkeling. We zijn er nog niet. Het zorgvuldig omgaan met gegevens en privacy is voor AbuseHUB een buitengewoon belangrijk aandachtspunt.
Mevrouw Oosenbrug vroeg wat het Nationaal Response Netwerk inhoudt en hoe de samenwerking met het NCSC is. Het NCSC is op het gebied van cybersecurity het centrale punt in Nederland, en daarmee de spin in het web, om organisaties buiten de eigen achterban van de rijksoverheid en vitale sectoren te kunnen bedienen. Indien nodig werkt het NCSC samen met schakel- en partnerorganisaties. Door nauw samen te werken met de partnerorganisaties wordt een zo groot mogelijk deel van de Nederlandse samenwerking bestreken. Hiermee worden ook organisaties buiten de primaire doelgroep van het NCSC, de rijksoverheid en de vitale sectoren, bereikt. Dit netwerk zal in stappen verder worden op- en uitgebouwd. De Informatiebeveiligingsdienst voor gemeenten (IBD) is in dit netwerk een belangrijke partner. Dit is verder ook nog in ontwikkeling, zo zeg ik duidelijk.
De heer Van Oosten vroeg naar de Cyber Security Raad. Deze raad is onafhankelijk en adviseert het kabinet gevraagd en vooral ook ongevraagd over de uitvoering van de strategie. De Cyber Security Raad bestaat uit vertegenwoordigers van publieke en private partijen en de wetenschap, zoals bekend. De raad heeft bij de totstandkoming van de strategie een belangrijk advies uitgebracht. Hij is ook actief betrokken bij de uitvoering van de strategie, bijvoorbeeld op het gebied van standaarden. De raad is een belangrijk voorbeeld van privaat-publieke participatie. Ik verwacht in de komende tijd veel van hun adviezen.

De heer **Van Oosten** (VVD): Ik hoorde de Minister spreken over de Cyber Security Raad, maar in een voorgaand blokje, in antwoord op de vraag of het NCSC in de lead was en wie de coördinerende rol heeft, gaf hij aan welke rol het NCSC pakt. Mijn voornaamste vraag is: spelen er competentiedisputen? Dat zou mij namelijk zorgen baren. Verder geloof ik helemaal dat de Minister erbovenop zit om de organisatie op de meest fantastische manier vorm te geven, zodat het goed loopt. Met name die vraag houdt mij dus bezig en daarom stel ik hem nu langs deze weg alsnog.

Minister **Opstelten**: Er zijn geen competentiezaken. Als die zich al zouden voordoen – ik ken ze niet – dan zijn ze heel snel kortgesloten. Het is natuurlijk een nieuw veld. Het is in ontwikkeling. Daarin moeten posities zich altijd ontwikkelen en worden bevestigd. Het gaat razendsnel, en dat is maar goed ook, maar de coördinatie door en de positie van het centrum zijn onomstreden. Er is wat dat betreft geen enkele competentiepositie aan de orde.
De heer Van Oosten vroeg of innovatieve clubs die met het oog op cybersecurity nieuwe tools ontwikkelen, in aanmerking komen voor overheidsopdrachten. Ik deel de observatie dat innovatie op het terrein van cybersecurity belangrijk is. Dat is ook een van de drie pijlers. Het is van groot economisch belang. Een belangrijk onderdeel van de rijksbrede cybersecurityresearchagenda is het aanbestedingsinstrument van EZ genaamd Small Business Innovation Research, dat juist is gericht op innovatieve en toepasbare cybersecurityoplossingen. In de afgelopen twee jaar was voor de nationale cybersecurityresearchagenda 6 miljoen euro beschikbaar. In de komende twee jaar is er wederom 6 miljoen euro beschikbaar om fundamenteel en toegepast onderzoek op het terrein van cybersecurity uit te voeren. Voor deze tweede onderzoekstender zijn reeds 150 onderzoeksvoorstellen ingediend.

Mevrouw **Gesthuizen** (SP): Ik heb even gezocht. We zijn inderdaad in een briefje van naar ik meen februari 2013 met één alinea geïnformeerd over de aanpak van botnets. Het was inderdaad een brief van de Minister van Economische Zaken. Het waren echter maar een paar regels. Daarin is nadrukkelijk vermeld dat het een initiatief is van private partijen, al is dat wel met subsidie van Economische Zaken tot stand gekomen. Ik wil er echter wel graag wat meer over weten. Misschien zegt de Minister nu: dan moet u zich even melden bij Economische Zaken. Het lijkt mij echter juist ook iets, die botnets, waarmee Veiligheid en Justitie zich zou moeten bezighouden. Misschien komt de Minister er nog op, maar ik heb zo doorgevraagd over de botnets omdat het juist voor een aantal van die privaten partijen volgens mij – ik hoor die signalen ook – niet helemaal duidelijk is hoever ze mogen gaan. Mag je bijvoorbeeld iemand waarschuwen? En hoe zit het dan met de bescherming van data die daarbij vrijkomen?

Minister **Opstelten**: Ik wil dat nog wel even verdiepend afstemmen met mijn collega van EZ. Dat kunnen we zeker doen. U krijgt daar een antwoord op. Misschien komen er nog meer vragen die om wat meer afstemming vragen. We kunnen er nu natuurlijk wel iets meer over zeggen, maar ik denk dat u er meer aan hebt als ik het verdiepend bij EZ laat checken.

Mevrouw **Gesthuizen** (SP): Ik wil de Minister daarvoor zeker ruim de tijd geven. Is het een idee dat we dat voor de zomer tegemoet mogen zien?

Minister **Opstelten**: Jazeker. Misschien kunnen we dat combineren met een aantal andere vragen die wellicht nog komen. Prima, we zullen dat doen.
Ik kom op een aantal vragen die, onder anderen door de heer Van Oosten maar ook door de heer Verhoeven en mevrouw Oosenbrug, zijn gesteld over het wetgevingstraject. De heer Van Oosten vroeg mij om aan te geven of er voldoende middelen en voldoende wettelijke basis voorhanden zijn om «cybercrime-as-a-service» aan te pakken. Volgens de Nederlandse wet kunnen cybercriminelen die dergelijke feiten plegen, worden aangepakt. Het illegaal binnendringen in computers en het verstoren van programma's is in Nederland strafbaar. Ik moet daarbij meteen aantekenen dat veel van de door de woordvoerders geschetste criminaliteit internationaal is. Dat is extra lastig voor de opsporing. Daarom investeren het Team High Tech Crime van de Nationale Politie en het Landelijk Parket in internationale samenwerking met relevante andere landen en in de relatie met Europol.
Zoals bekend wordt Europol binnenkort drastisch versterkt in de top door de directeur van ons NCSC. Europol gaat er dus op vooruit. Ik zeg het maar even «by the way». Hij blijft overigens in Den Haag op kantoor, maar dan in de directie van Europol. Dat is trouwens wel een eer voor Nederland, maar het is jammer voor het centrum. Er komt echter een nieuwe, en die is ook heel goed. Ik weet wie het is. De Kamer weet dat binnenkort ook. Het gaat dus om EC3, het European Cybercrime Centre, dat vanuit Europa is ondergebracht bij Europol – hij neemt dus ook wat mee – onder andere.
De wetgeving op dit gebied behoeft overigens wel versterking. Daarom heb ik het naar mijn idee bij de Kamer bekende wetsvoorstel computercriminaliteit III in voorbereiding. Het wetsvoorstel is vorig jaar zomer uitgebreid in consultatie geweest. Alle commentaren zijn bestudeerd. Deels zijn deze overgenomen, deels gemotiveerd niet meegenomen. In februari heb ik het wetsvoorstel via het kabinet naar de Raad van State gestuurd. Ik verwacht in het najaar het voorstel aan de Kamer te kunnen aanbieden. We wachten natuurlijk nu eerst het advies van de Raad van State af. Dat zullen we vervolgens zorgvuldig wegen.

De vraag of ik voor de aanpak voldoende middelen heb, is eerder een kwestie van prioritering dan van het beschikbaar hebben van middelen. In de komende jaren zal bij de inrichting van de Nationale Politie het onderwerp cybercrime zijn plaats krijgen. Ik ben nu ook bezig om samen met de burgemeesters in ons land en het Openbaar Ministerie de vier of vijf topprioriteiten vast te stellen. Cyber is een van die prioriteiten in Nederland. Dat is ook logisch. Je hoeft er niet erg veel kennis voor te hebben om dat tot een prioriteit te maken. Dat heeft heel veel draagvlak in ons land. Ik zal dit, deels samen met het gezag over de politie, borgen in de prestatieafspraken.
Ik kom op de vraag van mevrouw Oosenbrug en de heer Verhoeven over de vertaling van de motie-Hennis (26 643, nr. 202) over de verplichting tot het melden van security breaches. Ik streef ernaar om het wetsvoorstel rond de zomer in consultatie te geven, zodat het eind dit jaar bij de Tweede Kamer kan worden ingediend. Ik heb in de brief van 12 december bericht dat ik daarover een samenhangend wetsvoorstel voorbereid. Daarin wordt niet alleen de meldplicht geregeld maar ook enkele andere onderwerpen, zoals cybersecuritytaken van de Minister van Veiligheid en Justitie en gegevensuitwisseling met andere instanties. Voor het bedrijfsleven is het waarborgen van de vertrouwelijkheid bij een breach notification natuurlijk heel belangrijk. Je moet er ook draagvlak voor krijgen. Men wil meewerken, maar wijst daar natuurlijk voortdurend op. Volgens mij heeft VNO-NCW de Kamer daarover ook een brief geschreven. Deze uitbreiding van het wetsvoorstel vergt nog enige uitwerking en een goede afweging langs de door mij aangegeven pijlers.
Mevrouw Oosenbrug vroeg wat de voortgang is van het wetsvoorstel meldplicht datalekken. Dat is een verantwoordelijkheid van de Staatssecretaris. Het advies van de Raad van State dateert van september 2012. Het nader rapport is zo goed als gereed. Het wetsvoorstel zal binnenkort bij de Tweede Kamer worden ingediend.
Ik kom nog een keer op de vraag over het wetsvoorstel computercriminaliteit III. Volgens mij het ik het schema daarvan al goed aangegeven.
De heer Bontes vroeg of ook DigiD niet moet vallen onder «vitaal». Dat is gezien het toegenomen belang van DigiD zeer goed mogelijk. Daarom is dit reeds opgenomen in het wetsvoorstel over de meldplicht. Aan de Tweede Kamer is reeds toegezegd om met een bredere herijking van de lijst met vitale sectoren te komen. Met de Minister van BZK zal ik overleggen of hij de prioriteit wil geven aan het herijken van de vitale producten die vallen onder de verantwoordelijkheid van BZK.

De heer **Bontes** (Bontes): Het is fijn dat zo'n lijst er komt. Ik dank de Minister daarvoor. Wat is de tijdlijn? Wanneer zal dat ongeveer plaatsvinden?

Minister **Opstelten**: Het is de verantwoordelijkheid van mijn collega van BZK. Dat wil ik wel zo houden. Ik moet dit dus aan hem overlaten. Ik wil wel proberen om het in de net aan mevrouw Gesthuizen toegezegde brief op te nemen, dus voor de zomer. Is dat goed?
De heer Verhoeven vroeg of ik het optreden van opsporingsdiensten in het buitenland uit het wetsvoorstel computercriminaliteit III wil halen. Het wetsvoorstel ligt nu bij de Raad van State. Ik kan niet vertellen wat erin staat, zoals bekend. Kijkend naar de heer Verhoeven zeg ik: dit komt mij ook goed uit. Het ligt dus bij de Raad van State. Ik ben erg benieuwd hoe die zal reageren op dit mogelijke optreden. Ikzelf ben van mening – dat mag de Kamer wel weten – dat dit gelet op de aard van het internet, dat internationaal is, en op de verblijfplaats van de vele criminelen buiten ons land die hier wel criminaliteit plegen, wel noodzakelijk zal zijn om goed internationaal te kunnen samenwerken en over de mogelijkheden daartoe te beschikken. Mijn collega's in het buitenland hebben overigens buitengewoon veel belangstelling voor hoe het met dit wetsvoorstel

loopt. Dat moet de heer Verhoeven toch ook met enige trots vervullen. Als je niet weet waar je tijdens je onderzoek bent, dan zul je ook buiten de grens moeten doorgaan. We komen erop terug. De vraag die de heer Verhoeven niet alleen vandaag maar ook eerder heeft gesteld, is mij volstrekt duidelijk. Hij is mij niet ontgaan.
De heer Verhoeven heeft ook gevraagd naar de monitoring, die naar hij aanneemt slaat op het project Nationaal Detectie Netwerk (NDN). Dit is een samenwerking voor het beter en sneller waarnemen van digitale gevaren en risico's. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijk – dat is telkens het kernpunt – tijdig gepaste maatregelen nemen om mogelijke schade te beperken of te voorkomen. Zo werken we samen aan de digitale weerbaarheid van Nederland.
Verder vroeg de heer Verhoeven naar de stand van zaken van de pilot en vroeg hij wat die behelst. Ik zal daar een paar punten over noemen. Op 1 april zal een pilot van start gaan om digitale dreigingen op de rijksinternetvoorziening te detecteren. Het gaat echt door op 1 april; het had beter 2 april kunnen zijn. Bij het opzetten van deze pilot en het opbouwen van het NDN staat voor mij privacy by design voorop. Het onderwerp «detectie» kan gevoelig zijn en daarom streef ik ook in dit traject naar het vinden van die noodzakelijke balans tussen vrijheid, veiligheid en maatschappelijke groei. Een laatste opmerking hierbij: uiteraard is dit traject voorzien van de nodige waarborgen op het gebied van privacy en medezeggenschap. Zo heb ik dat ook met de opdrachtgever, de Minister voor Wonen en Rijksdienst, afgesproken. Het is absoluut niet zo dat de AIVD en het NCSC als uitvoerende partijen in de gegevens van medewerkers van de rijksoverheid kunnen kijken. Dat is absoluut niet het geval.

De heer **Verhoeven** (D66): De Minister had het over privacy by design. Dat is een prachtige term. Wat verstaat de Minister daaronder? Ik versta daaronder dat je bijvoorbeeld niet alles aan elkaar koppelt, dat je dus niet alle systemen maar lukraak via het internet aan elkaar vastkoppelt, waardoor een lek ergens eigenlijk een lek overal betekent. Wat dat betreft heb ik ook een vraag gesteld over bijvoorbeeld de sluizen en over de noodzaak om allerlei systemen via SCADA-achtige constructies aan elkaar te koppelen. Als de Minister de term «privacy by design» gebruikt, bedoelt hij dan in concreto dat je als overheid minder dingen op het internet zou moeten aansluiten en daar ook eens een keer een grens aan zou moeten stellen? Of is het gewoon een loze term, die wel goed klinkt in een debat? Dat is mijn zorg: de concretisering van wat de Minister zegt. Hij zegt het heel goed, maar wat zijn de daden?

Minister **Opstelten**: We zijn het aan het uitwerken, zoals ik ook al heb gezegd. Heel in het kort: privacy by design is in ons wetsvoorstel en in veel andere wetsvoorstellen het uitgangspunt en is in dat kader ook concreet vertaald. Daarmee waarborg je dat je, als je iets nieuws ontwikkelt, altijd de balans creëert tussen aan de ene kant de noodzakelijke maatregelen en aan de andere kant de privacy van de burger, de medewerker of anderszins. Daar zijn altijd concrete indicatoren voor, die we langslopen in dat programma. Privacy by design is dus niet alleen maar een term. Het is ook vertaald in concrete punten en criteria die je langsloopt. Dat zal ook hierbij weer het geval zijn. De heer Verhoeven kan daar echt van opaan. Ik ben daar ook op aanspreekbaar als we met concrete invullingen komen.

De heer **Verhoeven** (D66): Dat is in ieder geval prettig. Dank daarvoor. Ik had nog een ander punt. Als ik de Minister hoor praten over de mogelijkheden om alle dreigingen te detecteren en te monitoren en over het uitwisselen van gegevens, dan komt bij mij de volgende gedachte op. Als

men er dan dankzij bepaalde mogelijkheden – waarbij ik mijn twijfels heb, maar laat ik die het voordeel van de twijfel geven – achter komt dat er een dreiging is, bijvoorbeeld een virus, een botnet, een ddos-aanval of wat dan ook, dan blijft dat soms heel lang liggen in de verschillende lagen van het cybersecuritystelsel dat we hebben opgetuigd. Hoe gaan we dat voorkomen? Dan heb je iets ontdekt, maar laat je het op de plank liggen en heb je alsnog een probleem.

Minister **Opstelten**: Mag ik daar straks op terugkomen? Dit is weer een afzonderlijke vraag van u. De beantwoording ervan komt eraan. Nu zijn we namelijk in het blokje «wetgeving».

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

Minister **Opstelten**: Ik kom nu bij het blokje «personeel», over de capaciteit, de kwaliteit et cetera. Mevrouw Gesthuizen vroeg naar de stand van zaken betreffende de capaciteitsopbouw van het Team High Tech Crime van de Nationale Politie. De eerste uitbreiding heeft plaatsgevonden in 2012. De tweede werd eind 2013 afgerond. Op dit moment wordt een derde tranche geworven. Naar verwachting zal de selectieprocedure gerealiseerd zijn in het begin van het derde kwartaal van 2014. Momenteel heeft het team ongeveer 90 fte's, verdeeld over één algemeen team en twee tactische teams. Met de laatste werving komt er nog één volledig tactisch team bij. Op deze manier zal tegen het eind van 2014 een capaciteitsuitbreiding tot 119 fte's zijn bereikt.
Mevrouw Gesthuizen vroeg naar de sterkte van het NCSC. Op dit moment is de formatieve sterkte van het NCSC ongeveer 60 fte's. Het centrum zal groeien naar rond de 90 fte's eind dit jaar. De sollicitatieprocedure die nu loopt, is succesvol vol. Het is goed om ook dat even te zeggen. Men wil daar graag gezien worden. Dat is mooi.
Mevrouw Oosenbrug had een goede vraag – natuurlijk zijn alle vragen goed – namelijk: wat is het budget? Het bedrijfsleven en het kabinet investeren continu in cybersecurity. Dat heeft te maken met de awareness. Die neemt toe. Bij elke ICT-aanschaf wordt daardoor ook de rol van de informatiebeveiliging groter. Jaarlijks wordt bij overheid en bedrijfsleven voor tientallen, zo niet honderden miljoenen euro's geïnvesteerd in de ICT. Het gaat bij cybersecurity om de gezamenlijke inzet van overheid, bedrijfsleven en burgers. Iedereen moet zijn steentje bijdragen. Specifiek vanuit Veiligheid en Justitie investeren we jaarlijks ruim 30 miljoen euro in het vormgeven van cybersecurity. Denk daarbij aan specialisten bij de politie en het NCSC, alsook aan het stimuleren van onderzoek. Ik heb bijvoorbeeld op basis van het regeerakkoord structureel 4 miljoen euro extra geïnvesteerd in het NCSC. Hierdoor groeit het NCSC dit jaar met 30 fte's, dus van 60 fte's naar de net door mij genoemde 90 fte's.
Mevrouw Oosenbrug vroeg of ik ethische hackers wil overnemen, of liever: omarmen. Ik vraag de leden: kunt u hacken? Ik heb in ieder geval gezien hoe het moet. Ja, ik sta daarom enorm achter ethische hackers. Ik weet dus hoe het moet. Ik weet ook hoe ethische hackers eruitzien. Ik heb hen ontmoet. Vandaar mijn inzet op responsible disclosure, zoals bekend. Daar is ook heel veel belangstelling voor vanuit het buitenland. Na de zomer heb ik reeds een brief over responsible disclosure aan mevrouw Oosenbrug toegezegd. Over het gebruik van de leidraad zal ik nog rapporteren. Ik denk dat we dat meenemen in de brief die we hebben aangekondigd.
De heer Bontes vroeg wat ik eraan ga doen om het bewustzijn over digitale veiligheid te vergroten. Digitale veiligheid begint bij het zich bewust zijn van de risico's. Dan kunnen organisaties en burgers maatregelen nemen om de risico's te verkleinen. Het is daarom belangrijk om continu hierin te investeren. Een voorbeeld hiervan is de campagne Alert Online, die sinds 2012 wordt gevoerd met publieke en private partners. Dit

jaar vindt de derde editie van de campagne plaats, en wel van 27 oktober tot en met 6 november. De campagne Alert Online is gericht op overheid, bedrijfsleven en burgers. Daarnaast zal het NCSC ten behoeve van de burgers een structurele samenwerking aangaan om een portal voor veilig internetten in het leven te roepen. Deze portal zal speciaal op de burger zijn gericht.
Mevrouw Gesthuizen vroeg hoe de gebruiker meer grip kan krijgen als hij of zij de kennis niet heeft. Het is inderdaad belangrijk om het kennisniveau van de burgers te verhogen. Daarom zijn er twee speerpunten: een awareness-campagne, de door mij zonet genoemde Alert Online, en de oprichting van de Taskforce Cybersecurity Onderwijs door OCW.
Mevrouw Gesthuizen vroeg of ik de behoefte en het tekort aan cyberprofessionals goed in beeld heb. Dat is een van de zaken die door de Taskforce Cybersecurity Onderwijs wordt meegenomen.
Mevrouw Oosenbrug bracht een punt in over spionage. Gegevensuitwisseling tussen ambtenaren vindt plaats via de Haagse Ring. Dit is een beveiligd overheidsnetwerk, zodat communicatie tussen ambtenaren niet via het open internet gaat. Voor het uitwisselen van gerubriceerde informatie tussen ambtenaren zijn encryptiemiddelen beschikbaar die zijn goedgekeurd door het Nationaal Bureau Verbindingsbeveiliging, een onderdeel van de AIVD. Voor de communicatie met burgers bestaan verschillende beveiligingsoplossingen. Zo kan via mijn.overheid.nl informatie worden gedeeld, waarbij de toegang is beveiligd met DigiD. De communicatie via websites wordt zo veel mogelijk beveiligd met digitale certificaten. Voor veilige e-mail stimuleert het NCSC het gebruik van Pretty Good Privacy (PGP). Burgers die bijvoorbeeld een «responsible disclosure»-melding willen doen bij het NCSC, kunnen die melding beveiligen met PGP. Het NCSC bevordert beveiliging middels kennisproducten zoals factsheets en best practices.
Mevrouw Gesthuizen en de heer Verhoeven vroegen naar het waarom van een verkenning naar gescheiden netwerken en diensten, waaronder de cloud. Er zijn reeds veel initiatieven op dit vlak. Het is van belang om deze in kaart te brengen. Ik denk dat dat wel overtuigend is. Dat doen we samen met private en publieke partijen, zoals de Minister voor Wonen en Rijksdienst en de Minister van BZK. Het is dus niet een wens van de overheid. Met een gescheiden netwerk kunnen de mogelijkheden om de continuïteit van vitale processen te borgen, toenemen. Hier is herhaaldelijk om gevraagd vanuit het veld en naar ik meen ook vanuit de Kamer. Verder kan binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld, waardoor de privacy-integriteit van data in deze opslag of cloud kan worden verbetererd. Deze verkenning zal gezamenlijk in de eerste helft van 2014 worden gerealiseerd en voor het zomerreces aan de Tweede Kamer worden verzonden. Het is dus een verkenning en een soort kanalisatie van hetgeen al wordt ontwikkeld en ontstaat. Daar moet, denk ik, stroomlijning in komen. Uiteraard kijk ik ook naar internet en de internationale ontwikkelingen.
Gaat de overheid zich inzetten om een Nederlandse cloud, dus gescheiden internet, te bouwen? Nee, zo zeg ik nadrukkelijk. In de Nationale Cyber Security Strategie 2 wordt een haalbaarheidsonderzoek aangekondigd, dat gaat over de wenselijkheid en mogelijkheid tot het realiseren van een gescheiden netwerk voor zowel publieke als private vitale sectoren. In de notitie «Vrijheid en veiligheid in de digitale samenleving», die ook al in de Kamer is behandeld, wordt aan deze toezegging gerefereerd, mede in het licht van de door de Kamer aangenomen motie-Recourt (33 750-VI, nr. 55). Het gaat hierbij nadrukkelijk om een verkenning om te bezien welke initiatieven reeds spelen. Ik heb dat net al gezegd. Voordat een beslissing wordt genomen, zullen we de verkenning aan de Kamer toesturen. Ik wil met dit hele dossier telkens de Kamer meenemen, zoals we dat tot nu toe ook hebben gedaan. Daar is het belangrijk genoeg voor.

De heer Van Oosten vroeg welke risico's in verband met wetgeving de overheid loopt bij het gebruik van de cloud. De Staatssecretaris heeft de Kamer meerdere malen geïnformeerd over de toepasselijkheid van de Amerikaanse wetgeving in relatie tot Nederlandse data. Over het gescheiden netwerk, de cloud, loopt reeds een verkenning. Het is ook een van de actiepunten in de strategie.
De heer Verhoeven vroeg naar de stand van zaken van de ontwikkeling van standaarden die worden gebruikt om de veiligheid en privacy van ICT-producten en -diensten te bevorderen. Het gaat hierbij dus om de bevordering van veilige software. In de Nationale Cyber Security Strategie 2, die in oktober is vastgesteld, wordt het belang van het ontwikkelen van standaarden en het bevorderen van veiligheid en privacy voor ICT-producten en -diensten benoemd. Het bevorderen van veiligheid en privacy voor ICT-producten en -diensten moet in internationaal verband plaatsvinden. Belangrijke momenten om dit onderwerp op de internationale agenda te zetten, zijn de Cyberspace Conference die Nederland begin 2015 zal organiseren en waarvan het gastheer zal zijn, en het Nederlandse EU-voorzitterschap in de eerste helft van 2016.
De heer Verhoeven vroeg of ik meer met openbare broncodes wil werken. Ja. In het algemeen ben ik voorstander van openbare broncodes, zodat de ICT-community ons kan helpen met het bevorderen van de veiligheid. Recentelijk heeft de Minister van BZK het goede initiatief genomen om de broncode voor de basisregistraties te openbaren.
De heer Verhoeven vroeg of vitale sectoren wel gebruik moeten maken van internet. Daarop bestaat geen enkelvoudig antwoord. Het is niet ja of nee. Het is voor bedrijven uiteraard van belang om via internet te communiceren. Uiteraard is het ook van belang om een goede risicoafweging te maken bij de vraag of processen rechtstreeks aan het internet te koppelen zijn. Dat is een verantwoordelijkheid van de bedrijven zelf.
De heer Verhoeven vroeg of wel snel wordt gereageerd op meldingen en na monitoring. Dit is een cruciaal punt. Uiteraard moet er sprake zijn van een snelle opvolging van meldingen. Anders zou het opleggen van een meldplicht of het detecteren van dreigingen disproportioneel zijn. Daarom werken we zowel aan het Nationaal Detectie Netwerk als aan het Nationaal Response Netwerk. Detectie en respons gaan natuurlijk hand in hand. Ik kan niet uitsluiten dat er eens een keer iets gebeurt, maar ik kan verzekeren dat bij meldingen tot op het niveau van mijzelf wordt gereageerd en dat we erbovenop zitten. Ik heb er echt nog nooit een klacht over gehad, maar het kan zijn dat die er wel zijn.
Ik denk, voorzitter, dat dit mijn bescheiden antwoorden in eerste termijn zijn.

De **voorzitter**: Dank u wel, Minister. Ik kijk even rond om te bezien of er behoefte is aan een korte tweede termijn. Mij wordt aangegeven dat het voldoende is als er nog enkele interrupties kunnen worden gepleegd. Dan gaan we het rijtje af, te beginnen bij de heer Van Oosten.

De heer **Van Oosten** (VVD): Wat mij betreft voorkomen we een tweede termijn. Ik hoor nog wel wat de collega's doen. De Minister sprak over de Haagse Ring. Ik heb zelf een vraag gesteld over de mogelijkheid om communicatie tussen ambtenaren onderling, wellicht later ook die tussen ambtenaren en burgers, versleuteld te laten plaatsvinden. Ik kreeg als antwoord: we hebben de Haagse Ring en er zijn encryptiemiddelen die het mogelijk maken. Mijn vervolgvraag is: wordt er gebruik van gemaakt? Of zou daarvoor nog een nadere stimulering nodig zijn en wil de Minister dan toezeggen dat die ook zal plaatsvinden?

Minister **Opstelten**: Ja. Het wordt als zodanig gebruikt, maar het is altijd goed om deze ontwikkeling enorm hard te stimuleren. Dat zullen we dus ook doen. Op beide vragen is het antwoord dus: ja.

De **voorzitter**: De heer Bontes heeft geen interruptie meer. Dan gaan we naar mevrouw Oosenbrug.

Mevrouw **Oosenbrug** (PvdA): Ik had een vraag gesteld over de komende Wet meldplicht datalekken. Die valt onder het CPB. Daarnaast komt nog de Wet melding inbreuken elektronische informatiesystemen. Die valt onder het Nationale Cyber Security Centrum. Zo heb ik het althans een beetje begrepen. Wat gebeurt er als er een incident is dat onder beide wetten valt? Wie neemt dan de lead? Misschien kan ik het antwoord zelf al een beetje inkoppen. Tussen beide wetten zijn er namelijk verschillen, maar ook overeenkomsten. Ik ben nog wel benieuwd naar het antwoord.

Minister **Opstelten**: Daarop is geen eenduidig antwoord te geven. Het hangt ervan af wie de melding doet en wie de toezichthouder is. Wij moeten het zo coördineren dat de melding op de goede plaats terechtkomt en dat er wordt geageerd.

Mevrouw **Oosenbrug** (PvdA): En met «wij» bedoelt de Minister ...

Minister **Opstelten**: Het centrum. Ik zeg «wij», maar ik ben niet van het centrum. Ik ben er wel verantwoordelijk voor. Nee, ik ga niet mijn rechter buurman opvolgen. En hij mij ook niet. Daarover moet in deze publieke arena volstrekte duidelijkheid bestaan.

Mevrouw **Gesthuizen** (SP): Met één antwoord van de Minister ben ik niet helemaal tevreden, namelijk het antwoord op de vraag die ik stelde naar aanleiding van de opmerking in de strategie over de kwetsbaarheid van en het leggen van de eindverantwoordelijkheid bij de gebruiker. De Minister zegt: we hebben Alert Online. Dat is natuurlijk hartstikke goed. Ook die Taskforce Cybersecurity Onderwijs is hartstikke goed. Daarvoor krijgt de Minister van mij een dikke duim omhoog. Toch vind ik het antwoord iets te mager, iets te dunnetjes, zeker als ik in hoofdstuk 4, «Weerbaarheid: kwetsbaarheden», van het Nationale Cyber Security Beeld de volgende nadrukkelijke passage lees: «De standaardbeveiliging van deze apparatuur schiet vaak tekort of het is onduidelijk hoe een apparaat veilig ingesteld moet worden.» Ik proef daar toch ook een beetje in dat ik iets meer zou mogen verwachten van degenen die diensten aanbieden en van degenen die apparatuur op de markt brengen. Ik zeg dat nog maar eens een keertje, omdat ik ook wel merk – volgens mij weten we dat allemaal in de Kamer – dat er ook een ontwikkeling de andere kant op is. Dat geldt dan niet voor de veiligheid an sich, maar kijk bijvoorbeeld naar het feit dat banken in de afgelopen tijd hebben gezegd dat ze meer vrijheden zouden willen krijgen om meer met data te doen. Daarom breng ik dit nog maar eens extra onder de aandacht van de Minister.

Minister **Opstelten**: Ik heb die twee punten in mijn korte antwoorden ook genoemd. Samen met ECP is het initiatief genomen om een nieuwe portal voor de burger in het leven te roepen, ter vervanging van waarschuwingsdienst.nl. Dat zal in het najaar operationeel zijn. Ik ben het er helemaal mee eens dat het punt over die awareness en die kwetsbaarheid absoluut nog in ontwikkeling is. Ik merk het overal. We doen het overal ook met management by speech. Er is wel een enorme ontwikkeling in het bedrijfsleven, ook bij de banken. Ik heb onlangs een ontmoeting gehad met de leden van de raad van bestuur van de vier grote banken. Daarbij kwamen dit soort punten ook aan de orde. Er is daar een enorme wil om met ons samen te werken en naar ons te luisteren, maar ook om te investeren. In de strategie wordt de zorgplicht wat betreft het door mevrouw Gesthuizen ingebrachte punt absoluut neergelegd bij het bedrijfsleven zelf. Daar behoort die ook te liggen. Wij zullen hen daarop

aanspreken en blijven aanspreken. Het signaal is dus scherp en helder overgekomen.

Mevrouw **Gesthuizen** (SP): Ik dank de Minister hartelijk voor deze toezegging. Ik had het voor mezelf een beetje zitten uitschrijven. Ik denk dat de overheid niet alleen bepaalde normen aan het bedrijfsleven moet stellen, maar ook zelf heel actief moet zijn. Ik denk dan aan zoiets als de campagne «Auto op slot, buit eruit». In het digitale tijdperk moet je ook op dat soort zaken inzetten: campagnes die iedereen bereiken en simpel zijn. Het bewustzijn van het belang van het beveiligen van je gegevens is over het algemeen schrikbarend laag.

Minister **Opstelten**: De campagne in het najaar zal, denk ik, daarom ook weer anders zijn dan de vorige. Ik bedoel: moderner en meer to the point. Ik denk overigens wel, en dat blijkt ook uit allerlei monitors, dat bij de burger de gevoeligheid voor cyberveiligheid stijgt. Je kunt er somber over worden, maar ik ben dat niet. Het geeft aan dat men gevoel heeft voor de risico's die op dit vlak aanwezig zijn. Dat zetten we dus door.

De heer **Verhoeven** (D66): Ik had niet alleen gevraagd naar standaarden op het gebied van software maar ook naar de softwareaansprakelijkheid in de keten. Als bijvoorbeeld een van de partijen in de keten zijn verantwoordelijkheid niet neemt, waardoor de volgende partij aan een consument iets verkoopt wat eigenlijk niet meer veilig is, dan zou je daar wat mee willen. Je zou de partij die bijvoorbeeld de updates niet meer op orde heeft en toch partijen telefoons doorverkoopt zodat die als onveilige telefoons bij de consument terechtkomen, willen aanpakken. Ik hoor de Minister dus graag nog even over die softwareaansprakelijkheid. Mijn laatste vraag zal ik stellen als ik het antwoord op deze vraag heb gekregen.

Minister **Opstelten**: Ook de zorgplicht van het bedrijfsleven hebben we in de strategie neergelegd. Dit is daarvan natuurlijk ook een onderdeel. We spreken het bedrijfsleven daar ook op aan. Het bedrijfsleven spreekt ons aan, maar wij spreken het bedrijfsleven ook aan. We werken dus aan het investeren in veilige producten en diensten. Gezien de diversiteit van soorten en de inzet van software geldt hiervoor niet één enkele standaard. Dat weet de heer Verhoeven net zo goed als ik, misschien zelfs wel beter. De manier waarop we dit moeten bekijken, raakt aan het concept «zorgplicht» en de rol in dezen van zowel de leverancier als de klant en de gebruiker. Het concept «zorgplicht» wordt reeds in de volle breedte binnen de Cyber Security Raad verder opgepakt. Er komt ook een advies hierover.

De heer **Verhoeven** (D66): Ik begrijp van mijn collega's dat er geen tweede termijn komt. Dan heb ik gewoon een korte opmerking en kan ik een laatste vraag stellen. Dan is het wat mij betreft goed. Als de voorzitter dit tenminste toestaat.

De **voorzitter**: Dat mag. Gaat uw gang.

De heer **Verhoeven** (D66): De Minister zei op een gegeven moment dat Nederland trots kan zijn op het feit dat we zo vooroplopen en dat er zo veel interesse uit het buitenland is voor de hackpolitie. Ik ben daar niet trots op. De Minister heeft het over management by speech. Dat is leuk. Ik begrijp dat de Minister in veel zalen vertelt wat er moet gebeuren. Ik hoop dat daar dan ook het bijbehorende management by action bij komt. Mijn vraag zoomt daarop in. De Minister zei heel laconiek: ik heb nog nooit gemerkt dat er te lang een melding niet goed doorkwam. Ik noemde net het voorbeeld van de Autoriteit Consument & Markt, die drie dagen lang

een melding van een gevaarlijk gedetecteerd virus liet liggen. Lost de Minister zoiets op met management by speech, dus door te zeggen «joh, niet meer doen, volgende keer beter», om te proberen daarmee de Kamer gerust te stellen, of zegt de Minister dat hij daar bepaalde activiteiten op zet, zodat het niet nog een tweede keer gebeurt? Dan wordt er actie ondernomen die meer inhoudt dan alleen maar zeggen dat het niet meer moet gebeuren, dat het een uitzondering is en dat hij er niet voor kan instaan. Dit zijn nu juist de cruciale schakels die goed moeten zijn. Als ze niet goed zijn, dan is het systeem niets waard.

Minister **Opstelten**: Met «management by speech» bedoelde ik het volgende. Als je voor een hele zaal met vertegenwoordigers van het mkb staat om op hun verzoek hier iets over te zeggen, dan informeer je hen en zeg je dat dit een risico is waarvoor ze ook zelf verantwoordelijkheid moeten nemen, en dat je hen daarin wilt faciliteren. Zo bedoel ik het. Het is ook goed om de burger te leren omgaan met het risico dat zij met hun eigen veiligheidsomgeving lopen. We doen natuurlijk meer dan management by speech. Je kunt het combineren door te speechen over acties die je onderneemt. Dat ligt mijzelf ook beter. Wat dat betreft raken we elkaar wel.
In de door de heer Verhoeven genoemde casus heeft het NCSC direct na de eerste melding gereageerd. De bedrijven zijn alleen maar gewaarschuwd door het NCSC. De besmetting is direct verwijderd, door het NCSC. De ACM heeft later breder het publiek geïnformeerd. Nadat het centrum het heeft gehoord, heeft het dus direct gereageerd en opgetreden. Stel dat het een keer zou voorkomen dat later wordt gereageerd, dan wordt daarop in alle scherpte op het hoogste niveau, ook naar mij toe, geacteerd.

De **voorzitter**: Volgens mij zijn nu alle vragen beantwoord. Ik kijk even naar mijn collega's en zie dat dit klopt. We kunnen hiermee bijna het AO sluiten. Eerst lees ik echter de toezegging van de Minister aan de Kamer voor: de Minister zal in overleg met de Minister van Economische Zaken afstemmen inzake de botnets en voor de zomer met een brief naar de Kamer komen, alsook met een lijst met de vitale sectoren en DigiD.

De heer **Bontes** (Bontes): DigiD plus andere organisaties.

De **voorzitter**: Plus nog andere organisaties. Prima.

Minister **Opstelten**: Er wordt een lijst vastgesteld. Ik zal het met collega Plasterk opnemen.

De **voorzitter**: Dank voor de aanvulling, mijnheer Bontes. Die schrijven we erbij.
Ik dank de mensen op de publieke tribune, de Minister, de ambtenaren en mijn collega's.

Sluiting 16.12 uur.