Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

29 544 Arbeidsmarktbeleid

Nr. 702

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 25 februari 2016

De vaste commissie voor Veiligheid en Justitie heeft op 20 januari 2016 overleg gevoerd met Staatssecretaris Dijkhoff van Veiligheid en Justitie over:

- **de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 1 mei 2015 met de aanbieding van het onderzoek Arbeidsmarkt voor cybersecurity professionals (Kamerstuk 29 544, nr. 613);**
- **de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 1 juli 2015 over de stand van zaken onderhandelingen over EU-ontwerprichtlijn over Netwerk- en informatiebeveiliging (Kamerstuk 33 602, nr. 6);**
- **de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 13 augustus 2015 inzake de EU-evaluatie aanpak cybercrime in Nederland (Kamerstuk 28 684, nr. 446);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 2 oktober 2015 inzake het overzicht van gekoppelde databestanden bij de rijksoverheid (Kamerstuk 26 643, nr. 368);**
- **de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 14 oktober 2015 inzake de beleidsreactie Cybersecuritybeeld Nederland 2015 (Kamerstuk 26 643, nr. 369).**

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

De voorzitter van de commissie,
Ypma

De griffier van de commissie,
Nava

kst-29544-702
ISSN 0921 - 7371
's-Gravenhage 2016

Voorzitter: Tellegen
Griffier: Mittendorff

Aanwezig zijn vier leden der Kamer, te weten: Gesthuizen, Oosenbrug, Tellegen en Verhoeven,

en Staatssecretaris Dijkhoff van Veiligheid en Justitie.

Aanvang 10.00 uur.

De **voorzitter**: Goedemorgen. Ik heet eenieder van harte welkom. We spreken vijf minuten spreektijd en twee interrupties per Kamerlid af.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. We hebben een aantal lijvige rapporten en interessante brieven ontvangen die het onderwerp cybersecurity raken. Ik zou het wel internetveiligheid willen noemen, maar blijkbaar is het inmiddels cybersecurity geworden. De verscheidenheid in onderwerpen laat zien dat cybersecurity niet in een rapport te vangen is. Voor mij heel belangrijk is de brief over het arbeidsmarktbeleid. Ik lees daarin enerzijds dat er voldoende aanmeldingen van studenten zijn, maar anderzijds is er te weinig doorstroming naar specifieke cybersecurityfuncties. Worden, als de instroom niet voldoende is, ook zijinstromers overwogen? Want de werkloosheid onder ouderen is nog altijd hoog. Volgens mij ligt daar aardig wat aanbod. Ook lees ik dat er vooral wordt gezocht in hbo- en wo-opleidingen. Maar ik durf de uitdaging aan te gaan, te beweren dat de mensen die gezocht worden voor die specifieke functies niet de mensen zijn die je in hbo- of wo-opleidingen moet zoeken. Dat moet veel meer gebeuren in de grote groep jongens – ik heb gemerkt dat het vooral jongens zijn – die zijn uitgevallen in het vmbo en soms ook het hbo. Dat zijn toch de jongeren met een storing in het autistisch spectrum. Onze autisten, zal ik maar zeggen. Onder die enorm grote groep jongeren zijn er heel veel die heel slim zijn met computers, internet en veiligheidslekken, maar nou net niet passen in het reguliere onderwijs. Ik noem ze tegenwoordig mijn helpende hackers, mede naar aanleiding van het boek van Chris van 't Hof, die daar ontzettend goed over heeft geschreven. Wat voor mogelijkheden ziet de Staatssecretaris om deze jongeren eventueel met een startkwalificatie ook die kans te bieden op een goede opleiding op universitair niveau, ondanks dat ze niet hbo- of wo-geschoold zijn? Is de Staatssecretaris bereid om naast de eerdergenoemde ouderen ook deze groep jongeren mee te nemen, juist gelet op de doelstelling om over voldoende cyberkennis en – kunde te kunnen beschikken?
Binnen de cybersecurity vormen de toenemende cybercrime en digitale spionage de voornaamste dreigingen. Eerder gesignaleerde trends zetten zich door. Ik verzin dit niet, dit staat allemaal in die mooie, lijvige rapporten. De geopolitieke ontwikkelingen hebben daarbij een versterkend effect. Maar welke ontwikkelingen spelen op dit moment de belangrijkste rol en hoe werken ze door? Welke consequenties trekt de Staatssecretaris daaruit? Ook staat in het rapport dat het aantal cybercrimezaken in 2018 360 zal bedragen. Maar waarom precies 360? Is dat een kwestie van capaciteit? Moet het doel niet zijn om minimaal 360 zaken te behandelen, met de daarbij behorende capaciteit? Een ding weten we inmiddels namelijk zeker: cybercriminelen zitten de komende jaren ook niet stil.
Helaas komen bijna maandelijks offlineaanslagen voor. Denk aan Parijs en Istanbul. Maar er zijn ook diverse ontwrichtende onlineaanslagen, zoals ddos-aanvallen. Ook die kunnen funest zijn voor de samenleving, of in ieder geval behoorlijk ontwrichtend. Hoe gaat de Staatssecretaris, zeker nu Nederland EU-voorzitter is, de lead nemen om deze dreigingen het hoofd te bieden? Gaat hij intensief samenwerken met de Europese

collega's en concrete afspraken maken over samenwerking en uitwisseling van gegevens, in lijn met de afspraken die gemaakt zijn op de antiterreurtop op 11 januari? Gaat hij specifieke maatregelen nemen in verband met mogelijke aanvallen als gevolg van politieke gevoeligheden, zoals rond de vluchtelingen?
De economie en ons persoonlijke leven spelen zich inmiddels voor een groot deel af op het internet. In het algemeen is digitale communicatie de norm. Dit betekent dat, als internet plat gaat, bijvoorbeeld door een cyberaanval, de samenleving eveneens plat gaat. Om dit risico te verminderen, bleek een volledig gescheiden netwerk om vitale processen te beschermen niet haalbaar. Onderzoekt de Staatssecretaris nog andere opties? De vitale processen zijn soms letterlijk van levensbelang. Daarbij moeten de gebruikers van internet, zowel zakelijke als privégebruikers, zich nog beter gaan realiseren dat ook internet kwetsbaar is. Want hoe zit het bijvoorbeeld met de zorgplicht van softwareleveranciers? We hebben allemaal kunnen lezen dat de Consumentenbond een kort geding aanspant tegen Samsung, omdat de smartphonemaker te weinig informatie geeft over software-updates. Voorziet de huidige wetgeving in het veilig maken van de digitale wereld? Ligt de bal bij de leveranciers die hun software up-to-date moeten houden, of is het juist de gebruiker van het product die verantwoordelijk is, als zijn of haar hardware gebruikt wordt bij een cyberaanval?

De heer **Verhoeven** (D66): Voorzitter. Kwetsbaarheden van software zijn nog altijd de achilleshiel van de digitale veiligheid, is een van de conclusies uit het cybersecuritybeeld. Dat is een groeiend probleem. De ICT en internet worden steeds belangrijker. Ook worden steeds meer apparaten op internet aangesloten, waardoor het opsporen van kwetsbaarheden steeds belangrijker wordt. Hackers, of veiligheidsonderzoekers, kunnen ons daarbij helpen, zoals mevrouw Oosenbrug terecht stelde. Ze kunnen helpen ICT-systemen veiliger te maken. D66 wil dat hackers beter beschermd worden. Ik weet dat er een leidraad voor responsible disclosure is, die nu wordt benut. Dat is een heel goed begin en een heel goede stap van dit kabinet geweest. Maar het is nog niet voldoende, omdat het nog steeds te beperkt is. Verder is er onvoldoende bescherming van hackers, vooral vooraf. Is de Staatssecretaris het met D66 eens dat, als hackers de leidraad goed opvolgen, ze niet strafrechtelijk vervolgd zouden moeten kunnen worden? Wat vindt de Staatssecretaris van uitspraken van rechters die hackers verder laten gaan dan de leidraad? Is hij bereid te onderzoeken hoe hackers beter beschermd kunnen worden?
Bedrijven leren juist steeds beter omgaan met hackers. De Nederlandse start-up HackerOne beloont hackers voor het vinden van kwetsbaarheden in software van Yahoo, Twitter, Dropbox of Airbnb. Waarom doen we dat als overheid niet? Is de Staatssecretaris bereid, te onderzoeken hoe we hackers kunnen belonen voor het opsporen van kwetsbaarheden in ICT-systemen van de overheid?

Mevrouw **Oosenbrug** (PvdA): Ethisch hacken is mijn corebusiness. We hebben gekeken naar de responsible disclosure. HackerOne is een soort makelaar tussen de hacker en een bedrijf. Ik vind dat op zich een heel goed systeem, omdat je daarbij de hacker beschermt, waarbij HackerOne ervoor zorgt dat een en ander niet bekend wordt. Zou de overheid ook een soort makelaarsrol moeten gaan vervullen tussen de ethische hacker en het bedrijfsleven?

De heer **Verhoeven** (D66): Volgens mij ligt het zelfs nog een slag simpeler. HackerOne is dan een makelaar, maar je kunt als overheid ook gewoon kijken naar een systeem waarin je zelf beloningen geeft aan mensen die kwetsbaarheden in systemen vinden. Er zijn heel veel

bedrijven die dat rechtstreeks doen. HackerOne is inderdaad een voorbeeld van een start-up die inmiddels makelaar is geworden. Maar er zijn ook grotere bedrijven die zelf allerlei manieren van belonen hebben om hackers te verleiden om hun kwetsbaarheden in hun systemen op te sporen. Ik zit dus veel meer te denken aan een meer directe vorm om als overheid te kijken hoe je hackers kunt vragen om kwetsbaarheden in je systeem op te sporen en ze daarvoor een passende beloning te geven. KPN doet dat al heel lang.

Mevrouw **Oosenbrug** (PvdA): Ik zou zeggen: overheid, omarm de ethische hacker en vervolg hem niet. Drieënhalf jaar geleden zijn wij daarmee gestart en inmiddels werkt responsible disclosure. De overheid geeft beloningen, vaak in de vorm van een T-shirt. België volgt ons daarin. Maar hoe krijg je het nog scherper?

De heer **Verhoeven** (D66): Ik weet dat mevrouw Oosenbrug heel enthousiast is over deze gedachte, die ze zelf al vaak naar voren heeft gebracht. Ik heb ook het boek van Chris van 't Hof gelezen. Hij geeft heel veel voorbeelden van hackers die op een bepaalde manier een kwetsbaarheid in een systeem vinden en daarmee iets moeten, waarmee ze in een soort grijs gebied terechtkomen van wat wel en niet mag. Ze hebben dat grijze gebied wel nodig om aan te tonen dat zij die kwetsbaarheid hebben gevonden. Bedrijven reageren soms heel terughoudend, bijna autistisch op de opmerkingen van hackers. Ze gunnen de hackers vaak niet de credits voor het vinden van die lekken. Dat boek beschrijft dat heel aardig. Het concludeert dat er nog één ding niet goed gaat, ondanks allerlei positieve dingen, namelijk dat er nog steeds geen duidelijkheid is over al of niet vervolging. We moeten zoeken naar een goede omgang daarmee, want je mag zware hackers ook weer niet de vrije hand geven. Ik ben heel benieuwd naar de reactie van de Staatssecretaris daarop. Mijn laatste vraag aan de Staatssecretaris op dit punt is of hij bereid is te onderzoeken, hoe we hackers kunnen belonen voor het opsporen van kwetsbaarheden in de ICT-systemen.
In het cybersecuritybeeld zien we dat digitale spionage de grootste bedreiging blijft. Ik ben heel blij dat dit kabinet encryptie niet wil afzwakken. Het kabinet heeft daarover een paar weken geleden een brief naar de Kamer gestuurd. Twee maanden geleden heeft de Tweede Kamer een amendement van D66 aangenomen om een half miljoen te steken in het stimuleren van encryptie. Juist in deze tijden is encryptie een heel belangrijke bijdrage aan internetveiligheid. Het zorgt er namelijk voor dat je erop aankan dat je software veilig is en dat er geen kwetsbaarheden in zitten, waardoor allerlei anderen, zoals misschien wel inlichtingendiensten, jouw informatie kunnen bekijken. Daar is veel discussie over. Frankrijk heeft zich onlangs uitgesproken voor het afzwakken van encryptie. Het noemde daarbij specifiek het standpunt van Nederland. Ik ben heel blij dat er weer onderwerpen zijn waarbij Nederland, net als een paar jaar geleden bij netneutraliteit, vooroploopt. Dat is niet alleen belangrijk voor veiligheid en privacy, maar ook voor het verdienmodel van Nederland, omdat heel veel bedrijven Nederland als vestigingsplaats aantrekkelijker zullen vinden als ze weten dat hun informatiesystemen veilig zijn. Ik hoop dat de Staatssecretaris en het kabinet dit beleid voortzetten en niet zwichten voor de druk van andere partijen.
Veel cybercrime is niet hightech, maar lowtech. Daarmee bedoel ik dat heel veel cybercriminaliteit kan worden voorkomen met goede wachtwoorden, het volgen van updates en niet op rare bijdragen en linkjes klikken. Dat zijn dingen die iedereen zou kunnen doen. De «Alert Online»-campagne is goed, maar niet voldoende. We hebben echt een campagne nodig die bijna van mond tot mond gaat, zoals Bob, daar kom je mee thuis of de anti-inbraakcampagne Maak het inbrekers niet te makkelijk. Mensen moeten echt denken: ja, nu weet ik het wel. Zo'n campagne is er

nog niet. Ik vraag de Staatssecretaris of hij bereid is te bekijken of het mogelijk is, de campagne te intensiveren tot een campagne die door heel veel mensen wordt gezien.
We hebben gevraagd om een overzicht van de gekoppelde bestanden. Dat is er nu. Alleen al het ministerie zelf heeft 90 gekoppelde databestanden, met tal van organisaties die toegang hebben tot die databestanden. Ik ben oprecht geschrokken van dat aantal. Is dat aantal geleidelijk zo gegroeid, of zit er een plan achter? Zo ja, kan de Staatssecretaris dat plan dan naar de Kamer sturen? Zo nee, is de Staatssecretaris dan bereid het aantal gekoppelde databestanden kritisch tegen het licht te houden en erin te snijden? Wat betekent koppelen overigens precies? Betekent het niet gewoon vermenigvuldigen?

Mevrouw **Gesthuizen** (SP): Voorzitter. Kortheidshalve sluit ik mij aan bij de vragen die mevrouw Oosenbrug heeft gesteld over het voldoende ter beschikking hebben van professionals voor cyberveiligheid. De enige vraag die ik wil stellen over het onderzoek naar arbeidsmarktbeleid voor cybersecurityprofessionals gaat over het feit dat begin dit jaar het nieuws kwam dat de politie online-opsporingstaken niet goed kan uitvoeren, door bezuinigingen van 40 miljoen op de ICT. We kunnen cybersecurity intussen wel aantrekkelijker maken voor studenten en meer cyberagenten aantrekken, maar ze moeten natuurlijk ook hun werk kunnen doen. Gaat dit samen door een deur? Is door het WODC rekening gehouden met dergelijke bezuinigingen? Of is hun onderzoek intussen achterhaald door de realiteit? Cyberagenten kunnen nieuwe opsporingstaken, zoals de omstreden hackwet, niet uitvoeren door de bezuinigingen op de ICT. Wat zijn de gevolgen voor de huidige opsporingstaken met betrekking tot cybercrime? Waarom wordt er überhaupt bezuinigd op ICT, in een tijd waarin ICT steeds belangrijker wordt, niet alleen voor overheid en burger, maar uiteraard ook voor criminelen? Is door het WODC ook rekening gehouden met bredere bezuinigingen van deze regering, zoals de bezuinigingen op het OM? Wordt er ook bezuinigd op cybersecurity? Er worden nieuwe cyberagenten aangetrokken bij de politie. Komen die bovenop het huidige aantal fte, of wordt die capaciteit elders weggehaald? Hoe zit dat met het OM? Wordt er ook gekort op middelen om beter samen te werken met andere organisaties?
De EU-ontwerprichtlijn over netwerk- en informatiebeveiliging is half december aangenomen. Volgens mij wachten we nu op de implementatiewet. Wanneer komt die er?
De EU-evaluatie aanpak cybercrime in Nederland dateert van augustus vorig jaar. Goed dat we het er nu al over hebben. Ik begrijp dat een deel van de aanbevelingen al door deze regering ter hand wordt genomen. Om welk deel gaat het precies? Ik neem aan dat dat ook de aanbeveling betreft waarin staat dat regionale politie en rechterlijke macht verder moeten worden opgeleid om de kloof inzake communicatie en rechercheurs, aanklagers en rechters op het gebied van cybercrime te dichten. Wat is de reactie van de regering op de kritiek dat de bevoegdheid om cybercriminelen te bestrijden en voor de rechter te brengen, in handen wordt gelegd van de particuliere sector, omdat er geen sanctie staat op het niet melden van cyberinbraken en het NCSC? Ik ben niet direct zo geschrokken als de heer Verhoeven over het aantal gekoppelde bestanden. Waartoe, waarvoor en wat levert het op? Als niet duidelijk is wat we ermee opschieten, zou me dat wel heel grote zorgen baren. Ik vond het een wat onoverzichtelijk pakket, maar ik heb me er doorheen geworsteld. Welke inzichten heeft de regering daarmee bereikt en wat levert het de samenleving op?
In de beleidsreactie Cybersecuritybeeld Nederland 2015 van 14 oktober jongstleden wordt onder aandacht besteed aan de kwetsbaarheden in de software. De heer Verhoeven heeft daar ook een opmerking over gemaakt. We hebben daarover vaker gediscussieerd met de regering. Deze stelde

toen dat de kwetsbaarheden niet expres in stand worden gehouden. Maar in een bericht van RTL-Z van 4 januari, dus heel kort geleden, wordt toch weer aangegeven dat zerodatas worden verkocht aan overheden. Wat doen opsporingsinstanties en overheden dan eigenlijk als ze deze kwetsbaarheden tegenkomen? Melden ze die aan de eindgebruiker of aan de softwareleverancier? Hoe meer apparaten worden aangesloten, hoe risicovoller en hoe meer kans op kwetsbaarheden.
Over de beveiligingsadviezen van het Nationaal Cyber Security Centrum (NCSC) merk ik het volgende op. Aangezien er volgens de Inspectie Veiligheid en Justitie sprake is van een beperkte meerwaarde worden deze adviezen heroverwogen. Zal hierbij gekeken worden naar meer maatwerk? Veel informatie over beveiliging kan uit openbare bronnen wordt gehaald, wordt gesteld. Dan mogen bedrijven daar zelf actief naar op zoek, begrijp ik. Het mag dan wel gaan om veelal openbare bronnen, maar het NCSC verifieert en kwalificeert deze informatie wel. Ik zie dat bedrijven eerlijk gezegd zelf nog niet doen. Hoe ziet de Staatssecretaris dat voor zich? Wordt daarmee bij de heroverweging wel rekening gehouden?
Het is natuurlijk heel goed dat Nederland tijdens het EU-voorzitterschap de aanpak van cybercrime hoog op de agenda heeft staan. Af en toe vraag ik me af hoeveel tijd de EU nog heeft om ook voor dit onderwerpen breed aandacht te vragen, aangezien we met een nogal diepe crisis te maken hebben die met het voortbestaan van de EU te maken heeft. Ik heb het dan vooral over de asielcrisis, waarvan de Staatssecretaris een van de personen is die die crisis hopelijk oplost. Klopt de titel van het nieuwsbericht van RTL-Z waarin staat dat deze regering tegen achterdeurtjes als het gaat om cyberencryptie is? Is deze regering wel voor sterke encryptie? Of zegt ze: dat kan nu niet, maar misschien in de toekomst wel?
Over de hackwet heeft de vorige Minister toegegeven dat er op afstand wordt ingebroken. Volgens hem kon dat op basis van artikel 125i Wetboek van Strafvordering, maar daarin staat alleen het doorzoeken van een plaats. In het artikel staat niet dat het ook gaat om het op afstand inbreken op computer. Het feit dat het gebeurt of gebeurde, mag of mocht dat wel?

Voorzitter: **Oosenbrug**

Mevrouw **Tellegen** (VVD): Voorzitter. Allereerst kom ik op het Cybersecuritybeeld Nederland 2015. Nederland is een van de meest digitale landen van de wereld. Dat biedt kansen, maar het levert ook kwetsbaarheid op als het gaat om cyberaanvallen en -criminaliteit. Uit het laatste rapport blijkt dat cybercrime en -spionage de twee grootste bedreigingen zijn en blijven voor Nederland. De internationale veiligheidssituatie draagt daar niet aan bij. Nederlandse instellingen binnen en buiten Nederland zijn in toenemende mate doelwit van digitale spionageactiviteiten. Deze trend blijkt hardnekkig en vereist stevige maatregelen. Als ik de stukken van het kabinet lees, zie ik dat er heel veel werk is verricht als het gaat om de samenwerkingsstructuur en om betere samenwerking tussen de veiligheidsdiensten met als doel, de onderzoeks- en analysecapaciteit om cyberspionage aan te pakken, te versterken. Wat levert die betere samenwerking nu op en wat doen we concreet? Hoe krijgt het kabinet inzicht in de digitale capaciteiten, intenties en activiteiten van buitenlandse actoren? In het verlengde hiervan ligt de nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Die wet is er nog niet; er is een concept opgesteld dat nog niet in de Kamer ligt. Maar die herziening is nodig om de veiligheidsdiensten anno 2016 digitaal hun werk te kunnen laten doen. Daar komen we later nog uitgebreid over te spreken in dit huis. Kan de Staatssecretaris aangeven of deze wet, ook als het gaat om contraspionage, voldoende mogelijkheden biedt, als antwoord op de toenemende aanvallen van buitenaf? Als voorbeeld: de Russische geheime dienst breekt in in het aansturingssysteem van alle sluizen van

Rijkswaterstaat. Wat stellen wij daar in Nederland dan tegenover? Wordt er gewerkt met doemscenario's, met name als het gaat om de vitale infrastructuur? Worden alle systemen voldoende vaak getest?
Onlangs las ik in het FD een pleidooi voor het instellen van een cybercommissaris. Los van de vraag of dat echt zou helpen, las ik daar vooral een oproep in voor een hogere sense of urgency als het gaat om de veiligheid van de digitale infrastructuur. Nederland is kwetsbaar. Doordat we zo groeien, komen er vele bedrijven naar Nederland. Landen als het VK en Duitsland blijken in grotere mate een Fort Knox te bouwen als het gaat om digitale veiligheid.

De heer **Verhoeven** (D66): Mevrouw Tellegen stelt dat er veel bedrijven naar Nederland komen, doordat de cybersecurity hier goed is. Is de VVD op de hoogte van het feit dat er een grote groep internetgerelateerde bedrijven en brancheorganisaties is, zoals dataopslagbedrijven, maar ook Nederland ICT, Google, KPN en Netflix, die een brandbrief heeft gestuurd naar het kabinet vanwege wetten als de nieuwe Wet op de inlichtingen- en veiligheidsdiensten? Is er geen groot gevaar dat door alle eenzijdig op veiligheid gerichte maatregelen van dit kabinet juist het vestigingsklimaat door de VVD onder druk komt te staan, wat volgens mij absoluut niet de bedoeling is?

Mevrouw **Tellegen** (VVD): Dank voor deze interruptie. Dat is namelijk precies wat ons te doen staat: juist omdat we een gunstig vestigingsklimaat hebben, dat onder druk staat, is het zaak om met name in de wetten die dit voorjaar hopelijk in deze Kamer zullen worden behandeld, namelijk de hackwet en de Wet op de veiligheids- en inlichtingendiensten, naar een balans te zoeken. Want alleen dan kunnen we in dit land privacy en veiligheid samen laten gaan.

De heer **Verhoeven** (D66): Bij mijn partij is er oprechte bezorgdheid op dit punt. Het afgelopen half jaar hebben we met heel veel bedrijven hierover gesproken. Het kabinet zet op dit moment een aantal stappen. Eigenlijk zijn er vier vergaande wetsvoorstellen: de Wet bewaarplicht telecommunicatiegegevens, het PNR-systeem, computercriminaliteit III en de Wet op de inlichtingen- en veiligheidsdiensten. Alle vier hebben ze het zweem van eenzijdige, symbolische maatregelen om de veiligheid te vergroten, terwijl niet bewezen is dat die veiligheid daarmee wordt vergroot, terwijl bedrijven wel vinden dat Nederland daardoor als vestigingsplaats onder druk komt te staan, omdat de klantdata niet meer veilig zijn enzovoorts. Die balans is op dit moment ver te zoeken. Gaat de VVD er wat aan doen om te voorkomen dat het kabinet doorschiet naar de verkeerde kant, zich vooral richtend op symbolische veiligheid?

Mevrouw **Tellegen** (VVD): Ik herken mij niet in het beeld dat de balans zoek is of dat het gaat om eenzijdige wetgeving. Het gaat juist om het vinden van een balans. Tegelijkertijd zitten we hier ook om onze vitale digitale infrastructuur veilig te stellen. Daar moeten we iets tegenover kunnen stellen. Hoe kunnen we de economische belangen van het bedrijfsleven waarborgen, er daarbij ook voor zorgend dat ons land in al zijn kwetsbaarheid veilig is? Als we hier constateren dat digitale spionage op dit moment de grootste bedreiging vormt voor Nederland, dan mag ik hopen dat D66 daar iets tegenover wil stellen. We moeten dus zoeken naar een balans. Ik verzet me tegen het beeld dat de wetten die er liggen, een eenzijdige veiligheidscomponent hebben.
Legacy is een belangrijk fenomeen. De afhankelijkheid van ICT neemt alleen maar toe. ICT heeft net als melk en yoghurt een houdbaarheidsdatum. ICT-systemen die essentieel zijn voor het functioneren van vitale processen en diensten lopen risico op uitval en hacks, omdat een deel bestaat uit verouderde systemen. Het kabinet erkent deze risico's. Stel je

voor dat er op het gebied van transport, financieel verkeer of de energievoorziening systemen uitvallen, puur omdat ze verouderd zijn. In het rapport staat dat aanpassingen door instellingen vaak te laat of helemaal niet worden verricht. De VVD vindt dit zorgelijk. Nu heeft het NCSC een methode om deze legacy in kaart te brengen. Maar dat is pas de eerste stap. De VVD wil een stap verder gaan. Hoe gaan we bijvoorbeeld om met verouderde industriële systemen en hoe gaan we deze in snel tempo vervangen? Wat is de ambitie op dit punt van het kabinet?
Ik heb twee vragen over het EU-voorzitterschap. Wat is de laatste stand van zaken met betrekking tot uitvoering en implementatie van de richtlijnen netwerk- en informatiebeveiliging? Er ligt een evaluatierapport over cybercrime met een groot aantal aanbevelingen. Welke worden daarvan overgenomen en welke niet? Het kabinet typeert ze als nuttige aanbestedingen. Wat gaat daarmee gebeuren?
Tot slot kom ik op het punt van goed ICT-onderwijs. Een van de doelstellingen is dat Nederland beschikt over voldoende cybersecuritykennis en –kunde en investeert in ICT-innovatie. Dat valt en staat met voldoende goed opgeleide ICT-specialisten. Dat vergt druk op de ketel van OCW als het gaat om ICT-onderwijs. In de brief staat dat er weliswaar geen tekort is, maar in de toekomst mogelijk wel en dat er geen goede doorstroming is naar functies, terwijl er ook geen aansluiting is tussen onderwijs en praktijk. Dat vindt de VVD geen geruststellend geluid. Hoe kunnen we die kennis en kunde overeind houden? Veiligheid moet een integraal onderdeel worden van software programmeren. Is dat voldoende geregeld bij de informaticapopleidingen?

De **voorzitter**: Er is nog een aanvullende vraag van de heer Verhoeven.

De heer **Verhoeven** (D66): We hebben laatst een rondetafel gehad over safe harbours, een lastig vraagstuk. Breed werd toen gezegd: encryptie is een van de mogelijke oplossingsrichtingen. Het kabinet heeft daar een standpunt over. Maar het heeft ook de Wet computercriminaliteit III liggen. Blijft encryptie daarin volledig overeind? Er wordt immers gehackt in systemen, wat dan toch op een bepaalde manier via kwetsbaarheden zal moeten. Dat verhoudt zich allemaal heel moeilijk tot elkaar. Wat vindt de VVD van encryptie? Is ze daar een overtuigd voorstander van en wil ze dat dus overeind houden, of ziet ze toch mogelijkheden om achterdeurtjes en kwetsbaarheden in te bouwen, zodat daarin gehackt en ingebroken kan worden?

De **voorzitter**: Wellicht heeft de VVD daar zelf een antwoord op.

Mevrouw **Tellegen** (VVD): De laatste lijn die de heer Verhoeven aangaf, is de lijn van de VVD. Misschien een flauw antwoord, maar er moet een balans worden gevonden tussen beide opties. Enerzijds is de noodzaak van encryptie groot, anderzijds moeten er onder heel strikte voorwaarden mogelijkheden zijn voor opsporingsdiensten om achter cybercriminelen aan te gaan en spionage te bestrijden.

De heer **Verhoeven** (D66): Dit is wel precies waar ik bang voor was. Aan de ene kant roepen dat encryptie goed is, maar toch elke keer die mitsen erbij. Eigenlijk zegt de VVD: als het niet uitkomt, dan toch maar geen encryptie, waarmee wel kwetsbaarheden ontstaan en openingen worden geboden, zodat de politie in computers en smartphones van onschuldige burgers kan inbreken. Is de VVD echt gewoon voor encryptie? Of vindt ze: ja, we zijn voor, behalve als het ons even niet uitkomt?

Mevrouw **Tellegen** (VVD): Ik zou een wedervraag aan de heer Verhoeven willen stellen. Gaat hij deze beide wetten niet steunen als encryptie niet 100% gewaarborgd is? Wat doet de heer Verhoeven dan met al die

vraagstukken die op dit moment levensgroot op ons bord liggen als het gaat om digitale spionage en cybercrime? Hoe rijmt hij dat dan met zijn stellige overtuiging dat encryptie het antwoord is?

De heer **Verhoeven** (D66): Ik vind zo'n wedervraag hartstikke leuk. De VVD geeft echter geen antwoord en de voorzitter vindt dat goed. Ik beantwoord die vraag graag, maar alleen als mevrouw Tellegen eerst antwoord geeft op mijn vraag.

Mevrouw **Tellegen** (VVD): Zo ken ik de heer Verhoeven weer. Nogmaals: het antwoord ligt ergens in het midden. 100% encryptie zorgt ervoor dat er tegelijkertijd een probleem ontstaat als het gaat om het veiligstellen van onze digitale infrastructuur. Dus moet er ergens in het midden, onder heel strikte voorwaarden, wel een mogelijkheid worden gecreëerd. Dat is de kern van de voorliggende wetten. Ik ben benieuwd wat D66 precies met die wetten gaat doen als encryptie niet 100% gewaarborgd blijkt te kunnen worden.

De **voorzitter**: Als voorzitter grijp ik even in. Dit onderwerp leeft heel erg, maar we moeten wel bedenken dat deze wetgeving nog behandeld zal worden. Als de heer Verhoeven nog wil reageren op de wedervraag, mag hij dat doen.

De heer **Verhoeven** (D66): Ik wil er best op reageren.

De **voorzitter**: Dan geef ik de heer Verhoeven de kans om erop te reageren.

De heer **Verhoeven** (D66): U zegt het zelf terecht: ik loop nooit weg voor een antwoord op een vraag, maar we gaan deze wet nog behandelen. Er komen nog allerlei dingen. Ik ga niet zeggen of we de wet al of niet zullen steunen. Maar voor ons is encryptie en het toelaten van kwetsbaarheden in software om ervoor te zorgen dat de veiligheid kan worden vergroot, erg fundamenteel. Het kabinet is voor encryptie, zij het dat kwetsbaarheden op sommige momenten wel moeten kunnen. Daar moeten we nog eens met het kabinet over praten. Ik zou iedereen tekortdoen als ik nu ging zeggen dat we de wet al of niet gaan steunen. Daar geef ik dus geen antwoord op, in de volle overtuigding dat dat op dit moment de juiste weg is. Maar het is goed om deze discussie straks te voeren.

Voorzitter: Tellegen

De vergadering wordt van 10.41 uur tot 10.48 uur geschorst.

Staatssecretaris **Dijkhoff**: Voorzitter. Het belang van cybersecurity wordt breed gedragen. De lijn die we daarop inzetten, daarbij de samenwerking met private partijen zoekend, wordt eveneens breed gedragen. Ik vind dat prettig om te constateren. Wel zijn er over de maatregelen zelf nog veel vragen en verschillen van inzicht. Daarmee is het wel een breed AO geworden.
Voor ons is de brief bij het Cybersecuritybeeld Nederland 2015 leidend. Positief is dat we op koers liggen. De complimenten van België zijn leuk om te horen, maar ik had liever gezien dat andere landen verder waren. Ik heb het liefst dat een kwetsbaarheid wordt ontdekt. Hoe meer mensen aan de goede kant van de streep daarnaar op zoek zijn, hoe groter de kans dat we het snel kunnen fixen. Het blijft dus zaak om door te werken. Helaas zitten de mensen aan de verkeerde kant ook niet stil. De heer Verhoeven sprak over succesvolle campagnes, waardoor domme phishingmails niet meer worden verstuurd. Dat betekent wel dat de mensen aan de verkeerde kant veel intelligenter worden en zich ook met social

engineering richten op de persoon, waardoor het moeilijker wordt om te herkennen dat sprake is van foute mails. De tijd van foute logo's en spelfouten is helaas voorbij. We moeten ervoor zorgen dat we de ontwikkelingen bijbenen.

Mevrouw **Gesthuizen** (SP): Excuus voor het feit dat ik iets te laat binnenkwam. Een tijdje geleden heb ik de proef op de som genomen door aangifte te doen van een phishingmail. Ik heb contact opgenomen met een grote Nederlandse bank waar het rekeningnummer van de fraudeurs vandaan kwam. Maar vervolgens heb ik daar niets meer over gehoord. Wat is nou precies het beleid? Het lijkt me niet dat dit het doen van aangifte aanmoedigt.

Staatssecretaris **Dijkhoff**: Het beleid is natuurlijk wel dat de bank waar het om gaat de klanten waarschuwt. In brede zin is al de waarschuwing uitgegaan dat, als wordt verzocht ergens op te klikken, de mail nooit van een bank afkomstig kan zijn. Maar deze meldingen zijn wel nodig om te zien of er wel doorgepakt kan worden, vooral als het erop lijkt dat er grotere organisaties achter zitten die het vaak doen. De terugmelding daarvan zal inderdaad niet steeds gebeuren. Het vertrouwenwekkende imago van een verder bonafide bedrijf wordt misbruikt om de klanten te lokken. Dat bedrijf heeft ook een rol in de voorlichting. In bepaalde gevallen worden er via de media en het ministerie al bredere waarschuwingen gegeven.

Mevrouw **Gesthuizen** (SP): Waar ik als burger, maar zeker als volksvertegenwoordiger een beetje bevreesd voor ben, is dat er niet zo heel veel gebeurt. Fraude heeft over het algemeen niet de allerhoogste prioriteit. Ik kan me voorstellen dat een bank een onderzoek start en ermee aan de slag gaat, maar die garantie heb ik absoluut niet. Ik heb nog wel gevraagd of ik iets meer mocht horen over wat er in het algemeen gebeurt, maar toen bleef het erg stil.

Staatssecretaris **Dijkhoff**: Voor die bank kan ik verder niet spreken dan in algemene termen. Het is niet zo dat we iedere dag heel veel mensen oppakken die zulke mails hebben verstuurd. Ze zijn vaak handig bij het versturen van die mails. Een Nederlandse rekening biedt aanknopingspunten. Maar dan hebben we het over mails waarin wordt gevraagd geld over te maken naar een bepaald rekeningnummer. Ik moet eerlijk zeggen dat dat een vrij ouderwetse variant is, want er zijn intelligentere manieren om dat geld binnen te krijgen, zonder getraceerd te worden. Nogmaals, een Nederlands rekeningnummer kan een aanknopingspunt zijn. Maar ik ken de casus verder niet. Je zou verwachten dat je daarnaar door kunt zoeken.

Mevrouw **Gesthuizen** (SP): Ik zal de casus een keer aanleveren, met de aangifte erbij.

Staatssecretaris **Dijkhoff**: Een andere grote dreiging is dat je computer op slot komt te zitten. Ik denk dat het helpt het probleem breder bekend te maken, maar dan zijn we nog niet bij de oplossing. Het is niet alleen maar de last die je als individuele gebruiker kunt hebben als dit je overkomt, vervolgens kan je systeem worden overgenomen, daarbij bijdragend aan de kwetsbaarheid. Als je dat niet doet op je thuiscomputer, maar op je werk, open je misschien wel de deur voor anderen om bij de systemen van je werkgever te komen, wat ook weer gevolgen kan hebben voor vitale sectoren in Nederland. Er is inderdaad geen onderscheid te maken tussen een groot en een klein probleem. Een kleine onachtzaamheid of handeling kan grote gevolgen hebben, als de mensen die erachter zitten zich daar heel doelbewust op richten.

Wat doen we eraan? Bij Europese overleggen is het niet zo dat er iedere keer op het hoogste niveau een discussie over cybersecurity ontstaat. Dat is nog een kwestie van awareness bij overheden. We moeten een aanpak stimuleren waarin duidelijk wordt dat overheden niet meer in hun eentje van alles kunnen doen. We moeten dit ook niet alleen maar zien als een bedreiging. Daarom beleggen wij als EU-voorzitter een aparte sessie, waarvoor deskundigen die niet vaak naar allerlei raden komen, worden uitgenodigd om hun zegje te doen. Bij discussies hierover hoor ik wel eens: Ja, precies, we moet dat jihadfilmpje offline kunnen halen. Op zich is dat heel relevant, maar ik denk dat cybersecurity veel meer is dan dat. Het is aan Nederland en een aantal andere landen om ervoor te zorgen dat de andere landen het been bijtrekken en het systeem omarmen dat volgens ons goed is, namelijk het zoeken van een balans tussen het bieden van veiligheid en het creëren van een soort maakbaarheidsfilosofie. Bij encryptie zie je het laatste ook optreden: als wij het maar verbieden, gebeurt het niet. Zo simpel is de werkelijkheid niet. Dan gooi je ook te veel van het goede weg, niet alleen economisch gezien, maar ook qua persoonlijke vrijheden.
Wanneer wordt de NIB-richtlijn geïmplementeerd? Er is een politiek akkoord, wat nog niet hetzelfde is als «klaar om te implementeren». Er moeten nu nog technische meetings worden gehouden voor de detailuitwerking. Daarna heb je nog een termijn voor de vertaling, waarna er formele ondertekening moet plaatsvinden, gevolgd door een periode van 21 maanden voor omzetting, en dan nog zes maanden waarin moet worden bepaald op wie het van toepassing is. Dat is niet iets om op te wachten. We hebben zelf al de nodige bepalingen in werking gesteld. Het wetsvoorstel gegevensverwerking en meldplicht cybersecurity hebben we naar de Kamer gestuurd. We proberen zo min mogelijk dubbel werk te doen, maar het lijkt me niet gezond om niets te doen, in afwachting van een richtlijn.

Mevrouw **Oosenbrug** (PvdA): Ik heb een verhelderende vraag. De Staatssecretaris heeft het over de NIB-richtlijn. Wat is dat voor een richtlijn?

Staatssecretaris **Dijkhoff**: Netwerk informatie beveiliging. In het Engels is dat NIS. Daar zit je weer met de vertaling.

De **voorzitter**: De Staatssecretaris moet er zeker zes maanden voor uittrekken om dat goed te vertalen.

Staatssecretaris **Dijkhoff**: Een S die een B wordt; dat moeten we niet onderschatten!
Over responsible disclosure merk ik het volgende op. Ik ben het eens met de stelling van de heer Verhoeven dat als iemand zich aan de leidraad houdt, hij of zij niet vervolgd moet worden. Dat is het signaal. Ik heb nog geen casus gezien waarin iemand helemaal de leidraad volgde en toch vervolgd werd. Heel formeel: ik kan dat nooit garanderen, want die bevoegdheid heb ik niet. Maar ik heb het OM dat ook niet zien doen. Het OM onderstreept – daarom is het ook een leidraad – dat het volgen van de leidraad moet leiden tot niet-vervolging. Daarnaast zijn er organisaties die zelf, naast het OM, stellen: als je je aan deze regels houdt, doen wij sowieso geen eens aangifte. Sommigen zullen zelfs een nog ruimere policy hebben. Over iemand die beweert zich aan de richtlijn te hebben gehouden, kunnen toch twijfels bestaan. In dat geval kan besloten worden om vervolging in te stellen en om de rechter te laten oordelen. Ik verwijs naar het veelgenoemde en veel geroemde boek «Helpende hackers». Daarin worden voorbeelden genoemd, waarvan je op het oog denkt dat het gaat om mensen die zich aan de leidraad hebben gehouden, waarna op de rechtzetting een aantal zaken naar voren kwam die het tegendeel

aangaven. Ik denk dat de leidraad goed werkt. Ik bespreek hem internationaal met collega's. Misschien hebben we in Nederland wat ruimere ervaring met gedogen en met leidraden die niet leiden tot vervolging. Ik kan niet zeggen dat iedereen het meteen een briljant plan vindt. Het woord «hacker» heeft toch een slechte naam bij menigeen. Wij leggen altijd precies uit hoe het zit. Ik denk dus dat de leidraad die we nu hebben werkt. Het belonen via een prachtig T-shirt is één element, maar we organiseren ook evenementen en bug bounties. Ik denk dat dat goede middelen zijn, die we als Nederland op de Global Conference on Cyber Space naar voren hebben gebracht. Daarbij gaat het vooral om samenwerking met bedrijven en alle anderen met goede intenties. Niet alleen het niet misbruiken, maar ook het melden van kwetsbaarheden moet worden beloond.

De heer **Verhoeven** (D66): Dank voor het antwoord van de Staatssecretaris. Daar ben ik blij mee. We moeten zien wat we moeten doen als het gaat om vervolging. Als ik wel concrete cases heb die 100% voor vervolging in aanmerking komen, zal ik ze aanleveren.
Het andere punt betreft het belonen. De Staatssecretaris noemde dat T-shirt, naast faciliteiten en evenementen. Daaruit kan ik ook concluderen dat hij het te ver vindt gaan om te kijken naar een beloningssysteem, zoals bedrijven dat wel hebben.

Staatssecretaris **Dijkhoff**: Dat doen we nu, maar daar is geen standaardtarievenlijst voor. Er is geen standaardtarief voor een bepaalde soort kwetsbaarheid. Ik ben daar niet tegen, maar ik zie geen standaardisering voor ogen van wat we nu al doen.

De heer **Verhoeven** (D66): Dat begrijp ik. Ik zal er zelf ook over nadenken. Het is misschien ook wel een nadeel om te standaardiseren. Aan de andere kant hebben we, zoals de Staatssecretaris zelf zegt, een mooie traditie. We waren de eerste in Europa die netneutraliteit in de wet opnamen. In tegenstelling tot andere landen gaan we encryptie stimuleren. Ook op het gebied van hackers hebben we een rijke traditie. De overheid zou misschien iets meer kunnen aangeven wat ze al wel doet, niet zijnde een tarievenlijst op de website van het ministerie. Kan daar eens over worden nagedacht?

Staatssecretaris **Dijkhoff**: Nadenken wil ik altijd doen. Soms heb ik dan meteen een idee waar mijn gedachten heen gaan, maar dat heb ik nu nog niet. Dat vind ik hier lastig aan. Als er nog winst in zit, zou het mooi zijn om die te pakken, want het is een belangrijk thema. Uitdragen doen we sowieso, ook internationaal. «Hacken» is op zich nog een neutrale term, die niet bij voorbaat negatief is. Ik vind het eigenlijk wel mooi als er vanuit de samenleving zelf initiatieven komen op dat punt. Kwetsbaarheid is immers niet per se iets waarvan alleen de overheid last heeft, vooral niet als het een kwetsbaarheid is die is ontstaan door niet optimaal presteren van een private partij die iets ontwikkeld heeft. Ik zou daarbij niet in de plaats van die private partij willen treden om dat wel goed te doen.
Wat zijn de belangrijkste trends? Cybercrime en digitale spionage zijn de zaken die vaak in beeld komen. Daarom vond ik het van belang om in mijn inleiding ook de heel kleine dingen te noemen. Ze klinken niet zo wereldschokkend, maar er is nog een hele reeks bijna dagelijkse dingen die we, als we niet oppassen, gaan zien als dagelijkse overlast, terwijl ze wel te voorkomen zijn. Er is wel een verband tussen die zaken en de grotere kwetsbaarheden. Ik hecht eraan om beide te blijven onderstrepen. De overheid moet haar verantwoordelijkheid nemen, evenals de bedrijven. We moeten ze wijzen op het feit dat ze informatie hebben die interessanter is voor anderen dan ze misschien zelf doorhebben. Vaak wordt het diefstal genoemd. Het «voordeel» van een offline diefstal is dat

je weet dat je iets kwijt bent. Als er iets met je gegevens gebeurt, heb je het vaak niet eens door. Je mist niks en toch ben je het kwijt. Wordt er vijf jaar later een product gelanceerd dat je bekend voorkomt, dan is het te laat, dan ligt die informatie er al en misschien ook andere informatie.
De heer Verhoeven prikkelde ons om te komen tot een soort Bob-campagne. Ik zou dat ook wel willen. Hij heeft ook wat campagne-ervaring. Het is niet zo dat je een tarievenlijst bij een reclamebureau krijgt en dat het bureau dan zegt: voor dat geld heb je een aardige campagne en als je dit betaalt, heb je een briljante vondst. Het voordeel van de Bob-campagne was dat die uit België kwam. De campagne werkte daar perfect. Die konden we in Nederland zo overnemen. We proberen het wel, maar we zijn nog niet gekomen op zo'n catchy campagne. We hebben wel succesvolle campagnes gehad die goed werkten, maar ik moet eerlijk toegeven dat ik die ene catchphrase waardoor iedereen het meteen snapt, nog niet heb kunnen bedenken. We proberen om niet over de hoofden heen met een term te komen als we niet denken: dit wordt hem. We proberen juist om heel gericht ieder jaar er één sectie uit te pakken. Dit jaar gaat het om het mkb. We proberen heel gericht dicht bij de mensen het verhaal te brengen en het gesprek aan te gaan. Vervolgens zorgen we ervoor dat het zich verspreidt. We hangen niet alleen posters op waar een boodschap op staat, maar we lichten ieder jaar heel gericht een sector eruit. Daarmee duiken we dan de diepte in. Mocht de heer Verhoeven zelf een keer een briljante vondst hebben, dan horen we die natuurlijk graag. Ik denk dat er dan wel een T-shirt in zit.

De heer **Verhoeven** (D66): Toch niet met oranje letters en blauwe strepen?

Staatssecretaris **Dijkhoff**: Nee, zeker niet. Het is een zwart T-shirt met witte letters.
Ik zie hier een afkorting staan. Ik ben alvast aan het bedenken of ik die afkorting voor mevrouw Oosenbrug kan uitspellen. Mevrouw Oosenbrug zei dat er offline dreigingen zijn die ook online ontwrichtend kunnen werken en consequenties kunnen hebben. Die link wordt ook gelegd bij bredere thema's. Bij cybersecurity kijk je naar de kwetsbaarheden en niet per se naar het motief. De term «kwetsbaarheid» kan wel gebruikt worden als er sprake is van een crimineel met winstoogmerk maar ook als iemand vanuit een idealistisch motief probeert om iets kwaads te doen. Je hebt dus geen aparte cybersecurityhoek voor bepaalde typen misbruik, maar bijvoorbeeld in de antiterrorismehoek is er wel een cyberbeeld. Dan is er dus sprake van de omgekeerde situatie. Vandaaruit wordt cyber erbij betrokken. Ik vind dat ook goed. Ik vind dat het standaard zo moet zijn. Bij een dreiging moet je niet zeggen: deze mensen gebruiken ook internet en daarom moet de cyberhoek het alleen doen. Het moet er wel volledig in zitten.

Mevrouw **Oosenbrug** (PvdA): Ik weet dat ik altijd heel warrig ben, maar ik kwam hier ook niet helemaal uit. Misschien was mijn vraag niet heel duidelijk, maar het gaat erom dat cyberdreiging, bijvoorbeeld een ddos-aanval – ik spel het even uit: distributed denial of service attack – ontstaat als mensen hun systemen niet op orde hebben. Vervolgens zijn er kwetsbaarheden in hun systeem. Dan zie je dat we de hele tijd dat kringetje aan het doorlopen zijn. Je maakt dus het internet zwakker. Daarmee maak je niet alleen bedrijven maar ook burgers kwetsbaarder. Mijn specifieke vraag was: denken we met zijn allen na over de vraag waar we de verantwoordelijkheden neerleggen? Daarop sluit ook het verhaal van collega Verhoeven over die campagne aan. Hoe maken we mensen bewuster? Ik begrijp uit het eerste stukje dat de Staatssecretaris ook nog niet helemaal helder heeft hoe hij een pakkende campagne kan invoeren. Ik begrijp inmiddels wel dat vanuit de overheid Internet.nl is

opgericht en dat je daar in ieder geval je systeem kunt testen. Ik dacht altijd dat ik heel goed beschermd was, maar ook ik bleek niet helemaal goed beveiligd te zijn. Ik vind het ongelofelijk, maar schijnbaar doet mijn provider toch iets niet goed. De kernvraag is: hoe zorgen we er met elkaar voor, dus in de driehoek overheid, bedrijfsleven en particulieren/burgers/consumenten, dat we toch tot een goede bescherming komen? Dan beschermen we het internet en onszelf ook beter.

Staatssecretaris **Dijkhoff**: Dat is helder, maar het betreft alleen niet de vraag die ik net probeerde te beantwoorden. Ik denk dat je hierin een ontwikkeling ziet. In het begin gaat het heel erg om bewustwording. Dat is een blijvend traject, maar daar zet je dan op in. Dan moet de overheid de capaciteit hebben om het zelf op orde te hebben. We zijn als eerste de samenwerking aangegaan met de private partijen die er de grootste rol in spelen. Het gaat hierbij ook om bewustwording bij de individuele gebruiker. Doordat het gebruik van systemen die onderling verbonden zijn, om het maar breed te beschrijven, nog steeds explosief toeneemt, moeten we als overheid op dit punt ook doorgroeien. Het beeld dat ik voor ogen heb, is dat het in ieder geval niet gaat lukken als we als overheid zeggen: wij zorgen voor de veiligheid daarvan. Ook is niet te verwachten dat iedere individuele consument er precies genoeg van weet om het zelf te kunnen doen. Ik wijs op het vorige punt dat mevrouw Oosenbrug noemde. We kunnen helpen door te bekijken of het klopt. Dat doen we nu nog. Daarbij zul je altijd iemand nodig hebben om het voor je te fixen. We denken nu na over de vraag hoe we als overheid een en ander kunnen doen. Het is fijn om te zien dat heel veel mensen op een slimme manier erin duiken, soms met freeware en soms met open source. Ze stellen van beneden af remedies ter beschikking om de kwetsbaarheid te verhelpen. Maar er zijn ook bedrijven die daar een rol in spelen.
Ik kan mij voorstellen dat een ondernemer die zich ervan bewust wordt dat hij niet weet hoe het bij hem zit, zich zal afvragen: wie moet ik bellen om te checken of ik een probleem heb en kan ik diegene vertrouwen? Voor een bedrijf is het natuurlijk een interessant businessmodel als je belt met de vraag of je een probleem hebt en dat bedrijf vervolgens een oplossing biedt. Daar moet je dus ook voorzichtig mee zijn. De vraag is dus wie je kunt vertrouwen. Van onze kant wordt er nu een studie verricht om te bekijken op welke manier wij als overheid het beste onze rol kunnen spelen. Ik hoop de uitkomsten daarvan binnenkort naar de Kamer te sturen. Het is goed als je weet dat de overheid het niet allemaal voor je kan doen en met wie je dan in zee kunt gaan. Het is goed als daar een soort zekerheid in wordt geboden. Ik denk dat we op deze manier vervolgstappen te zetten. Dan weet iedereen op welke manier de boel veilig kan worden gemaakt.
Mevrouw Tellegen vroeg hoe we inzicht krijgen in de digitale capaciteiten, intenties en activiteiten van buitenlandse statelijke actoren. Op dat punt moet ik toch vertrouwen vragen in het werk van de diensten. Mijn collega, Minister Plasterk, die hierover gaat, zou dan moeten zeggen: ik kan niet publiekelijk ingaan op de modus operandi. Hij mag het niet en ik kan het niet omdat ik het niet weet. Voor mij is het dus nog makkelijker om te zeggen dat ik het niet kan. Wij hebben bepaalde kanalen om de Kamer te informeren. Het kabinet heeft natuurlijk wel het idee dat er een wetswijziging nodig is om dat goed te kunnen blijven doen. Over die wetsvoorstellen zal ik niet teveel zeggen, omdat ik daarmee uitlok ze toch hier te behandelen. Die wetsvoorstellen zijn naar de Kamer gestuurd en die zullen we ook uitvoerig bespreken.
Biedt dat wetsvoorstel dan voldoende antwoord op de vraag? Die vraag is ook gesteld. In onze ogen is er een balans gezocht waarbij niet meer wordt gedaan dan nodig is, maar waarbij er ook niet te weinig wordt gedaan. Maar goed, de Kamer zal dat wetsvoorstel uitvoerig behandelen.

Hoe meer ik hier een kwalificatie aan geef, hoe minder ik het eerbiedig. De Kamer heeft net ook gezegd: dat doen we nu even niet.
Ik kom op de vraag over de testen en de doemscenario's. We hebben oefeningen voor cybersecurity en voor de vitale sectoren, waarin worstcasescenario's het spannendst zijn en ook gebruikt worden. Ieder ministerie heeft daar zijn eigen verantwoordelijkheid in. De vraag ging heel specifiek over Rijkswaterstaat. I en M doet ook een en ander op dit gebied. Dat ministerie werkt ook samen met het NCSC om de recente oefeningen vorm te geven en daarna te evalueren wat eruit te leren was.
Mevrouw Tellegen vroeg naar de ambities voor het vervangen van verouderde systemen. Het SCADA-systeem werd daarbij expliciet genoemd. Daarom hebben we net voor kerst ook de NCSC-checklist voor SCADA-systemen weer geüpdatet en spreken wij actief met de beheerders van de vitale infrastructuur om eventuele verouderingen en kwetsbaarheden op te lossen.
Mevrouw Gesthuizen stelde een vraag over de handel in zero-days. Er werd net al gezegd dat je moet voorkomen dat ze worden verhandeld in de foute markt en dat je het moet belonen als ze op de goede manier worden gemeld.

De **voorzitter**: Ik heb daar als VVD-Kamerlid een vraag over. Als u het goed vindt, dan doe ik dat even zonder voorzitterswisseling. Het gaat inderdaad over legacyproblemen en de inventarisatie. Ik hoorde de Staatssecretaris zeggen dat die checklist net voor het einde van het jaar nog is geüpdatet. Mijn vraag ging echter één stap verder. We hebben inderdaad die inventarisatie en we weten waar de kwetsbaarheden zitten, maar wat nu? Welke ambitie ligt er om het een sluitend verhaal te laten worden? Heeft het kabinet de ambitie om te zeggen – ik noem maar wat – dat het er binnen zoveel jaar voor zorgt dat we er niet meer mee te maken hebben, opdat de kwetsbaarheden worden ondervangen? Desnoods kan dat gefaseerd worden gedaan.

Staatssecretaris **Dijkhoff**: Wij wijzen wel op de eigen verantwoordelijkheid van degene die verantwoordelijk is voor het systeem en op de plicht van mensen ervoor te zorgen dat het wordt opgelost. Zo zien wij onze taak.

De **voorzitter**: De Staatssecretaris weet dat eigen verantwoordelijkheid voor de VVD een groot goed is, maar in dit geval gaat het niet alleen om bedrijven maar ook om overheidsinstellingen en instellingen die waken over onze vitale infrastructuur. Ik zou zo graag één stap verder met de Staatssecretaris willen komen. Hoe kunnen we ervoor zorgen dat we niet elke keer achter de feiten aanlopen? Op het moment dat je de boel hebt vervangen, is het vaak alweer nodig om opnieuw een slag te maken. Ik zoek naar een manier om het iets meer handen en voeten te geven.

Staatssecretaris **Dijkhoff**: Een deel zal voortvloeien uit de NIB-richtlijn oftewel de NIS-richtlijn (richtlijn Netwerk- en Informatiebeveiliging) en uit de wet inzake de meldplicht, die we zelf naar voren hebben gebracht. Dan wordt het juridische kader om de zorgplicht en de eindverantwoordelijkheid vorm te geven nog dwingender. Dat zal ertoe bijdragen dat in de praktijk de kwetsbaarheden kunnen worden verholpen.

Mevrouw **Oosenbrug** (PvdA): Misschien is het flauw om er weer over te beginnen, maar ik wijs op het cirkeltje waar je in terechtkomt als je als overheid een kwetsbaarheid misbruikt in een systeem of die kwetsbaarheid zelfs actief inbouwt. Dan maak je het internet ook minder veilig. Aan de ene kant ben je dan bezig om gaten te dichten en aan de andere kant maak je gaten. Ik weet dat we dit punt niet in het AO zullen bespreken, maar ik wil het wel meegeven aan deze Staatssecretaris. Het is

toch een belangrijk punt. Ik snap de balans bij cybersecurity, maar hiermee haal je de veiligheid er toch weer uit.

Staatssecretaris **Dijkhoff**: Volgens mij ging het alleen maar over gaten dichten en anderen erop wijzen dat ze, als ze gaten hebben, die gaten moeten verhelpen. Met de wet inzake de meldplicht, die ik net al heb genoemd, zal er geen nieuw gat worden gecreëerd. Ik voorzie ook niet dat we op een andere manier een nieuw gat creëren.
Er is een vraag gesteld over de zorgplicht van softwareleveranciers. De vraag was waar de verantwoordelijkheid ligt. Er is nu een rechtszaak op dit gebied en het is een beetje lastig om het daarover te hebben, maar in brede zin vind ik het een goede ontwikkeling. Er is gevraagd of het nou gaat om de gebruiker of om de leverancier. Heel het beleid is erop gericht om weg te blijven van zulke tegenstellingen. Ik vind dat de leverancier een verantwoordelijkheid heeft in het niet al te moeilijk maken. Eerst moest je met een kabeltje firmware updaten, maar gelukkig wordt het allemaal steeds makkelijker. Je kunt zaken instellen waarmee het allemaal steeds makkelijker wordt en je zelf niet eens doorhebt dat de boel wordt geüpdatet totdat je opeens een nieuwe feature ontdekt. Aan de andere kant blijven gebruikers zelf de verantwoordelijkheid hebben om een en ander te doen. Ik wil met het beleid voorkomen dat men verantwoordelijkheden op elkaar afschuift. Ik laat mij nu niet uit over rechtszaken en concreta, maar ik denk dat mensen het prettig vinden als het allemaal zo geruisloos mogelijk wordt geregeld en dat dit een standaardbehoefte wordt. Er zijn natuurlijk altijd een paar eigenwijze mensen, die er hopelijk zelf ook van kennis van hebben, die de controle juist helemaal zelf willen behouden. Daarmee nemen zij een grote verantwoordelijkheid op zich. Ontwikkelingen in de markt leiden ertoe dat leveranciers van producten steeds meer de verantwoordelijkheid nemen om vanaf een afstand te updaten. De maatschappelijke ontwikkeling daarin waardeer ik positief.
Ik kom op het encryptiestandpunt. Dat is naar de Kamer gestuurd. De meeste vragen kwamen, samengevat, neer op de vraag of wij wat daarin stond, echt menen. Mijn antwoord is: ja, dat menen we echt. Het is onderwerp van een bredere internationale discussie. Daarom hebben wij er ook zelf goed over gediscussieerd en een standpunt ingenomen. Met het kabinetsstandpunt wordt het belang van sterke encryptie onderstreept. We kennen ook de noodzaak van rechtmatige toegang tot gegevens voor overheden in bepaalde situaties, maar dat betekent niet dat encryptie bij voorbaat wordt verzwakt. We hebben allerlei discussies over dit onderwerp. Ik zal geen namen noemen, maar ik heb een keer een discussie gevoerd met iemand die niet uit Nederland kwam en die zei: encryptie is heel belangrijk en er moet niemand bij kunnen; bedrijven moeten niet kunnen inzien wat er dan wordt besproken, maar er moet wel ergens een sleutel liggen voor de overheid voor het geval die erom vraagt. Het is een beetje lastig om dat tot elkaar te verhouden. Ik ben ook voor sloten en we hebben als overheid niet de sleutel van ieder huis – dat wil ik ook helemaal niet – maar er zijn situaties waarin de deur ingetrapt moet kunnen worden.
In het aangepaste wetsvoorstel computercriminaliteit III is het decryptiebevel eruit gehaald. Anders zou je zeggen: encryptie mag, maar je moet die gegevens toch geven. Dat is iets anders dan dat de overheid in bepaalde gevallen de bevoegdheid moet hebben om te proberen erin te komen. Dat is dus niet hetzelfde als inbouwen dat encryptie bij voorbaat wordt verzwakt. Wij zijn dus voorstander van encryptie. Er zijn geluiden dat er wordt geëist dat er toch een ingang is. Gelukkig vraagt een aantal bedrijven zich af: als ik die sleutel zelf niet heb en ik bied encryptie aan die op zo'n manier tot stand komt dat ik haar ook niet kan overrulen, wordt mij dan verboden zo'n dienst aan te bieden? Je ziet ook dat echte kwaadwillenden hun eigen encryptie- en messengernetwerk kunnen opbouwen. Voor wie ben je het dan aan het inbouwen? Wat is de

verwachting van zo'n achterdeur? Is zo'n achterdeur wel effectief voor het doel waarvoor je hem wilt hebben? Die vragen stel ik ook in internationale discussies, omdat ik het van belang vind dat we een antwoord hebben op die vragen voordat we over dit onderwerp discussiëren. Ik denk niet dat encryptie in het geheel wordt verzwakt als je alsnog de bevoegdheid hebt om in bepaalde gevallen toch te proberen erin te komen. Dat is iets anders dan eisen dat je overal in moet kunnen met een sleutel of een backdoor.

De heer **Verhoeven** (D66): Ik denk dat de Staatssecretaris er heel afgewogen algemene opmerkingen over maakt, die we in de komende maanden zullen verfijnen. Dat zal ik nu dus niet doen. In ieder geval dank ik de Staatssecretaris voor zijn opmerkingen. Hij zei wel tussen neus en lippen dat het decryptiebevel uit het wetsvoorstel computercriminaliteit III is gehaald. In 2013/2014 was het decryptiebevel een duidelijk onderdeel van het voorstel. Mag ik optimistisch concluderen dat het kabinetsdenken nog steeds in beweging is en dat er dus nog steeds mogelijkheden zijn om het wetsvoorstel op een aantal punten te veranderen binnen de kaders van de samenvatting die de Staatssecretaris net gaf? Mag ik in ieder geval de hoop hebben dat de hele discussie over encryptie en de verstrekkendheid ervan, nog een open discussie is, ook voor het kabinet?

Staatssecretaris **Dijkhoff**: Over encryptie hebben we net een standpunt ingenomen. Je kunt er natuurlijk altijd opnieuw over discussiëren, maar het standpunt over encryptie is nou net het einde van de open discussie die het kabinet reeds heeft gevoerd. Ieder wetsvoorstel wordt besproken, maar we dachten niet: schrijf maar iets op. We dachten ook niet: dit is eigenlijk niks, maar misschien komen er wel veel betere ideeën. De wijzigingen in het voorstel zitten er niet voor niks in. Ik heb zelf ook het beeld dat dit een goed voorstel is en dat het in balans is, maar in de discussie staan we open voor het feit dat er andere invullingen zijn. Er zijn niet alleen verschillen in opvatting tussen Kamer en kabinet maar ook tussen Kamerleden onderling. Het kan geamendeerd worden op zo'n manier dat het een breed draagvlak heeft. Ik ga altijd open een discussie in, maar ik wil niet net doen alsof ik zelf niet heel erg geloof in het voorstel en de aangepaste versie ervan.

De heer **Verhoeven** (D66): Helder. Ik zal een iets concretere vraag stellen. Ziet de Staatssecretaris spanning tussen het standpunt over encryptie dat in de brief is verwoord – dat standpunt juicht D66 zeer toe – en datgene wat staat in het wetsvoorstel computercriminaliteit III? Ik zie namelijk spanning tussen het wetsvoorstel en het kabinetsstandpunt. Ik denk dat dit uiteindelijk kan leiden tot een bijstelling van het kabinetsstandpunt in de praktijk en dat er dan toch op basis van het wetsvoorstel een bepaalde vorm van kwetsbaarheden en dus ondermijning van encryptie wordt toegestaan. Ziet de Staatssecretaris dat spanningsveld ook?

Staatssecretaris **Dijkhoff**: Het wordt een beetje platitude. Ik zie in het algemeen een spanningsveld. Het liefste zou je willen dat dit soort bevoegdheden helemaal niet nodig waren en daarom wordt het ook heel erg ingekleed. Er zijn uitzonderlijke omstandigheden waarin je die bevoegdheden mag gebruiken, bijvoorbeeld als iemand er al aanleiding toe heeft gegeven door de wet vermoedelijk flink te overtreden. Ik zie niet per se een spanningsveld wat betreft het encryptiestandpunt. Daarbij haal ik de metafoor met de sloten weer aan. Het is niet zo dat je daarmee het encryptiestandpunt onderuithaalt. Dit onderwerp past in een bredere discussie, waarbij ook vrij radicale standpunten aan de orde komen als het verbieden van encryptie, het eisen van altijd toegang, waarmee je dus vormen van encryptie verbiedt waarbij niemand anders dan de gebruiker het kan ontsleutelen, en de bevoegdheid om een systeem in te kunnen om eventueel zaken te volgen of te achterhalen. Daarbij gaat het om de vraag

of je in het systeem aan de encryptie zelf beperkingen stelt of dat je, zoals nu het geval is in de reguliere opsporing, in uitzonderlijke gevallen de bevoegdheid toekent om na een stevige verdenking en een toets heel gericht bepaalde handelingen te verrichten die in het normale verkeer niet zijn toegestaan.
Mevrouw Gesthuizen had een vraag over het doorontwikkelen van «advisories». Dat is weer een Engels woord. Het NCSC neemt de aanbevelingen over. Dat is ook de basis voor het project dat is gestart, Advisory 2.0, waarbij de meerwaarde van de adviezen die worden verstrekt verhoogd zal worden. Dat heeft ook te maken met de input van partners. Zij zeggen dat er minder behoefte is aan algemene adviezen. Het aantal nieuw uit te brengen veiligheidsadviezen zullen we ook verminderen. Uit de feedback bleek dat men het overzicht kwijtraakte. Nu koppelen we de updates aan bijbehorende bestaande adviezen. Die houden we up-to-date, maar die zullen we niet steeds opnieuw presenteren. Het is dan aan de partners die hierin betrokken zijn om op dagelijkse basis een en ander te doen als er iets te melden is. Het is de bedoeling om sneller iets te doen op het punt van ontwikkeling en om niet steeds algemene zaken te herhalen. Het idee is om niet alleen het aantal te verminderen maar om ook de inhoud van de adviezen die we nog geven, te verbeteren en om beter aan te sluiten bij de behoeften. Het komt dus vooral voort uit de wisselwerking met de afnemers van de adviezen. Samen bekijken we hoe we elkaar het beste kunnen helpen.
Mevrouw Gesthuizen vroeg naar de gevolgen van de bezuinigingen op ICT. Die raken op zich niet het wetsvoorstel computercriminaliteit III. Het is wel een meer algemeen pleidooi van de landelijke recherche dat betere voorzieningen leiden tot betere capaciteit in de opsporing. De politie kan haar werk doen, maar het kan beter, is de kreet. Met het meerjarenportfolio wordt erop toegezien dat er investeringen in gedaan worden. Ik zie het bedrag dus oplopen.
Ik kom op de huidige mogelijkheden voor het «binnentreden» in computers. Nu kun je wel een computer in als je fysiek erbij bent. Als je legaal in een huis bent en daar een computer staat waar je in kunt, dan kun je daar ook in kijken. Vandaaruit zijn er mogelijkheden om ook breder, in het netwerk waar je computer in hangt, te zoeken, maar het is niet zo dat je er nu op afstand in kunt. Daarom hebben we het wetsvoorstel naar de Kamer gestuurd.
Ik kom op het rapport ... Ik kijk even wat precies de titel is. Wellicht is het makkelijker om dat van tevoren op te zoeken. Het is vandaag wel afkortingendag. Ik zie «Genval» staan. Ik hoor zojuist dat dit geen afkorting is. Is het een plaatsnaam? Ik krijg net het antwoord dat Genval een raadswerkgroep is. Is «Genval» dan echt geen afkorting? De ambtenaar naast mij zegt dat het toch een afkorting is. Hij zegt iets in het Frans. Ik heb al Nederlands en Engels door elkaar gehutseld. Het betreft een heel eminente werkgroep. Die mensen zijn zo belangrijk dat niemand weet hoe de werkgroep heet. Die werkgroep heeft een rapport gestuurd. Nederland moet eind 2016 rapporteren over de uitvoering van de aanbevelingen. Er staan zeven aanbevelingen in het rapport. Een deel van de aanbevelingen betreft zaken die we al doen. Dat zullen we dan ook laten merken. Het gaat over aanbevelingen als het verbeteren van statistieken, het overwegen van een meldplicht voor private partijen, het opbouwen van expertise op regionaal niveau bij de politie en het verhelderen van de omschrijving van cybercrime voor statistische doeleinden. Daar zijn we nu dus al mee bezig. Er zijn ook aanbevelingen gedaan over het versterken van de weerbaarheid van burgers, overheidscommunicatie aan burgers, het verbeteren van opleidingen voor medewerkers in de strafrechtketen en het in die opleidingen versterken van de aandacht voor de Europese instellingen. Het is immers een Europees advies. We kunnen in zijn algemeenheid zeggen dat het goede aanbevelingen zijn. Nu wordt er dus bekeken hoe we die concreet kunnen omzetten in specifieke maatregelen.

We zullen de Kamer op de hoogte stellen als we reageren op de punten van deze mooi genaamde werkgroep.
Mevrouw Gesthuizen heeft ook een vraag gesteld over de bezuinigingen bij het OM. Die bezuinigingen hebben geen weerslag op de bijdrage aan het realiseren van de vastgestelde cybercrimedoelen. Het is dus niet waar dat we de doelen moeten bijstellen. Dat is de meest directe link. Ook mevrouw Oosenbrug vroeg of we dan stoppen met de 360 zaken. Nee, de ambitie is om het aantal zaken te laten doorgroeien. In 2015 waren er 175 zaken. We willen het stimuleren. Daarbij hebben we bepaalde targets voor ogen. We willen dat het in 2018 minimaal 360 zaken zijn, maar als er 361 zaken zijn, is het niet zo dat zaak 361 niet doorgaat. In de periode tot 2018 wordt ook in de regio's kennis, expertise en capaciteit opgebouwd om het steeds meer onderdeel te maken van het standaardwerk. Dat werk wordt dan niet alleen gedaan door de zeer goede maar aparte club die we daarvoor hebben.
Dan kom ik bij het blok onderwijs. Gevraagd is wat er is gedaan met de aanbevelingen. Het is een advies aan mij en mijn collega, de Staatssecretaris van OCW. We werken daarbij samen. Ik kan van alles willen, maar uiteindelijk worden er ook bij OCW besluiten genomen. Bij OCW wordt bepaald of het ook echt gebeurt; daar wordt de inhoudelijke invulling van het onderwijs mede bepaald. Ik onderschrijf de aanbevelingen wel. Ik ben met mijn collega bezig om daar invulling aan te geven. Dat proberen we zo veel mogelijk in te passen in de programma's die reeds lopen. Dan gaat het om de kennis van cybersecurity en het aantal mensen dat op dat gebied goed is opgeleid. We willen stimuleren dat de onderwijsinstellingen en de arbeidsmarkt onderling afstemming zoeken. Er komt een reactie aan van mijn collega van OCW op het advies Klaar voor de Toekomst. Het gaat over toekomstgericht onderwijs, waarbij ook cybersecurity aan de orde komt. De Kamer zal van de Staatssecretaris van OCW meer in detail horen hoe dit wordt opgepakt. Ik zal hem de vragen die zojuist zijn gesteld over het specifieke niveau van het onderwijs meegeven, opdat hij die in zijn reactie kan meenemen. Dat geldt dus ook voor de vraag over zijinstroom en de activiteiten, los van de activiteiten die we nu al hebben.
Mevrouw Oosenbrug zei het treffend: er zijn mensen met heel veel talenten die niet tot bloei zijn gekomen binnen het bestaande onderwijssysteem. Wij hebben daar ook vanuit het NCSC oog voor en werken constructief samen met veel van die jongens. Het zijn immers meestal jongens. We betrekken hen ook bij de NCSC One Conference. We hebben voor hen ook stagemogelijkheden. We willen dit punt ook onder de aandacht brengen bij het CyberSecurity Research and Education Platform. We willen vraag en aanbod bij elkaar brengen. Ik zal het ook bij mijn collega van Onderwijs onder de aandacht brengen.
Hetzelfde geldt voor codering en veiligheid als standaardonderdeel van het gerelateerde onderwijsprogramma. Dat onderdeel zit ook in het platform.
Dan kom ik op de vraag over de koppeling van databestanden. Er zitten onvergelijkbare grootheden tussen. Het is geen automatisme dat het een kopie is. Soms is er een koppeling waarbij er geen toegang is tot alle gegevens in het andere bestand. Soms wordt er informatie gedeeld zonder dat de andere partij inzicht krijgt in persoonsgegevens. Het kan bijvoorbeeld ook gaan om statistische informatie. De vraag was of ik een totaaloverzicht kan geven. Maar dan zit er wel van alles tussen en kun je niet zeggen dat iedere keer als er een koppeling is, ook iemand anders aan wie je je gegevens hebt gegeven, alles kan inzien.

Mevrouw **Gesthuizen** (SP): De Staatssecretaris zegt hiermee eigenlijk dat de regering de Kamer nog wat beter en nauwgezetter moet informeren. Op deze manier kunnen we er namelijk geen chocola van maken.

Staatssecretaris **Dijkhoff**: Iedere keer als een koppeling tot stand komt, wordt zij besproken bij de specifieke behandeling van de desbetreffende wet. Uiteindelijk kun je dan vragen om een totaaloverzicht. We hebben een kwantitatief overzicht dat voortvloeit uit jarenlang werk. Het zijn geen stiekeme dingen. Dan moet ik op zoek naar een antwoord op de vraag wat we precies willen bereiken en weten. Als ik een overzicht had aangeboden met een lager aantal, dan had er iets niet op gestaan en had ik gezegd dat er geen materiële koppeling is. Ik kan ze niet per stuk uitsplitsen.

Mevrouw **Gesthuizen** (SP): Ik schrik niet direct van het aantal koppelingen, maar ik wil wel graag weten wat het oplevert.

Staatssecretaris **Dijkhoff**: Dan probeer ik even te definiëren in hoeverre het cybersecurity betreft. Wat het oplevert, is vaak iets materieels wat niks te maken heeft met cyber. Als er een koppeling is tussen bestanden om fraude te voorkomen of om een verklaring om het gedrag af te kunnen geven of om een integriteitstoets af te nemen bij een nieuwe ondernemer en er wordt in verschillende bestanden gekeken, dan levert dat heel veel op. Ik denk echter niet dat het aan mij is om iedere keer dat de overheid een bestand koppelt of in twee bestanden tegelijk kijkt, de materiële meerwaarde daarvan op te sommen. Dat lijkt mij een herculische taak, die ook niet per se aan cybersecurity is gerelateerd.

Mevrouw **Gesthuizen** (SP): Voorzitter ...

De **voorzitter**: Is dit het derde deel van één interruptie, mevrouw Gesthuizen?

Mevrouw **Gesthuizen** (SP): Ja, ik houd het kort. Ik ben er wel een beetje verbaasd over dat de Staatssecretaris zegt dat hij niet zo goed inziet dat het iets met cybersecurity te maken heeft. Volgens mij heeft het heel veel met cybersecurity te maken. Het gaat namelijk onder andere over de risico's van informatie. Het zou prima zijn als het niet altijd gepaard gaat met persoonsgegevens, waardoor er een bepaalde protectie is, maar er zijn zeker risico's op het moment dat informatie op meerdere plekken wordt gedeeld en kan worden ingezien. Dat hangt natuurlijk ook nauw samen met privacyvraagstukken.

Staatssecretaris **Dijkhoff**: Ik heb de vraag wat het oplevert, op een andere manier opgevat. Ik dacht dat het ging over de waarde van de koppeling voor de overheid en over de vraag wat het in die zin oplevert. Het hangt zeker samen met privacyvraagstukken, maar daar ga ik niet over. Vanuit het oogpunt van cybersecurity is het aantal koppelingen niet indicatief als het gaat om de vraag of het daarmee veiliger of onveiliger wordt. Dat hangt natuurlijk ook af van de vraag of een systeem een extra zwak punt kent als er een externe toegang is gecreëerd en hoe het precies wordt vormgegeven. We kunnen het overzicht dat we bieden, wel actualiseren, maar volgens mij vraagt mevrouw Gesthuizen om een materiële verandering van wat we nu hebben aangeleverd. Ik zie niet een-twee-drie wat ik vanuit mijn verantwoordelijkheid op het gebied van cybersecurity zou moeten aanpassen aan het overzicht dat we hebben geboden, om het ook nuttig te laten zijn voor onze discussies hier.

De heer **Verhoeven** (D66): Heeft de Staatssecretaris weleens een koppeling of vermenigvuldiging van een bestand tegengehouden? Heeft hij weleens gezegd: deze doen we niet, want ze heeft geen meerwaarde maar levert wel bredere toegang tot allerlei informatie op? Heeft de Staatssecretaris of iemand anders bij het ministerie één keer gezegd: dit moeten we niet koppelen?

Staatssecretaris **Dijkhoff**: Die vraag kan ik onmogelijk beantwoorden, want er is geen algemeen koppelingsoverleg. Hoe gaat het in zo'n traject? Het is niet de intentie om bestanden te koppelen. Het heeft natuurlijk altijd een ander doel. Het is niet zo dat twee Ministers denken: laten we bij dit wetsvoorstel eens even lekker koppelen. Er is sprake van een materieel doel. Ik weet niet of er op ambtelijk niveau weleens iets dergelijks heeft plaatsgevonden. Het probleem is nooit dat er bestanden zijn ontkoppeld. Het probleem is vaak een materieel probleem, bijvoorbeeld fraude. Ook als we mensen een verklaring omtrent het gedrag willen geven, dan hebben we daar dingen voor nodig. Er zal best een keer een scenario zijn geweest waarbij is voorgesteld om het allemaal fijn te koppelen en waarbij is gezegd: als we die persoon toegang geven tot van alles, dan werkt het. Toen is er misschien op ambtelijk niveau gezegd: dat lijkt me nogal ver gaan, kan het niet op een andere manier? Dit soort trajecten zijn organische processen. Het is niet zo dat ik één keer in de zoveel tijd een lijst krijg met plannen van collega's om te koppelen en dat ik daar dan los een oordeel over geef. Laatst heb ik bij de verklaring omtrent het gedrag één scenario afgekeurd waarbij ook bepaalde andere typen informatie gekoppeld zouden worden. Het had allerlei redenen, maar ik noem er even één. Ik vind het moeilijk om die vraag te beantwoorden.

De heer **Verhoeven** (D66): Ondanks het feit dat er geen koppelingsoverleg is, heeft de Staatssecretaris zich weleens bemoeid met een voorstel uit een ambtelijke organisatie om dingen te koppelen. Dat doet mij goed. Het antwoord van de Staatssecretaris is op zich leuk, maar het ademt ook wel het automatisme waarmee er op ambtelijk niveau kan worden gezegd: laten we deze twee bestanden ook maar eens uitwisselen; laten we deze ook maar aan elkaar koppelen en laten we deze twee diensten ook maar de mogelijkheid geven om de verzamelde gegevens in te zien. Daarin zit toch een groot reëel gevaar, namelijk dat het onder de radar een steeds grotere boom van totaal aan elkaar gekoppelde bestanden wordt waarbij we zelf ook niet meer weten waarom we die bestanden koppelen.
Ik zal in dit AO niet voorstellen om een algemeen koppelingsoverleg in te stellen. De Staatssecretaris heeft het overzicht op verzoek van de Kamer overigens heel goed gemaakt. Ik zou het wel goed vinden om te bekijken of de uiteindelijke verantwoordelijke personen van ministeries, dus het kabinet, ervoor kunnen zorgen dat aan de ambtelijke organisatie, die het waarschijnlijk op een praktische manier doet, wordt gevraagd: moeten we dit nu altijd wel doen? De Engelse term daarvoor is «privacy by design». Daar hebben we het altijd allemaal over, maar op het moment dat we privacy by design in de praktijk zouden brengen, komen we toch op dit soort concrete keuzes uit: soms wel, maar soms niet. Daarom vroeg ik het op deze manier. Ik snap heus wel dat de Staatssecretaris zegt dat hij niet elke dag allerlei koppelingen langsgaat, maar wat doet hij concreet? Zegt hij soms een keer: nee, dit is niet nodig, het heeft geen meerwaarde, maar levert wel veel meer toegang tot informatie op?

Staatssecretaris **Dijkhoff**: Nu wordt er ook een vraag gesteld vanuit de privacyhoek. Dat terrein valt onder de Minister. Als bestanden worden gekoppeld, vereist dat wel een wettelijke grondslag. Het herken niet het beeld dat de heer Verhoeven schetst, waarbij ambtenaren zeggen: wat jij hebt is handig en dat wil ik ook wel; laten we het eens koppelen. Dat geldt in ieder geval niet op beleidsambtelijk niveau, maar op de werkvloer is die behoefte natuurlijk wel heel groot. We kiezen er vaak voor om in plaats van het koppelen van bestanden overleggen te creëren. Dat klinkt misschien niet heel spannend, maar in de overleggen kun je mensen van verschillende diensten naast elkaar zetten om snel een casus te bespreken. Natuurlijk hoor je dan ook mensen zeggen: als ik er toegang tot heb, dan kan ik het ook zelf. Vaak kiezen we ervoor om niet de

koppeling te leggen maar om het op een andere manier op te lossen en daarna met de Kamer in discussie te gaan over de vraag of er wel tot koppeling moet worden overgegaan. We zien dat er ook in de strafrechtketen, bij de politie, het OM en de rechterlijke macht, behoefte is aan een vloeiende overgang in elkaars bestanden. Dat zou praktischer zijn. Die zaken bespreken we echter in het parlement, waarbij we in het design van zo'n nieuwe regeling ook de privacyaspecten kunnen aangeven. Op een gegeven moment creëer je wel een overzicht. Dat is de optelsom van koppelingen die in al die jaren geleidelijk aan zijn ontstaan en die steeds met de Kamer zijn besproken. Dan heb je dus een overzicht. Zo zie ik datgene wat we nu hebben aangeleverd.

De **voorzitter**: De Staatssecretaris is aan het einde gekomen van zijn eerste termijn. Ik kijk even naar de Kamerleden. Is er behoefte aan een tweede termijn? Ik constateer dat er behoefte is aan een korte tweede termijn, met twee minuten spreektijd per spreker.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Ik dank de Staatssecretaris voor de heldere beantwoording. Ik heb niet voor niets een heel groot stuk van mijn inbreng gehouden over autistische jongeren. Ik heb vorig jaar een jongen onder mijn hoede genomen die op een vmbo zat waar hij helemaal kopje onder ging. Hij functioneerde ver beneden zijn niveau, maar hij ontdekte wel allerlei lekken. Ik heb geprobeerd hem aan onze kant te houden. Dat is mij ook gelukt. Hij is inmiddels 16 jaar en heeft een vaste baan bij een beveiligingsbedrijf. Deze jongen is niet de enige. Door hem heb ik heel veel van dit soort jongens leren kennen. Ik denk dat het juist in dit overleg over cybersecurity, over internetveiligheid, belangrijk is om te zeggen dat we oog moeten hebben voor deze jongeren. Het is mij gelukt om deze jongen aan de white side van de hackers te houden, maar als hij niet de juiste begeleiding en aandacht had gekregen, was hij makkelijk doorgeslagen naar de dark side. Ook als overheid hebben we op dit gebied een flinke taak liggen. Ik hoorde de Staatssecretaris zeggen dat hij het met zijn collega zal bespreken en dat hij een en ander zal doorgeven, maar ik wil toch de urgentie ervan meegeven, juist omdat ik het aan den lijve ondervind.
Ik heb mijn tweede termijn dus volledig besteed aan deze jongeren. Ik vind het een heel belangrijk onderwerp, aangezien het een groot onderdeel is van onze internetveiligheid.

De heer **Verhoeven** (D66): Voorzitter. Ik dank de Staatssecretaris voor zijn beantwoording. Ik heb nog een paar vragen. De eerste gaat over België. België heeft het initiatief genomen tot een onderzoek naar het decriminaliseren van bepaalde manieren van hacken. Is de Staatssecretaris bereid om contact op te nemen met zijn Belgische collega over het onderzoek en te bekijken in hoeverre we daar in Nederland wat mee kunnen? Die vraag is ook in lijn met wat we daar tijdens dit AO over hebben gezegd. De intentie die de Staatssecretaris uitsprak, is in lijn met hoe D66, mevrouw Oosenbrug van de PvdA en misschien ook mevrouw Gesthuizen van de SP de omgang van de overheid met hackers graag zouden zien.
De discussie over encryptie hebben we uitgebreid gevoerd. Die zal worden vervolgd. Het is een technische discussie, maar eigenlijk is het dat niet alleen. Zoals de Staatssecretaris zelf ook doet, kun je het altijd terugbrengen tot een beeld dat redelijk in de buurt komt, waarbij het gaat om het wel of niet toegang hebben tot informatie van mensen en de vraag wanneer dat wel of niet moet kunnen. Dat is iets anders dan een deur intrappen, maar ik snap de manier van denken daarbij. Daar komen we nog uitgebreid over te spreken. Ik ben wel blij met het feit dat de Staatssecretaris zegt: ik denk dat het kabinetsstandpunt overeind moet blijven, ondanks het wetsvoorstel computercriminaliteit III.

Tot slot kom ik op de campagne. Ik heb zelf ook weleens een campagneslogan bedacht. Eigenlijk heb ik vier keer dezelfde campagneslogan bedacht, namelijk: Nu vooruit. Die slogan sloeg enorm aan. Ik begrijp dat de Staatssecretaris zegt dat hij er prioriteit aan geeft. Hij heeft gezegd: we zouden graag zo'n campagne hebben, maar het gaat daarbij meer om het creatieve en niet zozeer om de vraag of we niet geloven in zo'n campagne. Eigenlijk zegt de Staatssecretaris dat hij graag een goede campagne wil, maar dat er een manier moet worden gevonden om die breed aan de man te brengen. Dat lijkt mij een positieve inzet.

Mevrouw **Gesthuizen** (SP): Ik begin met de uitspraak van oud-minister Opstelten. Hij heeft verteld dat er een wettelijke basis is voor het heimelijk en op afstand inbreken in computers. Mag ik daar van de Staatssecretaris een korte reactie op?
In eerste termijn had ik heel duidelijk gevraagd of het kabinet met zijn standpunt over encryptie ook een duidelijk voorstander is van sterke encryptie en of het tegen achterdeurtjes is. Dat heb ik de Staatssecretaris niet zo horen zeggen, maar ik wil het wel graag weten. Daarmee sluit ik ook aan bij het interruptiedebatje van daarstraks tussen de heer Verhoeven en de Staatssecretaris. Ik vind dat het hierbij gaat om een belangrijk verschil van standpunt. De vraag is vanuit welk standpunt je redeneert, ook gelet op het wetsvoorstel computercriminaliteit III, oftewel de hackwet.
De Staatssecretaris ging heel summier in op de kwetsbaarheden in software en zero-days. Begrijp ik het goed dat de Staatssecretaris zegt dat de Nederlandse overheid niet deelneemt aan de handel in zero-days?

Voorzitter: Oosenbrug

Mevrouw **Tellegen** (VVD): Voorzitter. Ik houd het heel kort. Mijn belangrijkste punten hadden te maken met cyberspionage en het vraagstuk rondom de verouderde systemen. Ik wil nog kort iets zeggen over het encryptiestandpunt. Daar komen we inderdaad nog uitgebreid over te spreken. Ik heb begrepen dat de Staatssecretaris zegt dat het geen of/of-vraagstuk is. Gelet op de manier waarop we de materie aanvliegen, gaat het nu wel om of/of, maar ik voorzie dat er een mogelijkheid is om een en-enformule te creëren. Daar komen we nog op terug.
Ik kom op de reactie van de Staatssecretaris op de vraag wat het kabinet doet in antwoord op de toenemende cyberspionage in Nederland en bij Nederlandse instellingen in het buitenland. Ik ben ook woordvoerder veiligheidsdiensten en weet dat we daar helaas heel weinig over kunnen zeggen. Misschien wordt er op dit moment ergens anders in het gebouw een formule verzonnen waarbij de Kamer duidelijker inzicht krijgt in dit soort zaken. Het blijft echter frustrerend om aan de ene kant in het cybersecuritybeeld te lezen dat de cyberspionage toeneemt en dat we aan de andere kant niet genoeg weten als het gaat om de vraag wat we kunnen doen om cyberspionage tegen te gaan. Wat dat betreft is er een spanningsveld, maar misschien komt het antwoord «as we speak» uit een ander deel van dit gebouw.
Op het punt van legacy ben ik nog niet helemaal tevreden. Het gaat immers ook om Windows en achterstallige systemen. Het ziet niet alleen toe op de bedrijven, maar juist ook op overheidsinstellingen die waken over de vitale infrastructuur in dit land. Mag ik de Staatssecretaris vragen om daar wat meer aandacht aan te besteden in aanloop naar het volgende cybersecuritybeeld? Dat wordt ongetwijfeld op dit moment al geschreven, want het vorige cybersecuritybeeld dateert alweer van een halfjaar geleden. Dan gaat het om de vraag hoe we op dit punt een slag gaan maken. Ik vraag dus niet alleen om een inventarisatie. Hoe gaan we ervoor zorgen dat we de verouderde systemen op zo'n manier uitfaseren dat het werkt?

Voorzitter: Tellegen

De **voorzitter**: De Staatssecretaris vraagt om een schorsing van een paar minuten.

De vergadering wordt van 11.55 uur tot 12.00 uur geschorst.

Staatssecretaris **Dijkhoff**: Voorzitter. Mevrouw Oosenbrug benadrukte terecht het punt van de autistische jongeren. Het NCSC komt vaak met hen in contact, bijvoorbeeld omdat ze iets melden. Wij proberen hen dan actief bij het NCSC te houden. Ik noemde al eerder de stages die er weleens plaatsvinden. Wij onderschrijven het belang en hebben daar zeker oog voor.
De heer Verhoeven had het over België. De term «decriminalisering» wekt inderdaad een bepaalde indruk. Staatssecretaris Tommelein was op bezoek en we hebben dit besproken. Daarna heeft hij in de Belgische pers gezegd dat hij de responsible disclosure van Nederland heel goed vond. Hij zei vervolgens: dat gaan we ook doen. Ik moet dan wel even kijken of hij al iets meer aan het doen is. Naar onze informatie wordt onze inspiratie daar omgezet in regelgeving. Verder dan dat gaat het niet. Staatssecretaris Tommelein gaat nog kijken hoe hij een en ander gaat doen. Hij heeft al een keer gezegd dat hij in zijn conclusie het Nederlandse model kan betrekken. Als er een andere conclusie uitkomt, zullen we die ook bekijken.
Ik kom op de vraag over de zero-days. Het NCSC koopt ze niet. Rijksbreed zijn er ook takken van sport waar ik geen inzicht in heb. Die vraag zou dus moeten worden gesteld aan de betreffende verantwoordelijke bewindspersonen. Ik kan het antwoord geven dat ik weet. Breder dan dat weet ik het niet.

Mevrouw **Gesthuizen** (SP): We praten nu met de verantwoordelijke bewindspersoon. Ik kan een set vragen indienen die aan alle bewindspersonen is gericht, maar ik vind eigenlijk dat ik mijn vraag hier wel beantwoord moet kunnen krijgen.

Staatssecretaris **Dijkhoff**: Ik ben maar een eenvoudige Staatssecretaris van Veiligheid en Justitie. Ik ga over cybersecurity, maar er zijn dingen waar ik niet over ga en waar ik ook niets over weet. Meestal betreft het de Minister van Binnenlandse Zaken als je zo'n vaag antwoord krijgt.

Mevrouw **Gesthuizen** (SP): Ik vind dat de Staatssecretaris er wel over gaat. Als iets hardcore cybersecurity is, dan is dit het wel.

Staatssecretaris **Dijkhoff**: Ik ben er ook voor dat we een lek zo snel mogelijk dichten. Mevrouw Gesthuizen vraagt mij echter niet of ik zero-days slecht vind en of ik ook vind dat de lekken gedicht moeten worden en dat we geen gebruik van zero-days moeten maken. In de cybersecurityhoek, bij het NCSC, worden ze niet gekocht. Ik weet niet wat bepaalde andere overheidsdiensten doen. Daar heb ik natuurlijk ook geen inzicht in. Ik ben geen fractievoorzitter. Bij mijn weten koopt de overheid ze niet. Dat vind ik echter een slap antwoord als ik nu al weet dat ik dingen niet weet. Daarmee wil ik overigens niet zeggen dat het wel gebeurt. Ik vind het wel zo eerlijk om te melden dat er ook zaken zijn die ik niet weet. Dan moet mevrouw Gesthuizen de geëigende kanalen bevragen via de betreffende bewindspersoon.

Mevrouw **Gesthuizen** (SP): Mag ik de gezaghebbende Staatssecretaris vragen wat hij ervan zou vinden als het kabinet wel handelt in zero-days?

De **voorzitter**: De Staatssecretaris heeft een poging gedaan om antwoord te geven op uw vraag. Het woord is nu aan de heer Verhoeven. Hij heeft, denk ik, een vraag over hetzelfde punt.

Mevrouw **Gesthuizen** (SP): Dit begrijp ik niet zo goed, want we hebben nog een uur.

De **voorzitter**: Ik wil het aantal interrupties beperken. U hebt nu in één interruptie vier keer dezelfde vraag gesteld.

Mevrouw **Gesthuizen** (SP): Nee, dit was de derde keer.

De **voorzitter**: Ik geef eerst het woord aan de heer Verhoeven. Als u nog een aanvullende vraag hebt, mevrouw Gesthuizen, kunt u die straks stellen.

De heer **Verhoeven** (D66): Ik wil sowieso een VAO aanvragen. Dat doe ik bij dezen.
Op dit punt ben ik het met mevrouw Gesthuizen eens. Het betreft een internationale discussie over het wel of niet gebruiken van zero-days om offensief andere landen aan te vallen en informatie op te halen. Is het kabinet bereid om op korte termijn een standpunt over het gebruik van zero-days in een brief te formuleren? Dan hebben we niet alleen het antwoord van de Staatssecretaris in dit AO. Dan kan het kabinet zijn eigen standpunt hierover formuleren, net zoals is gebeurd bij het onderwerp encryptie. Hoe gaat Nederland om met de handel in zero-days, in kwetsbaarheden die nog niet bekend zijn? Zegt de Nederlandse overheid: die willen we bekendmaken zodat de lekken gedicht kunnen worden? Of wil de Nederlandse overheid ze stiekem gebruiken om andere landen informatie te ontfutselen? Ik zou het heel goed vinden als de Staatssecretaris de Kamer op dit punt een toezegging doet.

Staatssecretaris **Dijkhoff**: Laat ik in ieder geval toezeggen dat we een brief zullen sturen naar aanleiding van de vraag. Die kan een standpunt bevatten. Ik zeg in ieder geval een brief toe naar aanleiding van de vraag van de heer Verhoeven op dit punt.

De heer **Verhoeven** (D66): Daar ben ik heel blij om. In het VAO gaat het mij om een ander punt, maar ik zou het fijn vinden om die brief te krijgen. Het is immers een heel belangrijk onderwerp. Ik dank de Staatssecretaris dat hij het bij het hele kabinet wil neerleggen, met al die verschillende diensten die misschien wel of niet allemaal dingen doen waar we geen weet van hebben. Zo kan de Tweede Kamer daar controle op uitoefenen.

De **voorzitter**: Ik vraag de Staatssecretaris om verder te gaan met zijn beantwoording.

Staatssecretaris **Dijkhoff**: Mevrouw Gesthuizen zei dat voormalig Minister Opstelten een en ander gezegd zou hebben. Ik heb de letterlijke tekst niet. Ik kan mij voorstellen dat er bij bepaalde zaken wel wordt gezocht in een andere computer in een netwerk, bijvoorbeeld via een computer die in beslag is genomen. Dat heb ik in abstracte zin eerder beschreven. Dan is die mogelijkheid er wel. Zoiets is weleens voorgevallen in een niet onbekende kinderpornozaak, maar dan heb je het dus over een netwerkzoeking die is voortgezet vanuit een ander in beslag genomen systeem. Ik zou echter precies moeten weten wat er is gezegd voordat ik op dit punt meer opheldering kan geven.

Mevrouw **Gesthuizen** (SP): Ik heb alle begrip voor het feit dat de Staatssecretaris de Minister heeft vervangen op dit punt, maar er zijn toch

ook ambtenaren binnen Veiligheid en Justitie die dit zouden kunnen weten? Ik vind het heel vreemd dat die vraag nu niet kan worden beantwoord. De Minister heeft letterlijk tijdens een algemeen overleg gezegd dat hij meent dat er grond voor is.

Staatssecretaris **Dijkhoff**: Binnen de context die ik net schetste, is die grond er in ieder geval. Ik heb verder niet het verslag van het AO voor me. Via de in beslag genomen computer heb je een voortgezette netwerkzoeking en dan ga je op afstand in een ander bestand.
Mevrouw Tellegen had een vraag over legacy en het Cybersecuritybeeld Nederland (CSBN). Ik zal dit punt meenemen in de beleidsreactie op het nieuwe cybersecuritybeeld. Dat beeld gaat vooral over de dreigingen, maar dit kan het effect van een dreiging kansrijker of minder kansrijk maken.

De **voorzitter**: Daarmee zijn we aan het einde gekomen van de tweede termijn.
De heer Verhoeven heeft een VAO aangevraagd. Bij dat VAO is hij de eerste spreker.
Er is zojuist een brief toegezegd naar aanleiding van vragen van mevrouw Gesthuizen en de heer Verhoeven over de handel in zero-days. Daarin zal het standpunt van het kabinet worden opgenomen.
Tot slot kom ik op de toezegging die de Staatssecretaris heeft gedaan inzake legacy en verouderde systemen. Een en ander wordt meegenomen in het kabinetsstandpunt bij het volgende cybersecuritybeeld. Heb ik dan nog zaken gemist?

Mevrouw **Gesthuizen** (SP): Mag ik nog één zaak overhandigen aan de Staatssecretaris? Het betreft een bericht waarin staat dat oud-minister Opstelten erkent dat de politie op afstand een computersysteem mag betreden en gegevens in beslag mag nemen. Ik wil dat meegeven aan de Staatssecretaris.

De **voorzitter**: Dat geven wij de Staatssecretaris mee.
Daarmee is er een einde gekomen aan dit algemeen overleg. Ik dank de Staatssecretaris, zijn ambtenaren en de mensen die hebben geluisterd naar dit algemeen overleg.

Sluiting 12.08 uur.