Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 240

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 24 mei 2012

De vaste commissie voor Veiligheid en Justitie en de vaste commissie voor Binnenlandse Zaken hebben op 10 april 2012 overleg gevoerd met minister Opstelten van Veiligheid en Justitie, minister Spies van Binnenlandse Zaken en Koninkrijksrelaties en staatssecretaris Teeven van Veiligheid en Justitie over **Cyber Security en veiligheid overheidswebsites.**
(De volledige agenda is opgenomen aan het einde van het verslag.)

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

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

De voorzitter van de vaste commissie voor Binnenlandse Zaken,
Wolbert

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

kst-26643-240
ISSN 0921 - 7371
's-Gravenhage 2012

Voorzitter: Çörüz
Griffier: Van Doorn

Aanwezig zijn zes leden der Kamer, te weten: Çörüz, Elissen, Gesthuizen, Hachchi, Hennis-Plasschaert en Recourt,

en minister Opstelten van Veiligheid en Justitie, minister Spies van Binnenlandse Zaken en Koninkrijksrelaties en staatssecretaris Teeven van Veiligheid en Justitie, die vergezeld zijn van enkele ambtenaren van hun ministerie.

De **voorzitter**: Ik heet de bewindslieden en hun staf van harte welkom. Ook heet ik alle aanwezigen op de publieke tribune van harte welkom. Dit debat duurt van 16.00 uur tot uiterlijk 20.00 uur. Ik stel een spreektijd per fractie voor van zeven minuten in eerste termijn. Woordvoerders mogen maximaal twee interrupties plegen.

Mevrouw **Hennis-Plasschaert** (VVD): Voorzitter. Al bijna twee maanden geleden waren wij bijeen voor het AO over nationale veiligheid. Toen stelde ik dat de uitzending van EenVandaag over SCADA weer eens duidelijk maakte hoe kwetsbaar onze vitale infrastructuur is. De controle van allerhande installaties zou zonder te veel inspanning gewoon kunnen worden overgenomen. De SCADA-brief van het kabinet van enkele weken geleden stelt enigszins gerust. Tegelijkertijd kan ik niet genoeg benadrukken dat als departementen, gemeenten en waterschappen allemaal hun eigen dingetje blijven doen, de overheid en dus ook grote delen van onze vitale infrastructuur zo lek als een mandje blijven.
Regie is cruciaal. Dat heb ik al vele malen eerder gezegd. Als er iets gebeurt, zal het de inwoners van Nederland geen bal interesseren wie de formele beheerder of eigenaar is. Ik hoop dat dit bij de bewindspersonen is geland. Alle eigenaren dienen doordrongen te zijn van de noodzaak van passende informatiebeveiliging en de updates hiervan en dienen conform te handelen. Als het dan toch fout gaat – garanties heb je natuurlijk nooit – ligt het voor de hand dat de eigenaar direct zicht heeft op de mogelijke impact en de eventuele gevolgen en dat hij of zij in staat is om direct en dus proactief actie te ondernemen. Graag wil ik van de ministers en de staatssecretarissen weten of zij over voldoende handvatten beschikken om de andere overheden en partijen te dwingen om de controle op de informatiebeveiliging daadwerkelijk uit te voeren en daarover te rapporteren. Eerder is geopperd om in de bedrijfsvoeringsparagraaf van het jaarverslag hierover een verplichte passage te laten opnemen. Volgens mij heeft minister Spies hier onlangs ook iets over gezegd, in het kader van onder meer de bespreking van de voortgang van de compacte rijksdienst. Wellicht kan minister Spies hier een kleine toelichting op geven.
We waren het er van links tot rechts over eens dat DigiNotar een belangrijke wake-upcall was. Dit geldt natuurlijk ook voor andere incidenten die al dan niet binnen de eigen landsgrenzen de afgelopen tijd op dit terrein het nieuws domineerden.
Een duidelijk beleid is van belang en is ook noodzakelijk. Niemand ontkent dat. Dat doet niets af aan het feit dat een kritische houding op zijn plaats is. Dit zeg ik in het bijzonder tegen minister Opstelten. Als een kip zonder kop te werk gaan, zet weinig zoden aan de dijk. Dat is precies wat we met elkaar hebben besproken in het AO over nationale veiligheid, begin juni 2011. Na dit AO heeft in het bijzonder minister Opstelten gesuggereerd dat Kamerleden het nut en de noodzaak van actie op het terrein van Cyber Security ietwat hadden gebagatelliseerd. Dat was en is echter geenszins het geval. Dat heb ik de minister eerder ook al proberen uit te leggen. Wel ga ik ervan uit dat deze liberale minister met mij van mening is dat een kritische blik altijd welkom is, ten aanzien van welke overheid dan ook,

zodat wij zeker weten dat wij steeds weer de juiste afweging maken, ook in relatie tot de welbekende fundamentele rechten.
Ik heb enkele vragen. Gesteld wordt dat het Cyber Security Beeld Nederland (CSBN) 2011 niet of onvoldoende objectief is. Kan de minister aangeven waarom hij van mening is dat dit CSBN wel voldoende objectief is? Is het onderzoek naar zijn mening voldoende onafhankelijk en is de informatie verifieerbaar? In hoeverre heeft wetenschappelijk onderzoek erbij een rol gespeeld? Kan de minister ook reageren op de critici die stellen dat het CSBN had moeten ingaan op de zogenoemde assets, aangezien zij een essentieel onderdeel zijn van een bruikbare dreigingsanalyse? Het zou volgens de critici niet mogelijk zijn om tot een juiste risicobeoordeling te komen zonder een goed begrip van de specifieke belangen, de assets, van de overheid en de vitale infrastructuur. Daarover zijn vele vragen gesteld.
Is in het CSBN 2011 alle beschikbare informatie verstrekt? Of is bepaalde informatie niet opgenomen in verband met het vertrouwelijke karakter ervan? Voor ons is dit cruciaal. Kunnen we op een andere wijze geïnformeerd worden als er sprake is van informatie met een vertrouwelijk karakter? Kan de minister verder concreet aangeven op welke punten het huidige juridische kader tekortschiet voor overheidsinterventies ten tijde van een dreigende cybercrisis? Welke aanvullende bevoegdheden worden overwogen? Als dit AO zich hiervoor niet leent, vraag ik de minister om dit in een vertrouwelijke brief nader uiteen te zetten.
De minister verwijst in zijn brief verder naar internationale trajecten, waarbij gekeken wordt naar de noodzakelijkheid om wet- en regelgeving aan te passen ten behoeve van opsporingsmogelijkheden op internet. Aan welke trajecten moet ik dan denken? Aan welke aanvullende instrumenten, zowel juridisch als niet-juridisch, denkt de minister in het kader van het bevorderen van de digitale veiligheid?
Hoe staan deze bewindspersonen tegenover de realisatie van een kwalificatieschema dat de kwaliteitsborging van de beroepsgroep van informatiebeveiligers eenduidig maakt en bewaakt?

Mevrouw **Hachchi** (D66): Mevrouw Hennis zei dat zij de brief over SCADA gelezen heeft en dat deze haar enigszins geruststelt. Kan zij toelichten wat zij met «enigszins» bedoelt? Welke zorgen heeft de VVD-fractie nog?

Mevrouw **Hennis-Plasschaert** (VVD): Ik denk dat ik die wel heb geduid. Alleen de theorie van de regie is niet genoeg. Regie moet ook aangetoond worden. Ik ben echt van mening dat we straks wellicht voor onaangename verrassingen komen te staan als we het overlaten aan gemeenten, waterschappen, departementen en ga zo maar door, Het gaat de VVD-fractie dus niet alleen om de opdracht om het te doen, maar ook op de controle daarvan.

Mevrouw **Hachchi** (D66): Ik kan mevrouw Hennis-Plasschaert helemaal volgen in wat zij zegt over regie. Wij hebben samen in de uitzending van EenVandaag gekeken naar het voorbeeld van de gemeente Veere. Is de VVD-fractie het met mij eens dat een belangrijke bron van de problemen een tekort aan ICT-kennis is? Op gemeentelijk niveau ontbreekt ICT-kennis. Door dit probleem hebben we uiteindelijk onbeveiligde systemen.

Mevrouw **Hennis-Plasschaert** (VVD): Het is de vraag wie die ICT-kennis moet hebben. De overheid hoeft niet altijd de expert te zijn. De overheid kan ICT ook uitbesteden. Wel moet er controle op zijn, bijvoorbeeld door middel van specifieke voorwaarden die in het programma van eisen zijn opgenomen. Het gaat er dus niet zozeer om dat de kennis aanwezig is bij de overheid, als zij er maar is. En er moet op gecontroleerd worden.

De heer **Elissen** (PVV): Voorzitter. Ik zal zo meteen naar voren kijken, maar ik wil eerst eventjes achterom kijken. Ik refereer daarmee aan het vorige algemeen overleg, over nationale veiligheid en crisisbeheersing, op 15 februari. Toen heeft minister Opstelten desgevraagd aangegeven dat er een ICT-crisisplan is. Deze zou de vorm hebben van een crisisresponsplan ICT. Dit plan werkt in ieder geval, zo zei hij. Tevens is er volgens de minister in 2011 een nationaal crisisplan opgeleverd. Ik vond dit prettig om te horen. Ik vond het jammer dat ik deze stukken niet al eerder zelf had gevonden. Dan had ik ze namelijk niet meer aan de minister hoeven te vragen.
Ik heb na het overleg met de minister nog maar eens driftig gezocht, want ik wilde die plannen wel eens inzien. Wat schetste mijn verbazing? Ik kon nog steeds geen openbaar ICT-crisisplan vinden en ook geen nationaal crisisplan. Wel heb ik op de website van het Nationaal CrisisCentrum kunnen lezen dat het nationaal crisisplan voor de zomer van 2012 gereed is. Liep de minister de vorige keer een beetje op de zaken vooruit? Komt er tegen de tijd dat de zomer begint een nationaal crisisplan? Is het ICT-crisisplan openbaar of is dit een vertrouwelijk document? Wel beschikbaar is in ieder geval het document met de nationale Cyber Security strategie. Dit is weliswaar een beknopt document, maar de onderdelen van het werkplan worden voortvarend opgepakt. Dit plan is de rode draad voor de ontwikkeling van onze Cyber Security . Het eerste punt uit het plan werd aan het begin van dit jaar al uitgevoerd. Op 12 januari is namelijk het Nationaal Cyber Security Centrum geopend. Ik was daarbij zelf aanwezig en kan zeggen dat dit niet alleen een bijzondere gebeurtenis was, maar toch ook wel een unieke en spectaculaire gebeurtenis. Daarvoor mijn complimenten.
Er is één Cyber Security centrum dat namens de gehele Nederlandse overheid samen met het bedrijfsleven zorgdraagt voor onze Cyber Security . De buitenlandse gasten die tijdens de opening aanwezig waren, bevestigden dat zowel het departementoverstijgende karakter als de samenwerking met het bedrijfsleven bijzonder genoemd kan worden. Dit betekent niet dat wij achterover kunnen leunen. Wij zijn namelijk nog maar net begonnen. Daarom wil ik van deze gelegenheid gebruikmaken om wat beelden met de ministers te delen en te vragen hoe zij de ontwikkelingen van het centrum zien. Daarbij zal ik ook aangeven hoe de PVV hiertegen aankijkt.
Het centrum verricht nu al heel goed werk. We vertrouwen erop dat dit in de toekomst alleen maar beter zal worden. Kort geleden doken in de media veel berichten op over de kwetsbaarheden in de zogenaamde SCADA-systemen. Mevrouw Hennis refereerde daar al even aan. Dit zijn industriële regelsystemen waarmee bijvoorbeeld waterpompen, maar ook nucleaire installaties bediend kunnen worden. Nu is er erg veel kennis over deze systemen voorhanden en is er veel informatie beschikbaar. Het Nationaal Cyber Security Centrum heeft een beetje orde in de chaos weten te scheppen, door een eenvoudige checklist te publiceren en handzame informatie te verstrekken waarmee eigenaren van SCADA-systemen op weg worden geholpen. Daarnaast heb ik uit een aantal gesprekken en briefjes begrepen dat het centrum sinds oprichting al verschillende Nederlandse bedrijven terzijde heeft gestaan bij aanvallen van hackers. Er is natuurlijk nog veel meer gebeurd, maar deze punten wilde ik graag even in het bijzonder noemen.
Het Nationaal Cyber Security Centrum is wat ons betreft dus goed op weg. Het dient een goede vertrouwensrelatie op te kunnen bouwen met Nederlandse bedrijven. Het is belangrijk dat dit centrum overal bij kan en zo goed mogelijk op de hoogte is van de wijze waarop belangrijke Nederlandse instellingen en ondernemingen zich voorbereiden op cyberaanvallen. Veel kan worden bereikt met vriendelijk vragen en met werken aan vertrouwen. Zou het ook niet een idee zijn om het centrum bevoegdheden te verlenen die de OPTA ook heeft? Als het echt nodig is,

kan de OPTA overal bij. Dat kan het in het uiterste geval gewoon afdwingen. Ik refereer hierbij aan het zogenaamde brede informatierecht, dat vanzelfsprekend omgeven is met de nodige waarborgen.
Er zijn in Nederland bedrijven die heel belangrijk zijn geworden. Zij dragen bijvoorbeeld zorg voor internet en voor het onderhouden van de software waarmee sluizen en gemalen worden beheerd. Het kan ook gaan om bedrijven die elektronisch betalingsverkeer mogelijk maken of die beveiligingsoplossingen op ICT-gebied aanbieden. Is de minister het met de PVV eens dat het belangrijk is voor de Nederlandse overheid om op zijn minst te weten hoe deze bedrijven zich beschermen tegen cyberaanvallen? Ik kan me voorstellen dat bedrijven voorzichtig zijn met het delen van informatie met de overheid. De overheid moet hiermee natuurlijk wel zorgvuldig omgaan. Tevens is het belangrijk dat deze gegevens vertrouwelijk worden behandeld en geclassificeerd zijn. De PVV is voor een open en transparante overheid, maar als deze gegevens worden verstrekt op basis van een WOB-verzoek, kan er geen sprake zijn van een vertrouwensrelatie tussen het Nationaal Cyber Security Centrum en het Nederlandse bedrijfsleven. Hoe kijkt de minister hiertegen aan? Is het nodig om hiervoor nieuwe wetgeving te ontwikkelen of voldoet de huidige wetgeving?
Tot slot wil ik een ander belangrijk punt aan de orde stellen: de organisatie van rampenbestrijding. Of het nu gaat om rampenbestrijding zoals wij deze al jaren kennen in Nederland, of om een digitale rampenbestrijding, wat de PVV betreft wordt Cyber Security zelfs analoog aan terrorismebestrijding behandeld. Nu begrijp ik dat het misschien een beetje vreemd is om iets wat zich in het digitale domein afspeelt, analoog te behandelen, maar ik denk dat de minister mijn punt wel begrijpt. De gevolgen van een cyberaanval kunnen namelijk zeer groot zijn. Daarom is het belangrijk dat er een duidelijke commandostructuur is. Nu bestaat onzes inziens het risico dat iedereen met iedereen overlegt en dat te lang onduidelijk blijft wie de leiding heeft. Dat moet wat de PVV betreft veranderen. Hoe kijkt de minister aan tegen een wat scherpere commandostructuur?
Ik ben uiteraard ook benieuwd hoe de minister de door mij ingediende en door de Kamer aangenomen motie gaat invullen. Ik zal daarop eventueel in tweede termijn terugkomen.

De heer **Recourt** (PvdA): Voorzitter. Iedere fractie kiest zo haar eigen invalshoek. Ik heb gedacht aan de wijze waarop we in de oude, predigitale wereld belangrijke gegevens beveiligden. Dit gebeurde in een kluis. Lang geleden had je genoeg aan een stethoscoop en een goed gehoor om die kluis te openen. Over een lange tijdsperiode zijn de kluizen technologisch sterk verbeterd, maar nog steeds kun je er binnenkomen, als je het echt wilt. Verder is het van belang dat de Nederlandsche Bank een grotere kluis heeft dan een particulier, omdat de belangen van de Nederlandsche Bank natuurlijk veel groter zijn. In de nieuwe wereld geldt eigenlijk hetzelfde, al is er een aantal verschillen. Met de nieuwe wereld bedoel ik de digitale wereld.
Als je de vergelijking doortrekt, stel je vast dat ook de digitale wereld nooit 100% veilig is. Hoe groter het belang, hoe zwaarder de beveiliging. Dit geldt natuurlijk in het bijzonder voor de overheid. Justitie, terrorisme, de fiscus en de gemeentelijke basisadministratie: ze rechtvaardigen allemaal een zware beveiliging. Een groot verschil is de snelheid waarmee de ontwikkelingen gaan. In de digitale wereld gaat het hoogstens om een aantal jaren in plaats van honderden jaren ontwikkeling van de kluizen. Hoe houden we dat bij en hoe stel je zo algemene normen dat je er niet voortdurend achteraan blijft rennen?
De rol van de overheid is uiteraard om haar eigen zaken op orde stellen, maar zij moet ook normen stellen voor het bedrijfsleven en voor de diffuse samenwerkingsvormen tussen overheid en bedrijfsleven. Daarbij moet zij niet alleen normen stellen, maar ook controleren en straffen.

Door dat controleren en straffen moet er prioriteit verkregen worden bij het bedrijfsleven.
Ik kom te spreken over wat concretere onderwerpen, om te beginnen bij werving en selectie door de overheid. De overheid is in veel gevallen een hiërarchische ambtelijke organisatie, Defensie in het bijzonder. Ik wijs op een artikel in het NRC Handelsblad van 17 januari 2012. Daarin staat dat de overheid voor de beveiliging van haar systemen zoekt in een markt van jonge, vrije mensen. Dat is lastig. Ik vraag de verantwoordelijke bewindspersoon daarom hoe deze twee op het oog niet op elkaar passende werelden toch op elkaar gaan passen. Het kan zelfs nog iets sterker. De overheid is terecht druk bezig met de opsporing van digitale criminaliteit. Je hebt het idee dat een grote boef iemand is die al wat ouder is, maar dan haalt men toch gewoon tieners, pubers, achter hun computers op het zolderkamertje vandaan. Zij krijgen een strafblad, waardoor je hen niet meer kunt inzetten voor diezelfde overheid, terwijl de overheid ze juist zo nodig heeft om haar creativiteit en kennis te organiseren en up-to-date te houden.
Ik kom te spreken over de wetgeving. Ik verwijs naar artikelen in de Volkskrant van 10 en 19 maart 2012. Ik heb zelf op 9 maart Kamervragen gesteld. In het artikel staat dat de politie illegaal hackt en dat de politie meer armslag nodig heeft om cybercrime en cyberveiligheid te kunnen aanpakken. De antwoorden op mijn vragen zijn vaag. Er komt nationale en internationale wetgeving, maar dit duurt even, is het antwoord. Kan het niet wat concreter? Hoe zit het bijvoorbeeld met het bewijs dat nu wordt verkregen terwijl er geen wettelijke bevoegdheid is? Is dat onrechtmatig verkregen bewijs? Wordt dit bewijs uitgesloten voor bewijslevering? Ik denk bijvoorbeeld aan veel zedenzaken, waarin veel bewijs op digitale wijze wordt verkregen. Mij lijkt het een groot gevaar als de wetgeving hieromtrent naar de lange termijn wordt verschoven. Op welke korte termijn kunnen we efficiënt opsporen?

Mevrouw **Hennis-Plasschaert** (VVD): Ik begrijp de heer Recourt misschien niet helemaal en daarom stel ik een verduidelijkende vraag. Suggereert hij nu dat wij mensen die de wet overtreden, ook al is het op een zolderkamertje, eigenlijk met enige liefde moeten behandelen omdat zij van nut kunnen zijn voor de overheid?

De heer **Recourt** (PvdA): Ja, dat suggereer ik inderdaad. Het geldt natuurlijk niet voor de grote, criminele internetboeven. Die moet je niet hebben, maar wel de jongens en meisjes die op een zolderkamertje zitten te sleutelen. Je kunt hun activiteiten met een strafrechtelijke bril bekijken, maar ik denk dat je jezelf daarmee tekortdoet. Ik zie namelijk een hoop creativiteit. Je moet die mensen niet meteen verder in het criminele milieu wegzetten. Dat krijg je natuurlijk, want als de overheid niet geïnteresseerd is, zijn criminele organisaties dat zeker wel. Ook die zijn namelijk op zoek naar dezelfde kennis. Het lijkt mij dus niet een heel verstandige strategie.

Mevrouw **Hennis-Plasschaert** (VVD): De PvdA doet dus een suggestie voor een banenplan voor jongens en meisjes die op hun zolderkamertje de wet overtreden. Mag ik het zo samenvatten?

De heer **Recourt** (PvdA): De PvdA doet een suggestie voor een banenplan voor creatieve internetnerds, maar dat is meteen een negatieve kwalificatie. Dat lijkt mij inderdaad heel verstandig voor heel adequate mensen. De stukken staan bol van de penetratietests en daar zou ik de beste mensen op de markt voor zoeken.
Voorzitter. Een ander punt is het opgeven van autonomie. Het is evident dat de aanpak van cybercrime een internationaal vraagstuk is. Neem alleen al het opslaan van gegevens «in the cloud»: zeg maar eens in welk land waar er rechtsmacht voor is, dat gebeurt. Het is onverstandig om

achter de dijken te verdwijnen. Willen de bewindslieden dan ook de consequentie aanvaarden dat wij autonomie weggeven? Uiteindelijk zal er sprake zijn van Europese autonomie of in de verre toekomst misschien van autonomie in een nog groter verband. Wat is de stand van zaken voor internationale samenwerking? Er is the Convention on Cybercrime, de Budapest Convention, maar hoe staat het daarmee; welke prioriteit wordt eraan gegeven?
Ik ga verder met de uitvoering door de politie. Het is evident dat alle misdaad een digitale component heeft. Ook een gewone diefstal laat vaak digitale sporen na. Dan hebben wij het niet over criminele activiteiten die alleen op internet wordt gepleegd. Ik heb het idee dat wij bij lange na geen beeld hebben van de grootte daarvan. Wordt er standaard digitaal gerechercheerd? Dat moet een onderdeel zijn van zo goed als iedere zaak.
Ik kom op de uitvoering van het toezicht. Ik spreek veel lof uit over de Cyber Security Strategie met zes actiepunten. Wij hebben natuurlijk incidenten met DigiNotar en KPN gehad. Er zijn analyses op losgelaten en adviezen aan de overheid gegeven. Dat is prima; die worden voor een belangrijk deel opgevolgd. Ik mis echter als belangrijk element de hardheid naar de markt toe. Als ik zelf mensen spreek, bijvoorbeeld bij KPN, hoor ik dat daar een groot aantal netwerken naast elkaar draait en dat er weinig overzicht is. Door de markt ingegeven, krijgen andere belangen dan het belang van veiligheid voorrang. Juist als de overheid dreigt met maatregelen als de veiligheid geen prioriteit krijgt, kan zij sturen op het hoger op het prioriteitenlijstje van private organisaties krijgen van de beveiliging van bijvoorbeeld persoonsgegevens die ook daar in databestanden staan.
De meldplicht voor datalekken bevindt zich in de voorbereidende fase. Ik ga even in op de stand van zaken. Ik vind dat uiteraard een goed initiatief. Ik vind het ook goed om te lezen dat de overheid zelf goed heeft gehandeld inzake DigiNotar. Het blijft echter opmerkelijk dat het zo lang heeft geduurd voordat DigiNotar zelf melding van een probleem heeft gemaakt. Een andere les was dat de papieren werkelijkheid heel wat anders is dan de echte werkelijkheid; die twee liggen uit elkaar. Het is mij nog steeds niet helemaal duidelijk hoe door de aanbevelingen in het kader van DigiNotar die twee elementen ook worden getackeld, zodat het in de toekomst niet meer kan gebeuren.

Mevrouw **Gesthuizen** (SP): Ik verbaas mij een beetje over de gemakkelijke manier waarop de verantwoordelijken er van de heer Recourt mee mogen wegkomen. Hij constateert namelijk dat juist in het kader van DigiNotar zo goed is opgetreden. Met name in de aanloop naar dat debacle heeft men volgens mij wel de nodige steken laten vallen. Dat werd in mijn ogen ook heel duidelijk uit de diverse gesprekken die de Kamer daarover met betrokkenen heeft gevoerd. Er schortte toch heel wat aan onder andere het toezicht?

De heer **Recourt** (PvdA): Mevrouw Hennis zei al dat DigiNotar een wake-upcall is geweest voor ICT-beveiliging bij de overheid en misschien nog wel breder. Als je gewekt moet worden, houdt dat in dat je daarvoor sliep; daar ben ik het helemaal mee eens. Ik verwijs ook naar het rapport dat over het handelen van de overheid inzake DigiNotar is opgemaakt. Dat is voor een groot deel gewoon een positief verhaal.

Mevrouw **Gesthuizen** (SP): Dat is inderdaad heel duidelijk. Wie zit te slapen, doet zijn werk niet goed. Ik begrijp dat er duidelijke kritiek is van de zijde van de PvdA-fractie.

Mevrouw **Hachchi** (D66): Voorzitter. Om te beginnen merk ik op dat ik blij ben dat de minister van Binnenlandse Zaken mijn voorstel bekijkt om studenten of whizzkids, zoals zij ze noemt, bij hacktesten te betrekken. Ik

blijf graag op de hoogte van de ontwikkelingen – dat geldt misschien ook voor mijn collega's – hoewel de minister heeft aangegeven dat zij die niet aan de grote klok wil hangen. Ik heb ook met de minister gesproken over een richtlijn voor de wijze waarop met hackers moet worden omgegaan. De overheid weet zelf niet goed op welke manier zij met hackers moet omgaan. Computerexperts die misstanden melden, krijgen wisselende reacties. De ene gemeente is dankbaar en dicht het lek, de andere gemeente doet aangifte of stelt de hacker meteen aansprakelijk. Ook heb ik begrepen dat de jurisprudentie over de vraag wanneer een hack al dan niet strafbaar is, nog onvoldoende is uitgekristalliseerd. Daarom heb ik voorgesteld om tot een richtlijn te komen voor de manier waarop met hackers moet worden omgegaan. Tijdens het vorige debat gaf minister Spies aan dat zij hier graag met haar collega Opstelten over wilde spreken. Vandaag hoor ik dan ook graag de reactie van beide ministers.
SCADA-systemen zorgen voor de aansturing van industriële installaties zoals waterpompen, windmolens, zwembadinstallaties, gas- en oliepompen en zelfs de infrastructuur van het openbaar vervoer. Het kan dus behoorlijke consequenties hebben als hiermee iets misgaat. Ik citeer: «Organisaties binnen de overheid en de commerciële sector zijn zelf verantwoordelijk voor hun SCADA-systemen.» Dat is het antwoord van de ministers op mijn schriftelijke vragen. Daar kunnen zij wel gelijk in hebben, maar dan moet er wel centraal hulp kunnen worden geboden. Het is namelijk duidelijk dat er een gebrek aan ICT-kennis is. Dat hebben wij gezien in de gemeente Veere. Het is volgens mij ook belangrijk om overheidsorganisaties niet steeds zelf opnieuw het wiel te laten uitvinden. Wij kunnen onze handen er op landelijk niveau niet helemaal van aftrekken, zeg ik tegen de ministers. De collega van de VVD had het over regie. Ik vind het ook belangrijk om op te merken dat er lokaal geen ICT-kennis is, zeker gelet op de bezuinigingen van vorig jaar en de extra bezuinigingen die daar wellicht bovenop komen. Volgens mij valt wat dat betreft op landelijk niveau wel degelijk een rol te spelen.
Het Nationaal Cyber Security Centrum heeft al richtlijnen opgesteld, maar ook hierbij geldt dat er in de eerste plaats mensen moeten zijn die de kennis hebben om die richtlijnen daadwerkelijk te kunnen uitvoeren. Daarbij zijn de leveranciers van SCADA-systemen vaak mkb-bedrijven met geringe kennis van informatiebeveiliging zijn. Leveranciers blijken soms zelfs de beveiliging niet serieus te nemen. Kortom: onderschrijft de minister het gebrek aan kennis over SCADA-systemen bij gemeenten en andere overheidsorganisaties en bij het mkb? Hoe gaat de minister de noodzakelijke kennis faciliteren aan gemeenten en andere overheidsorganisaties? Is de minister ook bereid, de leveranciers van gebrekkige SCADA-systemen aansprakelijk te stellen? Als het namelijk misgaat en Nederland half onder water loopt, kunnen wij wel spreken van een crisis oftewel een ramp. Ik neem aan dat de verantwoordelijkheid dan niet meer bij de burgemeester ligt, maar bij minister Opstelten.
Ik heb samen met mijn collega, woordvoerder op het gebied van VWS, vragen gesteld over SCADA-systemen en medische technologie zoals pacemakers en insulinepompen. Ik denk dat het tot ieders verbeelding spreekt wat de gevolgen zijn als de veiligheid hiervan niet op orde is. De gestelde vragen zijn nog niet beantwoord, maar misschien kan de minister hier alvast op ingaan.
Uit het onderzoek naar DigiNotar komt naar voren dat de overheid snel en adequaat heeft gereageerd, maar geldt dit ook ten aanzien van de Iraanse activisten? Hierover blijft het namelijk angstvallig stil. Ik weet dat het bij de AIVD op tafel ligt, maar kunnen de ministers aangeven wat de gevolgen waren en of gevaar voor mensenlevens zowel binnen als buiten Nederland een prominente plek heeft in het Cyber Security beleid?
KPN heeft lang gewacht met het melden van een cyberaanval. In de Telecommunicatiewet is een meldplicht voor het lekken van persoonsgegevens geregeld. Via een motie is verzocht, melding van een security

breach verplicht te stellen. Graag hoor ik van de minister of deze meldplicht voldoende is om alle vitale diensten, zoals 112 en nutsdiensten, op orde te houden. Of neemt de minister nog andere maatregelen zodat vitale communicatie bij incidenten zoals de Vodafone-brand beschikbaar blijft? Is er nu wel of geen back-upsysteem? De SP-fractie heeft daarover vragen gesteld, maar ook de antwoorden daarop zijn nog niet binnen. Zo nee, zou een back-upsysteem niet verplicht moeten zijn?
De Nationale ombudsman heeft grote twijfels over de veiligheid van DigiD. Zo constateert hij dat er niet drie veiligheidsniveaus zijn, basis, midden en hoog, maar slechts één: het basisniveau. Graag hoor ik hierop een reactie van de minister van Binnenlandse Zaken.
Op verzoek van mijn fractiegenoot Schouw heeft de minister van Veiligheid en Justitie een juridisch kader voor Cyber Security opgesteld. Ik dank de minister hiervoor. De minister concludeert dat de noodzaak bestaat om de bevoegdheden van de overheid uit te breiden in de strijd tegen cybercriminelen. Ik mis echter twee dingen. Ten eerste mis ik duidelijkheid over de noodzaak om bevoegdheden uit te breiden. Ten tweede mis ik een toelichting op de vraag hoe een dergelijke uitbreiding zich verhoudt tot internetvrijheid en andere grondrechten.
Tot slot merk ik op dat Cyber Security een belangrijk aandachtspunt van het kabinet is. Het is echter onduidelijk welke middelen het kabinet voor deze ambitie reserveert. Zo heb ik vernomen dat de personele capaciteit van het Nationaal Cyber Security Centrum achterblijft. Kan minister Opstelten hierover duidelijkheid geven?

Mevrouw **Gesthuizen** (SP): Voorzitter. Ik begin met DigiD. Vanochtend belde ik nog met DigiD om te informeren naar de mogelijkheden om een nieuwe DigiD aan te vragen. Ik begreep dat dit wat problemen opleverde. Die hadden volgens mij niet met de veiligheid te maken, maar met het feit dat er wat ICT-problemen waren waardoor de boel niet functioneerde. Daardoor kon ik in ieder geval vanochtend geen nieuwe DigiD aanvragen. Een ander belangrijk feit van vandaag is dat de rijks-CIO heeft aangegeven dat een veilige overheid een illusie is. Dat is heel belangrijk nieuws. Misschien kan de minister van BZK daar direct op reageren.
Er staat ontzettend veel op de agenda; het is eigenlijk niet te doen. Ik ga daarom snel en sec alle punten en vragen die ik wil stellen langs. Zoals de heer Recourt al aangaf, hebben wij hierbij eigenlijk te maken met overheidsfunctioneren op twee verschillende terreinen. In de eerste plaats moet het kabinet regels stellen voor anderen die actief zijn in de sector. In de tweede plaats is de overheid zelf ook een speler die zich met ICT bezighoudt. Zij is ook afhankelijk van de anderen waarvoor zij eerder regels heeft moeten vaststellen. Dat maakt het soms niet eenvoudig om op dit gebied heel daadkrachtig op te treden.
Vorig jaar achtte het kabinet het nog niet nodig om een integrale visie op ICT-veiligheid en -privacy uit te brengen. Intussen is er echter heel wat veranderd. Daarom mogen wij dit voorjaar wel een integrale visie op ICT-privacy en -veiligheid tegemoet zien. Naar aanleiding van DigiNotar – die affaire is door sommigen een wake-upcall genoemd – is ook de Kamer heel voortvarend aan de slag gegaan. Dat durf ik te zeggen, ondanks de vele kritische e-mails die ik van mensen uit de samenleving mag ontvangen. Zij schrijven: jullie doen nog lang niet genoeg en jullie weten er nog lang niet voldoende van af. Wij hebben wel vanuit verschillende invalshoeken een groot aantal gesprekken gevoerd met zeer veel verschillende deskundigen. Desalniettemin blijft er genoeg te doen en ik ben dan ook verheugd dat het parlement dit onderwerp op zijn eigen onderzoeksagenda heeft gezet.
Ik merk het volgende op over de overheid die zich zelf in de sector beweegt en van ICT gebruikmaakt. In de brief van 11 oktober jl. is aangegeven dat alle organisaties voor 1 april 2012 – dat was vorige week

– de ICT-beveiligingsassessments moesten hebben doorlopen. Nu blijkt echter dat de grootgebruikers van DigiD voor het einde van het jaar het ICT-beveiligingsassessment moeten hebben uitgevoerd. De overige organisaties dienen het assessment uiterlijk een jaar later te hebben uitgevoerd. Ik stel daarover dezelfde vraag die ik ook tijdens het vorige algemeen overleg heb gesteld – daarbij was alleen de minister van BZK aanwezig – want die kon toen nog niet helemaal worden beantwoord. Is de dringende noodzaak nu weg en is de huidige aanpak voldoende om de veiligheid te garanderen?
Wat vindt het kabinet van het idee om de richtlijnen voor beveiliging en privacy die het NCSC uitbrengt, bij het aanbesteden van overheidsopdrachten met een «comply or explain»-constructie als basis te laten fungeren? Daardoor wordt de kennis van het NCSC beter benut en wordt er een goede basis voor veiligheid gelegd. De adviezen voor het standaardbeheer van IT-systemen bij de overheid kunnen daarbij worden meegenomen. In hoeverre gebeurt dit al?
Ik ga verder met de SCADA-systemen. Er zijn acties, twee checklists, maar zijn deze voldoende om goede beveiliging van SCADA-systemen te garanderen; of kunnen wij nog andere, extra maatregelen ter beveiliging van die systemen verwachten? Moet er geen centraal toezicht op de systemen komen in plaats van toezicht door sectorale toezichthouders?
Ik kom op de punten van de overheid en de markt. Er zijn hoge verwachtingen van het NCSC gewekt. Het NCSC is al operatief en moet in 2012 bouwen aan de basis. Diverse mensen zeggen echter: wacht even, daar gaat natuurlijk wel redelijk wat tijd in zitten. Je hebt alle expertise ook niet zomaar bij de hand. Ik krijg graag een reactie van de minister van Veiligheid en Justitie op de volgende vraag. In hoeverre is het NCSC nu al de club waarvan hij zulke hoge verwachtingen heeft; is het de club die hij verwacht dat het is?
Ik sluit mij kortheidshalve aan bij de vraag die mevrouw Hachchi in het kader van het NCSC over KPN heeft gesteld. Wat denkt de minister van een verplichting voor bedrijven om het direct aan het NCSC te melden als zij constateren dat een inbraak heeft plaatsgevonden? Op die manier moet erger worden voorkomen.
Wanneer kunnen wij de eerste resultaten van het onderzoek van de inspectie naar de crisisbeheersingsaspecten rond het DigiNotar-incident verwachten?
De helft van de Nederlandse bedrijven en instellingen is het afgelopen halfjaar slachtoffer geworden van een cyberaanval. Slecht één op de vijf acht zichzelf in staat om zo'n aanval met succes te kunnen afslaan, blijkt uit onderzoek van KPMG. Graag hoor ik daarop een reactie van de minister van Veiligheid en Justitie.
Tijdens een eerder algemeen overleg met de minister kwam ook al de oproep van de heer Kohnstamm van het College bescherming persoonsgegevens ter sprake. Hij heeft namelijk aangegeven niet voldoende mankracht te hebben om alle schendingen van privacy afdoende te onderzoeken. Het jaarbudget van het CBP staat namelijk niet in verhouding tot het aantal grote bedrijven dat worstelt met gebrekkige beveiliging van persoonsgegevens. Voorzitter Kohnstamm schat in dat zijn college nu meer dan de helft van de zaken moet of zal moeten laten liggen. Ook verwacht hij dat er meer onderzoeken nodig zijn als bedrijven verplicht worden om datalekken te melden. Graag hoor ik hierop een reactie. Ik begrijp dat het voor iedereen, zeker in deze tijd, belangrijk is om prioriteiten te stellen, maar zeker in een steeds verder digitaliserende samenleving en met een overheid die zelf ook in steeds grotere mate afhankelijk is van ICT en dat ook van burgers vraagt, kun je zo'n oproep, zo'n vraag – ik zou het bijna een noodkreet noemen – natuurlijk niet in de wind slaan.
In het onderzoek van de Rijksauditdienst naar het handelen van overheidspartijen staat het volgende waarop ik graag een reactie van de minister

wil. «Er is een trend dat de overheid delen van haar eigen dienstverlening uitbesteedt. De vraag die gesteld kan worden is of de gedachte van marktwerking («laat het over aan de markt») wel in alle gevallen mogelijk en/of wenselijk is en of het in eigen beheer houden, gegeven de publieke taak van de overheid en de mogelijke maatschappelijke impact, in voorkomende gevallen niet een wenselijker optie is. De indruk is dat er te veel wordt vertrouwd op een «goede» naam in plaats van te focussen op kwaliteit. (…) Zaken op het gebied van digitale beveiliging worden door de overheid vrij vaak aan private partijen overgelaten. Het is van belang om de betreffende taken meer geaggregeerd bij de overheid te hebben. Daarbij zal meer specialistische kennis bij de overheid opgebouwd moeten worden.»
In het verlengde daarvan ligt het volgende. Mij is mondeling een heel aantal zaken ter ore gekomen waarin steeds duidelijker wordt dat juist de mensen die het meeste verstand hebben van ICT het eerst weer vertrekken bij de overheid. Ik weet niet of de minister dit beeld herkent, maar dit heb ik van heel veel verschillende kanten vanuit het veld gehoord. Ik zou graag van het kabinet weten of het dit beeld herkent en, zo ja, wat het plan van aanpak is om dat te voorkomen. Ik hoor het namelijk uit werkelijk alle lagen, niet alleen van de rijksoverheid, maar ook van de gemeenten.

De **voorzitter**: U bent dik over de acht minuten spreektijd heen. Wilt u afronden?

Mevrouw **Gesthuizen** (SP): Goed, dan laat ik het hierbij.

Voorzitter: Hennis-Plasschaert

De heer **Çörüz** (CDA): Voorzitter. Het is geluk hebben als je de laatste spreker bent, want dan zijn er al heel veel dingen gezegd. ICT geeft ontzettend veel mogelijkheden, maar wij zijn ook ontzettend afhankelijk van diezelfde ICT. Wij hebben ons ontzettend kwetsbaar opgesteld. Wij zijn kwetsbaar en wij zijn afhankelijk van de ICT. Ik denk aan sluisdeuren die met een simpel wachtwoord opengaan. Ik denk aan de fishingmails die wij krijgen; ik krijg ze ook en vraag mij dan af of ik aangifte moet doen. Altijd goed, zegt de minister. Dat moeten wij dan maar eens overwegen. Ik denk aan een groot telecombedrijf dat gehackt wordt. Dit zijn toch wel de risico's. Ik ben blij dat ik namens de CDA-fractie kan aangeven dat dit kabinet de urgentie van het aanpakken van dit probleem ziet. Het is niet meer iets van kwajongensstreken van whizzkids die af en toe iets hacken. Hier zitten grote dreigingen en landen achter. Het is goed om er hier heel alert op te zijn.
Dan komen wij gelijk al in een spanningsveld. Enerzijds moeten wij dit keihard aanpakken – misschien moeten wij hiervoor wetten maken; dat weet ik niet; daar kom ik straks op – en anderzijds willen wij de vrijheid van internet waarborgen. Tussen die twee waarden moeten wij «een maatpak snijden». Ik vraag de minister om een reactie op het volgende. Ik heb gehoord – ik weet niet of het klopt; volgens mij klopt het, maar als dat zo is, is het wel raar – dat Nederlandse bedrijven met name aan Iran en China producten verkopen terwijl daar vervolgens de vrijheid van internet wordt geblokkeerd. Dat staat op gespannen voet met elkaar. Als wij die vrijheid hier borgen, willen en waarderen – en dat doen wij – is het raar dat Nederlandse bedrijven kennelijk producten verkopen aan landen die dit tegengaan. Is dat waar? Als het waar is, is dat merkwaardig. Hoe kan de minister dat dan verklaren?
Een aantal collega's heeft al gezegd dat dit een internationaal probleem is. Criminelen gaan al heel snel de grens over. Hoe zit het met internationale samenwerkingsprojecten om de internetcriminelen aan te pakken? Zijn er

samenwerkingsprojecten met andere landen en, zo ja, hoe verlopen die? Met name de heer Recourt heeft dit punt genoemd.
Volgens mij was het ook collega Recourt die refereerde aan een artikel in de Volkskrant waarin stond dat onze rechercheurs misschien de soevereiniteit van andere landen moeten doorbreken om online op zoek te gaan naar criminelen, zoals pedofielen. De digitale wereld kent geen grenzen, maar de meeste wetgeving wel. Hoe kunnen wij dit met elkaar afstemmen om de criminelen te pakken? De Nationale Recherche heeft gepleit voor meer specifieke juridische kaders voor onlineopsporing. Is dat nodig? Zo ja, in welke richting denkt het kabinet dan?
De minister schrijft in zijn brief dat een belangrijke nieuwe ontwikkeling de aandacht vraagt, namelijk het toenemende gebruik van mobiele apparatuur. Deze ontwikkeling vormt door de hoge penetratiegraad een groot risico, zo lees ik. Er zijn steeds meer mensen met een smartphone die op elk moment van de dag, ook als zij onderweg zijn, online zijn. Kan de minister nader specificeren waarin de bedreiging precies gelegen is? Ik vind het overbodig om reeds gestelde vragen te herhalen. Ik wil nog even inzoomen op het Nationaal Cyber Security Centrum, NCSC. Mijn eerste vraag is: welke formele verantwoordelijkheden heeft dit centrum precies? Op het terrein van Cyber Security zijn in de afgelopen periode heel wat initiatieven opgestart die onze digitale veiligheid moeten versterken. Mijn tweede vraag is of het centrum als een spin in het web gaat fungeren om deze initiatieven met elkaar te verbinden. Dat zou mijn fractie een goede zaak vinden. Mijn derde vraag over het centrum is de volgende. Als ik het goed heb gelezen, gaat het centrum ook een rol spelen in de publiek-private samenwerking voor de aanpak van Cyber Security . Daarvoor is wel nodig dat bedrijven in vertrouwen hun informatie kunnen delen met het centrum. Klopt het – ik geloof dat collega Elissen daar ook aan heeft gerefereerd – dat de WOB, de Wet openbaarheid van bestuur, daaraan op dit moment in de weg staat en, zo ja, is de minister dan niet bang dat dit de publiek-private samenwerking ondermijnt? Mijn vierde vraag, tot slot, is of het centrum ook een meldpunt is. Ook dat vraagt om een duidelijk antwoord. Als bedrijven of organisaties te maken krijgen met een nieuwe en acute ICT-dreiging kunnen zij terecht bij het NCSC. Weten de bedrijven en organisaties uit de relevante sectoren dat? Is hierover voorlichting gegeven? Wat is na de melding precies de rol van het centrum? Welke bevoegdheden heeft het centrum? Kan de minister hierover meer duidelijkheid geven?
In het debat over nationale veiligheid heb ik ook een vraag gesteld over de rol van Defensie. Toen wij over Cyber Security spraken, heb ik gevraagd: waar is Defensie? De minister en staatssecretaris van Veiligheid en Justitie en de minister van Binnenlandse Zaken zitten hier nu achter de tafel. Ik zie wel een groen pak in de zaal, maar er zit niemand van Defensie achter de tafel. Hoe is de afstemming met Defensie? Dat was mijn laatste vraag.

Voorzitter: Çörüz

De **voorzitter**: Het woord is aan de minister van Veiligheid en Justitie. Ik sta de leden twee interrupties toe, met per interruptie een vervolgvraag.

Minister **Opstelten**: Voorzitter. Ik dank de leden voor hun inbreng. Het lijkt mij goed om eerst even in te gaan op de verdeling van verantwoordelijkheden, mede gelet op de inbreng van de heer Çörüz, die vroeg naar de rol van de minister van Defensie. De verantwoordelijkheden van de bewindslieden aan tafel zijn helder. Cyber Security is een prioriteit van het kabinet. Ik heb de eer om deze te mogen coördineren en de regie te mogen voeren voor zover aspecten van nationale veiligheid aan de orde zijn. Mijn collega van Binnenlandse Zaken behartigt dit thema voor zover de positie van de overheid in het geding is. De staatssecretaris gaat over de privacy en het wetsvoorstel voor het voorkomen van datalekken. Mijn collega van EL&I

gaat over de toepassing van de Telecommunicatiewet; hij draagt ook de verantwoordelijkheid voor de OPTA. De positie van de minister van Defensie is helder: hij gaat over de externe veiligheid en de krijgsmacht. Er zijn ook internationale aspecten aan dit onderwerp verbonden, zodat de minister van Buitenlandse Zaken hierin ook een rol speelt. Verder kunnen er op elk terrein verantwoordelijkheden zijn. Er zijn bijvoorbeeld ook vragen gesteld die bestemd zijn voor mijn collega van VWS. Andere collega's kunnen op dit onderwerp ook hun verantwoordelijkheid nemen. Het is belangrijk om dat even aan te geven.
Vele commissieleden hebben gezegd dat er in het afgelopen jaar een hele ontwikkeling tot stand is gekomen. Mevrouw Hachchi heeft bijvoorbeeld gesproken over het Cyber Security Beeld Nederland, het assessment en het juridisch kader daarbij. Ik zal de gestelde vragen beantwoorden aan de hand van een paar thema's.
De VVD-woordvoerder heeft gevraagd naar het Cyber Security Beeld Nederland. Het is de eerste keer dat we een Cyber Security Beeld hebben gegeven. Het is een nulmeting. De focus is geweest om informatie van politie en inlichtingendiensten in dit beeld te verwerken. De Cyber Security Raad heeft het kabinet geadviseerd over het Cyber Security Beeld Nederland. Zowel publieke partijen, als private partijen, als wetenschappers hebben zitting in die raad. De raad herkent zich goed in het Cyber Security Beeld Nederland en onderschrijft de daarin genoemde dreigingen. Daarnaast adviseert de raad het kwalitatief en kwantitatief verder versterken van het Cyber Security Beeld Nederland. Om dit te bereiken zal het Nationaal Cyber Security Centrum over meer informatie van de private partijen moeten beschikken. Het versterken van het Cyber Security Beeld Nederland is een continu proces. Medio dit jaar zal het kabinet het tweede Cyber Security Beeld Nederland naar de Kamer sturen. Dit zal op een paar punten worden aangescherpt. De opmerkingen van mevrouw Hennis zijn zeer to the point. Dit is het eerste beeld dat wij via informatie van onze eigen diensten hebben gekregen, nadat het door de molen van de raad is gegaan, met het advies van kwalitatieve en kwantitatieve aanscherping.
Mevrouw Hennis heeft ook gevraagd of alle beschikbare informatie en voorbeelden zijn verstrekt, of dat bepaalde informatie niet is opgenomen in verband met het vertrouwelijke karakter ervan. Voor het CSBN 2011 is ook informatie aangeleverd door de inlichtingen- en veiligheidsdiensten. Elementen hiervan hebben een vertrouwelijk karakter. Het CSBN 2011 moet publiek toegankelijk zijn. Gezien het publieke karakter van dit beeld wordt op bepaalde aspecten niet in detail ingegaan.
Mevrouw Hennis heeft mij gevraagd om betreffende het assessment en het Cyber Security Beeld Nederland te reageren op de opmerkingen van de critici. Assets zijn inderdaad een belangrijk onderdeel van het CSBN. In mijn brief van 23 december heb ik al gemeld dat ik de aanbevelingen van de raad op dit punt onderschrijf. Het lopende project Kwetsbaarheidsanalyse Spionage Nederland draagt bijvoorbeeld bij aan het inzichtelijk maken van belangen, van assets. Het CSBN zal kwalitatief en kwantitatief verder ontwikkeld moeten worden. Iedere keer zal het beeld worden aangescherpt en zullen de assets worden aangepunt.
De heer Çörüz heeft gesproken over een nieuwe ontwikkeling die de aandacht vraagt, namelijk het toenemend gebruik van mobiele apparatuur. Hij heeft om een toelichting gevraagd. In het CSBN staat dat het toenemende gebruik van mobiele apparatuur een groeiend risico is. De verwachting is dat serieuze aanvallen, gericht op mobiele apparatuur, de komende jaren zullen toenemen. Hierbij kan gedacht worden aan het afluisteren van gsm-verkeer en het misbruik van mobiele apparatuur als gevolg van onder andere de mogelijkheid van mobiel betalen. Het Nationaal Cyber Security Centrum volgt deze ontwikkelingen nauwgezet en heeft hierover goed contact met de banken en andere organisaties. Het zal hierover adviseren als dat noodzakelijk is.

Velen hebben suggesties gedaan, vragen gesteld of opmerkingen gemaakt over het centrum. De heer Elissen heeft gevraagd of het centrum nauwgezet moet samenwerken met het bedrijfsleven. Het antwoord daarop is «ja». Dat wordt ook al gedaan. De ambitie van het centrum is om de digitale weerbaarheid van de Nederlandse samenleving te vergroten. Het succes van het centrum hangt af van de inbreng van kennis en kunde van zowel publieke als private partijen. Wij hebben hierover eerder gesproken met elkaar. In 2012 wordt ingezet op de aansluiting van vitale sectoren bij het centrum. Op dit vlak zijn reeds goede stappen gezet, zoals de deelname van private partijen aan de publiek-private ICT Response Board. Tevens worden in 2012 de Information Sharing and Analysis Centers aangesloten bij het centrum.
De heer Çörüz heeft gevraagd wat de formele verantwoordelijkheden van het centrum zijn. Hij vroeg of het centrum gaat fungeren als een spin in het web. Dat is natuurlijk de crux. Als minister ben ik verantwoordelijk voor het handelen van het centrum. Het centrum richt zich vooral op advisering van de overheid en de vitale sectoren. Daarnaast heeft het centrum een brede kennis- en adviesfunctie voor de samenleving. Zo worden de burgers en het midden- en kleinbedrijf onder andere via de website van het centrum voorzien van algemene kennis en adviezen. Binnen het centrum wordt samengewerkt met diverse partijen, zoals de AIVD, het NFI, het ministerie van Defensie, de politie et cetera. Deze rol kan men zeker zien als die van een spin in het web. Er treedt dus geen versnippering op; alles komt op één plaats bij elkaar en dat is het centrum. Bij ICT-incidenten waarbij de nationale veiligheid in gevaar is of dreigt te komen, heb ik als minister van Veiligheid en Justitie een bijzondere rol als coördinerend bewindspersoon voor de nationale veiligheid. Ik zal daar straks nog meer over zeggen. Binnen de nationale crisisstructuur heeft het NCSC een specifieke, operationeel coördinerende rol, namelijk het leveren van een adequate respons bij ICT-incidenten, zoals het KPN-incident.
De heer Elissen heeft gezegd dat de overheid snel over relevante informatie moet komen te beschikken om ervoor te zorgen dat Nederland veilig is. Hij heeft gevraagd of ik het met hem eens ben dat de beveiligingssystemen van bedrijven bekend moeten zijn bij het NCSC. Mijn antwoord is «nee». Het NCSC is geen toezichthouder die beveiligingsarrangementen van alle bedrijven opvraagt. Het succes van het centrum hangt af van de inbreng van kennis en kunde van zowel publieke als private partijen. Een goede samenwerking, vertrouwen en het kunnen delen van informatie zijn daarbij belangrijke randvoorwaarden. Er moet uiteraard rekening worden gehouden met de vertrouwelijkheid van de informatie. De leden Elissen en Çörüz hebben hierover gesproken. Het vertrouwelijk kunnen delen van informatie is een belangrijke randvoorwaarde voor het succes van het centrum.
Een andere vraag was of het klopt dat de WOB samenwerking binnen het centrum in de weg staat. Dat moeten wij heel goed en precies onderzoeken. Om de publiek-private samenwerking te versterken, wordt in het NCSC momenteel samen met publieke en private partijen onderzocht hoe een omgeving kan worden gecreëerd waarbinnen partijen hun informatie op een veilige en vertrouwelijke wijze met elkaar kunnen delen. Daarbij wordt onder andere gekeken naar de ervaringen die zijn opgedaan binnen de bestaande samenwerking op het gebied van Cyber Security , zoals de Information Sharing and Analysis Centers van het Informatieknooppunt Cybercrime.
De heer Çörüz heeft gevraagd of het centrum ook een meldpunt is. Als een bedrijf of andere organisatie te maken krijgt met een nieuwe en acute ICT-dreiging kan het terecht bij het centrum. De heer Çörüz vroeg of organisaties uit de relevante sectoren weten dat het centrum bestaat. Is hierover voorlichting gegeven? Wat is na de melding precies de rol van het centrum? Ik heb een aantal documenten voor mij en er zijn er nog meer. Dit soort boeken is als voorlichtingsmateriaal de wereld in gegaan.

Er zijn er veel meer: over cloudcomputing, ICT-beveiligingsrichtlijnen voor webapplicaties, herkenning en aangifte van cybercrime et cetera. Inmiddels ken ik ze wel uit mijn hoofd. Ik kan aanbevelen ze te lezen. Sommigen van u zijn op bezoek geweest bij het centrum. Het bestaat uit buitengewoon enthousiaste, bekwame, heel goede mensen. Tegen mevrouw Hachchi zeg ik dat we met de werving volledig op schema liggen. We nemen natuurlijk alleen genoegen met de besten die we kunnen krijgen. Het antwoord is dus «ja», als het gaat over het meldpunt. Organisaties uit de relevante en vitale sectoren die te maken krijgen met een nieuwe en acute ICT-dreiging kunnen bij het centrum terecht. Het centrum zal advies geven en een coördinerende rol vervullen. Het centrum heeft samengewerkt met KPN ten tijde van de digitale inbraak in diens systemen. Op dit moment wordt gewerkt aan de invulling van de motie-Hennis-Plasschaert c.s. (26643, nr. 202 herdruk) over de wettelijke meldplicht, de «security breach notification». Ik heb al eerder gezegd dat ik de Kamer daarover vóór het zomerreces meer duidelijkheid zal geven. Dit is een cruciale motie, breed gesteund ook. Dit betreft een kernpunt van ons beleid; je geeft hiermee namelijk duidelijk aan wat de verantwoordelijkheden zijn van de overheid en de andere partijen.

Mevrouw **Hachchi** (D66): De minister blijft de toch al hoge verwachtingen ten aanzien van het NCSC hooghouden. Ik hoor hem verwijzen naar de stukken en suggereren dat we allemaal rustig kunnen gaan slapen; althans, ik krijg het gevoel dat we worden gerustgesteld. Ik vind het terecht dat dit kabinet Cyber Security de aandacht geeft die deze nodig heeft, maar ik vraag me af of de daarvoor benodigde middelen wel worden vrijgesteld. De minister stelt dat er een capaciteitsuitbreiding aankomt, maar waarover hebben we het dan? Het centrum heeft namelijk nogal een takenpakket.

Minister **Opstelten**: De middelen die we beschikbaar hebben gesteld, zitten in de begroting. Ik denk dat wij op dit punt alle aangekondigde slagen op het gebied van Cyber Security hebben gemaakt; in ieder geval alle toezeggingen over wanneer dat centrum zou komen, het assessment, het juridische kader. En het gaat verder, het is natuurlijk nog niet klaar. Als de formatie van het centrum op orde is, is het ook nog niet klaar. Het Cyber Security Beeld zal nog veel verder moeten worden ontwikkeld. Ik kom zo dadelijk te spreken over het juridisch kader; ook dat zal namelijk dynamisch zijn. Wij moeten uiteraard voortdurend kijken naar de bevoegdheden die uiteindelijk nodig zijn. Ik kan prima publiek-privaat samenwerken, maar op een bepaald moment is er gewoon een verantwoordelijkheid voor de overheid. Wij moeten deze formuleren; vandaar dat het kabinet voor het zomerreces zal aangeven hoe het de motie-Hennis-Plasschaert c.s. gaat uitvoeren.

Mevrouw **Hachchi** (D66): Als het NCSC in ontwikkeling is en er een uitbreiding komt, kan de minister dan iets concreters zeggen over de hoeveelheid personeelsgroei en binnen welk tijdsbestek, zodat we een beter beeld hiervan hebben? Ik kan me namelijk voorstellen dat dit nogal een uitdaging is in tijden van bezuinigingen. Ik wil dus graag concreet weten hoe het NCSC zal worden versterkt en met welk tijdpad.

Minister **Opstelten**: Het zal groeien tot een centrum van 45 tot 65 man. Dat is aangegeven in de begroting, daar zijn ook middelen voor. Ik zeg niet dat dit het einde is, het is niet statisch. Wij zijn daar nu mee bezig en het loopt volgens planning.
De heer Recourt had het over hardheid ten opzichte van het bedrijfsleven. Het NCSC is geen toezichthouder die de beveiligingsarrangementen van alle bedrijven opvraagt. Dat moeten we ook niet hebben, want dan gaat iedereen achteroverleunen, terwijl iedereen zijn eigen verantwoorde-

lijkheid moet dragen. Het succes van het centrum hangt af van de inbreng van kennis en kunde van zowel publieke als private partijen, van een goede samenwerking en het vertrouwelijk kunnen delen van informatie. Daarbij gelden belangrijke voorwaarden. Ik kom zo dadelijk terug op de crisisstructuur.
De heer Çörüz vroeg welke plannen er bestaan voor het vergroten, via het centrum, van het bewustzijn van cyberdreigingen bij het grote publiek. Ik heb wat beelden hiervan gezien. Wij zeggen absoluut niet dat iedereen wel kan gaan slapen, integendeel. De sense of urgency rondom deze problematiek moet bij iedereen tussen de oren komen te zitten. De vergroting van het bewustzijn bij het grote publiek is buitengewoon belangrijk. Ik zal bij de uitwerking van de plannen samenwerken met het Platform voor de InformatieSamenleving, bekend van eerdere campagnes. Het centrum bedient het grote publiek via zijn website waarschuwingsdienst.nl. Een paar weken geleden is via waarschuwingsdienst.nl gewaarschuwd voor een mogelijke besmetting van de website nu.nl.
Mevrouw Hachchi stelde een vraag over de werving. Aan de werving en selectie wordt hard gewerkt. Een en ander verloopt volgens planning, want in deze situatie vindt men het een feest om daar te werken. De crisisstructuur is op zichzelf helder, want het is dezelfde structuur die wij nationaal hebben en die bijvoorbeeld is toegepast bij DigiNotar. Het uitgangspunt van crisisbeheersing op nationaal niveau is het Nationaal Handboek Crisisbesluitvorming. Daarnaast bestaat het generieke Nationaal Crisisplan, waarop het Nationaal Crisisplan ICT een aanvulling vormt. In interdepartementaal verband is vorig jaar het Nationaal Crisis Plan ICT ontwikkeld, waarin de crisisstructuur in het specifieke geval van een ICT-crisis is vastgelegd. Er is verschillende malen met deze crisisstructuur geoefend. Omdat Cyber Security zich snel ontwikkelt, in verschillende omgevingen – publiek, privaat, civiel, militair – en met verschillende actoren, is het van belang om op gezette tijden, aan de hand van incidenten en oefeningen, te bezien of de huidige crisisstructuur voor ICT-crises moet worden aangepast. De Inspectie Openbare Orde en Veiligheid evalueert de crisisaanpak met betrekking tot DigiNotar. Dit gaat voor de zomer naar de Kamer. Als de nationale crisisstructuur is toegepast, als sprake is van de Interdepartementale Commissie Crisisbeheersing (ICCb) en de Ministeriële Commissie Crisisbeheersing (MCCb), komt er altijd een evaluatie. Of de minister-president of ikzelf deze MCCb voorzit, hangt af van het overleg tussen de minister-president en mijzelf. De andere rechtstreeks betrokken verantwoordelijke bewindslieden zijn daarbij.

De heer **Elissen** (PVV): Om even alle verwarring weg te nemen: is er nu wel of geen openbaar Nationaal Crisisplan? Op de website van het Nationaal CrisisCentrum wordt aangekondigd dat dit voor de zomer van 2012 gereed zal zijn. Ik vind dit wat verwarrend, misschien kan de minister het even wat duidelijker formuleren.

Minister **Opstelten**: Als u dat op prijs stelt, kunt u het ICT-crisisplan toegezonden krijgen. Zoals elk crisisbeheersingsplan is ook dit dynamisch van karakter; telkens wordt het na toepassing geëvalueerd en voorzien van verbeteringen en nadere accenten. Ik heb er geen enkel bezwaar tegen om dit naar de Kamer te zenden.

De heer **Elissen** (PVV): Begrijp ik dat het nu in een soort afstemmingsfase zit, dat de laatste puntjes op de i worden gezet, dat het nog een ambtelijke status heeft en in ieder geval, zoals op de website van het NCC staat, voor de zomer van 2012 gereed is? Of is de informatie op de website niet in orde?

Minister **Opstelten**: Nee, die is in orde. Er is een ICT-crisisplan, alleen de zaken veranderen telkens. Het nationale centrum, dat nog niet zo lang geleden van start is gegaan, moet er nu in geschreven worden en een plaats krijgen. Het gaat dus om een bijstelling van het plan. Wij zijn bereid om wat nu voorhanden is, naar de Kamer te zenden, maar misschien kan dit ook even wachten tot de laatste versie. Die is ook voor de zomervakantie beschikbaar. Het is prettig dat de heer Elissen dit heeft gevraagd, dan kunnen we ook op dat gebied de puntjes op de i zetten. Ik hoor het zo dadelijk graag.
Mevrouw Hennis van de VVD-fractie vroeg aan mij welke aanvullende instrumenten ik denk om de digitale veiligheid te bevorderen. Wij maken hierbij gebruik van verschillende middelen. Op internationaal niveau worden afspraken gemaakt met verschillende landen, bijvoorbeeld recent een intentieverklaring met de Verenigde Staten, waarover ik de Kamer een brief heb gestuurd. Op nationaal niveau wordt hard gewerkt aan het verhogen van de digitale veiligheid. Wij zullen in het kader van het nationaal centrum in gesprek gaan met leveranciers van hardware en software, om de digitale veiligheid te vergroten.
Welke aanvullende bevoegdheden worden overwogen? Als minister van Veiligheid en Justitie ben ik de coördinerende bewindspersoon voor de nationale veiligheid bij ICT-incidenten waarbij de nationale veiligheid in gevaar is of dreigt te komen. Op dit moment wordt onderzocht of, en zo ja welke, aanvullende bevoegdheden nodig zijn. Voor de zomer rapporteren wij daarover aan de Kamer. De resultaten van de onderzoeken van de Inspectie Openbare Orde en Veiligheid naar aanleiding van de DigiNotar-kwestie zullen hierin worden meegenomen. Ik zal de Kamer vóór het zomerreces informeren over de uitkomsten van het onderzoek.
Een aantal leden sprak over het juridisch kader. Dat betreft natuurlijk altijd de bevoegdheden, de opsporingsbevoegdheden, het buitenland. De heer Recourt sprak over het pleidooi van de Nationale Recherche en het OM voor wettelijke instrumenten. Ik wijs erop dat het European Cybercrime Centre in Den Haag zal worden gevestigd; misschien heeft u dat al in de media gelezen. Dat is een prettige beslissing van Commissaris Malmström. Over dit onderwerp heeft de Kamer schriftelijke vragen gesteld, die ik medio maart heb beantwoord. Het vorige kabinet heeft zich in 2010 laten adviseren over een aantal conceptwetsvoorstellen. Het adviestraject had als uitkomst dat er meer tijd nodig is voor de daadwerkelijke wetsvoorstellen. Ik zal de Kamer vóór de zomer van 2012 hierover nader berichten. Gelet op het inherent grensoverschrijdende karakter van cybercriminaliteit is internationale regelgeving net zo belangrijk, wat natuurlijk betekent dat je van tijd tot tijd moet durven spreken over je soevereiniteit en autonomie. Nederland is actief hierbij betrokken, vooral via het comité van verdragsluitende partijen bij het Cybercrimeverdrag van de Raad van Europa. Ook in de Brusselse arena is de afstemming tussen nationale en internationale kaders essentieel. Gelet op het belang van ieder land bij de nationale soevereiniteit is dit geen zaak die op korte termijn, op nationaal én internationaal niveau, kan worden geregeld.

Mevrouw **Hennis-Plasschaert** (VVD): Dank aan de minister voor deze hoeveelheid woorden. Ik vroeg naar de internationale trajecten waaraan de minister refereerde in zijn brieven. Hij verwijst in dat kader naar de Letter of Intent Cyber Security. Dat vind ik op zich prima, maar het is iets anders dan de trajecten waarin wordt gekeken naar de noodzakelijkheid van de aanpassing van wet- en regelgeving. Het kan zijn dat ik de letter of intent niet goed heb begrepen, maar volgens mij moet dit ook in Europese context worden gedaan. Ik hoop in ieder geval niet dat de 27 EU-lidstaten allemaal zelf het wiel moeten gaan uitvinden; dan wordt het namelijk helemáál een patchwork van allerlei mogelijkheden. Ik wil ook graag weten op welke punten het juridische kader tekortschiet voor overheidsinterventie ten tijde van dreigingen van cybercrises. Zoiets staat namelijk

zwart op wit in een van de stukken die ik vandaag heb zitten lezen voor dit AO. Ik ben daar nieuwsgierig naar en wil weten op welke punten dat huidige juridisch kader tekortschiet, voordat we weer doorschieten in het maken van allerlei aanvullende bevoegdheden die we misschien wel of niet nodig zullen hebben.

Minister **Opstelten**: Laat ik iets zeggen over de eerste arena. Het is duidelijk dat de Brusselse en Straatsburgse arena hierin erg actief zijn. Nederland speelt daarin een prominente rol, met een paar andere landen. Dit is echter niet iets wat je kunt beperken tot Europa; dit speelt wereldwijd. Tijdens mijn bezoek aan Washington heb ik gesproken met mijn collega Janet Napolitano. Daar was een heel goede uitwisseling tussen onze mensen, wetenschappers en deskundigen, ook Amerikaanse. Wij hebben niet van tevoren opgeschreven wat er volgens ons in die letter of intent moest staan, de inhoud is op dat moment tot stand gekomen. Ik was daar zelf bij en kon het ook samenvatten, dus dat is belangrijk.
Bij ICT-incidenten waarbij de nationale veiligheid in gevaar is of dreigt te komen, heb ik als minister van Veiligheid en Justitie een bijzondere rol waar te maken: die van de coördinerend bewindspersoon voor de nationale veiligheid. Het is duidelijk dat de bevoegdheden vaak per sector zijn geregeld, evenals het toezicht. De vraag of extra bevoegdheden op het gebied van Cyber Security nodig zijn, wordt meegenomen in de toezegging aangaande het onderzoek naar aanvullende interventiemogelijkheden. Nu is niet zomaar te zeggen wat die moeten behelzen, dit moet zorgvuldig worden bekeken. Ik zal de Kamer vóór het zomerreces over de uitkomsten van het onderzoek informeren. Ik verwijs hiervoor ook naar de internationale trajecten. Ik kan een voorbeeld geven van de resultaten van Nederlandse druk. In het zogenaamde «Stockholm Programma» van de EU is opgenomen dat het juridisch kader op dit punt vóór 2015 moet worden bekeken en zo mogelijk zal moeten worden geüpdatet aan de hand van de nieuwe Cyber Security vereisten. Zoals mevrouw Hachchi zei, het is heel belangrijk dat dit geüpdatete juridische kader wordt getoetst aan elementen van de Grondwet, grondrechten en wat dies meer zij. Natuurlijk moet dit ook worden getoetst aan de bestaande wetgeving op het gebied van de terrorismebestrijding. Ik zeg niet dat het allemaal hetzelfde moet zijn. We gaan alles gewoon heel goed bekijken. Ik wil dit proces van fase tot fase met de Kamer delen, zodat we dit samen kunnen volgen. Het is veel te belangrijk om dit niet te doen.

Mevrouw **Hennis-Plasschaert** (VVD): Het is inderdaad geen probleem dat zich tot Europa beperkt en wij moeten inderdaad mondiaal opereren. Ik bepleit alleen wel dat de lidstaten gezamenlijk optrekken, dat we ons niet door de Amerikanen uiteen laten spelen. De letter of intent juich ik toe, die is verder prima, evenals de Nederlandse voortrekkersrol, maar ik blijf een enigszins harmonieus optrekken van de 27 EU-lidstaten bepleiten. Begrijp ik het goed dat informatie over de eventuele aanvullende bevoegdheden, en dus ook over de punten waarop het juridisch kader tekortschiet, vóór het zomerreces naar de Kamer wordt gezonden? In dat geval raad ik de minister aan om het in het vervolg iets minder zwart-wit in zijn brief op te nemen. Als ik word gealarmeerd met de boodschap dat het huidige juridische kader tekortschiet, wil ik namelijk weten op welke punten dat is en hoe we dit probleem gaan oplossen. Dat was nog niet het geval.

Minister **Opstelten**: Dat laatste ben ik met u eens. Het was natuurlijk ook het assessment, het beeld, en op verzoek van de Kamer heb ik daarbij het juridische kader gegeven. Het is pas een start en zo wil ik het nu ook nadrukkelijk noemen. Het is nog weinig concreet. Ook ik ben uit het hout gesneden dat ik zo snel mogelijk wil weten waarover we het precies hebben, zodat ik daarover met u kan discussiëren. Op deze manier krijgt u

wel een impuls om hier zelf mede richting aan te geven. Ik zou dat ook waarderen.

De heer **Recourt** (PvdA): Een vraag over hetzelfde punt, om dit toch wat concreter te maken. Ik heb al twee zaken gehoord. De Kamer krijgt vóór de zomer een brief over de wettelijke veranderingen op dit punt. Ik vraag de minister of ik het goed heb gehoord dat uiterlijk in 2015 de Europese wetgeving op dit punt op orde is, een en ander in het kader van het Stockholm Programma. Maar wat doen we tot die tijd met informatie die de politie vergaart zonder wettelijke grondslag?

Minister **Opstelten**: De eerste punten kloppen. Het voornemen is om in 2015 het Stockholm Programma gereed te hebben. Wij moeten dit dus volgen en hier een prominente rol in spelen. De andere zaken kloppen ook. Vóór de zomer worden die verder ontwikkeld.
De heer Recourt vroeg naar de aanpak van cybercrime door de politie, hoe het zit met het bewijs, hoe het opsporen zal moeten gaan op de korte termijn. Ik neem aan dat ook hij bij de politie op bezoek is geweest. Het gebruik van bij opsporing verkregen bewijs met betrekking tot hackers als zulks mogelijk niet toelaatbaar is, doet zich in de kern niet voor in Nederland. Voor dergelijke zaken zijn er internationale samenwerkingsverbanden. Zo is het bewijs in de BredoLab-zaak bijvoorbeeld overgedragen aan de opsporingsinstanties in de Verenigde Staten, om de verdachten uit de Verenigde Staten voor de rechter te kunnen brengen.
Dit is gelijk een opstapje naar de vraag van mevrouw Hachchi over de ethische hackers: moeten die eenduidig worden behandeld?

De **voorzitter**: Voordat u verder gaat, minister, heeft de heer Recourt nog een opmerking en dan kunnen we dit stukje afsluiten.

De heer **Recourt** (PvdA): Ik ben ondertussen heel hard aan het zoeken naar het krantenbericht waarin staat dat de politie soms illegaal bezig is, bijvoorbeeld bij het ophalen van gegevens die in het buitenland zijn opgeslagen.

Minister **Opstelten**: Zij zoeken natuurlijk de grenzen op, maar gaan daar niet overheen. Tenminste, daar ga ik van uit. Uiteindelijk – maar dat hoef ik de heer Recourt niet te vertellen – is het de rechter die daar een beslissing over neemt. Dat is duidelijk. Daarvoor moet nog jurisprudentie ontwikkeld worden. Dat volgen wij natuurlijk met spanning.
Dan kom ik bij het punt van mevrouw Hachchi over de ethische hackers, waar mijn collega Spies ook nog op in zal gaan. Het is van belang dat hackers eenduidig worden behandeld. Op dit moment wordt gewerkt aan de procedure van responsible disclosure. Hierbij wacht de hacker met openbaarmaking van een lek totdat het lek is gedicht. Het Nationaal Cyber Security Centrum speelt hierin een rol als intermediair om kennis van hackers bij bedrijven te adresseren. Verder wordt onderzocht hoe ethische hackers op een verantwoorde wijze een rol kunnen spelen bij het inzichtelijk maken van kwetsbaarheden. Volledigheidshalve betekent dit niet dat hackers een vrijbrief krijgen om lekker aan de slag te gaan. Dat standpunt is mevrouw Hachchi al bekend uit het DigiNotar-debat.
De heer Çörüz vroeg wat er gebeurt op het gebied van de internationale samenwerking. Dit is ook een prioriteit van de EU in het domein van recht en ruimte. Het onderwerp is geregeld aan de orde in de JBZ-Raad.
Mevrouw Gesthuizen en de heer Recourt vroegen wat ik denk te doen aan de verplichting om te melden. Mevrouw Hennis-Plasschaert heeft in dit verband de motie over een security breach notification ingediend (26 643, nr. 202). Voor de zomer zal ik de Kamer hierover informeren.

De **voorzitter**: Mevrouw Hachchi heeft een vraag aan u. Dit wordt haar tweede interruptie.

Mevrouw **Hachchi** (D66): Ja, dit wordt mijn tweede interruptie. Ik ken het standpunt van de minister naar aanleiding van het debat over DigiNotar. Toen waren minister Donner en minister Opstelten van mening dat niet moet worden gekeken naar de positie van hackers die bij de overheid aan de bel trekken. Begrijp ik hieruit dat er wel een richtlijn komt? Ik heb opgeschreven dat aan responsible disclosure wordt gewerkt.

Minister **Opstelten**: Dat is de bedoeling. Wij zijn daarmee bezig. Mijn collega van BZK zal hier ook op ingaan. Wat dat betreft, werken wij binnen de marges die ik toen heb aangegeven. In het centrum hebben wij de kennis beschikbaar om te kunnen hacken. Die kennis moet er natuurlijk zijn. Mij is voorgedaan hoe je dat doet. Ik weet het. Ik zeg het niet, maar ik weet het wel. Wij zijn die kennis dus enorm aan het ontwikkelen om zo goed mogelijk beslagen ten ijs te komen.

Mevrouw **Hachchi** (D66): Mijn vraag was heel duidelijk: komt er een richtlijn voor hoe de overheid moet omgaan met hackers die zich op een eenduidige manier melden? Dan is er in ieder geval een kader voor de overheid als zij door een hacker wordt benaderd.

Minister **Opstelten**: Ik houd meer van het woord kader dan van het woord richtlijn.

Mevrouw **Hachchi** (D66): Responsible disclosure, het is een soort kader of richtlijn.

De **voorzitter**: Ook de heer Elissen heeft een vraag op dit punt. Het is ook zijn tweede interruptie.

De heer **Elissen** (PVV): Als ik de woorden responsible disclosure hoor, denk ik aan een verantwoorde ontsluiting. Ik hoop toch echt niet dat we gaan bevallen van een overbodige richtlijn. Volgens mij zijn hier binnen de wettelijke kaders al regelingen voor. Heb ik dat goed begrepen?

Minister **Opstelten**: Dat hebt u redelijk goed begrepen, maar toch is het, gelet op het debat, nodig om in een kader aan te geven wat wel en wat niet kan.

De heer **Elissen** (PVV): Wat ons betreft, is redelijk duidelijk wat wel en wat niet kan, maar als u zegt dat u tot een aanscherping en verduidelijking komt, kunnen wij dat uiteraard van harte steunen.

Minister **Opstelten**: Dan ga ik door met de vraag van mevrouw Gesthuizen over het KPMG-onderzoek. Slechts een op de vijf bedrijven acht zich in staat om een aanval af te slaan. Steeds meer bedrijven worden zich bewust van de risico's. Je merkt dat absoluut. Het is zaak om awareness te verhogen. Het centrum vervult die expertiserol en brengt dagelijks adviezen, white papers, factsheets en dat soort zaken uit. Het vraagt wel om een gezamelijke inspanning. We moeten als overheden met verschillende verantwoordelijkheden samen met de private markt dat centrum bemensen.

Mevrouw **Gesthuizen** (SP): Ik snap natuurlijk ook wel dat het niet gemakkelijk is als je als overheid zelf nog zo veel te leren hebt om dan anderen de les te lezen. Toch moeten we dat doen. Ik geloof er niet in dat we er alleen maar komen met white papers, factsheets en dat soort zaken. Ik verwacht van deze regering echt meer. Ik verwacht dat hier wel

regelgeving voor komt, hoewel het niet helemaal dichtgeregeld hoeft te worden.

Minister **Opstelten**: Dan kom ik op het punt dat wij het juridisch kader nog aan het bekijken zijn en dat dit voor het zomerreces terugkomt. De taak van het centrum is drieledig. Ten eerste moeten we de kennis bij elkaar krijgen. Ten tweede moeten we een goede strategie ontwikkelen. Ten derde – niet onbelangrijk – moeten we een goede operationele responsfunctie kunnen waarmaken. Het is de overheid die in het kader van de nationale veiligheid uiteindelijk zegt: «dit moet gebeuren» of «nu is het einde oefening». Dit staat los van de verschillende verantwoordelijkheden, bijvoorbeeld de verantwoordelijkheid van de minister van EL&I voor het toezicht van Opta op de telecommarkt.

Mevrouw **Gesthuizen** (SP): Ik wil precies weten hoe het zit met het thema nationale veiligheid. Hoe breed of hoe eng moeten we dat zien? Wanneer raakt het aan de nationale veiligheid en wanneer valt het buiten de verantwoordelijkheid van de minister?

Minister **Opstelten**: Als er sprake is van ontwrichting van de samenleving. Die beoordeling moet ik telkens opnieuw maken. Daar ben ik verantwoordelijk voor. Als ik te snel vind dat de nationale veiligheid in het geding is, hebben velen daar last van. Dan moet ik daarover in de Kamer verantwoording afleggen. Ben ik te laat, dan moet ik dat ook doen. De thema's zijn bekend. Ontwrichting van de samenleving is een heel belangrijk punt. Dat kan heel klein beginnen. Op een gegeven moment moet ik ingrijpen. Daarom is de uitvoering van de motie van mevrouw Hennis-Plasschaert belangrijk. Daarin staat namelijk wanneer iemand zich moet melden. Het is niet goed om daarmee te wachten en telkens te proberen, het zelf op te lossen.
Dan kom ik bij de motie-Franken die door de heer Çörüz naar voren is gebracht. Wie zouden wij zijn als wij de motie-Franken niet serieus nemen en uitvoeren? Natuurlijk, het belang van de motie-Franken zit bij betrokkenen voldoende tussen de oren. Tijdens het AO over nationale veiligheid heb ik het belang van de motie-Franken benadrukt. Daarna heb ik in mijn brief van 23 december uiteengezet dat het kabinet zeer hecht aan de bescherming van de persoonlijke levenssfeer en dat het dit bij de formulering van nieuwe wet- en regelgeving op het terrein van Cyber Security zeer ter harte neemt. Ook de staatssecretaris zal daar zo dadelijk op ingaan.
Tot slot nog twee punten. Eerst een opmerking naar aanleiding van de vraag van mevrouw Hachchi over de pacemaker. Samen met mijn collega van VWS wordt gewerkt aan de beantwoording van de Kamervragen. Mijn collega van VWS zal deze vragen beantwoorden tijdens het AO van de commissie voor VWS op donderdag 12 april.
Mevrouw Hennis heeft gevraagd hoe ik tegenover de realisatie van de kwalificatieschema's sta, in het bijzonder tegenover de kwaliteitsborging van de beroepsgroep informatiebeveiligers. Het is van belang dat wij in Nederland een kwalitatief hoogwaardige groep informatiebeveiligers hebben. Initiatieven van de beroepsgroep op dit punt juich ik toe. Wij zullen zorgen dat wij met hen in gesprek komen en blijven.

De **voorzitter**: Ik dank de minister van Veiligheid en Justitie voor zijn antwoord en geef nu het woord aan de minister van Binnenlandse Zaken en Koninkrijksrelatie.

Minister **Spies**: Voorzitter. Ik bedank de leden voor hun vragen in eerste termijn. Wij hebben de afgelopen dagen allen ervaren hoe afhankelijk wij zijn geworden van moderne technologie, van ICT. Mevrouw Gesthuizen had daar vanmorgen nog een ervaring mee. We hebben zo ongeveer

allemaal geleden onder de Vodafone-perikelen van de afgelopen dagen. Dat geeft eens te meer aan hoe kwetsbaar onze samenleving is geworden door het soms niet goed functioneren van ICT. Wij zien allen het belang van het goed functioneren van ICT-voorzieningen en van het goed beveiligd zijn van deze voorzieningen. De overheid heeft met de DigiNotar-situatie een behoorlijke wake-upcall gekregen. Als je ziet wat er de afgelopen jaren in rij en gelid is gezet, is duidelijk geworden dat wij met z'n allen goed wakker zijn geworden. Ook de rijksoverheid is met de i-strategie en tal van activiteiten het been behoorlijk aan het bijtrekken. Dat is ook nodig.
Mevrouw Hennis zegt dat de regie in tijden van crisis daarbij cruciaal is. Zij vraagt of het kabinet voldoende doorzettingsmogelijkheden heeft op het moment dat er iets fout is. Op het moment dat er sprake is van een acute dreiging van een crisis of ramp treden tal van rampenplannen in werking en worden verschillende bevoegdheden opzijgeschoven. Ten aanzien van de rijksoverheid zijn er kabinetsbreed tamelijk sluitende afspraken. Ieder departement moet voldoen aan rijksvoorschriften. Ten opzichte van andere overheden en van het bedrijfsleven liggen de doorzettingsvragen anders. Die hebben eigen verantwoordelijkheden. Toen wij er bijvoorbeeld achterkwamen dat bepaalde overheidswebsites niet veilig waren, zijn deze uit de lucht gehaald. Dat waren er een stuk of veertig. In het kader van de mogelijkheden die wij met DigiD hebben, worden die sites op zwart gezet. Tot op de dag van vandaag is dat voor een van die overheidswebsites nog steeds het geval. In acute situaties hebben wij zeker doorzettingsmogelijkheden. Wij zullen in het kader van de voortgangsrapportages over de compacte rijksdienst in het bedrijfsvoeringsjaarverslag van het Rijk de Kamer blijven informeren over de voortgang van activiteiten die wij uitvoeren.
De heer Elissen heeft gevraagd naar de nadere stand van zaken ten aanzien van de moties die in het verleden zijn ingediend en aanvaard. Wij hebben daar in een brief van 9 november vrij uitvoerig antwoord op gegeven. Ik geef willekeurige voorbeelden. Ten eerste de motie-Elissen/Gesthuizen op stuk nr. 209, waarin de regering wordt verzocht om bij de ontwikkeling van nieuw te starten ICT-projecten privacy by design en safety by design toe te passen. Daarbij hebben wij heel nadrukkelijk aangegeven dat beveiligingskaders voor het Rijk een verplicht uitgangspunt zijn bij welk informatiesysteem dan ook.
De heer Elissen heeft ook een motie ingediend op stuk nr. 221 over eerstelijnstoezicht. De minister van EL&I en ik hebben daarover in een brief van 14 maart aangegeven dat Opta bedrijfsbezoeken gaat afleggen bij certificatenverleners, waarbij het systeem ter plekke gecontroleerd zal worden.
Dat zijn zo even voor het vaderland weg een aantal concrete activiteiten die wij inmiddels ter uitvoering van de moties hebben ontplooid.
De heer Recourt vraagt hoe wij aanbevelingen voortvloeiend uit het DigiNotar-rapport hebben verinnerlijkt en hij wil weten hoe wij dit soort situaties in de toekomst kunnen voorkomen. Hiervoor hebben wij een soort drietrapsraket ontwikkeld. In de eerste plaats proberen wij de weerbaarheid van bestaande systemen te vergroten, onder andere door de DigiD-assessments en het aanpassen van PKI-stelsels. Vervolgens proberen wij het responsvermogen van de overheid en de toezichthouders zo effectief mogelijk te laten zijn. Ik ben blij dat de onderzoeken die tot op heden zijn uitgevoerd, laten zien dat wij daarin redelijk adequaat hebben gehandeld. Ook proberen wij internationaal nog tot betere afspraken te komen dan misschien in het verleden het geval was.
Mevrouw Hachchi vraagt of wij in het vervolg op DigiNotar in beeld hebben of er in Iran negatieve consequenties zijn voortgevloeid voor mensen die daarbij betrokken zijn geweest. Ik kan in dit algemeen overleg niet meer melden dan dat wij de commissie voor de Inlichtingen en

Veiligheidsdiensten daarover hebben geïnformeerd en dat het gesprek daarover ook in die commissie gevoerd moet worden.
Mevrouw Hachchi refereert aan een vorig algemeen overleg waarin ik inderdaad heb aangegeven voornemens te zijn om met een aantal universiteiten of hogescholen een samenwerkingsverband aan te gaan om studenten een prachtige stageplek te gunnen. Het is de bedoeling dat zij ons lerenderwijs kunnen helpen bij het beter beschermen van overheidsinformatiesystemen tegen ongewenste invallen. Wij zijn op dit moment met een aantal universiteiten en hogescholen in gesprek. In de voortgangsrapportages waar ik net aan heb gerefereerd, zullen wij de Kamer verslag doen van de voortgang daarvan.
Mevrouw Hachchi en mevrouw Gesthuizen hebben beiden opgemerkt dat DigiD wellicht nog onvoldoende veilig is. Net voor 1 april hebben zo'n zeven miljoen mensen in Nederland weer met succes via DigiD hun belastingaangifte kunnen doen. Dat is zonder al te veel problemen verlopen. «Leuker kunnen we het niet maken, makkelijker wel», valt mij dan altijd weer in. Laten we wat dat betreft onze zegeningen tellen. Misschien mag ik met enige gepaste trots melden dat in een recent onderzoek van de Verenigde Naties Nederland op de tweede plaats van de wereld terecht is gekomen waar het gaat om de elektronische dienstverlening door de overheid. Dat is toch een prestatie van formaat als je ziet dat wij landen als Groot-Brittannië, Denemarken, de Verenigde Staten, Frankrijk, Zweden, Noorwegen, Finland en Singapore achter ons laten. Dit is ook een compliment aan al diegenen die daar hun best voor doen. Dit laat onverlet dat «goed» altijd «beter» kan. Wij luisteren ook naar signalen die tot een verdere verbetering kunnen leiden. De Ombudsman constateert dat er op dit moment bij DigiD nog één niveau van beveiliging is. Er is achter een tweede niveau, dat beschikbaar is. Wij werken daarnaast op wat dan het hoogste niveau heet, aan de zogeheten elektronische identiteit. Ik heb recent via de commissie voor Binnenlandse Zaken aangegeven dat ik de Kamer na de zomer hoop te kunnen informeren over de mogelijkheden die de elektronische identiteitskaart daarin zou kunnen vervullen.
Ik kom bij de vragen van mevrouw Gesthuizen. Natuurlijk is het even schrikken als je in een kop ziet staan dat een veilige overheid een illusie is. Als je dan het artikel waaraan mevrouw Gesthuizen refereert doorleest, blijkt dat het niet meer dan realistisch is om aan te geven dat een 100% veilige overheid, ook op het gebied van Cyber Security , een illusie is. Natuurlijk streven we naar een zo groot mogelijke veiligheid, maar wij zitten in een rat race tussen allerlei types met verkeerde bedoelingen, die wij vanzelfsprekend een stap voor proberen te blijven. Wij zijn daar tot op heden behoorlijk succesvol in. Ik kan hier echter geen garantie geven dat er voor 100% veiligheid is. Dan zou ik beloftes doen die ik niet waar kan maken en daar heb ik een hekel aan. Sterker nog, ik heb mezelf voorgenomen dat ik nooit beloftes zal doen die ik niet waar kan maken.
Mevrouw Gesthuizen heeft allerlei signalen gekregen dat mensen met ICT-kennis bij de overheid zouden vertrekken. Dat is niet het beeld dat ik heb. Sterker nog, ik hoor uit de ICT-wereld ook wel precies het omgekeerde, namelijk dat de overheid met zulke interessante projecten op het gebied van ICT bezig is dat daar een uitdaging voor heel wat ICT'ers in gelegen is, die om die reden juist proberen een plek bij de overheid te krijgen. Wij proberen overigens kennis vast te houden en verder te ontwikkelen, ook omdat er binnen het Rijk een i-interimpool is. Dat is een stevige pool van projectleiders op het gebied van ICT op bovendepartementaal niveau. Op die manier zal het Rijk voldoende kwaliteit en kunde in huis hebben.
Dat doet overigens ook het bureau KING, het Kwaliteitsinstituut Nederlandse Gemeenten. Dat bureau is ingericht als een soort deskundigheidspool voor gemeenten. Daar wordt veel kennis en kunde op bovengemeentelijk niveau verzameld en vervolgens gedeeld. Niet alle gemeenten

kunnen altijd over alle kennis beschikken, maar dit kan gefaciliteerd worden door het bureau KING. Er worden best practises verzameld en soms worden mensen gedetacheerd om tijdelijk een gemeente te ondersteunen bij het verbeteren van de ICT-dienstverlening. De dienstverlening van bureau KING wordt mede gefaciliteerd door het Rijk. De rijksoverheid stelt daar ook geld voor beschikbaar. De gemeenten leveren vanzelfsprekend ook individueel een bijdrage aan het bureau. Op die manier organiseren zij gezamenlijk een schaalgrootte die de gemeenten beter in staat stelt om de ICT-dienstverlening op niveau te brengen. Mevrouw Gesthuizen heeft daarnaast gezegd dat de beveiligingsassessments vertraagd zijn. Daar heeft zij helaas gelijk in. Dat heeft alles te maken met onvoldoende capaciteit zowel binnen de overheid als op de markt om alle assessments voor 1 april uitgevoerd te hebben. Wat mij betreft geldt het adagium liever goed dan snel. Zonder afbreuk te doen aan de noodzakelijke urgentie is er een fasering aangebracht. Daarbij zijn VNG en KING voluit ingeschakeld. Ik heb de Kamer erover geïnformeerd dat wij een ander tijdpad hebben moeten doorlopen dan aanvankelijk was gehoopt. De grootverbruikers moeten de assessments in 2012 hebben afgerond. In een eerder debat over ICT en de e<i-strategie heb ik de Kamer toegezegd dat ik in het bestuurlijk overleg met VNG en IPO aandacht zal vragen voor ICT-beveiliging. Het overleg met het IPO heb ik al gehad en het overleg met de VNG is op korte termijn voorzien.

Mevrouw **Gesthuizen** (SP): Op 11 oktober 2011 is ons nog meegedeeld dat alle gebruikers de ICT-beveilingsassessments op 1 april 2012 zouden moeten hebben doorlopen. Dat was dus vorige week. Daar wordt nu dus van afgeweken. Het verhaal dat veiligheid niet voor 100% gegarandeerd kan worden, hoor ik al heel erg lang. Dat begrijp ik ook wel. Iedereen weet dat er onwaarheden worden verkondigd als wordt gesteld dat alles voor 100% veilig wordt gemaakt. Dat kan niet. Ik maak er echter bezwaar tegen dat men bepaalde zaken laat liggen. Het duurt te lang voordat onze eisen zijn ingewilligd. Daardoor kunnen wij ook niet in de buurt van die 100% veiligheid komen.

Minister **Spies**: Wij laten niks liggen; zeker niet! Eind februari heb ik de Kamer gemeld dat de oorspronkelijke planning van begin oktober 2011 veel te optimistisch was. In oktober vorig jaar hadden wij de hoop dat wij in elk geval alle assessments van de grootverbruikers voor 1 april 2012 klaar zouden hebben. De daarvoor benodigde capaciteit op de markt is er gewoon niet. Wij willen het goed doen. Wij willen juist niks laten liggen en daarom houden wij vast aan de kwaliteitseisen. Omdat wij willen borgen dat al die assessments uiteindelijk tot het gewenste resultaat leiden, hebben wij heel 2012 nodig om het traject voor de grootverbruikers te doorlopen. Ik zou graag willen dat het sneller kon, maar op basis van de kennis die ik nu heb, weet ik dat dit echt niet voor eind 2012 lukt. Daarbij laten wij dus zeker niets liggen.

Mevrouw **Gesthuizen** (SP): Volgens mij laat de minister wel iets liggen. We moeten namelijk een jaar lang doorgaan in de onzekerheid of iets wel veilig is. Het kan gebeuren dat je een te optimistische inschatting maakt, maar hoe zit het nu met de urgentie? Uit alle correspondentie van het kabinet die ik dit najaar over ICT en veiligheid heb ontvangen, sprak een enorme urgentie. Er was een wake-upcall. Men zat er in één keer bovenop. Ik heb het gevoel dat dit nu al weer aan het wegebben is. Over welke datum hebben wij het nu eigenlijk precies? De grootverbruikers hebben kennelijk tot eind van dit jaar en de kleinere zouden dan nog een jaar langer hebben, dus tot eind 2013. Dan hebben wij nog ruim anderhalf jaar te gaan. Kortom, ik snap niet waar de urgentie is gebleven.

Minister **Spies**: De urgentie is absoluut niet weg, maar het moet wel goed en zorgvuldig. Het gaat over meer dan 400 gemeenten. De VNG heeft samen met mij de gemeenten geïnformeerd over de noodzaak van het uitvoeren van de assessments. KING is begonnen met de ondersteuning van gemeenten bij de uitvoering van die DigiD-assessments. Er loopt tot juni een impactanalyse bij een aantal gemeenten en hun leveranciers. KING start daarna een samenwerkingstraject met die leveranciers en met de auditors van de gemeenten. Gemeenten zijn soms al begonnen met de voorbereidingen van de assessments en de testen. VNG en KING zullen gemeenten structureel ondersteunen op het gebied van de ICT-beveiliging. Het is nogal een operatie waar wij nu over praten. Het spijt mij zeer dat de raming aanvankelijk te optimistisch was, maar er wordt op dit moment een zeer groot aantal activiteiten ontplooid en het duurt een poos voordat die allemaal zijn afgerond. Ik kan niet tot een andere conclusie komen dan dat de doorlooptijd tot eind 2012 gewoon nodig is om het goed, zorgvuldig en met de bijbehorende urgentie aan te pakken. Ik zie geen mogelijkheden om dat te versnellen.

Mevrouw **Gesthuizen** (SP): Klopt het dat voor de kleinere gebruikers de doorlooptijd tot eind 2013 is verlengd?

Minister **Spies**: In de brief van 2 februari jl. heb ik gemeld dat de overige organisaties de assessments voor het eind van 2013 klaar moeten hebben. Zij kunnen gebruikmaken van ervaringen die de gemeenten opdoen.

De heer **Recourt** (PvdA): Er is uitgebreid gesproken over de assessments, maar mij bekroop een vraag over de achterliggende problematiek. Een aantal incidenten heeft de media gehaald, maar voor veel incidenten geldt dit niet. Is er een cijfermatig overzicht over 2010 of 2011 van alle geslaagde hacks of veiligheidslekken bij de overheid en bij bedrijven die de beschikking hebben over persoonsgegevens?

Minister **Spies**: Dat is mij niet bekend en ik vrees dat een dergelijk overzicht er niet is. Zoals de heer Recourt in zijn vraag al aangaf, hebben wij te maken met mogelijke hacks waarvan niet is geconstateerd dat zij hebben plaatsgevonden. Ik kan die informatie dus niet geven.

De heer **Recourt** (PvdA): Ik snap dat wij dat niet kunnen weten, maar is er een lijstje met de gevallen die wel bekend zijn?

Minister **Spies**: Voor zover mij bekend niet.
Ik ben alleen de heer Çörüz nog een antwoord schuldig op zijn vraag over de export van producten die vrijheden zouden kunnen beperken, zoals aftap- of filtertechnologie. Voor zover bekend, zijn er in Nederland geen exporteurs van dergelijke producten. In januari 2012 heeft de staatssecretaris van EL&I vragen hierover beantwoord. In geval van twijfel wordt er nog wel eens contact opgenomen met EL&I om te vragen of bepaalde producten onder specifieke regimes vallen.

Staatssecretaris **Teeven**: Voorzitter. Ik bedank de leden voor de paar vragen die zij gesteld hebben over onderwerpen die onder mijn portefeuille vallen. De minister van BZK heeft al iets gezegd over de uitvoering van de gewijzigde motie-Elissen c.s. (26 643, nr. 209, was nr. 204). In deze motie wordt gevraagd om bij elk project safety by design en privacy by design toe te passen. Wij moeten daarbij rekening houden met de concept-EU-verordening inzake gegevensbescherming. Op grond van die verordening wordt iedereen die met persoonsgegevens werkt, verplicht om die veiligheidseisen toe te passen. Om die reden alleen al, maar ook omdat het de inzet van het kabinet is, zullen wij hier zeker toe overgaan.

De heer Elissen heeft gevraagd wat er gebeurd is met de gewijzigde motie-Elissen c.s. (26 643, nr. 210, was nr. 205) over een notitie over integrale privacybescherming. Ik wijs op de notitie van 29 april van het vorig jaar die de voorganger van de minister en ik aan de Kamer hebben gestuurd. In april 2012 zal de minister van EL&I een notitie het licht doen zien over de bescherming van privacy van internetgebruikers. Op dit moment stem ik de inhoud van deze notitie met hem af. Zij verschijnt dus deze maand.
De heer Recourt heeft gevraagd hoe het zit met het wetsvoorstel over de meldplicht van datalekken. In de consultatiefase zijn er veel reacties ontvangen en die worden op dit moment verwerkt. Voor de zomer gaat het wetsvoorstel naar de ministerraad en na het zomerreces, nadat het is terugontvangen van de Raad van State, zullen wij het naar de Kamer sturen.
Mevrouw Gesthuizen heeft de vraag die zij altijd stelt over de menskracht van het College bescherming persoonsgegevens, opnieuw gesteld. Kan dit college zijn taak nog wel geloofwaardig vervullen? De Kamer weet dat de begroting van het college in de periode van 2001 tot 2008 structureel verhoogd is door voorgaande kabinetten. Vanaf 2008 is er een zekere afvlakking van het budget van het CBP te zien. Die heeft te maken met de toen al ingezette bezuinigingen. Ook het CBP zal een beetje moeten leven met de financiële omstandigheden waar wij mee te maken hebben.
Mevrouw Gesthuizen zei al dat er prioriteiten gesteld moeten worden. Dat houd ik de heer Kohnstamm in de driemaandelijkse gesprekken steeds opnieuw voor. De afspraak is dat er een scherpe prioritering moet plaatsvinden. Wij hebben ook met het CPB afgesproken dat na de inwerkingtreding van het wetsvoorstel over de meldplicht van datalekken bezien wordt wat dit voor de werkzaamheden van het CPB betekent. Wij gaan nu na of de suggestie uit de Kamer overgenomen kan worden om prejudiciële vragen tegen betaling te beantwoorden. Wellicht kan op die manier de financiële armslag van het CPB vergroot worden. De Kamer hoort voor de zomer of dit mogelijk is.
Tot slot een vraag die gedeeltelijk al door mijn voorgangers is behandeld en dat is de vraag van de heer Çörüz of de Wob een sta-in-de-weg is voor publiekprivate samenwerking. Dat is niet het geval. Wanneer gegevens met nadruk als bedrijfsvertrouwelijk worden aangemerkt, kan een beroep worden gedaan op de desbetreffende weigeringsgrond in de Wob. Dit is verwerkt in de jurisprudentie van de Afdeling bestuursrechtspraak van de Raad van State.

De **voorzitter**: De spreektijd in tweede termijn is twee minuten per fractie. Tijdens de beantwoording zijn opnieuw twee interrupties toegestaan.

Mevrouw **Hennis-Plasschaert** (VVD): Voorzitter. Dank voor de over het algemeen heldere antwoorden. Ik heb gevraagd hoe de bewindspersonen staan tegenover de realisatie van een kwalificatieschema dat de kwaliteitsborging van de beroepsgroep informatiebeveiligers eenduidig maakt en bewaakt. Minister Opstelten antwoordde dat hij een initiatief van de beroepsgroep toejuicht. Is hij ook bereid om de beroepsgroep daartoe enigszins te kietelen? Ook ik ben natuurlijk voor eigen initiatief, maar de beroepsgroep mag ook wel gestimuleerd worden. Is de minister daartoe bereid en, zo ja, op welke wijze?
Ik sloeg aan op het antwoord van minister Spies over het niet exporteren van aftap- en spytechnologie. Ik geloof haar graag, maar ik vrees dat wij ons niet heiliger moeten voordoen dan wij zijn. Ik heb het ministerie van Veiligheid en Justitie eerder gealarmeerd omdat mensen actief op de markt werden benaderd om in Indonesië workshops te geven over onderwerpen die wel degelijk zijn gerelateerd aan aftap- en spytechnologie. Indonesië is nu net een land waarbij je daar niet prat op zou moeten

gaan. Ik roep alle bewindslieden hier aan tafel nogmaals op om hier strikt in te zijn en zeker niet het eigen ministerie op de markt te laten zoeken naar mensen om vervolgens in naam van de Nederlandse overheid workshops te geven in Indonesië, China of een ander land dat het niet zo nauw neemt met de mensenrechten.

De heer **Elissen** (PVV): Voorzitter. Ik bedank de bewindspersonen voor hun soms bondige, soms wat minder bondige antwoorden. Ik heb twee punten van zorg. In de motie op stuk nr. 204 wordt gevraagd om een jaarlijks overzicht van systemen en organisaties waarvoor de overheid verantwoordelijk is. Daarbij gaat het onder andere om penetratietesten. Ik constateer dat men kennelijk moeite heeft om het pakket aan beveiligingsassments af te werken. Dit kan wat meer tijd kosten omdat het de eerste keer is, maar ik verwacht wel dat dit jaarlijks wordt gedaan.
Ik ben het niet eens met de conclusie dat de brief van 9 november 2011 duidelijk is over de motie op stuk nr. 205. Deze motie is namelijk eerst aangehouden en pas op 22 december 2011 in stemming gebracht en aangenomen. Mijn verzoek aan de minister is om toch nog wat uitvoeriger toe te lichten op welke wijze zij uitvoering gaat geven aan deze motie over het eerstelijnstoezicht en een jaarlijks overzicht van kwetsbare systemen.

De heer **Recourt** (PvdA): Voorzitter. Dank. Ik begin met het grote belang van het op orde hebben van de veiligheid in de private sector en de overheid. Dat is goed aan te tonen bij het voorbeeld van DigiNotar. Die hack was erop gericht dissidenten op te sporen in het buitenland. Degene die het lek gevonden heeft, mijnheer Hypponen, zegt dat bekend is wat Iran met dissidenten doet. Dit wordt overigens ergens anders verder besproken, maar voor mij is zeer duidelijk dat het potentieel om mensenlevens gaat. Er is geen lijstje van geslaagde hacks. Op z'n minst is dat vreemd. Via mijn digitale kanalen kreeg ik door dat het helemaal niet om incidenten gaat. Er vinden vrij frequent geslaagde hacks plaats. Mijn vraag is dus of dat lijstje er alsnog kan komen.
Als het misgegaan is, moet je een boete kunnen opleggen aan civiele partijen. Wat mij betreft moet dit ook vooraf het geval kunnen zijn, namelijk als bij een test de zaak niet op orde blijkt te zijn. Ik verwacht dat het kabinet dit met mij eens is, want het houdt van een stevige aanpak en repressieve maatregelen. Dat betekent dat er op dit punt een steviger insteek moet worden gekozen. Er wordt nu wel erg vertrouwd op de gevoeligheid voor reputatieschade. Er moet een stok achter de deur zijn zodat je zeker weet dat de urgentie beter gevoeld wordt.
Ik ben blij met de toezegging over de komende wetgeving. Tot is die tijd is het kwetsbaar om het aan de rechter over te laten om te bepalen of het door de beugel kan of niet. Als de rechter vindt dat het niet kan, is de zaak kapot. Vooral bij zedenzaken lijkt mij dit zeer onwenselijk. Ik benadruk de haast die met de wetgeving geboden is. Misschien moeten er ook nog wel noodverbanden aangelegd worden. Het lijkt mij niet verstandig om het op de rechter te laten aankomen.

Mevrouw **Hachchi** (D66): Voorzitter. Ik bedank de bewindslieden voor hun antwoorden in eerste termijn. Ik heb erop gewezen dat de overheid nu verschillend omgaat met hackers die een melding doen. De ene gemeente neemt de melding ter harte en lost het probleem op, maar de andere gemeente belt gelijk de officier van justitie waarna de hacker een probleem heeft. Ik heb gevraagd of er geen richtlijn kan komen om ervoor te zorgen dat de overheid zo veel mogelijk op dezelfde manier omgaat met dit soort meldingen. In eerste instantie was het antwoord van minister Opstelten helder. Het ging hem om de benaming. Een richtlijn zag hij niet zitten, maar hij was wel voor een kader. Hij vond in ieder geval ook dat hier eenduidig mee moet worden omgegaan. In een interruptiede-

batje met de heer Elissen ontstond er toch weer wat onduidelijkheid. Ik krijg graag op dit punt toch duidelijkheid van minister Opstelten.
Ik snap dat de commissie voor de Inlichtingen en Veiligheidsdiensten de gevolgen voor de Iraanse activisten van de situatie bij DigiNotar bespreekt en dat wij dat niet hier doen. Ik heb echter gevraagd of vanaf nu mensenlevens zowel binnen als buiten Nederland een prominente plek krijgen in het Cyber Security beleid. Kan een van de ministers hierop ingaan?

Mijn laatste vraag is gericht aan minister Spies. Zij gaf terecht aan dat de overheid weliswaar regie kan voeren ten aanzien van provincies en gemeenten en dat zij dat ook doet, maar dat er ook een zekere mate van afhankelijkheid van het bedrijfsleven is. Volgens de minister kan daarop alleen achteraf worden ingespeeld door bijvoorbeeld websites offline te laten gaan. Ik ben een echte liberaal en vind dat we de zaken die de markt beter kan doen dan de overheid, aan de markt moeten laten, maar de overheid moet wel haar rol als opdrachtgever goed weten te vervullen. De overheid moet dus niet alleen aan de achterzijde reactief optreden. Zij moet ook aan de voorkant de zaken beter regelen, zelfs in termen van aansprakelijkheid voor het geval dat bepaalde beveiliging tekortschiet. Kan de minister aangeven wat de overheid aan de voorkant doet op het gebied van de afhankelijkheid van het bedrijfsleven?

Mevrouw **Gesthuizen** (SP): Voorzitter. Ik heb nog vier punten. Allereerst heb ik een vraag aan de minister van Veiligheid en Justitie. Het onderwerp van de ontwrichting van de samenleving zit mij toch niet helemaal lekker. Ik kan mij heel goed indenken dat wij in de toekomst toch weer alleen zullen kijken naar de grote incidenten, terwijl het juist bij kleinere incidenten, waarbij je niet direct denkt aan ontwrichting van de samenleving, van belang kan zijn dat bedrijven weten dat zij zich aan bepaalde regels moeten houden. De minister laat zich nu nog niet uit over specifieke maatregelen, maar hij kan ervan verzekerd zijn dat wij een en ander met argusogen zullen bekijken. Ik wil namelijk niet dat de verantwoordelijkheid van de overheid wordt weggezet.
Ik ben ook een beetje verbaasd over het betoog van de minister waaruit blijkt dat justitie illegaal hackt in het buitenland. Uit het punt dat de heer Recourt naar voren bracht, begreep ik namelijk dat de minister eerder had aangegeven dat hij samen met het OM bekeek of de wet mogelijk zou moeten worden aangepast. Uit de beantwoording van zojuist bleek echter dat er volgens de minister niets aan de hand is; men zoekt wel de grenzen op, maar begaat geen overtredingen.
De minister van BZK heeft gezegd dat wij toch echt tot eind 2013 moeten wachten. Ik denk dat ik het niet zover wil laten komen en ik overweeg om een VAO aan te vragen en een motie in te dienen om het moment waarop de assessments gedaan moeten zijn, naar voren te halen.
Mijn laatste punt betreft uiteraard de staatssecretaris. Als mijn woorden blijkbaar aan dovemansoren gericht zijn, voel ik mij genoodzaakt om ze te herhalen. De voorzitter van het College Bescherming Persoonsgegevens zegt niet zomaar iets. De staatssecretaris komt niet weg met alleen maar het argument dat het CBP al meer budget heeft gekregen, want dan zouden wij ook moeten kijken naar de hoeveelheid werk en de factor waarmee die is toegenomen. Als wij niet willen dat het college dat moet toezien op de privacy en de bescherming van persoonsgegevens, een tandeloze tijger is, moeten wij ook op dit gebied boter bij de vis leveren.

De **voorzitter**: Als woordvoerder van de CDA-fractie wil ik de bewindslieden slechts bedanken. Ik heb geen behoefte aan een tweede termijn, want een aantal verhelderende vragen is al door de collega's gesteld. Ik sluit mij daar kortheidshalve bij aan.

Minister **Opstelten**: Voorzitter. Ik bedank de geachte afgevaardigden voor hun reacties in tweede termijn.
Mevrouw Hennis heeft gelijk met haar oproep om niet te wachten tot de beroepsgroep zich meldt. Mijn mensen en ikzelf onderhouden in dat verband uiteraard contact met allerlei groepen. Wij gaan het gesprek zeer actief aan, want het is heel belangrijk om de informatiebeveiligers kwalitatief en kwantitatief scherp te houden en te interesseren voor onze aanpak.
De heer Recourt heeft gevraagd naar een lijst. Er is slechts een beperkt beeld. Een aantal incidenten is gemeld bij het centrum. In het volgende Cyber Security Beeld Nederland zullen wij opnemen wat er is gemeld en wat daarmee is gedaan. Dat lijkt mij heel goed. Dit geeft overigens slechts een zeer beperkt beeld, want niet elke melding is nuttig of nodig. Wij moeten ter uitvoering van de motie-Hennis bekijken hoe dit zit. Wij zullen zowel bij bedrijven als bij de overheid aandacht hiervoor vragen, opdat men weet dat men bij melding in het assessment wordt meegenomen. De Kamer krijgt daar een overzicht van.
Het punt van de heer Recourt en mevrouw Gesthuizen over de grenzen van de opsporing blijft interessant. Wij moeten de vraag of we binnen de grenzen blijven, niet op het rechterlijk oordeel laten aankomen. Het Openbaar Ministerie en politie pakken cybercrime aan. Bijvoorbeeld bij de KPN-hack is er direct zelfstandig onderzoek gedaan door het OM. Zij zoeken de grenzen op. Voor de zomer zullen wij met een nadere stand van zaken komen, als onderdeel van het juridisch kader. Dit is een nieuw terrein, dus het is ook heel logisch dat wij een en ander nog moeten verkennen.
De heer Recourt heeft gevraagd naar een boete voor civiele partijen. Ook dit is onderdeel van de bestudering van het juridisch kader. De uitvoering van de motie-Hennis is hier ook onderdeel van. Wij bezien wat wettelijke verplichting wordt voor diverse partijen. Voor de zomer zullen wij de Kamer hierover nader informeren.

De heer **Recourt** (PvdA): Het punt dat mevrouw Gesthuizen en ik maken, gaat volgens mij verder dan de minister nu zegt. Het Openbaar Ministerie zegt zelf namelijk dat men over de grenzen van de wet gaat. De minister zegt echter dat zij op het randje zitten. Hoe zit dat nu?

Minister **Opstelten**: Het is nog niet vastgesteld waar de grens precies ligt. Niemand kan dat zeggen. De enige die dat uiteindelijk bepaalt, is de rechter, zo luidt mijn min of meer formalistische antwoord. Ik ben het met de heer Recourt eens dat wij niet achterover moeten leunen en zeggen dat de rechter het uiteindelijk wel zal vertellen. Wat dat betreft is zijn interventie wel nuttig. Wij zullen hier nog eens goed naar kijken en er voor de zomer op terugkomen. De heer Recourt heeft gezegd dat hij een ongelooflijk gevoel van urgentie heeft; ik deel dat met hem.

De heer **Recourt** (PvdA): Uiteraard, waar niet duidelijk is hoe de wet op dit moment precies geduid moet worden, is het aan de rechter om dat te doen. In die zin ben ik het helemaal met de minister eens. Zijn eigen ambtenaren zeggen echter dat zij te weinig instrumenten in handen hebben en dat zij over de grenzen heen gaan. Dat is een heel ander verhaal. Uiteindelijk gaat de minister over zijn ambtenaren. Begrijp ik het goed dat ik het anders moet uitleggen en dat hij zich namens de regering in ieder geval op het standpunt stelt dat zij binnen de grens opereren? Het kan toch niet zo zijn dat de overheid zelf zegt dat zij de wet overtreedt!

Minister **Opstelten**: Daarom zeg ik dat ook niet. Als dat wel gebeurt, hebben wij daar een enkel gesprek over met betrokkenen, maar daarover hoef ik geen mededelingen te doen. Het is wel een nieuw terrein, waarop wij zoekende zijn. Daarom zeg ik dat het juridisch kader snel scherp moet

worden. Dat is niet eenvoudig. Internationale aspecten spelen hierbij een rol. Voor het zomerreces komen wij met het juridisch kader en dat reces komt elke dag dichterbij. Laten wij niet doen alsof er een tegenstelling is; wij voelen beiden de urgentie.
Tegen mevrouw Hachchi kan ik slechts herhalen wat ik al heb gezegd. Wij vinden dat er duidelijkheid moet zijn over de responsible disclosure. Er moet een duidelijk kader zijn waar iedereen zich aan moet houden. Wij kunnen hier zeggen dat het helder is, maar het is voor een heleboel mensen niet helder, want wij voeren telkens die discussie. Wij geven een kader aan. Nogmaals, het uitgangspunt is responsible disclosure. Dit kader komt eraan. Wij zullen het publiceren om overheid en bedrijfsleven eraan te kunnen binden.
Mevrouw Gesthuizen heeft het punt van de ontwrichting van de samenleving nog eens aangestipt. Ik ga dat goed volgen. Dat lijkt me volkomen terecht. Het kernpunt is dat de verantwoordelijkheden van de verschillende sectoren bij wet apart zijn geregeld. Is dat niet het geval, dan moet dat nader vorm krijgen. De nationale crisisbeheersingsstructuur is gericht op het tegengaan van de ontwrichting van de samenleving en op het bewaken van de nationale veiligheid. Dat is de verantwoordelijkheid van mij en van het Nationaal Cyber Security Centrum. Wij moeten dit telkens van geval tot geval beoordelen. Natuurlijk speelt het leven van mensen daar een belangrijke rol in. Ik ga echter niet zo ver dat ik zeg in welk geval dit wel en niet van toepassing is. Dit zal zichzelf moeten ontwikkelen.

Mevrouw **Gesthuizen** (SP): Ik maak even de vergelijking met de niet-virtuele wereld. Voor alle bedrijven die werken met gevaarlijke materialen of die andere zaken doen waarbij de veiligheid in het geding zou kunnen zijn, hebben wij regels opgesteld die in acht moeten worden genomen. Die gelden voor alle bedrijven evenzeer. Het gaat dus niet alleen maar om de grote incidenten. Dat is wat ik de minister steeds duidelijk wil maken. Ik zie hem begrijpend knikken en ik ga er dus van uit dat mijn boodschap luid en duidelijk is aangekomen.
Overigens moet ik de vergadering over enkele minuten verlaten.

Minister **Opstelten**: Laat ik er nog het volgende over zeggen. Het gaat om nationale ontwrichting en de sector is zelf verantwoordelijk. Dat zijn de twee ankerpunten. Ik hoop dat het ons gegund wordt om hierin een volgende stap te zetten. Ik weet dat mevrouw Gesthuizen dit kritisch volgt. Daar houden wij rekening mee. Veiligheid zit niet alleen in iets heel groots. De toestand die zich destijds in Veere heeft voorgedaan, had tot iets groots kunnen uitgroeien, terwijl het in de kern om iets kleins ging.

Mevrouw **Hachchi** (D66): Ik vond de DigiNotar-affaire nu juist een uitstekend voorbeeld van een geval waarin naar de buitenwereld te weinig aandacht is getoond voor mensenlevens buiten Nederland. Dat zie je ook in de evaluatie en de rapporten. Het is gelukkig goed gegaan en het viel mee, maar geven wij mensenlevens zowel binnen als buiten Nederland wel een prominente plek in ons Cyber Security beleid? Ik hoor in het antwoord van de minister nog iets te veel een slag om de arm. Ik zou graag een helder antwoord krijgen.

Minister **Opstelten**: Mensenlevens spelen een cruciale rol, altijd. Er zijn nooit uitzonderingen. Laat ik daar duidelijk over zijn. Bij DigiNotar zijn alle aspecten meegenomen, ook die aspecten.

Minister **Spies**: Voorzitter. In de weinige minuten die mevrouw Gesthuizen nog in deze zaal is, zal ik beginnen met de vragen die zij mij heeft gesteld in tweede termijn.
Bij de assessments hebben wij uiteraard geprobeerd om prioriteiten te stellen en onderscheid te maken tussen de grote en de wat kleinere

gebruikers. Wij hebben moeten constateren dat de personele capaciteit in Nederland om deze assessments uit te voeren, op dit moment onvoldoende voorhanden is om dit te doen in het tempo dat ons aanvankelijk voor ogen stond. Dat heeft niets te maken met een gebrek aan urgentie, maar wel met de ambitie om dingen goed te doen. Overigens leidt een assessment ook maar tot een tijdelijk certificaat, waaraan bovendien een heel proces is voorafgegaan. Ik had heel graag de urgentie van mevrouw Gesthuizen persoonlijk willen overbrengen aan de decentrale overheden en andere organisaties. Dit bestuurlijk overleg was voor morgen gepland. Helaas moet ik morgen de hele dag in de Kamer zijn. Ik ga het dus op een andere manier zo snel mogelijk doorgeven aan deze gebruikers. Ik kan helaas echt niet toezeggen dat het eerder kan dan het tijdspad dat ik eerder heb geschetst.
Mevrouw Hachchi heeft terecht gevraagd hoe we bij overheidsaanbestedingen vanuit onze rol als opdrachtgever de aandacht voor ICT-beveiliging voluit kunnen meenemen. Dit gebeurt al. ICT-continuïteit is een belangrijke voorwaarde bij het gunnen van opdrachten. Er is overigens ook regelmatig contact met de brancheorganisatie van leveranciers van ICT-diensten. Dat is een belangrijk informatiekanaal waardoor wij ook het opdrachtgeverschap van de overheid zo goed mogelijk invullen.
Tot slot probeer ik graag de zorgen van de heer Elissen over het uitvoeren van moties weg te nemen. Op 14 maart heb ik de Kamer een brief gestuurd waarin ook de uitvoering van de motie op stuk nr. 221 ter hand wordt genomen. OPTA en de Policy Authority gaan bedrijfsbezoeken afleggen bij de certificatenleveranciers. Dat is het eerstelijnstoezicht waar de motie-Elissen om vraagt. Deze organisaties zullen ter plekke controles uitvoeren. Ik zal bezien hoe wij een jaarlijkse rapportage van kwetsbare overheidssystemen het beste kunnen vormgeven. Idealiter wordt dit verwerkt in bestaande rapportages. De Kamer krijgt bijvoorbeeld jaarlijks een rapportage over de compacte rijksdienst die is opgenomen in de bedrijfsvoeringsrapportage van de rijksoverheid. Als het mogelijk is, neem ik dit onderwerp graag in deze rapportage mee. Mocht de heer Elissen van oordeel zijn dat dit onvoldoende is, dan hoor ik het graag, want dan moet ik in overleg met de collega van EL&I bezien of wij op een andere manier tegemoet kunnen komen aan de wensen die in de motie zijn verwoord.

De heer **Elissen** (PVV): Ik begrijp dat er ten aanzien van de motie op stuk nr. 204 nog steeds de ambitie is om jaarlijks, onder andere met behulp van penetratietesten, te onderzoeken hoe de gegevens van burgers beveiligd zijn om zo een adequaat beeld van gegevensbescherming te krijgen. Er treedt nu weliswaar wat vertraging op, maar de ambitie blijft overeind. In de motie op stuk nr. 205 vraag ik om eerstelijnstoezicht. Ik begrijp dat dit er komt. Om goed vast te kunnen stellen waar dat wel en niet noodzakelijk is en daarin een bepaalde flexibiliteit te houden om er adequaat op te kunnen sturen, is het mijns inziens wel nodig om jaarlijks een goed overzicht te krijgen. Ik zou het prettig vinden als wij dat bij dit thema konden blijven betrekken. Het moet niet verdrinken in het grotere geheel.

Minister **Spies**: Als ik dat zo mag uitleggen dat de OPTA het toezicht bij de certificatenleveranciers gaat uitoefenen, dan hebben wij op die manier invulling gegeven aan het eerstelijnstoezicht. Ik zal bezien op welke manier wij hierover eventueel verdere informatie kunnen verschaffen, aanvullend op de rapportages over dit onderwerp die de Kamer bereiken.

De heer **Elissen** (PVV): Ik wil graag een misverstand voorkomen. De OPTA beperkt zich tot de post- en telecommarkt, maar de strekking van de motie is veel breder. Ik heb het meer generiek gehad over eerstelijnstoezicht waar dat maar nodig is.

Minister **Spies**: De OPTA beperkt zich niet alleen tot de telecombranche. Ik heb nadrukkelijk de certificatenleveranciers genoemd. Zij zullen ook door de OPTA bezocht worden. Daarmee introduceren we voor het eerst een vorm van eerstelijnstoezicht voor de certificatenleveranciers. De Kamer zal daar verslag van krijgen.

Staatssecretaris **Teeven**: Voorzitter. Ik bedank de leden voor hun complimenten, ook in het algemeen. Mevrouw Gesthuizen is bang dat wij de voorzitter van het CBP aan zijn lot overlaten. Wij doen dat niet. Wij vinden dat het CBP een belangrijke taak uitoefent, maar, om in de taal van mevrouw Gesthuizen te blijven praten, dan moet je wel boter bij de vis leveren en je niet met spierinkjes bezig houden, zoals deze zomer even leek te gebeuren. Wij monitoren heel scherp wat het college doet. Het oefent een belangrijke taak uit. Wel onthouden we altijd dat er boter bij de vis moet komen.

De **voorzitter**: Dank u. Ik bedank de bewindslieden, de Kamerleden en de toehoorders. Mevrouw Gesthuizen heeft een VAO aangevraagd. Zij zal daarbij als eerste het woord voeren. Alle toezeggingen komen in het verslag.

Volledige agenda

1. Cyber Security
26 643-220 – Brief regering d.d. 23-12-2011
minister van Veiligheid en Justitie, I.W. Opstelten

2. Reactie op moties ingediend tijdens het VAO over verwerking en bescherming van persoonsgegevens
32 761-15 – Brief regering d.d. 20-12-2011
staatssecretaris van Veiligheid en Justitie, F. Teeven

3. Reactie op verzoek van de leden Gesthuizen en El Fassed inzake een hack bij de certificatenleverancier Gemnet en inzake de intrekking van duizend certificaten door KPN
26 643-218 – Brief regering d.d. 13-12-2011
minister van Binnenlandse Zaken en Koninkrijksrelaties, J.P.H. Donner

4. Stand van zaken moties Diginotar en ICT-problemen bij de overheid
26 643-214 – Brief regering d.d. 11-11-2011
minister van Binnenlandse Zaken en Koninkrijksrelaties, J.P.H. Donner

5. Stand van zaken vervolgacties n.a.v. DigiNotar
26 643-222 – Brief regering d.d. 02-02-2012
minister van Binnenlandse Zaken en Koninkrijksrelaties, J.W.E. Spies

6. ICT-beveiligingsassessments DigiD gebruikende organisaties
26 643-224 – Brief regering d.d. 03-02-2012
minister van Binnenlandse Zaken en Koninkrijksrelaties, J.W.E. Spies

7. Reactie op verzoek Gesthuizen over de hack bij KPN
26 643-225 – Brief regering d.d. 14-02-2012
minister van Veiligheid en Justitie, I.W. Opstelten

8. Reactie op verzoek Heijnen omtrent het «op straat liggen van persoonsgegevens uit grote databestanden»
32 761-16 – Brief regering d.d. 07-02-2012
staatssecretaris van Veiligheid en Justitie, F. Teeven

9. Voorstel van het Europees Parlement en de Raad over de aanval op informatiesystemen
32 317-60 – Brief regering d.d. 22-06-2011
staatssecretaris van Veiligheid en Justitie, F. Teeven

10. Resultaten van een drietal onderzoeken inzake DigiNotar (min ELI)
26 643-230 – Brief regering d.d. 16-03-2012
minister van Binnenlandse Zaken en Koninkrijksrelaties, J.W.E. Spies

11. Letter of Intent Cyber Security tussen Nederland en de Verenigde Staten
26 643-227 – Brief regering d.d. 19-03-2012
minister van Veiligheid en Justitie, I.W. Opstelten

12. Beveiliging van Supervisory Control And Data Acquisition (SCADA)-systemen en de gebeurtenissen in de gemeente Veere
26 643-228 – Brief regering d.d. 19-03-2012
minister van Veiligheid en Justitie, I.W. Opstelten