26
DigiNotar

Aan de orde is het **debat** over **DigiNotar en ICT-problemen bij de overheid.**

De **voorzitter**:
Ik heet de ministers Donner en Opstelten welkom. De spreektijd voor de Kamer is vijf minuten per fractie.

Mevrouw **Gesthuizen** (SP):
Voorzitter. Het is altijd goed om voor een debat te bedenken wat je zelf zult gaan zeggen, maar het is ook goed om je af te vragen wat de ministers zullen zeggen en welke reacties er zullen komen op vragen en voorstellen. Ik neem een schot voor de boeg. Minister Donner gaat zeggen dat de wereld misschien wel in zeven dagen is geschapen, maar dat hijzelf niet bij machte is om wonderen te verrichten.

Minister **Donner**:
Zes dagen!

Mevrouw **Gesthuizen** (SP):
Goed, dat is waar. Dat ben ik met hem eens, niet dat over die wereld en ook niet over de zes dagen, maar ik ben het wel met hem eens over de onmogelijkheid van deze ministers om wonderen te verrichten.

Wij staan voor een serieus drama, een digitaal doemscenario. Gegevens liggen op straat. Burgers in Iran zijn in groot gevaar gebracht en zijn mogelijk hierdoor zelfs dood. Nederlandse overheidssites bleken onbetrouwbaar, zelfs de sites waar burgers en bedrijven gedwongen gebruik van maakten. Denk aan de site van de Belastingdienst, denk aan DigiD. Ik heb het over het grootste ICT-probleem voor de Nederlandse overheid dat in de openbaarheid is gekomen in de geschiedenis. Ik heb het over het lek via het bedrijf DigiNotar en de problemen die hierdoor ontstonden met de zogenaamde certificaten die de garantie van echtheid van websites moesten geven, maar die vals bleken te zijn.

Hadden wij het maar over een jammerlijk incident, maar helaas is dat niet zo. Het is eerder regel dan uitzondering dat ICT-projecten bij de overheid tot veiligheidsproblemen leidden. Veiligheid is bij ICT-zaken steeds het ondergeschoven kindje. Dat hoor ik van steeds meer mensen, ook van mensen die voor en met de overheid werkten. Het gevoel van urgentie op het thema ontbreekt ten enenmale. Op 31 augustus van dit jaar, iets meer dan een maand geleden, zei een ambtenaar van minister Donner dit.

"DigiD is veilig. Wij hebben geen enkele twijfel aan de beveiliging van DigiD naar aanleiding van dit nieuws. De Staat der Nederlanden werkt via een gescheiden traject voor hun certificaten. Andere certificaten worden via een andere procedure uitgegeven. De hoofdsleutel ligt dan ook bij DigiD in de kluis en niet bij DigiNotar."

"Welke kluis?", vraag ik mij af. Hoe kan dit? Hoe kan het dat deze ambtenaar niet doorhad dat de schuur in de fik stond terwijl dikke rookwolken in de lucht hingen? Waarom is niet door GOVCERT, Logius of OPTA ingegrepen toen dit bericht verscheen? Daar moeten toch mensen hebben gezeten die zich de haren uit de kop trokken toen dit het verhaal van het ministerie was? Of is het nog erger? Was er echt niemand die wist hoe het zat? Hoe zat het met de interne controle? Wie informeerde de minister of had dit moeten doen? Welk team is verantwoordelijk voor het optreden van de overheid als een situatie ontstaat zoals rond DigiNotar en de certificaten? Wil het kabinet erkennen dat de regie ontbrak, evenals de kennis, en wil het ook erkennen dat de overheid in dezen geheel afhankelijk was van Fox-IT, een privaat bedrijf?

Dit willen wij niet meer meemaken. Dat staat voor de SP-fractie als een paal boven water. Ik doe dan ook twee concrete voorstellen. Beide zal ik toelichten.

Ten eerste is de gang van zaken op het gebied van veiligheidskwesties bij ICT in de jaren die achter ons liggen, mij een doorn in het oog. Ik wil de collega's in dit huis dan ook voorstellen om zelf onderzoek te doen. Ik vind dat de onderste steen boven moet komen. Er zijn fouten, missers en gebreken in overvloed die allemaal te maken hebben met de manier waarop diverse kabinetten, en deze Kamer, de veiligheid op het gebied van ICT hebben geregeld: de ov-chipkaart, DigiD, DigiNotar en alles waarmee wij nog geconfronteerd zullen worden gedurende deze "lektober": zo is de maand oktober uitgeroepen door de technologiewebsite Webwereld. Iedere dag een lek van een overheidssite. Een parlementair onderzoek is dan ook op zijn plaats. Het mag kort zijn. We mogen ons beperken tot een aantal dossiers, maar het moet er komen. De onderste steen moet boven. Ik durf mijn hand er niet voor in het vuur te steken dat kabinet en Kamer steeds op basis van de juiste informatie beslissingen hebben genomen over ICT en het gebruik of de inzet daarvan door de Nederlandse overheid.

Ten tweede zag en zie ik met lede ogen het gestuntel aan van de ministeries en de toezichtorganen zoals OPTA en Logius. Kan de minister mij nou eens precies uitleggen wie in een crisissituatie moeten optreden? Wie rukken uit om orde op zaken te stellen als er een groot ICT-probleem is?

Goed initiatief hoor, die nationale Cyber Security Raad, maar dat is toch niet het A-team dat gaat uitrukken als er een acuut probleem is? Het is prima als mensen in nette pakken een paar keer per jaar vergaderen, maar wij willen toch gewoon actie, als er urgentie is? Dan willen we toch dat de digitale brandweer uitrukt, met experts van het KLPD, NFI en GOVCERT, ondersteund door hackers die de overheid helpen om lekken op te sporen? Een team met de slimste experts – in ICT-jargon: nerds – dat gemeenten die urgente problemen hebben, kan ondersteunen, het roer kan overnemen en orde op zaken kan stellen, maar dat bovenal onderzoekt hoe groot het lek is en erger voorkomt.

Kan de minister mij toezeggen dat er een crash team of een gelijksoortige dienst komt die op dezelfde manier als politie en brandweer 24/7 oproepbaar is en kan uitrukken als door ICT-problemen de veiligheid, de privacy en de zekerheid van diensten in het geding komen? Wordt die dienst ingericht in het nieuwe cyberzekerheidscentrum, het NCSC? Krijgt Nederland een digitale brandweer met doorzetmacht?

Heijnen

□

De heer **Heijnen** (PvdA):
Voorzitter. Vijf minuten is veel te kort, gelet op het belang van de zaak, maar gelukkig hebben wij een hoorzitting gehouden en een briefing gekregen van ambtenaren.

Het vertrouwen in de informatie- en communicatietechnologie is van groot belang, ook economisch. We praten hier iedere dag over de schade van de bankencrisis, maar zelden of nooit over de mogelijke schade van een crisis in onze informatie- en communicatietechnologie. Tegelijkertijd blijkt die ICT kwetsbaar. De cybercrime neemt toe, zowel voor financiële als voor maatschappij-ontwrichtende zo niet terroristische doeleinden.

De DigiNotar-affaire heeft die kwetsbaarheid aangetoond. Het certificaatsysteem ligt in het bijzonder onder vuur. Als ik het goed heb begrepen, heeft de minister in een van de antwoorden geschreven dat men dit aspect ook in internationaal verband aan de orde wil stellen. Ik denk dat zijn collega van EL&I daar in het bijzonder een rol in heeft, maar daar kom ik straks op terug.

Ik heb de indruk dat de aanpak vanaf 2 september de toets der kritiek kan doorstaan, maar ik hecht er wel aan dat de Onderzoeksraad Voor Veiligheid toch een evaluatie laat plaatsvinden van datgene wat de minister vanaf dat moment heeft gedaan om de crisis het hoofd te bieden.

Bij datgene wat aan 2 september vooraf is gegaan, wil ik één punt uitlichten, namelijk de PKI-Overheid. Was er nu wel of niet sprake van extra beveiliging? In een van de antwoorden staat dat jaarlijks een audit plaatsvindt over de opzet en werking van de eisen, zoals vastgelegd in het programma van eisen PKI-Overheid, en dat door een gecertificeerde auditor een rapportage plaatsvond aan de public authority van PKI-Overheid. In een van de andere brieven staat letterlijk: "Ten aanzien van de uitgifte van PKI-Overheid certificaten geldt een zwaarder veiligheidsregime." In de hoorzitting is niets van dit alles gebleken. Daar is gebleken dat PricewaterhouseCoopers een audit heeft uitgevoerd in opdracht van OPTA, maar dat daarbij uitsluitend werd getoetst aan de Europese normen en dat de verslaglegging plaatsvond aan het bedrijf en aan niemand anders. Desgevraagd was noch OPTA noch PwC op de hoogte van enige andere audit die zou hebben plaatsgevonden bij DigiNotar.

Ik geloof dat dit een essentieel punt is. De vraag is of datgene wat de regering heeft geschreven, juist is. Heeft de regering de Kamer wel juist geïnformeerd? Er is mogelijk helemaal geen sprake geweest van extra veiligheidseisen bij PKI-Overheid, ja, misschien wel op papier, maar niet in de praktijk, niet qua handhaving. Het punt is dat het vertrouwen in de veiligheid van deze systemen cruciaal is, en dan kom ik weer terug op het eerste punt van mijn inleiding.

Mevrouw **Gesthuizen** (SP):
Ik kan me natuurlijk voor een heel groot gedeelte vinden in de lijn die de heer Heijnen hier uitzet, want ik ben ook bij de hoorzitting aanwezig geweest en ik heb dezelfde horrorverhalen meegekregen. Ik hoorde hem ook heel duidelijk zeggen dat hij er hier niet zomaar van uit durft te gaan dat het kabinet de Kamer wel volledig, wel correct heeft geïnformeerd. Ik geloof dat hij dat heeft gezegd. Vraagt hij zich dat ook af wat betreft andere ICT-dossiers?

De heer **Heijnen** (PvdA):
Met mevrouw Gesthuizen maak ik al ietsje langer deel uit van deze Kamer, namelijk al vanaf 2007. Ik heb het genoegen gehad om met een collega van haar deel te nemen aan een parlementaire werkgroep Grote ICT-projecten. Volgens mij heeft die werkgroep nuttig werk verricht. Hij heeft op basis van onderzoeken van de Algemene Rekenkamer de vinger gelegd op een aantal oorzaken van het financieel uit de hand lopen van grote IT-projecten en de werkgroep heeft op basis daarvan een aantal aanbevelingen gedaan. Toegegeven, de veiligheid maakte daar een minder prominent onderdeel van uit, maar de kostenbeheersing, het opknippen, de beheersing en de aansturing waren belangrijke elementen. ik durf wel te zeggen dat ik er volstrekt niet overtuigd van ben dat de veiligheid van de IT bij de overheid in goede handen is. Dat is de strekking van mijn opmerking van zojuist. Het gaat immers niet alleen om DigiNotar, het gaat ook om het gemak waarmee hackers gemeentelijke systemen binnen kunnen komen en waarmee collega Brinkman – net zo deskundig als ik, vermoed ik – in de provincie Noord-Holland het BABS naar zijn hand weet te zetten.

Ik maak me met mevrouw Gesthuizen grote zorgen over de veiligheid van de IT bij de overheid in het algemeen. Dat is de kern van dit debat.

Mevrouw **Gesthuizen** (SP):
Voorzitter. Als ik de heer Heijnen goed heb begrepen, vraagt hij zich af of, naast dit DigiNotar-debacle, de Kamer bij andere ICT-problemen, andere ICT-debacles en andere ICT-zaken, wel correct geïnformeerd is door dit en andere kabinetten.

De heer **Heijnen** (PvdA):
Zo ver durf ik niet te gaan. Ik kan me nu geen cases voor ogen halen waarin er door het kabinet dingen zijn gezegd over veiligheid en waar wij toen niet goed op hebben gelet. Met uw welnemen beperk ik me even tot Diginotar, omdat het zo evident is dat wat het kabinet ons heeft geschreven, gewoon afwijkt van de praktijk. Het gaat om die extra beveiliging voor PKI-Overheid. Als mijn veronderstelling juist is, dan vind ik dat het kabinet dat ook moet zeggen. Het moet zeggen: Kamer, samenleving, wij hebben u op het verkeerde been gezet, want onze PKI-Overheid was niet zo beveiligd als ons wel werd verteld en wij vervolgens aan u hebben verteld. Als het kabinet dat niet doet, heeft het een probleem. Het vertrouwen hebben in een oplossing, begint met het erkennen van het probleem. Ik verwacht dat van dit kabinet.

Voorzitter. Ik vervolg mijn betoog. Ik heb nog een paar korte andere punten. Er is nog een zijaspect, maar dat is misschien nog veel belangrijker. Dat is namelijk de vraag of via dit Nederlandse bedrijf 300.000 mensen in Iran risico hebben gelopen op onderdrukking door de staat als gevolg van de mogelijkheid dat die heeft ingebroken in hun e-mailverkeer. Ik weet dat het kabinet onderzoek heeft toegezegd en dat ter hand neemt. Ik wil de ministers vragen of zij dat, daar waar noodzakelijk, willen delen met de commissie Stiekem. En waar dat niet noodzakelijk is, kan dat met de Kamer als geheel worden gedeeld.

De hacktivisten zijn op dit moment, gegeven de onzekerheid over de veiligheid van overheids-ICT, een zegen. Wij moeten hen beschouwen als mensen die ons scherp houden, die de wake-upcall doen plaatsvinden, die voorkomen dat mensen met foute bedoelingen het systeem frustreren en daar misbruik van maken. Tegen die achter-

grond vraag ik de ministers om in te gaan op mijn suggestie om die mensen bescherming te bieden, daar waar ze worden achtervolgd door juristen, het OM, mensen die aangifte willen doen, terwijl ze, als het gaat om nobele bedoelingen, niets anders doen dan feilen van de overheid aangeven.

In het regeerakkoord staat dat als het gaat om overheidsbedrijfsvoering, inclusief ICT, er sprake zal zijn van een doorzettingsmacht. Welke minister heeft doorzettingsmacht en heeft de echte verantwoordelijkheid voor de ICT? Is dat de minister van EL&I, de minister van Justitie of de minister van Binnenlandse Zaken en Koninkrijksrelaties? Wie is "in charge" en wie is aanspreekbaar? Ik vraag een onafhankelijk onderzoek naar de staat van de veiligheid van de ICT bij de overheid. Een heleboel dingen zijn al toegezegd, maar ik wil graag dat er door een onafhankelijke naar wordt gekeken.

De **voorzitter**:
Tot slot.

De heer **Heijnen** (PvdA):
Tot slot kent het Nationaal Uitvoeringsprogramma, het samenwerkingsverband met andere bestuursorganen, nog geen programmaonderdeel digitale veiligheid. Ik vraag de regering, dat expliciet onderdeel te laten zijn van het Nationaal Uitvoeringsprogramma opdat alle andere bestuursorganen de veiligheid van de ICT de prioriteit geven die zij verdient.

☐

Mevrouw **Hachchi** (D66):
Voorzitter. De overheid gaat met haar tijd mee en zet ICT en internet in bij haar communicatie met mensen. D66 is daarvan groot voorstander, maar de overheid moet niet de veiligheid uit het oog verliezen. Na alle ICT-problemen van de laatste tijd twijfel ik of de overheid wel "in control" is als het gaat om de betrouwbaarheid en veiligheid van haar belangrijkste communicatiekanaal met de mensen.

De minister was er in eerste instantie stellig van overtuigd dat er niets aan de hand was met PKI-Overheid. Kan hij toelichten waarop deze stelligheid was gebaseerd? Per welke datum heeft de overheid het operationeel beheer van DigiNotar overgenomen? De minister koos voor een langzame overname van het operationeel beheer. Kan ik vaststellen dat hij bij zijn besluitvorming het belang van operationele systemen hoger heeft ingeschaald dan het belang van Iraanse mensenlevens? Dat zou ik een uiterst kwalijke zaak vinden. Heeft de minister al een totaaloverzicht van de gevolgen van de hack? Daarmee doel ik niet alleen op de schade binnen Nederland maar vooral op de gevolgen die de hack heeft voor de Iraniërs.

De minister was duidelijk: hij heeft geen vertrouwen meer in DigiNotar. Tegelijkertijd is de Belastingdienst nog tot ver in 2012 afhankelijk van de certificaten van DigiNotar. Waarom moet dit zo lang duren? Is deze handmatige manier van werken wel veilig? Zijn er extra kosten aan verbonden voor ondernemers? Gaat dit ten koste van de efficiency en het gemak waarmee ondernemers belastingzaken digitaal kunnen regelen?

DigiNotar is helaas slechts een voorbeeld van ICT-problemen bij de overheid. Vorige week bleken websites van verschillende gemeenten beveiligingsproblemen te hebben. Op relatief eenvoudige wijze konden interne documenten worden bekeken en aangepast. DigiD-gegevens maar ook persoonsgegevens van medewerkers van gemeenten en de politie waren niet veilig. De vraag rijst hoe deze beveiligingsproblemen zich kunnen voordoen. Daarnaast was de schade beperkt geweest als er een plan B was. Nu gaan digitale loketten en internetdiensten van de overheid meteen uit de lucht. Is er inmiddels wel een plan B zodat systemen kunnen blijven doordraaien bij een digitale aanval?

Vooruitkijkend stel ik vier punten aan de orde, te beginnen met het belang van privacy. Het is maar de vraag of meer toezicht op certificaatverstrekkers bijdraagt aan meer veiligheid. De oplossing ligt wat mij betreft in zo veel mogelijk voorkomen. De overheid dient uiterst terughoudend te zijn met het verzamelen van persoonsgegevens of andere gevoelige gegevens. Is de minister het op dit punt met mij eens?

Mijn tweede punt is het alternatief voor het certificatensysteem. In de brief van 16 september zeggen de ministers toe dat zij op internationaal niveau de DigiNotar-problematiek actief zullen uitdragen. Ik vraag de ministers, hierin een stap verder te gaan en internationaal uit te dragen dat moet worden gezocht naar een alternatief voor het certificatensysteem. Ook vraag ik de ministers, een onafhankelijk wetenschappelijk onderzoek hiernaar te laten doen.

Mijn derde punt is het opdrachtgeverschap. Tijdens de hoorzitting werd door verschillende partijen beaamd dat er binnen de overheid te weinig ICT-kennis aanwezig is. Dit heeft gevolgen voor de kwaliteit van aanbestedingen en contractmanagement. Dit geldt ook voor lokale overheden. Is de minister bereid, te onderzoeken – voor zover dat nog niet gebeurt – hoe de ICT-kennis en -expertise binnen de overheid het beste kan worden gedeeld?

Mijn vierde punt: de hackers. In de afgelopen weken hebben hackers de beveiliging van computersystemen van de overheid blootgelegd. Is de minister bereid te onderzoeken hoe de overheid de beveiliging van haar computersystemen kan verbeteren met de expertise van hackers, zonder dat de hackers hier strafrechtelijke consequenties van ondervinden? Zo kunnen hackers bijvoorbeeld overheidssites testen voordat deze online gaan. Welke mogelijkheden ziet de minister?

Voorzitter. Tot slot. De ICT-problemen bij de overheid vragen om een uitgebreid, onafhankelijk en zorgvuldig onderzoek. De D66-fractie acht het wenselijk dat de Algemene Rekenkamer onderzoek pleegt naar, en een deskundig oordeel velt over, DigiNotar als specifieke casus en ICT bij de overheid in het algemeen.

☐

De heer **El Fassed** (GroenLinks):
Voorzitter. De Nationale ombudsman zei het al: als de overheid een bank was, was ze allang failliet. Het lukt banken blijkbaar beter om gegevens van haar klanten te beveiligen dan de overheid. Het DigiNotar-debacle, hoe ernstig ook, is een symptoom van een chronisch zieke relatie tussen ICT en de overheid, en voor het gebrekkige belang dat door de overheid wordt gehecht aan de veiligheid van ICT en onze privacy. Dan kan de overheid wel naar een dokter gaan of naar een specialist, maar wat echt nodig is, is het aanpassen van de levensstijl.

Ik begin met DigiNotar. Er wordt al tien jaar gewaarschuwd voor de risico's van het certificaatsysteem. Tien jaar, en nog zijn de alarmbellen niet gehoord. Ook niet toen in 2009 Turkse en Iraanse hackers toesloegen, toen

in maart 2011 het bedrijf Comodo, een andere leverancier van certificaten, werd gehackt en toen in juni opnieuw een hacker toesloeg bij DigiNotar. Na onderzoek bleek hoe ernstig het was. Het leek wel alsof op de service van DigiNotar een heel grote sticker zat met de tekst: Ahmadinejad, kom maar binnen met je knecht. De gevolgen van die laksheid zijn enorm, hier in Nederland, waar het vertrouwen in het systeem is beschadigd, maar bovenal voor de meer dan 300.000 afgetapte Iraanse internetgebruikers, wier leven letterlijk afhangt van de anonimiteit van internet.

Afgelopen weekend kwam het bericht dat ongeveer 50 websites van gemeenten lek zijn. Persoonlijke gegevens bleken slecht beveiligd te zijn, de systemen draaiden op oude software en het was mogelijk om bestanden op te halen, te bekijken, te verwijderen of iets toe te voegen. De vraag van vandaag is of de minister eindelijk bereid is om daar lessen uit te trekken. Het is mooi dat er een meldplicht is voor datalekken, maar niet elk ICT-incident is een datalek. Het vertrouwen van mensen is gebaat bij openheid. Is de minister bereid de mogelijkheid te onderzoeken om de meldplicht niet te beperken tot datalekken, maar uit te breiden naar ICT-beveiligingsincidenten?

Vooralsnog laat deze minister niet zien dat het belang van een veilig beheer van privégegevens tot hem is doorgedrongen. Deze minister koketteert met zijn vulpen. Ik gun hem die van harte, maar ik wil hem er wel op wijzen dat het digitaal opslaan van persoonsgegevens andere risico's met zich meebrengt dan papieren dossiers. De overheid slaat gulzig allerlei gegevens van haar burgers digitaal op in de GBA, het elektronisch patiëntendossier of in een database van biometrische gegevens. De burger heeft vaak geen keuze in de opslag van die gevoelige informatie. Dan is toch het minste wat de overheid kan doen, daar zo zorgvuldig mogelijk mee om te gaan? Liever zien we grote terughoudendheid met de opslag van die gegevens. Waarom loggen we nog steeds in met alleen een wachtwoord, en niet met een identifier zoals bij de banken? Waarom worden privacy en veiligheid nog steeds gezien als een toevoeging aan het eind van een project, en niet als een fundamenteel onderdeel ervan? In de aanbesteding moeten er eisen komen voor de controle van opgeleverde systemen en diensten, met name op het gebied van veiligheid en privacy. Is de minister bereid om dat te regelen? Controle moet gericht zijn op procedures, mensen én techniek. Procedures moeten waterdicht én openbaar toegankelijk zijn; ze moeten bovenal worden nageleefd. Hoe gaat de minister ervoor zorgen dat de controle wordt verbeterd?

Mensen willen weten of het veilig is en of de privacy wordt geborgd. Wat doet de minister met de aanbevelingen die de WRR doet in haar rapporten over de e-overheid? Waarom heeft het kabinet nog steeds geen reactie gegeven op die rapporten?

Voorzitter. Het DigiNotar-debacle is een symptoom. De overheid verspilt nog altijd enorm veel geld met grote ICT-projecten. Tegelijkertijd besteedt de overheid te weinig aandacht aan privacy en veiligheid en kiest ze niet voor de beste beveiliging. We weten wat er misgaat. Onderzoek na onderzoek, lek na lek kunnen we hier staan om ons ongenoegen kenbaar te maken. We weten hoe het wel moet, maar niet waarom het de overheid nog steeds maar niet lukt om privacy en veiligheid bovenaan te zetten.

Die vraag moet beantwoord worden. Dat kan middels een parlementair onderzoek. Misschien is het echter ook een idee dat de minister een gezant voor ICT en veiligheid aanstelt, een expert van buitenaf, bijvoorbeeld uit de financiële sector, die het ICT-beleid van de overheid kan doorlichten, net als minister van VWS Hoogervorst in 2004 de topman van TPG aanstelde om de logistieke processen in de ziekenhuiszorg door te lichten. Ik hoor graag een reactie op dit voorstel.

□

Mevrouw **Hennis-Plasschaert** (VVD):
Voorzitter. De zaak Diginotar was en is een enorme wake-upcall. Er lijkt heel lang sprake te zijn geweest van een welhaast ongefundeerd vertrouwen in ICT-infrastructuur, -diensten en -producten en vooral in de veiligheid daarvan. Dat geldt niet alleen voor de overheid, maar veelal ook voor burgers en bedrijven. Passende informatiebeveiliging moet een vast gegeven zijn, maar is het nog niet. Integriteit, continuïteit en beschikbaarheid zijn de uitgangspunten en vertrouwen in een vrije en veilige digitale samenleving het doel.

Voor de VVD-fractie is het van belang dat de verdere uitwerking van de Nationale Cyber Security Strategie niet tot stand komt aan de hand van incidenten. Het draait uiteindelijk om het voorkomen van incidenten en het inbouwen van de juiste waarborgen daarvoor. Uiteraard realiseert ook de VVD-fractie zich dat er vele ontwikkelingen gaande zijn op het terrein van cyber security, maar zij moet vaststellen dat het hapsnapgehalte nog altijd aanzienlijk is. Er is sprake van onvoldoende samenhang en onvoldoende samenwerking.

In dat kader verwacht de VVD-fractie veel van het nog op te richten Nationaal Cyber Security Centrum, het NCSC. De vraag is of het NCSC straks beschikt over alle benodigde instrumenten en mogelijkheden om daadwerkelijk zaken af te dwingen. Wat is precies het takenpakket van het NCSC? Gaat het centrum die vraagbaak in brede zin zijn? Wordt opgebouwde kennis en expertise beschikbaar gesteld aan derden, overheden en bedrijven, bijvoorbeeld in de vorm van good practices? Krijgt het centrum de regie wat betreft een eenduidig beveiligingsbeleid, inclusief beveiligingseisen?

De minister van Veiligheid en Justitie, zo lezen wij in beleidsstukken, heeft de regie op de samenhang en samenwerking op het terrein van cyber security. Daarnaast behoudt ieder departement zijn eigen taken en verantwoordelijkheden. Dat klinkt natuurlijk logisch, maar ik mag toch hopen dat dit in de praktijk niet betekent dat ieder departement opnieuw het wiel moet gaan uitvinden. Ik mag hopen dat straks ook daar regie op zit vanuit het NCSC. Als ieder departement, maar ook iedere gemeente, zijn eigen dingetje blijft doen en daarbij vooral niet wordt gehinderd door enige kennis van zaken dan blijft de overheid, zo kan ik verzekeren, zo lek als een mandje.

Mevrouw **Gesthuizen** (SP):
Wat het laatste betreft, was ik in elk geval teleurgesteld in de zin in de brief naar aanleiding van de lekken bij de gemeenten waarin werd gesteld dat het in eerste instantie allemaal bij de gemeenten zou blijven en dat het een verantwoordelijkheid van de gemeenten is.

Mevrouw Hennis heeft een aantal zaken genoemd die wat haar betreft mogelijkerwijs bij het NCSC ondergebracht kunnen worden. Moet volgens haar het NCSC ook een soort dienst worden die – ik noem het een digitale brandweer, maar iemand anders kan dat heel anders noe-

men – orde op zaken stelt, direct kan uitrukken en kan ingrijpen als er een noodsituatie is, zoals bij Diginotar het geval was?

Mevrouw **Hennis-Plasschaert** (VVD):
Je kunt spreken over een digitale brandweer of een digitale ambulance. Het gaat erom dat wij een expertisecentrum hebben dat de expertise direct beschikbaar stelt als er brand is, als er een zieke is of als er een gewonde is. In dat opzicht sluit ik mij aan bij de formulering die eerder is gebruikt.

Mevrouw **Gesthuizen** (SP):
Een expertisecentrum is een instantie die ik bel als ik advies wil. Moet het NCSC ook uitrukken?

Mevrouw **Hennis-Plasschaert** (VVD):
Ja, wat mij betreft rukt het ook uit.

Gaat het NCSC ook rol spelen of, beter nog, de leiding nemen bij het stellen van nadere eisen aan certificatenleveranciers die onder het PKI(-Overheid) stelsel certificaten verstrekken? Zal het NCSC samenwerken met de OPTA waar het gaat om nader overleg met de auditorganisaties over de wijze waarop de audits beter kunnen bijdragen aan de kwaliteit van de certificaatverstrekkende bedrijven?

De Cyber Security Raad is onlangs van start gegaan, maar de exacte rol van die raad is mij volstrekt onduidelijk. Stuurt deze bijvoorbeeld straks het NCSC aan? Wat kunnen wij van deze raad verwachten en waarop is deze aanspreekbaar?

Het vergroten van de eigen weerbaarheid is cruciaal om het vertrouwen in de digitale overheid terug te winnen. De vraag is of de vitale organisaties in de sectoren openbaar bestuur en openbare orde en veiligheid inmiddels beschikken over een continuïteitsplan.

Is er een beveiligingskader vastgesteld voor informatiebeveiliging van de rijksdienst? Wat is de huidige responscapaciteit van de Nederlandse overheid bij ICT-verstoringen, incidenten en cyberaanvallen?

De brede meldplicht datalekken voor alle aanbieders van informatie is al genoemd. Die brede meldplicht is reeds afgelopen voorjaar aangekondigd. De VVD-fractie juicht de komst van zo'n meldplicht toe. Hierbij gaat het echter vooral om inbreuken die rechtstreeks leiden tot het verlies van persoonsgegevens en minder om een security breach, een systeeminbreuk zoals in het geval van DigiNotar. Hoe denkt de minister hierover?

De drie sporen die zijn uiteengezet in de brief van 16 september jl. zijn hoopgevend. Er zijn echter nog vraagtekens te plaatsen. De heer Heijnen plaatste er al een paar. Ik noem als voorbeeld de eisen aan certificatenleveranciers die onder het stelsel PKI-Overheid certificaten verstrekken. Zijn er wel of niet gekwalificeerde certificaten gebruikt? Als dat niet het geval is, welke eisen zijn dan aan de beveiliging van de systemen van certificatenleveranciers en aan hun organisatie gesteld? Hoe vond de controle op de naleving daarvan plaats? Kan de minister verklaren dat hij jaarlijks een controle liet uitvoeren op de naleving? Was er ook sprake van controle op de locatie van DigiNotar? Hoe kon het gebeuren dat DigiNotar ondanks certificering de meest basale beveiliging niet op orde had? Wordt de rol van de auditeur in dezen nog nader onderzocht? Ik noem nog een open zenuw: wat was de rol van Logius? In hoeverre kan hier überhaupt nog worden gesproken over goed opdrachtgeverschap? Welke maatregelen heeft Logius getroffen om het opdrachtgeverschap goed in te vullen? Kan de minister ons hierover nader informeren en zo nodig rapporteren? Ik noem ook de blunders die keer op keer worden gemaakt met DigiD. Welke maatregelen is de minister in dezen voornemens te nemen?

De VVD-fractie wil ook meer informatie over de financiële consequenties van heel dit gebeuren. Nu DigiNotar failliet is verklaard, lijkt de kans op schadevergoeding immers zo goed als nihil.

De VVD-fractie wil tot slot graag benadrukken dat wij het aan onze stand verplicht zijn om tot op de bodem uit te zoeken in welke mate het Iraanse regime betrokken is geweest bij de inbraak en falsificatie, of welk voordeel het regime hiervan heeft gehad. Ook andere collega's hebben benadrukt dat het hierbij gaat om mensenlevens.

De heer **Heijnen** (PvdA):
Ik sluit mij zeer aan bij wat mevrouw Hennis zei over de rol van het Iraanse regime. Verder viel het mij op dat mevrouw Hennis een vraagteken plaatst achter iedere zin uit naar ik meen het antwoord van het kabinet op een van de vragen in de bijlage bij de brief van 16 september. In dat antwoord omschrijft het kabinet hoe het zit met de PKI-Overheid. Heeft de jaarlijkse extra controle wel plaatsgevonden? Wat was het plan van eisen voor de PKI-Overheid? Welk gecertificeerd bedrijf deed de audit? Uit het feit dat mevrouw Hennis die vraagtekens plaatst, blijkt dat zij, net als ik, de waarheid van die zinnen in twijfel trekt. Dat doen wij uiteraard totdat het tegendeel is gebleken.

Mevrouw **Hennis-Plasschaert** (VVD):
Zo is dat.

De heer **Heijnen** (PvdA):
Is mevrouw Hennis het met mij eens als ik zeg dat wij daarop eerst echt goed zicht moeten hebben voordat wij überhaupt over de toekomst kunnen spreken?

Mevrouw **Hennis-Plasschaert** (VVD):
Als de heer Heijnen nu probeert mijn steun te krijgen voor een diepgaand onderzoek naar het verleden, dan zeg ik hem dat de ministers prima in staat zouden moeten zijn om daar voor eens en voor altijd duidelijkheid over te geven. Ik wil graag vooruit kijken, het NCSC op gaan tuigen en ervoor gaan zorgen dat dit zich niet herhaalt.

De heer **Heijnen** (PvdA):
Op dit punt zou ik niets liever willen dan zelfs leden van dit kabinet en zelfs de man met de vulpen het vertrouwen geven. Voor mij begint dat vertrouwen echter bij de erkenning dat er iets fundamenteel mis was. Dat treft niet alleen de ministers, maar ook de mensen die dat voor hen hebben opgeschreven. Dat moet echt uit de wereld worden geholpen. De ministers kunnen dat straks proberen te weerleggen. Ik zie daarnaar uit. Ik vrees dat zij daar echter niet in slagen. Als dat niet uit de wereld geholpen kan worden, dan moet dat consequenties hebben. Ik vraag niet om een parlementaire controle naar het begin van de mensheid en naar de vraag over zes of vijf dagen, maar ik wil wel dat de onderste steen vanavond boven komt.

Mevrouw **Hennis-Plasschaert** (VVD):
Net als de heer Heijnen wacht ik de beantwoording met belangstelling af.

Koopmans

□

De heer **Koopmans** (CDA):
Voorzitter. Voor ondergetekende was er in de nacht van 2 op 3 september letterlijk sprake van een wake-upcall. Mij werd gezegd: ga eens even voor de tv zitten jongen, want de minister van BZK gaat een persconferentie geven. Ik moet zeggen dat ik, ondanks het feit dat de daarbij zittende journalist drie keer uitlegde wat er aan de hand was, direct na de persconferentie in een soort staat van grote verbijstering voor de televisie zat.

Wat betekent dit en wat betekende dit? Ik moet zeggen dat de CDA-fractie op zich eigenlijk heel tevreden is over de manier waarop de regering de zaak heeft aangepakt vanaf het moment dat zij wist wat er aan de hand was. VNO-NCW heeft dit de afgelopen week ook aan de Kamer laten weten. Het is heel interessant om te zien dat er sprake is van een zekere weerbaarheid van het systeem. De eerste uren en dagen waren er velen die zeiden dat het systeem zou imploderen. Dat is niet gebeurd. Die conclusie is gelukkig ook te trekken.

Is de CDA-fractie tevreden over het feit dat het zo ver kon komen? Nee, mevrouw de voorzitter, dat is de CDA-fractie niet. Het toezicht is, blijkens het gebeurde, niet goed genoeg geregeld en de regelgeving dateert al uit 2003. Regelgeving voor internet die stamt uit 2003, dat is toch op zich al een tegenstrijdigheid? Is het niet zo dat de kaderstelling die de Rijksoverheid op het punt van veiligheid van internet formuleert continu aandacht moet krijgen? Je kunt zelfs niet zeggen dat je het jaarlijks of tweejaarlijks moet doen, want er kunnen zich iedere dag nieuwe ontwikkelingen voordoen die nopen tot een nieuwe kaderstelling voor veiligheid. Deelt de regering deze opvatting? Wil zij het toezicht en de kaderstelling op dit punt aanpassen, zodat er continu stappen gezet kunnen worden? De audits zijn natuurlijk ook onvoldoende geweest, te veel procedureel en te weinig het echte werk. Ik kan niet meer de vraag stellen of het tweedelijnstoezicht bij de OPTA op basis van die audits voldoende was, want uiteindelijk is gebleken dat het niet voldoende was.

Het is van belang dat de overheid zorgvuldig en precies kaders stelt. Ondanks dat er Kamerleden zijn die zeggen dat het lek boven moet komen, weet iedereen dat internet uiteindelijk nooit 100% veilig zal zijn. Er zullen altijd lekken zijn. Eerlijkheidshalve zullen wij dit tegen de Nederlandse samenleving moeten zeggen. Suggereren dat er sprake zou kunnen zijn van 100% veilig internet is een utopie.

De **voorzitter**:
Uw bijdrage maakt blijkbaar veel los, mijnheer Koopmans. Twee collega's willen u een vraag stellen. Als eerste is het woord aan mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP):
Het valt reuze mee, voorzitter, maar ik meende uit het tweede deel van de opmerking van de heer Koopmans te proeven dat ik zou suggereren dat er 100% veiligheid moet zijn. Dat is zeker niet het geval. Ik heb ook een vraag aan de heer Koopmans. We weten inderdaad dat internet niet 100% veilig is. Risico's kun je niet uitsluiten. Je kunt wel het gevaar beperken door de risico's zo veel mogelijk in kaart te brengen en daar een passend systeem voor te vinden. Is de heer Koopmans het met mij eens dat we in de virtuele wereld, net als in de tastbare, dagelijks werkelijke wereld waarin we ook nooit kunnen voorkomen dat er ongelukken en rampen gebeuren, instituten moeten hebben die à la minute kunnen uitrukken als er zich een ramp, een crash of een debacle voordoet zoals bij DigiNotar?

De heer **Koopmans** (CDA):
Daar ben ik het mee eens. Daarom sluit ik mij kortheidshalve aan bij de vragen die mevrouw Hennis-Plasschaert heeft gesteld over de NCSC.

Mevrouw **Hachchi** (D66):
Ik denk dat iedereen het met de heer Koopmans eens is dat 100% veiligheid op internet niet mogelijk is. Hij begon zijn inleiding positief door te zeggen dat de crisissituatie goed werd opgepakt door het kabinet. Vervolgens vroeg hij zich af hoe het zo ver kon komen. De heer Koopmans zit al een wat langere periode in de Kamer. Als hij in het licht van zijn opmerkingen naar andere ICT-problemen bij de overheid kijkt, vindt hij dan niet dat je verschuilen achter 100% veiligheid van internet eigenlijk te ver gaat? Het is geen argument; er is natuurlijk meer aan de hand op het vlak van ICT en overheid.

De heer **Koopmans** (CDA):
Ik denk dat er verschillende trajecten zijn waarbij je deze parallel zou kunnen trekken. De ov-chipkaart is er daar een van. In dat geval is vooral de Kamer op zoek geweest naar een ultiem, doch uiteindelijk niet-bestaand, systeem. Bij het EPD was een andere discussie aan de orde, die ik hier niet in haar geheel wil overdoen. In dat geval ging het veel meer over privacy.

Ik denk dus dat wij elk project op zich moeten bekijken. Dat doen wij in deze Kamer. Het lijkt mij te gemakkelijk om alle ICT op één hoop gooien en te stellen dat het altijd een bende wordt zodra de overheid erbij betrokken is. Het is ingewikkeld, zoals ook het bedrijfsleven weet. Er zijn veel problemen te overwinnen en die moeten wij aanpakken. Daarom is het goed dit soort debatten te voeren.

Mevrouw **Hachchi** (D66):
Ik deel de opmerking van de heer Koopmans dat wij niet alle ICT-problemen bij de overheid op één hoop kunnen gooien, maar ook de heer Koopmans heeft tijdens de hoorzitting gehoord over de verschillende vormen van ICT-problemen bij de overheid. Wij kunnen op grond daarvan toch de conclusie trekken dat er meer aan de hand is. Dat kunnen wij toch niet afdoen met de opmerking dat wij 100% veiligheid op het internet niet kunnen garanderen? Dat is de heer Koopmans toch met mij eens?

De heer **Koopmans** (CDA):
Dat ben ik absoluut met mevrouw Hachchi eens. Daarom ook heb ik een paar conclusies getrokken en vragen gesteld over het voortraject tot aan 2 en 3 september.

De heer **El Fassed** (GroenLinks):
De heer Koopmans is blij dat het vanaf 3 september allemaal goed is gegaan. Op de maandag daarvoor werd bekend dat er een ernstige inbreuk had plaatsgevonden. Dat kreeg GOVCERT te horen van haar Duitse collega's. Op dat moment was er eigenlijk al sprake van een vertrouwensbreuk, omdat DigiNotar op dat moment had moeten melden dat er een probleem was. DigiNotar heeft dat niet gedaan, want OPTA en PwC wisten van niets. Had men op dat moment niet expliciet het vertrouwen moeten op-

zeggen en een onderzoek moeten doen? Nu was het probleem er al een week.

De heer **Koopmans** (CDA):
Als DigiNotar sneller was geweest en GOVCERT.NL eerder conclusies had getrokken, hadden wij inderdaad een aantal uren kunnen winnen.

De heer **El Fassed** (GroenLinks):
De ministers namen het besluit pas vrijdagnacht, terwijl zij dat besluit al op maandag hadden kunnen nemen.

De heer **Koopmans** (CDA):
Op basis van wat ons op dit punt gemeld is en wat ik gelezen heb, kan ik niet anders dan de conclusie trekken dat vanaf het moment dat de bewindslieden ingelicht zijn, zij in mijn ogen hebben gedaan wat zij moesten doen: niet ongeïnformeerd in het wilde weg aan de slag gaan, maar, na enkele juiste stappen gezet te hebben, zo snel mogelijk conclusies trekken, die delen en maatregelen nemen. Natuurlijk hadden de bewindslieden eerder ingelicht moeten worden en had het contract met DigiNotar een verplichtender karakter moeten hebben op het vlak van het melden van problemen.

De heer **El Fassed** (GroenLinks):
DigiNotar werd vertrouwd door OPTA. Het was een trust party, dus dat betekent extra verplichtingen, onder meer het melden als er iets mis is. Toen de ministers hoorden dat op maandag niet gemeld was dat er iets mis was, hadden zij meteen het vertrouwen moeten opzeggen. Is de heer Koopmans het daarmee eens?

De heer **Koopmans** (CDA):
De heer El Fassed kent mij als een net iemand, maar toch heb ik zo-even in nette bewoordingen een tikje uitgedeeld aan de OPTA. Ik begrijp dus wat de heer El Fassed zegt. Er had tijd bespaard kunnen zijn, maar vanaf het moment dat de bewindslieden van de inbreuk in kennis zijn gesteld, is er gehandeld zoals er gehandeld had moeten worden.

Vervolgens een opmerking over lektober. Hackers blijven interessant. Je kunt het vergelijken met je eigen woning. Er zijn twee manieren om je te vertellen dat je huis niet goed beveiligd is. Volgens de eerste manier loopt iemand van de politie om je huis heen en attendeert je vriendelijk op de zaken waar je iets aan zou moeten doen. Volgens de tweede manier komt er iemand langs met een bivakmuts en een koevoet. Als die geweest is, weet je dat de beveiliging van je huis niet op orde was. Hoe kijkt met name de minister van BZK daar tegenaan? Op zich is het interessant om te zien dat Webwereld, de technologiewebsite, bezig is met lektober, de maand van het privacylek. Als burgers gaten aanwijzen in de beveiliging van overheidssites, zouden wij hun eigenlijk een bos bloemen moeten geven. Tegelijkertijd kunnen wij ons afvragen of door de activiteiten van die burgers geen schade ontstaat.

Is het eigenlijk niet veel beter als de dames en heren hackers – en dan doel ik op het vriendelijke deel ervan, want het onvriendelijke deel zal ik niet kunnen aanspreken – een bv'tje maken, van negen tot vijf werken op een adres dat we allemaal kennen en daarna gewoon de rekening sturen? Dat lijkt mij veel beter dan de huidige werkwijze.

De **voorzitter**:
Ik geef mevrouw Hachchi de gelegenheid voor een korte vraag, anders zitten we hier straks om twee uur nog.

Mevrouw **Hachchi** (D66):
Ik houd het heel kort. Kan de heer Koopmans zich aansluiten bij mijn vraag aan beide ministers om te kijken wat de mogelijkheden zijn om de expertise van hackers te gebruiken om de overheidssites beter te beveiligen? Dan stellen we die vraag natuurlijk samen aan het kabinet.

De heer **Koopmans** (CDA):
Ja, mijn opmerkingen daarover impliceren dat absoluut. Ik wil zelfs nog een stapje verder gaan en er hier en daar voor betalen. Ik kan me daar echt wat bij voorstellen.

De **voorzitter**:
U rondt nu uw verhaal af!

De heer **Koopmans** (CDA):
Voor de burger moet duidelijk zijn wat veilig is en wat niet. Dat is nu nog niet helemaal het geval. Het systeem is niet geïmplodeerd, maar het moet duidelijk zijn dat iedereen weet waarop hij wel en niet kan vertrouwen. Ik zie dat mijn spreektijd op is, maar ik wil de minister vragen om er in elk geval met de gemeentelijke overheden voor te zorgen dat de huidige situatie, waarin te veel sites van gemeentelijke overheden niet veilig zijn, zo snel mogelijk conform de gestelde kaders wordt georganiseerd.

□

De heer **Elissen** (PVV):
Voorzitter. Dit debat had in plaats van DigiNotar en ICT-problemen bij de overheid ook DigiD en ICT-problemen bij de overheid kunnen heten, of het elektronisch patiëntendossier en ICT-problemen bij de overheid, of systemen voor de politie en ICT-problemen bij de overheid. U begrijpt wat ik bedoel: neem een deel overheid en een deel ICT en je hebt het recept voor mislukking in handen: een deel overheid en een deel ICT, "shaken, not stirred". Laten we deze cocktail in dit geval maar niet de DigiNotar Sunrise noemen, want voor DigiNotar komt de zon voorlopig niet meer op.

Tijdens de hoorzitting had een van de deskundigen het over consultants die in hun leasebak gierend van het lachen rondjes reden om de ministeries. Gierend van het lachen, omdat ze vorstelijk betaald werden en niemand binnen de muren van de ministeries ook maar een idee had waar ze mee bezig waren. Tijdens de hoorzitting werd ook pijnlijk duidelijk dat de huidige audits tekortschieten. Volgens de audit was het zogenaamd allemaal prima in orde, maar in de praktijk was DigiNotar zo lek als een mandje. Daar gaat iets dus structureel fout.

Ook bleek dat toezicht in andere opzichten te falen. Kan de minister nog eens uitleggen hoe het toezicht is geregeld en hoe hij ervoor gaat zorgen dat de certificaatautoriteiten onder eerstelijns toezicht worden gesteld? Gaat de minister er ook voor zorgen dat minimaal jaarlijks penetratietesten uitgevoerd worden op belangrijke overheidssystemen? Zo nee, waarom niet?

Ondertussen is het de maand "lektober" geworden. Deze maand zal de website webwereld elke dag een overheidslek openbaren. Wat je er ook van vindt, de overheid is echt zelf aan zet. De overheid is aan zet om het vertrouwen van de burger terug te winnen. We kunnen nu heel

diep op de DigiNotar-zaak ingaan, maar we kunnen ook kijken welke lessen we kunnen leren.

ICT is niet iets magisch; wel is het moeilijk, nieuw en complex. Niemand heeft een recept voor absoluut succes in handen. We weten inmiddels wel wat de ingrediënten zijn die gegarandeerd tot falen leiden. Uit de brief over DigiNotar wil ik twee korte citaten geven. "Het kabinet kreeg op 2 september onmiskenbare signalen dat de uitgifte door het bedrijf DigiNotar van PKI-Overheid-certificaten mogelijk gecompromitteerd was door een inbraak in de bestanden van het bedrijf met als eventueel gevolg dat deze certificaten frauduleus uitgegeven zouden zijn. "In aansluiting daarop is het kabinet in overleg getreden met verschillende overheids- en bedrijfssectoren teneinde een volledig beeld te krijgen van de mogelijke risico's, de maatregelen die in verband daarmee nodig zijn en de stappen die nodig zijn om het vertrouwen in veilige digitale communicatie zo snel mogelijk te herstellen."

Uit deze citaten blijkt zeer duidelijk dat de overheid niet goed genoeg nadenkt over internetveiligheid en de bescherming tegen cybercrime. De PVV-fractie pleit er al langer voor om databeveiliging te benaderen op soortgelijke wijze als rampenbestrijding. Nu wordt er steeds gewacht tot er een incident optreedt. Er worden onvoldoende voorzorgsmaatregelen getroffen en er ligt geen noodplan klaar. Als je een schuur bouwt die je volstopt met gevaarlijke stoffen terwijl je geen brandveiligheidsmaatregelen treft, dan kun je wachten op een brand. Op dezelfde manier is de inbraak bij DigiNotar een gevolg van het slecht op orde hebben van de veiligheid.

Het gaat op een gegeven moment fout. Dan moet er dus een plan klaarliggen en dient er een eenkoppige leiding te zijn en een duidelijke commandostructuur. Het dient duidelijk te zijn wie er "in charge" is. Dat moet niet elke keer als er iets misgaat ter plekke besproken en beslist worden, maar dat moet vooraf duidelijk zijn. Afstemmen en samenwerking zijn vanzelfsprekend, maar regie is broodnodig. Gelukkig hebben wij bij het algemeen overleg over de voortgangsrapportage van de terrorismebestrijding eindelijk duidelijkheid gekregen van minister Opstelten: hij heeft de regie. Punt. Daar is de PVV-fractie erg blij mee, maar misschien kan de minister dit in zijn beantwoording nogmaals benadrukken.

Laat ik verdergaan met het benoemen van wat de PVV graag anders ziet aan de kant van de overheid. De overheid moet haar rol als opdrachtgever beter waarmaken. Om iets te bouwen, moet je zelf enige kennis van zaken hebben. Waar het de ICT betreft, denkt de overheid een flatgebouw te kunnen bouwen door twintig bungalows te bestellen die vervolgens door een interieurarchitect op elkaar worden gestapeld. Dat is vragen om problemen. Daarom: meer kennis en kunde bij de overheid, meer ruimte voor vakmanschap op het departement en strakker toezicht op leveranciers. De overheid moet onafhankelijker worden en meer controle uitoefenen. Nu is de overheid wat betreft ICT te veel een speelbal van het bedrijfsleven. De aanwezige kennis en kunde moeten beter aangewend en desgewenst gecentraliseerd worden.

De PVV blijft ook pleiten voor het gebruik van privacy by design en safety by design bij alle ICT-projecten van de overheid. Vindt de minister dit ook een goed idee? Zo nee, waarom niet? Hier wil ik het in eerste termijn bij laten.

De **voorzitter**:
Ik zie dat mevrouw Gesthuizen een korte vraag heeft,

Mevrouw **Gesthuizen** (SP):
Ik heb zelfs twee korte vragen. De eerste vraag slaat op de opmerking van de heer Elissen waar ik heel blij mee ben: wij leren ook lessen. Wij kunnen natuurlijk inzoomen op DigiNotar, maar er zijn ook allerlei andere debacles en wij moeten lessen leren. Is hij bereid dat te doen via een onderzoek en zo ja, in welke vorm moet dat gebeuren? Mijn tweede vraag is de volgende. Het is natuurlijk heel plezierig dat minister Opstelten de regie heeft, maar hij kan niet iedere keer als er ergens een ICT-probleem is in zijn eentje uitrukken. Wie, waar en wat moet minister Opstelten – ik zie dat minister Donner hem wil vergezellen, dat scheelt natuurlijk weer – aansturen om een goede digitale brandweerman te zijn?

De **voorzitter**:
De vraag is helder, de heer Elissen gaat antwoorden.

De heer **Elissen** (PVV):
Ik dacht even in de twinkeling in de ogen van mevrouw Gesthuizen een beeld te zien van het A-team dat onderweg was, maar ik heb alle vertrouwen in de beide ministers. Ik moet inderdaad bekennen dat voor ons belangrijk is dat een bewindspersoon duidelijk de regie voert. Afhankelijk van de situatie die zich aandient, of dat nou cyber warfare is of dat de wind uit een andere hoek waait, moet een persoon de boel constant in de peiling houden. Ik hoop dat daarmee de vraag voldoende beantwoord is.

Mevrouw **Gesthuizen** (SP):
En het onderzoek?

De heer **Elissen** (PVV):
Het onderzoek was mij inderdaad even ontschoten. Wat ons betreft moet dit volledig gefileerd worden. Wij hebben schriftelijke vragen gesteld en tot mijn grote vreugde was er vrijdagnacht om 01.00 uur al een persconferentie en werden er stappen gezet. Er zijn ook middels de brief en anderszins toezeggingen gedaan en er lopen al onderzoeken. Laten we eerst afwachten wat daaruit komt en of we daarmee genoegen kunnen nemen. Ik onderschrijf uw pleidooi om ervoor te zorgen dat we dit glashelder krijgen. Nogmaals, de burger heeft recht op een betrouwbare overheid en internet moet veilig zijn. Ik ben het met u eens dat 100% veiligheid niet bestaat, maar laten we dan wel gaan voor een zo hoog mogelijk percentage.

De **voorzitter**:
Hiermee zijn wij gekomen aan het einde van de eerste termijn van de Kamer. De ministers hebben een korte schorsing gevraagd.

De vergadering wordt van 21.37 uur tot 21.55 uur geschorst.

□

Minister **Donner**:
Voorzitter. De directe aanleiding voor het debat van vandaag is hetgeen gebeurd is rond DigiNotar. We spreken breder over de sindsdien voortgaande discussie over de veiligheid van het gebruik van internet, in het bijzonder door de overheid. Dat heeft deze maand in het bijzonder de aandacht met de actie "Iektober". Ik wijs er overigens op dat die evenzeer gericht is op andere sites dan die van de overheid. Wellicht zijn BlackBerrygebruikers onlangs

ook gestoten op problemen die zich buiten de overheid voordoen. We hebben te maken met een verschijnsel, een gegeven, dat we in onze samenleving steeds meer afhankelijk raken van het gebruik van internet, op tal van toepassingen. Daarnaast geeft de overheid – laat ik het voorzichtig zo zeggen – er steeds meer de voorkeur aan dat het verkeer met de overheid op tal van punten gebeurt via internet of ICT-voorzieningen. Zeker in het verleden is de aandacht daarbij vooral uitgegaan naar de wijze waarop we dat zo snel mogelijk zo goed mogelijk kunnen doen. Wellicht is in dat proces soms minder adequaat aandacht besteed aan de veiligheidsaspecten. Door de voorvallen rond DigiNotar zijn ze allemaal weer scherp op het netvlies gekomen. In mijn antwoorden zal ik in het bijzonder ingaan op de aspecten van de overheid, die gebruikmaakt van internet, de specifieke situatie bij DigiNotar, de verschillende maatregelen en de discussiepunten die sinds die tijd aan de orde zijn geweest. Mijn collega van Veiligheid en Justitie zal breder ingaan op het beleid met betrekking tot cyber security en de maatregelen die in die sfeer worden genomen, op de beveiliging van persoonsgegevens en in het bijzonder op het functioneren van de voorzieningen op het terrein van crisisbeheersing en crisisbestrijding.

Omdat er door verschillende sprekers vragen zijn gesteld over wie de regie heeft en had, wou ik mijnerzijds alvast aan het begin duidelijk maken dat in het hele proces de minister van Veiligheid en Justitie de regie had. Ik was alleen de uitrukkende instantie onder die omstandigheden en daarom zag men mijn gezicht op de televisie. Hij lag grinnikend in zijn bed, terwijl ik nog op de televisie moest komen. Dat is de praktische situatie. Maar er is geen twijfel over dat hij de regie had.

Daar is een goed werkend systeem voor bij de overheid, dat kan worden aangepast naargelang de crisis waar je het over hebt. Op het terrein van ICT is het grote gevaar dat, omdat de letters ICT gebruikt worden, het beeld bestaat dat alles wat er op dat terrein kan gebeuren, van dezelfde aard is. Maar het kan heel verschillend zijn. In voorkomende gevallen zal steeds opnieuw bekeken moeten worden op welke wijze het best kan worden gereageerd.

Ik wil nog kort ingaan op de specifieke feiten, aangezien mevrouw Gesthuizen op het verloop van de feiten is ingegaan en ook de heer El Fassed daar vragen over heeft gesteld. Overigens verwijs ik naar de brieven die daarover geschreven zijn, waarin zo goed mogelijk de chronologie is weergegeven van wat er is gebeurd. Zoals bekend is GOVCERT.NL de organisatie die zich in het bijzonder bij de overheid bezighoudt met de beveiliging van websites en het gebruik door de overheid van ICT en internet. GOVCERT.NL heeft op maandag 29 augustus kennis gekregen van het gegeven dat een onbetrouwbaar certificaat werd gebruikt en toen onmiddellijk contact opgenomen met DigiNotar. GOVCERT.NL adviseerde op dinsdag 30 augustus afnemers van het eigen-merkgedeelte van DigiNotar over de certificaatproblematiek middels een factsheet "frauduleus uitgegeven beveiligingscertificaat ontdekt".

Voor alle duidelijkheid, het gaat om verschillende soorten certificaten. Ingevolge de wetgeving die in deze Kamer is behandeld berusten de beveiliging en het toezicht op de certificaten op zelfregulering. Hierbij ging het, althans volgens het bericht, om een eigen merkcertificaat van DigiNotar, een organisatie die dit soort certificaten afgeeft. Op het moment dat wordt meegedeeld dat een dergelijk certificaat frauduleus wordt gebruikt, is er op dat punt geen enkele bevoegdheid of geen enkel toezicht van de overheid. Die zaken zijn primair aan de organisatie die de veiligheid van zijn eigen producten moet bewaken. Tegelijkertijd is er door GOVCERT bij DigiNotar doorgevraagd.

Bij DigiNotar vindt een eerste terugkoppeling plaats op dinsdag 30 augustus, waarin meegedeeld wordt dat enkel de eigen merkcertificaten zijn geraakt en niet de PKI-Overheid-certificaten. Ik ga overigens straks in op de eisen die we daaraan stellen. Dat is zeer wel mogelijk, aangezien juist met het oog op de beveiliging voor PKI-Overheid-certificaten zwaardere eisen zijn gesteld aan onder andere de beveiliging. Op dat moment hadden we geen aanwijzingen dat andere dan de eigen merkcertificaten waren gecompromitteerd. DigiNotar schakelt op dinsdag 30 augustus Fox-IT in, mede om uit te sluiten dat PKI-Overheid-certificaten gecompromitteerd waren.

Op woensdag 31 augustus heeft een conferencecall plaats met DigiNotar. Daarin wordt aangegeven dat er geen nieuwe informatie is naar aanleiding van het onderzoek door Fox-IT.

Op donderdag 1 september heeft wederom een conferencecall plaats met DigiNotar, waarin wederom geen nieuwe informatie wordt gemeld naar aanleiding van het onderzoek door Fox-IT. Daarop wordt aangedrongen bij het bedrijf op inzage in de resultaten van dat onderzoek. Er wordt toegezegd dat die inzage gegeven zal worden op vrijdag 2 september. Bij de beheerorganisatie Logius, die verschillende overheidsvoorzieningen beheert die gebruikmaken van DigiNotar-certificaten, komen vragen van afnemers binnen over wat ze moeten doen. Omdat met alle scenario's rekening moet worden gehouden, adviseert Logius donderdag aan zijn doelgroep om te starten met een inventarisatie van de aanwezigheid van de PKI-Overheid-certificaten van DigiNotar, door welke processen die worden gebruikt en wat de gevolgen zijn als de PKI-Overheid-certificaten van DigiNotar niet meer zouden worden vertrouwd.

Ondanks aandringen geeft DigiNotar pas vrijdagmiddag middels een eerste mondelinge rapportage van Fox-IT aan dat niet kan worden uitgesloten dat de PKI-Overheid-certificaten mogelijkerwijs zijn gecompromitteerd. Het kabinet besluit vervolgens in overleg met DigiNotar en het moederbedrijf Vasco in de Verenigde Staten om het operationeel beheer van de systemen voor certificaten van DigiNotar over te nemen.

Mevrouw Hachchi heeft gevraagd waarom het voorgaande niet sneller kon. Het is in drie uur gebeurd, dus ik weet niet of het sneller kon. In ons rechtssysteem kunnen we niet zomaar binnenlopen bij een bedrijf en zeggen: weg hier, we nemen het over. Er heeft overleg plaatsgevonden met het Amerikaanse moederbedrijf. De reden waarom ik pas om 1.00 uur op televisie verscheen was omdat de gesprekken tussen 21.00 uur en 0.00 uur plaatsvonden.

In dat proces moest ook het moederbedrijf wennen aan het idee dat het om hun aansprakelijkheid ging en dat het geen poging van de Nederlandse overheid was om een Nederlands bedrijf over te nemen. Om twaalf uur was de toegang verleend aan een beheerder van de overheid. Het beeld dat wij dit langzaam hebben gedaan is dus ten enenmale onjuist.

De heer El Fassed vroeg: waarom heeft de overheid niet op maandag ingegrepen bij DigiNotar? Dat was, zoals gezegd, omdat het bericht dat een eigen-merkcertificaat

gecompromitteerd was pas op maandag binnenkwam. Dat biedt geen enkele basis voor de overheid om op dat moment in te grijpen. Ik heb een beschrijving gegeven van de cijfers. Toen op vrijdag aan het einde van de middag bekend werd dat de PKI-certificaten gecompromitteerd waren, is onmiddellijk een crisisorganisatie opgezet en is er vrij staccato besloten en ingegrepen.

De heer **El Fassed** (GroenLinks):
Ik zal het kort houden. Was DigiNotar niet verplicht om de OPTA te melden dat er een probleem was?

Minister **Donner**:
Met de kennis die wij achteraf hebben, kunnen wij zeggen dat DigiNotar hier eigenlijk al veel eerder melding van had moeten maken, namelijk al in juli, toen gebleken was dat er ingebroken was. Vanaf het moment dat DigiNotar de melding kreeg op die maandag, is er dinsdag, woensdag en donderdag contact geweest over de stand van zaken, ook met GOVCERT.NL. In die informatie is steeds aangegeven dat het om een eigen-merkcertificaat ging. In zo'n situatie heeft de overheid geen basis om in te grijpen.

De heer **El Fassed** (GroenLinks):
Had het onderzoek dan niet moeten plaatsvinden om te laten zien dat het het vertrouwen waard was?

Minister **Donner**:
Dat onderzoek heeft plaatsgevonden. DigiNotar heeft die dinsdag Fox-IT ingeschakeld om dat onderzoek te doen. Uit het onderzoek van Fox-IT volgde vrijdag, volgens de mededeling van DigiNotar, dat de PKI-Overheid-certificaten mogelijk ook gecompromitteerd waren. Achteraf heb je natuurlijk altijd meer kennis en zeg je "had ik niet toen ...". Gegeven de informatie die er was, is er vanaf vrijdag aan het einde van de middag, toen het bekend werd, staccato gehandeld. Toen bleek wat de omvang van het probleem was, is binnen drie uur een heel deel van een bedrijf onder controle van de overheid gebracht. Doorgaans doen wij het niet sneller.

Ik was gekomen bij de beschrijving van de beslissing van de overname. Om 01.00 uur heb ik een persconferentie gegeven. Het spijt me dat de heer Koopmans dat niet begrepen heeft. Ik heb vooral uit medische hoek complimenten gekregen voor de presentatie, omdat al die artsen op dat uur van de nacht, als ze in de wacht zitten, naar de televisie kijken; toen zagen zij daar opeens een minister. De reden dat wij de conferentie op dat tijdstip gaven, is dat wij in een internetwereld leven, waarin de zon niet op- of ondergaat en waarin je zo snel mogelijk moet handelen. Dat heeft in dit geval het effect gehad dat de grote browserorganisaties vervolgens, onder verwijzing naar het besluit van de Nederlandse overheid, ook de certificaten afgekoppeld hebben. In het vervolg van het proces heeft dat weer de basis gelegd voor het vertrouwen van onder andere het bedrijf Microsoft in het handelen van de Nederlandse overheid. Dat was de reden om niet onmiddellijk en abrupt alle certificaten af te sluiten in Nederland, wat grotere gevolgen had gehad. Dat wat dus allemaal onderdeel van een naar mijn gevoel verantwoorde aanpak van het probleem.

De heer **Elissen** (PVV):
Minister Donner zei dat het feit dat DigiNotar een Amerikaans moederbedrijf had, kennelijk nogal wat extra complicaties met zich bracht. Is dat iets waarmee in de toekomst serieus rekening moet worden gehouden? Kan de minister daar nu al iets over zeggen? Is het inderdaad een extra complicerende factor?

Minister **Donner**:
Dat weet ik helemaal niet. Als er een Nederlandse raad van bestuur en raad van commissarissen was geweest, had daarnaar verwezen moeten worden. Ook dan moet men niet onmiddellijk een belangrijk deel van het bedrijf onder controle stellen als een telefoontje van de overheid binnenkomt. Een Nederlandse raad van bestuur zegt dan ook niet "oh, als u dat zegt, hier hebt u de sleutels". Dit zal dus altijd enige tijd vergen. Bovendien gaat het bij de certificaten niet om een Nederlandse opzet van het hele systeem, maar om een wereldwijde opzet waarin dit soort certificaten en het beheer daarvan in bepaalde handen geconcentreerd is. Dat heeft uit een oogpunt van beveiliging ook weer voordelen. Dan heb je immers niet met een groot aantal verschillende soorten organisaties te maken. Ik denk niet dat wij daar anders tegen aankijken.

De heer **Elissen** (PVV):
Ik stelde deze vraag met name in het licht van bijvoorbeeld conflicterende jurisdictie en van verhaalsmogelijkheden en, uiteraard, de daaraan gerelateerde verhaalsproblematiek.

Minister **Donner**:
Dat kan zonder meer een punt zijn in het vervolg van het verhaal. Op het moment van ingrijpen is dat echter niet relevant. Bovendien kan ieder Nederlands bedrijf ook buitenlandse PKI-certificaten gebruiken en dan ontstaat precies hetzelfde probleem.

Mevrouw Gesthuizen refereerde nog aan een eerste reactie op ambtelijk niveau inzake de systematiek van de beveiliging van PKI-Overheid. Dat gebeurde op een moment dat het beeld bestond dat alleen de eigen merkcertificaten in het geding waren.

Mevrouw **Gesthuizen** (SP):
Het is echt belachelijk dat hier wordt beweerd dat op woensdag bij de hele overheid nog nergens een lichtje was opgegaan, niet bij Logius, niet bij GOVCERT.NL, niet bij de OPTA. Nergens. Niet op het ministerie van Binnenlandse Zaken, niet op het ministerie van Veiligheid en Justitie, dat de regie had. Was nergens een lichtje opgegaan dat het wel eens heel erg mis kon zijn, ook met de overheidssites, ook met PKI-Overheid?

Minister **Donner**:
Ik heb net beschreven dat al op de dinsdag door GOVCERT.NL aan de eigen groep is meegedeeld dat een frauduleus uitgegeven beveiligingscertificaat was ontdekt. Ik herhaal dat er op dat moment iedere dag contact was met DigiNotar. Het beeld was dat de PKI-Overheid-certificaten niet waren gecompromitteerd. Dat doet er niet aan af dat de ambtenaar op dat moment het verschil beschreef tussen de gekwalificeerde certificaten en de niet gekwalificeerde certificaten. Dat achteraf blijkt dat zij wel gecompromitteerd waren, doet er niet aan af dat men op dat moment juist alles had ingezet, ook via het Fox-IT-onderzoek door DigiNotar, om erachter te komen of dat het geval was. Als een ambtenaar dan die woensdag uitlegt wat het verschil is tussen het ene certificaat en het andere

certificaat, zie ik niet dat dit anders is. Alleen in "1984" van Orwell veranderde de werkelijkheid iedere dag.

De **voorzitter**:
Goed, we laten de literatuur even rusten en mevrouw Gesthuizen stelt nog een vraag.

Mevrouw **Gesthuizen** (SP):
Dit is in ieder geval heel duidelijk. Ik ben het voor een heel groot gedeelte met de minister eens. Ik heb ook waardering voor de rustige toon waarop hij het nog eens allemaal uiteenzet, maar ik vind het gewoon niet kunnen dat op het moment waarop iedereen aan zijn water voelt dat er iets helemaal mis is, het ministerie nog denkt dat er niets aan de hand is. Het is erger dan ik dacht. Als ik de minister mag geloven, is er inderdaad niemand geweest die zich de haren uit het hoofd heeft gerukt, toen hij de ambtenaar dit zag beweren. Dat vind ik heel ernstig.

Minister **Donner**:
We hebben voor situaties van crisis de organisatie om, als er reden toe is, dan ook zo snel mogelijk in te grijpen. Ik heb beschreven op welke wijze wij de vinger aan de pols houden om de informatie zo tijdig mogelijk te krijgen. Ik weet niet of het aan de maatschappelijke rust bijdraagt om op ieder moment onmiddellijk in paniek te schieten. Nee, de verantwoordelijkheid van de overheid is om te onderzoeken en te handelen naar de feiten.

Mevrouw **Hennis-Plasschaert** (VVD):
Mogen we dan ook vaststellen, met de kennis van nu, dat we te lang op de blauwe ogen van DigiNotar hebben vertrouwd?

Minister **Donner**:
Dat weet ik niet. We hebben te lang op de blauwe ogen van DigiNotar vertrouwd, omdat inderdaad is gebleken dat men al veel eerder wist van de pogingen tot inbraak. Er was al eerder gebleken dat die inbraken er waren. Die hadden gemeld moeten worden. Om die reden is er niet alleen discussie over de meldingsplicht bij de compromittering van persoonsgegevens, maar over de bredere vraag van een meldingsplicht met betrekking tot de veiligheidssystemen die doorbroken worden. Daar zijn wij het over eens.

Mevrouw **Hennis-Plasschaert** (VVD):
Kunnen we dan misschien een keer luid en duidelijk zeggen dat DigiNotar de zaak willens en wetens heeft geflest?

Minister **Donner**:
Het is een privilege van vele anderen om dat soort zaken te zeggen, maar niet van ministers, want dan is de Staat onmiddellijk aansprakelijk, als er ook maar iets miszegd is.

Voorzitter. Mevrouw Gesthuizen vroeg in het algemeen wie bij overheidsorganisaties verantwoordelijk is om bij een incident op te treden. Net als bij particuliere organisaties staat voorop dat departementen en andere overheden als eigenaar van de informatiesystemen zelf eindverantwoordelijk zijn voor de veiligheid van hun systemen en websites. Ik wijs erop dat het proces met betrekking tot de compacte overheid in gang is gezet en dat een onderdeel daarvan is om op het niveau van de rijksoverheid het aantal beheerders van rekencentra terug te brengen en te beperken, maar er blijven systemen zoals door het UWV of door andere diensten worden gerund. De desbetreffende departementen of organen zijn daarvoor primair verantwoordelijk. Iets anders zou betekenen dat verantwoordelijkheid en beheer uit elkaar worden getrokken en dat is riskanter voor de veiligheid. Departementen en andere overheden moeten dan ook zelf ingrijpen als er sprake is van een veiligheidsprobleem of een lek. Het huidige GOVCERT.NL en straks het NCSC adviseren partijen over beveiligingsproblemen en lekken. De minister van Justitie zal hier straks verder op ingaan. GOVCERT.NL zal bij incidenten ondersteuning en advies geven. Dat is in het verleden ook enkele malen gebeurd.

Een ander punt is de algemene vraag op welke wijze we ervoor zorgen, niet alleen bij de overheid, dat er een adequate melding is bij een bepaalde instantie van potentiële inbraken in de systemen. Dat moet onverlet laten dat ook de melding niet de verantwoordelijkheid weghaalt bij de eigenaar van het systeem, want anders gaan we de verantwoordelijkheden anonimiseren.

De minister van Veiligheid en Justitie gaat verder in op de vraag die mevrouw Gesthuizen stelde met betrekking tot het crashteam en de uitrukkende instanties.

Door verschillende sprekers is gevraagd of er onderzoek gedaan moet worden. Dat sluit aan bij het gevoelen dat de minister van Veiligheid en ik ook al eerder hadden. Wij zouden dat invulling willen geven door de Raad voor Veiligheidsonderzoek te vragen of hier een onderzoek gedaan kan worden. Dat moet dan niet primair op het concrete geval betrekking hebben, maar dat moet breder gesteld worden. Het gaat om vragen als: wat moet er nu nog gedaan worden, hoe moet je kijken naar de hele situatie zoals die hier aan het licht gekomen is, maar die ook speelt bij de gemeentesites, waar de veiligheid ondergeschikt is? Er is gevraagd naar een onafhankelijk onderzoek. Ik wijs erop dat het een instantie is die bewezen heeft dat zij op dat punt goed onderzoek doet. Dat leek ons de betere keuze. Dat zal naar onze mening ook een resultaat opleveren waarvan vervolgens gezegd kan worden: daar kunnen we verder mee werken.

Dat laat onverlet dat ondertussen ook door de departementen verder wordt gewerkt aan de verschillende maatregelen die al in gang worden gezet. We zeggen dus niet: en nu gaan we wachten op het resultaat om te weten wat er onveilig is. Nee, er wordt gewerkt. Er wordt daarnaast ook gewerkt met de beelden, de informatie die van hackers wordt verkregen. Hier is al de dubbelzinnigheid met betrekking tot dat punt geschetst. Je kunt ook niet zeggen van de hacker die bij DigiNotar binnen is gekomen: geweldig, die heeft ons gewezen op een gebrek. Hij heeft het vervolgens echt geadverteerd op de site waar dit soort informatie bijeengebracht wordt. Men zou vreemd opkijken als de Nederlandse overheid hem met open armen ontvangt en zegt: geweldig, en zeker ook wat u gedaan hebt met de certificaten die u daar weggehaald hebt. Het is gewoon ordinaire diefstal. Vervolgens is het, voor zover de spullen ook nog gekocht zijn, heling. Dit is een punt waar de minister van Veiligheid en Justitie nader op in zal gaan. Het laat onverlet dat wij dankbaar gebruikmaken van informatie van hackers dat bij bepaalde instanties de voordeur openstaat.

Ik heb al een aantal vragen van de heer Heijnen beantwoord. Hij is in het bijzonder ingegaan op de mededelingen die ook aan de Kamer zijn gegeven.

De **voorzitter**:
Ik zie dat een aantal collega's nog wil interrumperen over het vorige punt.

Minister **Donner**:
Ik wilde het verloop van de feiten nu laten voor wat het is.

De heer **El Fassed** (GroenLinks):
Dat lijkt me verstandig. De minister heeft het over het onderzoek van de Raad voor Veiligheidsonderzoek. Wij hebben een heleboel vragen. Wij hebben vragen gesteld over de relatie tussen ICT en overheid en wat daar misgaat. Kunnen wij inzage krijgen in de vraagstelling voor dat onderzoek? Dat scheelt namelijk een hoop werk.

Minister **Donner**:
Het punt is wel het volgende. De Raad voor Veiligheidsonderzoek bepaalt ingevolge wettelijke bepalingen zelf wat de vraagstelling is. Er zal zeker overleg plaatsvinden. Wij zijn gaarne bereid om ook met de Kamer nog te wisselen waar de vragen zitten. Maar let wel: de raad zal met name het veiligheidsaspect bekijken. Vragen met een breder karakter over overheid en ICT vallen weer net onder een ander punt. Ik kan overigens wel aangeven wanneer de reactie komt op het WRR-rapport. Ik mag niet uit de ministerraad klappen maar de Kamer zal sneller worden bediend dan zij denkt.

Mevrouw **Hachchi** (D66):
Het is mij niet helemaal duidelijk of de minister heeft gereageerd op mijn verzoek om te kijken naar de mogelijkheden om gebruik te maken van de expertise van hackers. Ik hoorde hem iets zeggen over hacken, namelijk dat hij het ziet als inbraak en dat wij de deuren niet opengooien. Komt de minister daar nog op terug? Mijn vraag is behoorlijk open: welke mogelijkheden er zijn en of de minister bereid is om daarnaar te kijken.

Minister **Donner**:
Ik kan de Kamer verzekeren dat wij waar mogelijk gebruikmaken van de expertise van hackers. Waar ze zich aanbieden, zullen wij ze inhuren. Mevrouw Hachchi schetste het beeld dat wij de hackers laten controleren of een site veilig is. De problematiek in de hele ICT-wereld is echter dat een vaststelling dat een site veilig is, net zoiets is als een zwangerschapstest: morgen kan het weer anders zijn.

De **voorzitter**:
Goed. Mevrouw Hachchi denkt hierover na.

Mevrouw **Hachchi** (D66):
Nee voorzitter, daar hoef ik niet over na te denken. Ik denk dat ik die metafoor toch even loslaat. De minister zegt dat reeds wordt gebruikgemaakt van de expertise van hackers. Kan hij toelichten op welke manier dat gebeurt? Gebeurt het ook wanneer er overheidswebsites worden gebouwd of wanneer er wordt aanbesteed? Bij welke trajecten worden hackers betrokken of wordt hun expertise gebruikt?

Minister **Donner**:
Ik kan dat niet nader toelichten. Er wordt echter gebruikgemaakt van de deskundigheid. Ik kan niet zeggen dat er op dit moment bij iedere site gebruik van wordt gemaakt. De meeste overheidssites zijn juist bedoeld om informatie te geven, dus daarvoor doet het er helemaal niet toe of ze er komen. Wij krijgen dan meestal de klacht dat de sites ontoegankelijk zijn en dat de richtlijnen op dat terrein niet goed worden toegepast. Op andere punten proberen wij zo goed mogelijk gebruik te maken van de informatie die beschikbaar is. Ik geef in die context toe dat wij waar mogelijk gebruikmaken van de expertise van hackers. Ik zal dat niet nader specificeren. Wanneer wij informatie krijgen doordat hackers zelf zaken mededelen over de toegankelijkheid, maken wij daarvan dankbaar gebruik. Dat laat onverlet dat ook ik vaststel dat tal van sites nog onveilig zijn.

De **voorzitter**:
Nog één keer heel kort, mevrouw Hachchi, anders telt het als uw tweede interruptie.

Mevrouw **Hachchi** (D66):
Het gaat mij erom dat ik de minister goed begrijp, dus dat er niet alleen vanwege "lektober", zoals wij deze maand kennen, maar ook vooraf van wordt gebruikgemaakt. Het gaat uiteindelijk om een betere beveiliging van onze overheidssites. Ik neem aan dat ik de minister goed begrijp dat het al gebeurt.

Minister **Donner**:
Ja. Wel waarschuw ik voor het volgende. De heer Koopmans suggereerde om ze in een beveiligings-bv te organiseren. Mijn beeld is dat zodra hackers er hun brood mee verdienen, het een beveiligingsinstituut wordt en dat de volgende hacker zal inbreken bij dat beveiligingsinstituut. Je kunt ze er dus maar beter niet hun dagelijks brood mee laten verdienen.

Voorzitter. Ik kom bij de vragen van de heer Heijnen. Laat ik beschrijven wat het zwaardere regime van de gekwalificeerde certificaten inhoudt met PKI-Overheid. Daarvoor geldt het regime van de Europese richtlijn inzake de elektronische handtekening. Daarnaast worden in het programma van eisen aanvullende en invullende eisen gesteld aan alle PKI-Overheid-certificaten, dus niet alleen aan de gekwalificeerde certificaten maar ook aan certificaten die voor inloggen, slotjes en SSL worden gebruikt. Een en ander gebeurt door middel van een overeenkomst tussen de certificatiedienstverlener en de Staat.

Voorbeelden van die nadere eisen zijn: face-to-face-identificatie van de certificaatbeheerder van een organisatie, je moet hem dus gezien hebben en anonimiseren kan niet volstaan; nadere eisen aan de functiescheiding bij de certificatiedienstverlening. Het programma van eisen wordt beheerd door de zogenaamde Policy Authority, die valt onder het ministerie van Binnenlandse Zaken. Dat is logisch. De certificering conform zowel de EU-richtlijn als het programma van eisen van PKI-Overheid is verplicht. Die certificering vindt plaats door een externe partij, of BSI Management Systems of Pricewaterhouse Coopers. Beide zijn geaccrediteerd. In geval van een goedkeuring geeft de auditor na de beoordeling een conformiteitscertificaat af. Dat certificaat heeft een geldigheidsduur van drie jaar. De certificatiedienstverlener overlegt een kopie van het conformiteitscertificaat aan de Policy Authority, evenals kopieën van de audit en de controle rapporten. Ook OPTA kan als controleur van de certificatiegevers, van de certificatieorganisaties, rapporten opvragen. Tevens is de certificatiedienstverlener verplicht, zich jaarlijks te laten beoordelen door een onafhankelijk externe auditor, middels een controle-audit. Belangrijke tussen-

tijdse wijzigingen, die van invloed kunnen zijn op de certificatiedienstverlener, meldt de certificatiedienstverlener bij de auditor. De auditor voert desgewenst ad hoc een controlebeoordeling van de certificatiedienstverlener uit. In geval van een negatieve beoordeling adviseert de Policy Authority de minister van Binnenlandse Zaken, die dan een besluit neemt tot technische of administratieve verwijdering. DigiNotar ontving tot op heden, althans tot 2 september 2011, positieve beoordelingen van de auditor.

De heer **Heijnen** (PvdA):
Ik denk dat w medewerkers ook hebben gezien dat wij tijdens de hoorzitting aan PwC hebben gevraagd of zij op de aanvullende eisen die in het programma van eisen voor PKI-Overheid ook auditen. Zij zeiden dat ze dat uitsluitend deden op de Europese richtlijnen voor de elektronische handtekening. Daar zit een probleem.

Minister **Donner**:
Dat is dan een feitelijke mededeling van PwC. Ik beschrijf u het systeem zoals het opgezet is. PwC is gehouden het volgens dat systeem te doen. Als PwC het naar eigen mening niet zo doet, ben ik gaarne bereid om dat te onderzoeken. Dat is echter niet conform het systeem dat is opgezet en waar ik over geschreven heb aan de Kamer.

De heer **Heijnen** (PvdA):
Ik heb dat goed gelezen. Vandaar dat ik mij er ook over verbaasd heb dat u dat hebt opgeschreven, vergeleken bij de mededelingen die zijn gedaan in de hoorzitting. Niet alleen PwC bevestigde dat. OPTA bleek evenmin op de hoogte te zijn van aanvullende eisen waarop dan in opdracht van Logius – ik geloof dat dit de Policy Authority is bij de minister – die audits plaatsvinden. Laat ik het anders formuleren. De minister, althans zijn ministerie, beschikt over een jaarlijks, specifiek afschrift van een audit op het programma van eisen dat voor PKI-Overheid geldt. Daar ben ik dan erg benieuwd naar. Ik zeg dat allemaal – ik moet dit punt maken, anders begrijpt niemand er meer wat van – omdat het zo ernstig is dat bij DigiNotar is gebleken dat alle servers verbonden waren, zowel voor PKI als SSL, dat er één windowsomgeving was die vanuit internet te benaderen was, dat de wachtwoorden makkelijk te kraken waren en dat er dus geen antivirussoftware was geïnstalleerd. Dat is zo ernstig dat ik me niet kan voorstellen dat men dat niet gezien heeft, met al die extra eisen die klaarblijkelijk gesteld worden voor de public infrastructure. Het is niet zomaar iets, het gaat om de public infrastructure hiervoor.

Minister **Donner**:
Op dat punt ben ik het met de heer Heijnen eens. Daarom vindt er op dit moment ook, juist naar aanleiding van wat we aangetroffen hebben bij DigiNotar inzake de oorzaken, een onderzoek plaats naar de mate waarin door PwC en de OPTA invulling is gegeven aan de taken die ze hadden ingevolge dit systeem.

De **voorzitter**:
Nog één zin, mijnheer Heijnen. Anders tel ik het als tweede interruptie, want dit wordt wel heel lang.

De heer **Heijnen** (PvdA):
De OPTA heeft een verantwoordelijkheid, in het algemeen. Die geeft vervolgens PWC een opdracht om te auditen bij Diginotar. Daarnaast, zo schrijft de minister, is er een opdracht verstrekt – ik weet niet aan wie, het kan PwC zijn geweest of dat andere bedrijf – om specifiek te controleren op de aanvullende eisen voor PKI-Overheid. Mijn vraag is en blijft of dat nu is gebeurd of niet. Ik heb nog steeds het idee dat dit niet is gebeurd.

Minister **Donner**:
De heer Heijnen vraagt mij naar een heel concreet feitelijk gegeven dat ik niet paraat heb. In dit systeem geeft de auditor het certificaat aan de certificaatdienstverlener, die krijgt een conformiteitcertificaat. Ik zal gaarne, zo nodig in tweede termijn, ingaan op deze concrete vraag van de heer Heijnen. Hij vroeg heel concreet hoe het zit in dit concrete geval. Ik zei net al dat er een onderzoek loopt naar de wijze waarop daar invulling aan is gegeven. Het is dus mogelijk dat die gegevens er nog niet zijn. Daar kom ik in mijn tweede termijn op terug.

De heer **Elissen** (PVV):
Ik zal proberen om het kort te houden. In de hoorzittingen bleek ook dat de audits eigenlijk vrijblijvend en belabberd waren, net als het toezicht erop. Komt de minister nog te spreken over kwaliteit van de audits en het toezicht erop?

Minister **Donner**:
Ik schetste dat net al. Je krijgt audits van de verschillende certificaatdienstverleners. Als vervolgens blijkt dat het zo niet werkt, is er alle reden om ernaar te kijken. Er is overigens wel heel duidelijk gebleken dat Diginotar binnen het systeem van de PKI-Overheid-certificaten de uitzondering was. Dat laat de vraag onverlet hoe dat door de mazen heen kon slippen. Het is niet zo – dat zou bevestigen dat er geen controles waren – dat de andere evenzeer gecompromitteerd konden worden. Dat is niet gebleken. Er zijn ook daar aanvallen op gedaan.

De heer **Elissen** (PVV):
Ik weet voorlopig genoeg. Eventueel kom ik er straks op terug.

Minister **Donner**:
De heer Heijnen vroeg of er jaarlijks een extra audit was bij Diginotar. Dat was het geval. De certificering conform de EU-richtlijn post-programma van eisen zou plaatsgevonden hebben. Dat onderdeel heb ik net ook al genoemd. De feitelijke vragen worden straks beantwoord.

Geldt de interne controle ook voor andere ICT-projecten dan alleen PKI? De interne controle geldt voor meerdere ICT-projecten die worden uitgevoerd binnen of in opdracht van de overheid en ook voor stelsels en systemen die in beheer zijn genomen. Voorbeelden zijn de gateway reviews en andere reviews op de grote ICT-projecten en de periodieke audits na opzet en werking van bijvoorbeeld de GBA en het bsn-stelsel. Dat zijn gewoon de algemene systemen van interne controle. In de technische briefing is al ingegaan op de wijze waarop het werkt. Er is inmiddels een evaluatieonderzoek gestuurd, zoals ik al zei.

De heer Heijnen en anderen vroegen naar het gegeven dat is gebleken dat één certificaat van Diginotar – die informatie is althans gekomen – is gebruikt in Iran om verkeer door te leiden naar Gmail. Dat is uiteraard op dit moment nog onvoldoende bekend. De minister van Veiligheid en Justitie zal ingaan op het onderzoek dat wordt ingesteld naar de daders en het gebruik. Het is onduidelijk

op welke manier dit daar in handen is gekomen en waarom dat is gebeurd. De AIVD heeft onderzoek gedaan naar de digitale inbraak. In dat onderzoek richt men zich vooral op de identiteit van de hacker. Het KLPD doet onderzoek naar de strafrechtelijke kant van de zaak. Beide onderzoeken zijn nog in volle gang.

Mevrouw Hachchi vroeg of er een overzicht is van de gevolgen. Het antwoord is nee. Er valt geen inzicht in de gevolgen te krijgen. In de eerste plaats weten wij niet welke 300.000 mensen het betreft. Je weet ook niet welke berichten zij in die tijd hebben doorgegeven en welke berichten niet op de bestemming zijn gekomen. Om een overzicht te krijgen van de gevolgen is onderzoek in Iran nodig. Op dit moment hebben wij geen samenwerkingsverdragen met Iran op grond waarvan wij daar eventueel gezamenlijk onderzoek zouden kunnen doen. Het spijt mij, maar dat overzicht is dus niet te geven. De heer El Fassed had het over slachtoffers. Wij kunnen dus ook niet zeggen of er slachtoffers zijn en op welke manier dit is gebeurd. Wij constateren alleen dat de informatie daar is gebruikt. Verder kunnen wij slechts speculeren over de vraag wie het heeft gedaan, waar de informatie wel en waar zij niet is terechtgekomen. In antwoord op de vraag van mevrouw Hennis zeg ik dat er onderzoek wordt gedaan zoals ik heb aangegeven.

Er is gesproken over de overheidsbedrijfsvoering. Ik heb al gezegd dat de ICT onderdeel is van de veranderingen in de bedrijfsvoering bij de rijksoverheid. Die leiden tot een sterkere concentratie van in ieder geval de rekencentra. Systemen zullen wel op het niveau van de verschillende departementen blijven functioneren. Alle beveiligingsaspecten worden geconcentreerd bij de organisatie GOVCERT.NL Mede in het licht van de beelden van de lekken vindt bij de lagere overheden op dit moment in hoog tempo een proces plaats waarbij de organisatie KING vooral de gemeenten adviseert. Ook bij de lagere overheden is men zich hiervan dus bewust.

De heer Heijnen vroeg of het aspect van de beveiliging in het nationale uitvoeringsprogramma kan worden opgenomen. Inderdaad is beveiliging op dit moment geen expliciet onderdeel van het Nationaal Uitvoeringsprogramma. De kaderstelling eisen aan beveiliging zijn helder, maar de toepassing laat aantoonbaar te wensen over. Het budget voor het i-NUP kan mede worden aangewend om toepassing van beveiligingseisen op een adequaat niveau te brengen. Zoals gezegd is de organisatie KING op dit moment doende bij de gemeenten om hieraan invulling te geven.

De heer **Heijnen** (PvdA):
Aan het begin van de kabinetsperiode schreef het kabinet dat de minister van Binnenlandse Zaken adequate doorzettingsmacht zou krijgen op het vlak van de bedrijfsvoering, inclusief de ICT. Daarover hebben wij al vaker van gedachten gewisseld, maar wij hebben nooit gemerkt dat er op dit punt echt iets is veranderd ten opzichte van de tijd voordat het kabinet aantrad. Je vraagt je daarom af waarom dit is opgeschreven. Laat ik het echter toespitsen op wat de minister eerder zei. GOVCERT adviseert ministeries, zelfstandige bestuursorganisaties en instanties in de keten over aspecten van veiligheid. Als die instanties die adviezen niet opvolgen, wie grijpt er dan in?

Minister **Donner**:
Dat heb ik net uitgelegd. Dat is de verantwoordelijkheid van de eigenaar van het systeem. Dit is essentieel: de doorzettingsmacht betreft de organisatie. Die maakt dat het inderdaad niet mogelijk is dat allerlei processen worden tegengehouden. Ik ben blij dat de heer Heijnen er in die zin niets van merkt, want dat maakt duidelijk dat het op dit moment vloeiend verloopt. Het gehele proces ligt op schema. Waar de doorzettingsmacht gebruikt moet worden, wordt die ook gebruikt. Het zit echter niet daarin. Waar de heer Heijnen op doelt, is dat één instantie belast wordt met het toezicht op en de handhaving van dit soort aspecten bij de verschillende overheden. Dat is niet beoogd met de doorzettingsmacht. Het zou betekenen dat niet meer iedere minister verantwoordelijk is voor het eigen onderdeel, maar dat beheer en veiligheid in verschillende handen komen te liggen. Dat is onwenselijk.

De **voorzitter**:
Ik stel voor om de vragen kort en bondig te stellen. Ik kijk ook even naar minister Donner en vraag hem of dan ook de antwoorden ietsje bondiger kunnen.

Dan is nu het woord aan de heer Heijnen.

De heer **Heijnen** (PvdA):
Dit gaat niet werken. Als iedere instantie zelf in staat is om adviezen van GOVCERT – aangenomen dat die adviezen heeft gegeven – naast zich neer te leggen, blijft het zo lek als een mandje. Het zal zo moeten zijn dat als GOVCERT constateert dat een instantie adviezen niet opvolgt, dit wordt opgetild naar een niveau waarop erover kan worden besloten en waarop er kan worden doorgezet. Als daarin niet wordt voorzien, kan de minister ook wel de SIO's af te schaffen. Dan hoeft hij niet eens een CSIO (Central Security Information Officer) aan te stellen, wat eigenlijk wel nodig is. Dat heeft dan helemaal geen zin, want iedere – negatief gezegd – onderknuppel is dan zelf verantwoordelijk voor zijn eigen IT-systeem. Zo werkt het niet, mijnheer de minister.

Minister **Donner**:
U hebt het wel over ministers.

De heer **Heijnen** (PvdA):
Nee, nee, nee. U hebt mij verkeerd begrepen. Ik trek dat woord terug. Laat ik het zo zeggen: iedere medewerker, ook op een basisniveau, die betrokken is bij IT van de overheid is dan verantwoordelijk voor de veiligheid en kan adviezen naast zich neerleggen. Dat moeten we niet willen.

De **voorzitter**:
Deze verandering van woordkeuze is verstandig. De minister zal nu antwoorden.

Minister **Donner**:
Zoals de heer Heijnen het nu beschrijft, wordt het voor mij ook beter begrijpelijk, voorzitter. Er is heel duidelijk wel een onderscheid met de doorzettingsmacht waaraan hij refereert. Die betreft de bedrijfsvoering. Hier gaat het om het aspect van de beveiliging. Ik zeg de heer Heijnen dat dit aspect meegenomen zal worden bij de evaluatie van de vraag waar de knelpunten zitten. Dat is een heel andere vorm van doorzettingsmacht, namelijk op welke wijze wordt, als de adviezen van GOVCERT niet worden opgevolgd – daar kunnen legitieme redenen voor zijn, zoals het functioneren van het systeem – ervoor gezorgd dat het niet blijft hangen op een bepaald niveau maar naar

boven komt. Ik denk dat de minister van Veiligheid en Justitie nader op dit punt zal ingaan.

Mevrouw **Gesthuizen** (SP):
Ten eerste. Waarom zou een minister geen onderknuppel kunnen zijn? Ten tweede. Ik ben blij dat de minister het nu net iets anders opvat, want het komt op mij over als: we hebben politie, brandweer en een inspectiedienst maar als die vertellen dat er iets niet deugt op het ministerie, maakt dat ministerie zelf wel uit of het die waarschuwing serieus neemt. Zo kan het inderdaad niet zijn bedoeld. Als het goed is, is dit misverstand nu rechtgezet.

Minister **Donner**:
Ja.

De **voorzitter**:
Dat is helder. Dan is het woord aan de heer Koopmans.

Minister **Donner**:
Behalve één punt. Ik maak er bezwaar tegen dat ministers als onderknuppel worden afgeschilderd. Ik dacht dat we bij de algemene politieke beschouwingen hebben gezien waar dat toe leidt.

De **voorzitter**:
Goed. Mevrouw Gesthuizen glimlacht. De heer Heijnen had zijn woorden veranderd.

De heer Koopmans heeft een vraag.

De heer **Koopmans** (CDA):
Begrijp ik het goed dat indien GOVCERT een melding doet aan een systeemverantwoordelijke bewindspersoon en in de gaten krijgt dat die bewindspersoon en de onder hem ressorterende diensten niets met die melding doen, GOVCERT een afschriftje van de waarschuwing aan de verantwoordelijke minister voor GOVCERT, namelijk de minister voor Veiligheid en Justitie, stuurt, zodat we een bredere verantwoordelijkheid hebben? Het zou onze wens zijn dat ik het zo mag opvatten. Misschien zou GOVCERT ook nog een afschriftje naar de minister van BZK kunnen sturen, dat maakt mij niet zoveel uit, als iedereen in zo'n geval maar in de gaten krijgt dat er bewindslieden zijn die onder hun verantwoordelijkheid onveilige situaties accepteren, waarvoor overigens mogelijkerwijs een reden kan zijn.

Minister **Donner**:
Ik herhaal dat dit een van de knelpunten is die meegenomen worden bij het bekijken hoe daarin voorzien kan worden. Ik ben het volstrekt eens met de verschillende sprekers dat deze zaak niet kan blijven hangen in een ambtelijk geschil over wie wat moet doen. Daar komen wij op terug.

De heer **Koopmans** (CDA):
Naar mijn mening hoeft dat niet meegenomen te worden in de evaluatie. Het lijkt mij verstandig dat de regering nu toezegt dat indien GOVCERT een constatering doet, die in een cc'tje naar de minister van Veiligheid en Justitie gaat.

Minister **Donner**:
Ja.

De **voorzitter**:
Tegen de heer Elissen zeg ik dat dit zijn derde en tevens laatste interruptie van vanavond wordt.

De heer **Elissen** (PVV):
Dank u, voorzitter, ik waardeer uw strengheid.

Ik meende de heer Donner zo-even te horen zeggen dat hij het onwenselijk vindt om beheer en veiligheid te scheiden. Tegelijkertijd heb ik hem ook horen zeggen dat hij eigenlijk niets uitsluit en wil afwachten wat de evaluaties en de onderzoeken zullen brengen. Ik wijs in dit verband op het feit dat wij op het vlak van de nationale internetveiligheid de Nationale Cyber Securiteit Strategie hebben. Daar zit een regievoerder, die monitor en coördineert. In dat licht vraag ik de minister expliciet op dit moment nog niet uit te sluiten dat wij daar misschien wat strakker in moeten gaan zitten en zelfs niet uit te sluiten dat wij beheer en veiligheid scheiden.

Minister **Donner**:
Ik heb bedoeld te zeggen dat de verantwoordelijkheid voor de veiligheid van een systeem en de verantwoordelijkheid voor het beheer in één hand moeten liggen, omdat wij anders de aansprakelijkheid verliezen. Natuurlijk blijft veiligheid een apart aspect. Om die reden werken wij met GOVCERT.NL, dat ons adviezen kan geven en de zaak kan doorlichten. Eventueel moet er een regeling komen voor het geval die adviezen niet worden opgevolgd. Fundamenteel is dat echter de verantwoordelijkheid voor beheer en voor veiligheid in één hand moeten liggen.

De heer **Elissen** (PVV):
Voor mij is heel principieel en ook heel fundamenteel dat wij, nu nog niet helder is waar dit alles vandaan is gekomen, welke lessen wij kunnen leren en hoe wij een en ander kunnen verbeteren, niet zo ver moeten gaan om al zaken uit te sluiten.

Minister **Donner**:
Ik kom bij de vragen van mevrouw Hachchi. Ik ben al ingegaan op de vragen over de wijze waarop het systeem is overgenomen.

Mevrouw Hachchi vroeg tevens waarom de belastingaangifte nog zo lang gebruik maakt van de specifieke wijze van beveiligde communicatie, de BAPI. De eigenschappen van en de werkwijze rond de BAPI leiden tot de conclusie dat vervanging weliswaar zo snel mogelijk moet plaatsvinden, maar dat dit wel gecontroleerd en beheerst moet gebeuren. Anders zou op een goed moment de informatiestroom naar de Belastingdienst onderbroken worden, met veel grotere gevolgen. Van meet af aan was duidelijk dat overgaan tijd zou kosten, gelet op de inschakeling van een nieuwe certificaatleverancier, de aanpassing van de software van de betrokken onderneming en de Belastingdienst, en het uitrollen van de ruim 16.000 certificaten die in het hele systeem worden gebruikt. Er zijn in het BAPI-netwerk voldoende procedurele en andere maatregelen getroffen die de continuïteit en betrouwbaarheid gedurende het overgangstraject borgen. Vanaf dag één is daar met de verschillende organisaties en de belastingsadviseurs van de bedrijven over overlegd, teneinde iedereen voldoende vertrouwen te laten behouden en tegelijkertijd te voorkomen dat de communicatie verstoord wordt. Meteen is er intensief overleg geweest met de sector, zoals ik al heb opgemerkt, en is er in samenwerking

getest. Het hele proces zal naar verwachting in de eerste helft van 2012 worden afgerond.

Mevrouw **Hachchi** (D66):
Ik dank de minister voor dit antwoord, maar ik heb hem ook gevraagd naar de extra kosten. Ik zie echter dat de minister daar nog niet aan toe is.

Minister **Donner**:
De ondernemer moet een nieuw certificaat aanschaffen en installeren. Beide zijn normale ondernemersrisico's. De voormalige leverancier DigiNotar is immers niet meer vertrouwd en dus is het de verantwoordelijkheid van de ondernemer om die overgang te maken. De Belastingdienst heeft bij de nieuwe certificatenleverancier bedongen dat de nieuwe certificaten geen hogere prijs kennen dan de huidige. De Belastingdienst betaalt het centrale deel, dus de wijzigingen die op het centrale deel moeten worden aangebracht. Dat maakt dat je juist door de overgang de kosten kunt beheersen, omdat altijd betaald moet worden voor de certificaten. Wel moet de overgang betaald worden. Op deze wijze menen wij dat wij onder de voorwaarden van optimale zekerheid de kosten zo beperkt mogelijk hebben kunnen houden, evenals de verstoring van het verkeer.

Mevrouw **Hachchi** (D66):
Voorzitter. Ik heb een heel simpele vraag voor deze minister. Is hij het met mij eens dat het bedrijfsleven niet de rekening voor het DigiNotar-debacle op zijn bord mag krijgen?

Minister **Donner**:
Dat ben ik niet met u eens! Ieder kiest voor een certificaathouder. Een aantal bedrijven heeft DigiNotar gekozen als degene die de certificaten afgeeft. Daar is ieder bedrijf zelf verantwoordelijk voor. Men moet zijn vertrouwen vinden waar men het gelaten heeft. Dat is een zeer oud Germaans rechtsbeginsel.

Mevrouw **Hachchi** (D66):
Ik vrees dat de minister en ik langs elkaar heen praten. Ik heb het over de bedrijven die aangifte moeten doen via de Belastingdienst en daardoor meer moeten gaan betalen vanwege de diensten of vanwege het DigiNotar-debacle, waardoor de veiligheidseisen veranderd zijn.

Minister **Donner**:
Ik heb aangegeven dat op dat punt de kosten voor een nieuw certificaat bij de onderneming liggen. Door de Belastingdienst is onderhandeld dat die niet hoger zullen zijn dan die van DigiNotar. De Belastingdienst betaalt de kosten van de omschakeling voor het centrale deel van het systeem, maar iedere ondernemer draagt zijn eigen lasten. Dat zijn de risico's die hij neemt. Ook als hij een auto koopt die vervolgens kaduuk blijkt te zijn omdat niet aan de veiligheidsvoorschriften is voldaan, moet hij zelf een nieuwe kopen.

De **voorzitter**:
Een kort zinnetje nog!

Mevrouw **Hachchi** (D66):
Een kort zinnetje: ik zou wel graag willen weten wat die kostenstijging dan is. Ik heb met collega Verhoeven hierover al vragen gesteld. Ik vraag de minister bij dezen om die vragen zo spoedig mogelijk te beantwoorden.

Minister **Donner**:
Ik ben me er niet van bewust dat die vragen aan mij gericht zijn; vermoedelijk zijn die aan de staatssecretaris van Financiën gericht. Maar ik zal het verzoek doorgeven.

Mevrouw Hachchi is ook nog ingegaan op het belang van de privacy. Daar zijn we ons volledig van bewust. Dat aspect speelt hierbij een rol, omdat ik het beginsel onderschrijf dat de overheid van haar zijde moet doen wat mogelijk is aan de beveiliging van het geheel als zij communicatie mogelijk maakt, ook met persoonsgegevens. Dat laat de verschillende aansprakelijkheden onverlet. Nogmaals, iedereen heeft er kennelijk bezwaar tegen als je informatie met een vulpen verstuurt. Ik wijs erop dat er ten tijde van de vulpen ook talloze vormen van fraude en verlies van gegevens waren en dat iedereen daarin de eigen verantwoordelijkheden droeg. Dat is het uitgangspunt van onze samenleving.

De discussie over DigiNotar is alleen al daarom een internationale discussie geworden, omdat de hacker op internet aangaf dat hij nog een aantal andere instanties had gehackt. Daarmee is vanaf dat moment de discussie een internationale geworden.

Dan de discussie over onvoldoende ICT-kennis. Nogmaals, die discussie voeren wij in verschillende standen. Een tijd lang is het idee geweest dat alles ingehuurd moest worden, waardoor die kennis werd ingehuurd. Op dit moment wordt op verschillende plaatsen de kennis van ICT weer aangevuld. Het blijft zonder meer een punt van aandacht, want het gaat om kennis die je alleen maar tijdelijk nodig hebt en niet permanent. Dat is een van de redenen waarom wij proberen zo veel mogelijk in de bedrijfsvoering de aanbesteding en het opdrachtgeverschap te concentreren, zodat wij de aanwezige kennis kunnen gebruiken voor de verschillende opdrachten.

De heer El Fassed merkte op dat er een veiligheidsgezant moet komen. De minister van Veiligheid en Justitie zal ingaan op het bijzondere aspect van de cyber security. Ik heb aangegeven dat GOVCERT de adviezen geeft over het beheer van overheids-ICT. We hebben net besproken hoe er beter gevolg aan gegeven kan worden als adviezen van GOVCERTvcert niet goed worden doorgevoerd. Externe deskundigheid wordt betrokken waar dat kan, bijvoorbeeld in de vorm van het laten uitvoeren van penetratietesten, stresstesten, risicoanalyses en externe audits. Ik wees net al op de Gateway reviews die voor sommige systemen worden gehouden. De Algemene Rekenkamer geeft jaarlijks een onafhankelijk oordeel over het financieel beheer en het materieel beheer en dat betreft ook ICT. Daarnaast moeten de eisen ten aanzien van de beveiliging en privacy zijn opgenomen in de aanbesteding. Een groot aantal maatregelen is genomen en wordt nog genomen. Ik pleit ervoor om niet opnieuw nieuwe instituten in te stellen, maar te kijken of wat we hebben, goed functioneert.

De **voorzitter**:
Ik zeg tegen de heer El Fassed dat dit zijn derde en tevens laatste interruptie wordt.

De heer **El Fassed** (GroenLinks):
Ik zei al dat we het niet alleen moeten hebben over een incident. Het belangrijkste is dat er een cultuuromslag nodig is. Als dat besef er is, dan lijkt het mij verstandig om

iemand van buiten de sector erbij te betrekken en niet iemand uit de bestaande instituten en structuren. Deze persoon moet bekijken welke cultuur er op het gebied van veiligheid en privacy is in de relatie van ICT en overheid.

Minister **Donner**:
Dat is nu net een aspect waarom we de Onderzoeksraad Voor Veiligheid zullen vragen om te kijken waar de problematiek bij de overheid zit. Ook als blijkt dat er een cultuurprobleem is, ben ik de laatste om te pleiten voor een veiligheidsambassadeur of -gezant, want dan leg je al je problemen bij die persoon neer en is het voor niemand anders meer een probleem. Als er een cultuurprobleem is, is dit juist niet een geschikte oplossing. Je moet dan kijken hoe je op een andere wijze de cultuur kunt veranderen.

De heer El Fassed vroeg nog waarom er niet terughoudender wordt opgetreden met de gegevens en met het mechanisme dat de banken daarvoor gebruiken. Ik kan de termen daarvoor niet helemaal herhalen, want die kan ik niet lezen. Privacy en bijbehorende eisen voor de beveiliging worden meegenomen bij de aanbesteding van de systemen.

Logius zal een strikt beleid voeren rondom de veiligheid van systemen. Ook wordt het volgende probleem aangevoerd. Als iets digitaal is, worden al gauw de letters digi gebruikt met een woord daarachter, waardoor het beeld ontstaat dat alles een probleem is van DigiD. DigiD is tot nu toe niet een probleem gebleken, maar is wel een instrument waarmee de communicatie plaatsvindt. Daarom is deze of vorige week de maatregel genomen dat alle sites die onveilig blijken te zijn, onmiddellijk afgesloten worden van DigiD en pas na een audit van de veiligheid weer worden aangesloten. Alle sites die gecompromitteerd zijn met mogelijke gevolgen voor DigiD, worden dus afgesloten. Dat is de afgelopen week al gebeurd, ook met de gemeentelijke sites die gecompromitteerd bleken te zijn. De organisaties die zijn afgesloten, kunnen alleen weer worden aangesloten als blijkt dat de ICT-beveiliging weer op orde is. Alle DigiD-gebruikende organisaties dienen uiterlijk voor het einde van het eerste kwartaal van 2012 hun ICT-beveiliging getoetst te hebben op basis van een ICT-beveiligingsassessment.

De **voorzitter**:
Hoeveel minuten tekst hebt u nog, minister?

Minister **Donner**:
Ik heb nog antwoorden voor mevrouw Hennis en de heren Koopmans en Elissen.

De **voorzitter**:
Goed. Laten wij allen proberen het iets bondiger te doen.

Dan mag mevrouw Hennis nu haar vraag stellen.

Mevrouw **Hennis-Plasschaert** (VVD):
Ik zal het kort houden, maar ik sloeg even aan op de woorden "logisch" en "strikt beleid", die de minister bijna uitsprak als één woord. Ik neem aan dat hij daar later nog op ingaat. Als het gaat om strikt beleid, is de minister het dan met de VVD eens dat enige vorm van risicospreiding van belang is, dat het dus niet logisch is, zeker met de kennis van nu, om de nieuwe PKI-Overheid-certificaten slechts door één bedrijf te laten verstrekken, maar dat ook daar aan risicospreiding moet worden gedaan?

Minister **Donner**:
Ik meen dat PKI-Overheid-certificaten op dit moment nog bij drie andere bedrijven lopen. DigiNotar was een van de vier Nederlandse bedrijven. Daarnaast zijn er nog tal van buitenlandse bedrijven. Bij DigiNotar waren ook buitenlandse bedrijven aangesloten. Er is dus een heel netwerk waarin de risico's verspreid zijn.

Mevrouw **Hennis-Plasschaert** (VVD):
Ik heb het nu even specifiek over de nieuwe PKI-Overheid-certificaten. Daarvan gaan de verhalen dat die slechts bij één verstrekker worden betrokken.

Minister **Donner**:
Ik geef mevrouw Hennis daar in tweede termijn antwoord op, want dit vergt een technische kennis die ik niet heb.

Op de vragen van de heer El Fassed over de WRR, was ik al ingegaan.

Mevrouw Hennis vroeg of er al dan niet gekwalificeerde certificaten gebruikt waren. Ik heb al uiteengezet hoe het systeem werkt. Vervolgens vroeg zij ook naar Logius en het goed opdrachtgeverschap. Logius is geen opdrachtgever. Dat is dus niet aan de orde. Logius was alleen de policy authority waar de verschillende auditrapporten naartoe moesten. Tot het uitbreken van de DigiNotar-crisis heeft Logius geen indicatie gekregen dat er sprake was van problemen bij DigiNotar.

De vragen over de "brandweer", de cyber security en de brede meldplicht heb ik behandeld.

Ik kom op de vragen over de financiële consequenties van het geheel. Tot dusver heeft de prioriteit van de overheid gelegen bij het beperken en voorkomen van de schade.

De Staat heeft DigiNotar op 5 oktober aansprakelijk gesteld. Over de omvang van de schade valt nog niets te zeggen. Vermoedelijk zal er een schadestaatprocedure voor gevolgd worden.

Op de vraag over verantwoordelijkheden van andere bedrijven ben ik reeds ingegaan.

Het feit dat DigiNotar failliet is, zal zonder meer tot juridische complicaties leiden.

Ik kom op het beveiligingskader van de rijksoverheid voor de rijksdienst. Voor de informatiebeveiliging geldt een aantal regelingen. Voor informatie waarvoor een verhoogde mate van vertrouwelijkheid is vereist geldt een aanvullende regeling, namelijk het Besluit voorschrift informatiebeveiliging rijksdienst. Dat bevat regels en maatregelen gericht op de bescherming van de vertrouwelijkheid. Alle ministeries hebben ervoor gekozen, een of meer gemeenschappelijke stelsels van betrouwbaarheidseisen, normen en maatregelen af te spreken, ofwel: de rijksbrede baseline. Daardoor bestaan geen grote verschillen meer tussen ieder van de departementen. De rijksbrede baseline is bijna klaar. De vaststelling ervan verwacht ik begin volgend jaar.

De heer Koopmans heeft gevraagd hoe het zover kon komen. Ik ben ingegaan op de aanloop en herkomst van de ontwikkelingen.

De heer Koopmans sprak over de problematiek van de hackers. Daar ben ik ook op ingegaan.

Ten slotte vroeg de heer Koopmans hoe het zit met het kader. Voor het Rijk zijn de kaders waaraan de sites moeten voldoen bijna klaar. Uiteraard zijn die beschikbaar voor de gemeenten. Ik heb net gezegd dat de handhaving daarvan plaats zal vinden door afkoppeling van DigiD. Ik

begrijp dat daarover gisteren een brief aan de Kamer is gestuurd.

De heer **Koopmans** (CDA):
Ik heb de minister ook gevraagd of hij het met ons eens is dat het een continu en dynamisch proces is. Het heeft dagelijks aandacht nodig, en niet ieder jaar of iedere twee jaar.

Minister **Donner**:
Mijn reactie op de mededeling dat de veiligheidsverklaring van een site slechts een relatief beperkte waarde heeft, net zoals andere tests, is dat ik het daar geheel mee eens ben. Dat is nu net een probleem van regelgeving. Hoe meer we de regelgeving in allerlei wettelijke voorzieningen leggen, des te rigider wordt het om de regelgeving aan te passen. Daarom wordt er nu gewerkt met kaders en regels die tussen betrokkenen worden afgesproken.

De heer **Koopmans** (CDA):
Dat delen wij. De vraag is wel of de organisatie er voldoende op is ingericht dat die dynamiek werkelijkheid kan worden. De ministers en ondergetekende weten natuurlijk ook dat juist binnen departementen vaak de neiging bestaat om te komen tot zoiets als met zeven parafen tot aan de bewindslieden vastgestelde voorwaarden.

Minister **Donner**:
Ik meen dat de heer Koopmans hiermee een toch ietwat sjabloonachtig beeld geeft van de wijze waarop dit soort zaken wordt vastgesteld. Juist omdat je het breed doet, is er inderdaad een betrokkenheid bij. Ik kan garanderen – en zeker als blijkt dat dit een van de knelpunten is op dit moment – dat dit een van de aspecten is die ongetwijfeld bekeken zal worden.

Voorzitter. De heer Elissen vroeg om een minimaal jaarlijkse test. In de brief die gisteren aan de Kamer is gestuurd staat dat voortaan jaarlijks een ICT-beveiligingassessment zal plaatsvinden voor de organisaties die gebruikmaken van DigiD. Daarvoor zal GOVCERT.NL het toetskader aanleveren. Pentesten zullen daar een onderdeel van zijn. Ik heb aangegeven dat de basis die daarvoor zal gelden vermoedelijk begin volgend jaar klaar zal zijn.

De minister van Veiligheid en Justitie zal ingaan op de regie, wat er gebeurt en wat er fout is.

Op het kennisniveau bij de overheid ben ik ingegaan. Er zijn verschillende maatregelen die nu al op de systemen worden toegepast, er zijn Gatewayreviews, er zijn opleidingen, met name de opleiding van ICT-mensen. Er is ook een ontwikkeling gaande om de kennis bij de overheid te verruimen, zeker als het gaat om grotere opdrachtgevers zoals het UWV, om niet afhankelijk te zijn van de kennis die op ieder moment wordt ingehuurd. Er worden raamcontracten afgesloten voor ontbrekende of specialistische kennis. Ik heb uiteengezet hoe het PKI-Overheid-systeem in elkaar zit. Op de commandostructuur zal de minister van Veiligheid en Justitie ingaan.

Daarmee heb ik volgens mij de vragen beantwoord. Ik wil nog een algemene samenvatting geven, omdat dit anders te veel blijft hangen in de individuele beantwoording. Naar aanleiding van de DigiNotar-problematiek is door ons inmiddels een groot aantal maatregelen getroffen. Voor de meldingssystemen heb ik een toezegging gedaan over de persoonsgegevens en de problematiek van inbreuk op organisaties. In het verlengde van de oprichting van het Cyber Security Center worden aanvullende kaders gemaakt voor de ICT-beveiliging. Verder wordt overleg gevoerd met de VNG en andere medeoverheden over het op peil brengen van de ICT-beveiliging. Een belangrijk instrument zijn de beveiligingsadviezen van GOVCERT.NL; daarop zal de minister van Veiligheid en Justitie nog ingaan. In de brief aan de Kamer van 16 september is een groot aantal andere vervolgacties weergegeven. Zoals gezegd is er gisteren een brief aan de Kamer gestuurd, waarin vooral wordt ingegaan op de wijze waarop wordt gereageerd op de recente kwetsbaarheden van sites die DigiD gebruiken. Dat laat onverlet dat wij blijven kijken waar verdere verbeteringen mogelijk zijn.

□

Minister **Opstelten**:
Voorzitter. Ik dank de leden voor de op mijn terrein gestelde vragen. Ik zal daarop graag ingaan. Het is een belangrijk debat, zoals door de aanwezige leden is aangegeven. Inbreuken op de veiligheid van het internet raken ons direct. Als coördinerend minister op het terrein van de cyber-security – dat doe ik samen met de collega's van EL&I en Defensie – en in dit geval ook als verantwoordelijk minister voor crisisbeheersing vind ik het essentieel dat de juiste kennis en expertise beschikbaar zijn, zodat deze zowel in de voorbereiding op een incident als op het moment dat er iets gebeurt direct kunnen worden ingezet. Ik denk dat ik dit bij een aantal van de leden ook heb bespeurd. Daarover zijn vragen gesteld en deze zal ik ook beantwoorden. De gebeurtenissen met DigiNotar en recente incidenten rondom lektober onderstrepen het belang van de actielijnen van de Nationale Cyber Security Strategie zoals deze zijn ingezet. Ze zijn ook met de Kamer besproken, in een AO van 1 juni jongstleden.

Een aantal Kamerleden had aarzelingen over de scherpte en de noodzaak van die strategie. Ik denk dat de hele DigiNotar-affaire die noodzaak in een ander daglicht heeft geplaatst. GOVCERT, het computer emergency response team van de overheid, monitort de lektoberincidenten en zorgt ervoor dat passende maatregelen genomen kunnen worden. Ook in de toekomst zullen voor deze incidenten in lijn met de nationale cybersecuritystrategie passende maatregelen worden genomen. Twee grote onderdelen zijn het inrichten van het Nationaal Cyber Security Centrum en de cybersecurityraad. Ik ga daar straks nog iets specifieker op in.

Het Nationaal Cyber Security Centrum vervult echt een coördinerende rol voor alle betrokken publieke en private partijen, wetenschap- en kennisinstituten. Daarnaast levert het Nationaal Cyber Security Centrum een adequate respons bij dreigingen en incidenten. De cybersecurityraad vervult op strategisch niveau de governancefunctie. De raad is samengesteld uit vertegenwoordigers uit publieke, private en wetenschappelijke sectoren – als ik dat mag zeggen: het beste wat in ons land beschikbaar is – en maakt afspraken over de uitvoering en de uitwerking van de nationale cybersecuritystrategie. Met de strategie zijn de lijnen uitgezet voor de integrale aanpak van cyber security, waarbinnen publiekprivate maar ook civiel-militaire samenwerking en internationale samenwerking op innovatieve wijze vorm krijgt. Vandaar de betrokkenheid van onze collega van Defensie.

Nog belangrijker uiteraard is dat het ook in de praktijk werkt. Ik ben er dan ook blij mee dat deze samenwerking

meteen haar nut bewees, ook in de afgelopen periode. De extra ondersteuning van expertise van Defensie voor GOVCERT is daarvan een voorbeeld, net zoals de zeer nauwe samenwerking in de periode van crisisbeheersing met VNO-NCW tijdens de gebeurtenissen inzake DigiNotar. Wij plukken daar dus nu al de vruchten van.

De cybersecurityraad is inmiddels op 30 juni jongstleden geïnstalleerd en op een zeer enthousiaste en ook betrokken wijze van start gegaan. Tijdens DigiNotar mocht ik ook daarvan al meteen resultaat zien.

Op 1 januari aanstaande zal het centrum van start gaan. Het centrum wordt ingericht langs de volgende lijnen. Het centrum is hét platform voor uitwisseling van informatie, kennis en ervaring tussen alle betrokken publieke en private partijen, wetenschap- en kennisinstituten en het is het kenniscentrum voor alle betrokken publieke en private partijen, wetenschap- en kennisinstituten. Het levert adequate en slagvaardige respons bij incidenten en dreigingen, waar een aantal van de leden ook over heeft gesproken. Deze lijnen worden nu verder uitgekristalliseerd. Ik zal de Kamer voor het eind van het jaar hierover nader informeren en een en ander concretiseren. Ik denk dat wij de onderzoeken die lopen, daarbij zullen betrekken. GOVCERT, het cyber security en incident response team van de overheid, maakt daarvan een belangrijk onderdeel uit. Dat team wordt daar ondergebracht.

Ook in dit debat hoor ik veel Kamerleden vragen naar de beschikbare kennis en expertise bij de overheid in dit verband. Ik kan de Kamer melden dat die er wel is. GOVCERT bestaat uit experts op het gebied van ICT-beveiliging en maakt onderdeel uit van een groot internationaal netwerk van responsorganisaties. Ik denk dat we dat hier ook wel een keer moeten zeggen. Het centrum pakt daarbij nadrukkelijk zijn verantwoordelijkheid om de risico's op het gebied van digitale veiligheid te beperken of zelfs voor te zijn. Het is daarom van groot belang dat bedrijven en overheidsorganisaties de adviezen die het centrum zal geven, ter harte nemen en investeren in de kennis in huis om dat te doen. Daarnaast speelt het KLPD High Tech Crime-team, waarbij een aantal Kamerleden op bezoek zijn geweest, als ik mij niet vergis, een belangrijke rol bij de opsporing. Het onderzoek van het Openbaar Ministerie in dit kader gebeurt natuurlijk door dit team. Internationaal zijn deze twee teams bekend om de kwaliteit van de mensen die wij daarbij hebben.

Ik zal ingaan op een aantal specifieke vragen die nog niet zijn beantwoord door collega Donner. Door mevrouw Gesthuizen, de heer Koopmans en mevrouw Hachchi is gevraagd of het Rijk de deskundigheid van sommige hackers die kunnen helpen, voldoende benut en hoe. Wij staan positief tegenover het inzetten van externe deskundigen. Ik vind dat de heer Koopmans dit heel goed heeft geformuleerd. Hackers zijn inbrekers, als zij kwade bedoelingen hebben, dus ik moet wel een scheiding maken tussen al of niet te goeder trouw. De woordvoerders en ik zullen het erover eens zijn: mits het binnen de juridische kaders valt. Als ik dit uitspreek, vind ik het vanzelfsprekend, maar ik moet wel die grens trekken. Ik merk erbij op dat wij natuurlijk al de nodige expertise op dit terrein hebben. Ik kan ook melden dat er in opdracht van de Nationale Coördinator Terrorismebestrijding reeds beveiligingstesten worden gedaan, waarbij ook hackmethodes worden toegepast. Wij zullen dat natuurlijk verder uitwerken, maar ik denk dat het goed is om dat hier al te zeggen.

Mevrouw Gesthuizen sprak over de crash teams. Zij kent mij, dus zij weet dat dit mij wel aanspreekt. Ik houd ook van uitrukken en nog meer van blussen. We hebben GOVCERT, het Cyber Security en Incident Response Team van de overheid. Dat gaat per 1 januari 2012 deel uitmaken van het Nationaal Cyber Security Centrum. Vanuit de strategie wordt er tevens geïnvesteerd in het versterken van de weerbaarheid van de vitale sectoren. Het is de eigen verantwoordelijkheid van de organisaties om indringende adviezen ter harte te nemen, zoals collega Donner heeft gezegd. Iedereen dient te investeren in kennis en kunde. Dat is bij iedereen zo, als het gaat om veiligheid. Ook een onderneming is allereerst verantwoordelijk voor zijn eigen veiligheid. Elke burger is dat. Als er echt iets aan de hand is, handelen we volgens het Nationaal Handboek Crisisbesluitvorming. Specifiek voor ICT-crises hebben wij de ICT Response Board, die per 1 januari is verbonden aan het Nationaal Cyber Security Centrum.

Wat dit betreft zie ik een nieuwe vliegende brigade of crash team niet als noodzakelijk. In het AO over de Cyber Security Strategie hebben we twee heldere afspraken gemaakt. Er komt een dreigingsanalyse van wat er precies aan de hand is in ons land; wat zijn de bedreigingen. Daar betrekken we nu alle deskundigen bij. The state of the art op dit terrein. Die komt er. Die zal in november er zijn. Ook de Cyber Security Raad zal daarnaar kijken.

Het tweede punt is dat ik, ook op verzoek van de Kamer, heb afgesproken dat ik tegelijkertijd het juridisch kader zal schetsen. Wat is de wettelijke positie ten aanzien van de situaties die ons bedreigen en wat is er voor extra juridisch instrumentarium voor nodig? Ik denk dat ik in dat verband ook deze positie zal bekijken. Ik zal bekijken in hoeverre doorzettingsmacht noodzakelijk is om, als we gaan blussen, dan ook te kunnen doorzetten. Als GOVCERT een advies uitbrengt, kan dat niet vrijblijvend zijn.

De **voorzitter**:
Ik zie dat mevrouw Gesthuizen toch een vraag heeft. Voor haar is dat de derde interruptie.

Mevrouw **Gesthuizen** (SP):
Die gebruik ik hier graag voor. Het is hartstikke mooi dat de minister hier toezegt dat we nog eens gaan kijken naar die doorzettingsmacht. Ik heb hierover toch nog een vraag. Wij hebben een Gezondheidsraad. Die komt met adviezen. Maar dat is niet de ambulance die zal uitrijden als ergens een ongeluk is gebeurd. En dat zijn ook niet al die verschillende artsen die bij verschillende acute complicaties kunnen ingrijpen en die zo'n patiënt in een ziekenhuis onder handen kunnen nemen. Daarom stel ik de minister de volgende vraag. Hij zegt: we hebben al GOVCERT. Dat is in mijn ogen vooral een kennisplatform. Als wij GOVCERT hebben en dat is, zoals de minister hier zegt, wel die uitrukkende instantie waar hij zo van houdt en die we nodig hebben, waarom is er dan zo nadrukkelijk steeds gebruikt gemaakt van de expertise van bijvoorbeeld een bedrijf als Fox-IT bij de DigiNotar-crisis? Waarom hadden we dan niet zelf alle middelen in huis om te onderzoeken, om te analyseren en om het lek te dichten?

Minister **Opstelten**:
Ik denk niet dat u dat goed ziet. Het GOVCERT is juist niet alleen een kenniscentrum maar ook een optredend instituut. Er is net discussie over geweest. Ik kan ook alle data weer aangeven die collega Donner net heeft nagelopen. Ik zal dat met het oog op de tijd niet doen. Het KLPD High Tech en Crime Team, de AIVD en straks het Nationaal Cyber Security Centrum waar al deze instituten in worden

ondergebracht, in ieder geval GOVCERT, is natuurlijk een optredende organisatie. Geeft u mij nu de ruimte! U wilt ook niet iets nieuws hebben als het niet nodig is. Zo ken ik u niet. Ik denk dat we gewoon, wat dat betreft, ongeveer in dezelfde situatie zitten. Er moet opgetreden worden als dat nodig is. Er mag niet meer een instituut zijn dat, als GOVCERT zegt "dat moet je doen", dat naast zich neerlegt. Dat zijn de punten waar het hier in de kern om gaat. Wij pakken dat aan. We leggen dat neer en zullen dat ook aan de Kamer zenden. Dat krijgt de Kamer in november. Dat is al heel snel.

Mevrouw **Gesthuizen** (SP):
Ik ben inderdaad geen voorstander van het oprichten van overbodige instituten. Als iets overbodige instituten kenmerkt, dan is het ook wel dat zij vaak veel te dure en overbodige directeuren hebben. Dat willen we allemaal niet. Ik wil wel het volgende van de minister weten. Als het allemaal al zo goed klopt, waar waren al die instanties dan toen het zo verschrikkelijk misging met DigiNotar?

Minister **Opstelten**:
Dan moet ik weer gaan herhalen wat collega Donner heeft gezegd. Dat zou ik niet willen doen. Ik sluit me aan bij wat collega Donner heeft gezegd.

Ik wil tegen de heer Heijnen nog het volgende zeggen. Die coördinerende rol heb ik. Er is dus ook regie bij de crisis. Dat ligt in mijn handen. Ik kom nu op het punt van het onderzoek van de Raad voor de Veiligheid, met die aspecten die daar ook thuishoren, in hun absolute onafhankelijkheid. Dat is een groot goed. De crisisbeheersingcoördinatie is op topniveau ingezet. Daarbij hoort altijd onafhankelijk onderzoek van de Inspectie Openbare Orde en Veiligheid naar hoe het is gegaan en hoe wij het hebben gedaan. De Raad en de Inspectie Openbare Orde en Veiligheid zullen dat zeker op elkaar afstemmen.

De heer Elissen heeft het meest nadrukkelijk gevraagd naar de regie. Hij wil voortdurend iemand met regie; nou, hier staat hij dan! Zo ziet hij eruit! Of daarvoor extra doorzettingsmacht nodig is, bezie ik op basis van ... Ik herhaal het nog een keer, want wij hebben dat al met de Kamer afgesproken en het heeft nu een extra dimensie gekregen, wat ik heel plezierig vind. Hoewel het vervelend is wat er is gebeurd, geeft het duidelijk een sense of urgency aan, een dreigingsbeeld van de cyber security. Waarmee hebben wij te maken, niet alleen nu op basis van een incident, wat is state of the art? Waar loop je vast als je het dreigingsbeeld ziet? Wat heb je juridisch nodig? Ik heb gezegd dat ik het in november klaar zal hebben. De Kamer heeft mij destijds gevraagd om geen haastwerk te leveren maar om er liever iets meer tijd voor te nemen. De Kamer krijgt het in november.

Ik denk dat ik de heer Heijnen genoeg heb gezegd over het onderzoek. Ik moet zeggen dat ik denk dat het belangrijk is.

Nu de hele DigiNotar-kwestie zich heeft afgespeeld, wij deze ervaring met elkaar hebben en wij dit debat voeren – dat naar onze mening een belangrijk debat is – lijkt het mij goed om niet alleen te evalueren hoe wij het met elkaar allemaal gedaan hebben, hoewel het altijd goed en nuttig is om ervan te leren. Het is echter ook belangrijk om de situaties die ik heb aangekondigd, mee te geven aan de Raad voor de Veiligheid om ze van een toets te voorzien. Wij zijn met elkaar bezig om hier sterker uit te komen. Zo zie ik het ook. Wat dat betreft willen wij ons er kwetsbaar in opstellen. Wat ik aankondig, gebeurt gewoon. Het zal geen vertraging opleveren. Ook als wij het niet vragen, zal de Raad het doen. Zo ken ik de Raad en zo moet hij ook krachtig opereren. Dat nemen wij dus mee.

Ik heb al over het Openbaar Ministerie en het onderzoek van de politie gesproken. Ik kan daar verder niets over zeggen.

Tot mevrouw Hennis heb ik al het nodige gezegd over de positie van het Nationaal Cyber Security Center. Ik wil nog wel iets zeggen over de responscapaciteit. Die vraag is natuurlijk heel relevant. De overheid heeft een eigen responscapaciteit met GOVCERT. Het team van GOVCERT bestaat uit experts op het gebied van ICT-beveiliging en maakt onderdeel uit van een groot internationaal netwerk van responsorganisaties. Per 1 januari komt er een verandering in de positie. Ten aanzien van de ICT-veiligheid is het uitgangspunt dat organisaties zelf verantwoordelijk zijn. Laten wij daaraan alsjeblieft scherp vasthouden. ICT-veiligheidsincidenten dienen dan ook in eerste instantie door de eigen organisatie of sector te worden opgelost. Bepaalde organisaties van vitale sectoren voorzien daarin door het hebben van een eigen incidentresponsteam voor de dienstverlening. Wanneer de betreffende overheidsorganisatie er niet in slaagt, een ICT-veiligheidsincident op te lossen, kan GOVCERT actief optreden. Collega Donner heeft al het nodige gezegd over de meldplicht.

De **voorzitter**:
Voordat u verder gaat, wil mevrouw Hennis beginnen aan haar derde interruptie.

Mevrouw **Hennis-Plasschaert** (VVD):
Voorzitter. De minister spreekt over eigen verantwoordelijkheid van de organisatie. Als liberaal spreekt die eigen verantwoordelijkheid mij zeer aan. Mijn roep is echter vooral om regie, om heldere richtlijnen, om de invulling van de regiefunctie door de minister en in de toekomst door het NCSC, om de vraagbaakfunctie en ook om enige verplichting voor organisaties om aan bepaalde richtlijnen te voldoen. Mijn roep is dus om de vrijblijvendheid er vanaf te halen. Ik hoop dat dit niet wordt verstaan onder de eigen verantwoordelijkheid.

Minister **Opstelten**:
Nee. Ik heb daar, dacht ik, ook al het nodige over gezegd. We geven dat natuurlijk in de dreigingsanalyse en in het juridische kader ook aan. Daarin geven we eveneens heel precies aan – ik heb dat net in het debat met mevrouw Gesthuizen ook gezegd – wat een responsteam doet en wat het NCSC is. Dat is natuurlijk een platform, het is een kenniscentrum, een centrum voor adequate en slagvaardige respons bij incidenten en dreigingen. Dat gaat per 1 januari werken. Het wordt nu uitgekristalliseerd en voor het eind van het jaar zal ik de Kamer concreter informeren over het takenpakket en de positie van het centrum.

Ik houd niet van vrijblijvendheid, maar wel van eigen verantwoordelijkheid. Als iemand zijn verantwoordelijkheid niet draagt, dan moet er ingegrepen worden als de veiligheid van het hele systeem dat vereist. Dat is de positie waarin we verkeren en dat is het punt dat zowel collega Donner als ik graag willen bezien en analyseren. Regie betekent immers niet alleen maar vergaderingen bijwonen en abstracte visies over de toekomst van cyber security met elkaar behandelen. Bespreken is ook belangrijk, evenals visionair ernaar kijken en daar internationaal leidend in zijn. Het betekent echter ook concreet zaken doen die van belang zijn. Dat hebben we geleerd in deze Digi-

Notar-kwestie. Het was een incident, maar dat incident heeft ook wat blootgelegd zoals blijkt in dit debat.

Mevrouw Hennis heeft voorts gevraagd naar de exacte rol van de raad. Daar wil ik ook nog iets over zeggen. In het kader van de concrete resultaten heeft de raad in eerste vergadering besloten om zich in de komende periode te richten op vijf hoofdpunten. Ik deel deze nog een keer met de Kamer. Het eerste punt is de opbouw van een adequate responscapaciteit. Dit zijn dus de op dit terrein leidende mensen uit het bedrijfsleven en uit de overheid, en het is belangrijk dat die daar een duidelijke mening over ventileren. Het tweede punt is het beschikken over een actuele en betrouwbare dreigingsanalyse. Die krijgt de Kamer dus in november, nadat die mensen daar hun licht over hebben laten schijnen. Het derde punt is het versterken en aansturen van onderzoek en kennisopbouw. Dat moeten we niet vergeten. Punt vier is aandacht voor een proactieve benadering naast preventieve maatregelen, en punt vijf is het vergroten van het bewustzijn van cyberdreigingen bij het publiek, de overheid en het bedrijfsleven. Er moet een "sense of urgency" komen, want die urgentie is natuurlijk nadrukkelijk aangetoond de laatste tijd.

Dan blijven voor mij nog twee punten over. Dat is ook wat mevrouw Hennis heeft gevraagd. Is er een continuïteitsplan? In de derde voortgangsbrief Nationale Veiligheid van februari 2011 is de Kamer geïnformeerd over initiatieven van het kabinet ten aanzien van ICT-continuïteitsplannen binnen de sectoren openbare orde en veiligheid en openbaar bestuur. Op dit moment wordt binnen de sectoren openbare orde en veiligheid en openbaar bestuur hard gewerkt aan het opstellen van continuïteitsplannen. Dat betreft onder andere de provincies, de veiligheidsregio's, de gemeenten, de politieregio's, de waterschappen en ook het Rijk. De sectoren binnen de openbare orde en het openbaar bestuur zijn actief benaderd middels een brief en een informatiepakket. Zij worden ook verder gefaciliteerd vanuit mijn ministerie. Dit verloopt volgens de planning.

In januari 2012 zal een meting plaatsvinden in hoeverre binnen de sectoren daadwerkelijk continuïteitsplannen zijn opgesteld. Ook hier zal het niet vrijblijvend zijn. Er zal monitoring plaatsvinden en het zal worden gecheckt.

Mevrouw Hennis stelde dat de meldplicht persoonsgegevens niet voldoende is. Minister Donner heeft daar al over gesproken. In onze brief hebben wij aangekondigd dat de wijze waarop de meldplicht in het NCSC wordt ingericht, wordt meegenomen in de brief aan de Kamer over de inrichting van het NCSC. Die zal de Kamer voor het einde van het jaar ontvangen. Voor het verplicht melden van "security breaches" is een bredere meldplicht noodzakelijk. Daarbij is van groot belang dat het vertrouwelijke karakter van de melding absoluut wordt gewaarborgd. Er dient een zeer goede balans te zijn. Bedrijven hebben immers privacybelangen. Sommige gegevens zijn vertrouwelijk. VNO-NCW heeft zich daar duidelijk in opgesteld. ICT-infrastructuurproducten en -diensten worden voor het grootste deel door private partijen geleverd. Wederzijds vertrouwen tussen publieke en private partijen is essentieel om te kunnen samenwerken en informatie met elkaar te kunnen delen. Ongeacht zo'n meldplicht, is het van groot belang dat zo min mogelijk drempels voor effectieve samenwerking worden ingebouwd en dat de te bieden hulp voorop staat. Ik zal voor het einde van het jaar in een brief aangeven hoe wij dat gaan uitwerken.

De **voorzitter**:
Dank u wel, minister. Voordat wij verder gaan met een korte tweede termijn, geef ik minister Donner de gelegenheid om twee feitelijke vragen te beantwoorden.

☐

Minister **Donner**:
Voorzitter. De heer Heijnen vroeg of er expliciet is getoetst aan de aanvullende eisen van de PKI-Overheid. Het antwoord daarop is ja. De auditor heeft jaarlijks bij Diginotar expliciet getoetst op de aanvullende eisen van PKI-Overheid. Diginotar was onder het stelsel van PKI-Overheid verplicht om dat rapport aan de Policy Authority te sturen. Dat is gebeurd. De Policy Authority is in het bezit van het rapport, dat dateert van eind 2010. Ook in dat rapport heeft de auditor een goedkeurende verklaring afgegeven. Het rapport zelf is vertrouwelijk conform het contract tussen de auditor en het gekeurde bedrijf. Ik heb hier voor mij het certificaat dat is afgegeven door PwC eind vorig jaar, waarin uitdrukkelijk de toetsing wordt gemeld op de aanvullende PKI-Overheid-eisen die zijn gesteld.

Mevrouw Hennis had het idee dat de nieuwe certificaten slechts door één certificaatdienstverlener zouden worden gegeven. Dat beeld is niet juist. De nieuwe certificaten worden door verschillende organisaties gegeven, namelijk ESG, QuoVadis, KPN-Getronics en Digidentity. Dit is dus niet beperkt tot één certificaatdienstverlener.

De **voorzitter**:
Is er bij de leden behoefte aan het houden van een tweede termijn? Ik zie dat dit het geval is. In die termijn kunnen de woordvoerders nog slechts enkele opmerkingen maken en moties indienen. Rekenkundig hebben zij namelijk recht op niet meer spreektijd dan 100 seconden.

☐

Mevrouw **Gesthuizen** (SP):
Voorzitter. Ik dank de beide ministers voor de beantwoording. Ik ben erg gelukkig met wat ik opvat als de toezegging dat de Onderzoeksraad Voor Veiligheid een onderzoek gaat doen naar de gang van zaken en naar de manier waarop wij het veiligheidssysteem voor de ICT hebben ingericht. Ik ben daarover verheugd omdat de Onderzoeksraad Voor Veiligheid onlangs onderzoek heeft gedaan naar de casus Alphen aan den Rijn en daarbij uitstekend werk heeft geleverd. Wij gaan daarover nog met de minister van gedachten wisselen.

Ik ben echter niet overtuigd van de expertise en van de juistheid van de bevoegdheden. Ik ben er ook niet van overtuigd of de verwachtingen terecht zijn die de ministers hebben van bijvoorbeeld GOVCERT. Men was niet aanwezig bij de hoorzitting zelf, maar ik vond die hoorzitting ontluisterend. Het was ontluisterend om te horen hoe de experts zich niet konden uitlaten over wat ons in de weken ervoor was overkomen. Mensen verdienen in deze branche goed geld, zowel bij bedrijven als bij de overheid. Ik vind dat wij terecht de vraag kunnen stellen of zij hun werk wel goed doen. Daarom dien ik de volgende twee moties in.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat door onvoldoende regie op het gebied van veiligheid en privacywaarborg rond ICT bij de overheid de afgelopen jaren diverse gebreken aan het licht zijn gekomen welke de privacy en veiligheid van burgers in gevaar bleken te hebben gebracht;

overwegende dat het van belang is om inzichtelijk te krijgen of en welke misstappen in het verleden gemaakt zijn, zodat in de toekomst de hoogst mogelijke veiligheid en waarborg van privacy rond ICT-diensten en -systemen bij de overheid kan worden geboden;

constaterende dat het niet uitgesloten is dat naast de al bekende problemen op het gebied van de ICT bij de overheid, nog nieuwe problemen zich zullen openbaren;

van oordeel dat een parlementair onderzoek naar de oorzaken, gevolgen en mogelijke verbeteringen van de debacles van de ICT-veiligheid bij de overheid, op een nader te bepalen aantal dossiers gewenst is;

van mening dat bij een dergelijk onderzoek tevens duidelijk moge worden of zowel huidige als voorgaande Kamers en kabinetten op basis van voldoende en correcte informatie hebben besloten tot introductie van ICT-diensten en -systemen bij de overheid;

verzoekt het Presidium, zo spoedig mogelijk voorstellen te doen over de opzet en de vorm van zo'n parlementair onderzoek,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Gesthuizen en El Fassed. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 194 (26643).

De **voorzitter**:
De heer Koopmans gaat voor de derde keer interrumperen.

De heer **Koopmans** (CDA):
Mevrouw Gesthuizen begon haar bijdrage terecht met het trekken van de conclusie dat het goed is dat de regering de Onderzoeksraad Voor Veiligheid inzet. Ik meen echter dat wel de vraag moet worden gesteld of het parlement die raad niet voor de voeten gaat lopen bij het doen van zijn onafhankelijk onderzoek, als het parlement ook aan de slag gaat met een onderzoek.

□

Mevrouw **Gesthuizen** (SP):
Ik wacht wat dat betreft de conclusie van de bewindspersoon af. Ik zeg de heer Koopmans echter één ding. Als het verstandig is om de onderzoeksresultaten af te wachten, dan ben ik uiteraard bereid om deze motie aan te houden.

De heer **Koopmans** (CDA):
Ik zou wel willen suggereren om dat te doen. Ik ben ook benieuwd naar het antwoord van de regering op dat punt, hoewel de motie aan het Presidium is gericht. Het past dus minder om de regering hierover een vraag te stellen. Toch vraag ik de ministers om ook even op dat aspect in te gaan. Mevrouw Gesthuizen, ikzelf en ook andere woordvoerders van de SP en het CDA hebben in het verleden hierin goed samen opgetrokken, omdat wij graag de onderste steen boven willen hebben. Die onderste steen moet echter wel op de juiste manier boven worden gebracht.

Mevrouw **Gesthuizen** (SP):
De onderste steen op de juiste manier boven brengen; dat is een mooie metafoor. Wat de heer Koopmans zegt, klopt. Ik verwacht een advies, niet over de vraag of het parlement wel of niet een parlementair onderzoek zou moeten doen, maar vooral over de vraag of een dergelijk gegeven mogelijk strijdig is met de taak die bij de Onderzoeksraad Voor Veiligheid wordt neergelegd.
Daarmee kom ik op mijn tweede motie, voorzitter.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat bij urgente ICT-problemen het gewenst is dat een daartoe wat betreft intellect, middelen als doorzetmacht geëquipeerde dienst direct de regie kan nemen om de risico's te beperken voor wat betreft de veiligheid, privacy en zekerheid van overheidsdiensten voor burgers;

constaterende dat bestaande toezichtorganen niet in staat zijn gebleken te zijn gesteld om bij acute ICT-problemen het roer over te nemen en direct actie te ondernemen om dit te bewerkstelligen;

van mening dat een "crashteam" of een vergelijkbare dienst derhalve noodzakelijk is om eerdergenoemde regie te nemen bij ICT-problemen die zich bij overheden voordoen;

verzoekt de regering, zo spoedig mogelijk met een voorstel te komen voor een dergelijk "crashteam" of een gelijksoortige dienst en hoe dit geëquipeerd en vormgegeven zal worden, alsmede waar dit ondergebracht dient te worden,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Gesthuizen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 195 (26643).

□

De heer **Heijnen** (PvdA):
Voorzitter. Ik heb gevraagd naar het Nationaal Uitvoeringsprogramma en daar heeft minister Donner adequaat op geantwoord. Ik heb gevraagd naar de doorzettingsmacht en daar is gedeeltelijk adequaat op geantwoord, maar de discussie over de doorzettingsmacht van de bedrijfsvoering zullen we op een ander moment voeren. Ik begrijp dat het afdwingen van opvolging van de advie-

zen wordt opgeschaald tot het niveau dat controleerbaar is door de Kamer. Het derde punt, de evaluatie van deze crisis, is door het kabinet ruimhartig opgepakt door te verwijzen naar de Onderzoeksraad voor Veiligheid alsook naar de Inspectie Openbare Orde en Veiligheid. Wij zien beide rapporten met belangstelling tegemoet. Ik heb eigenlijk de neiging om naar de collega's te kijken om bijvoorbeeld aanvullend parlementair onderzoek, als dat nodig is, daarna te doen plaatsvinden

Ik ben blij dat de minister duidelijk heeft gemaakt dat er sprake is geweest van audits op PKI-Overheid volgens het programma van eisen. Tegelijkertijd maakt dat geweldig duidelijk dat wij een ernstig probleem hebben, want deze audits hebben niet kunnen voorkomen dat de belangrijke taak van het uitgeven van certificaten is terechtgekomen bij een bedrijf dat er een potje van heeft gemaakt. Die audits waren dus een wassen neus; ze stelden niets voor. Het waren papieren audits, gericht op de processen en niet op de resultaten. Dat dwingt ertoe dat de regering uitstraalt, zegt en erkent dat er een fiks probleem is. Immers, aan wie de problemen niet onder ogen ziet, kan de oplossing niet worden toevertrouwd.

☐

Mevrouw **Hachchi** (D66):
Voorzitter. Dank aan de beide bewindspersonen voor hun beantwoording in eerste termijn. De minister begon met te zeggen dat DigiNotar de ogen geopend heeft voor veiligheid en internet. Het minste wat we kunnen verwachten is dat veiligheid hoog op de agenda komt bij de overheid en bij het bedrijfsleven. In mijn eerste termijn heb ik een onderzoek door de Algemene Rekenkamer genoemd. Ook ik heb goed geluisterd en ik wacht het onderzoek van de onafhankelijke raad af.

Op vragen over de hack van DigiNotar en de gevolgen voor met name de Iraanse mensenlevens kon de minister niet veel antwoorden geven. Er is een AIVD-onderzoek gaande. Ik vraag de minister of het kabinet bereid is om de resultaten van dit onderzoek met de Kamer te delen.

Op mijn vragen over de hackers heb ik van beide bewindspersonen een positieve reactie gehad. Ik krijg echter geluiden uit de praktijk dat een en ander niet zo rooskleurig is als de bewindspersonen stellen. Daarom dien ik de volgende motie in. Mocht deze overbodig zijn, dan ben ik bereid deze in te trekken.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat hackers gebreken in de beveiliging van computersystemen van de overheid kunnen ontdekken, zoals het geval was bij de stemcomputers en de ov-chipkaart;

overwegende dat het in het algemeen belang is dat hackers hier melding van maken bij de overheid;

overwegende dat hackers illegaal systemen binnendringen wat strafrechtelijke consequenties kan hebben;

overwegende dat de ICT-kennis van hackers ver vooruitloopt op die van de overheid;

verzoekt de regering, te onderzoeken hoe de overheid de beveiliging van haar computersystemen kan verbeteren door gebruik te maken van de kennis van hackers zonder dat hackers hier strafrechtelijke consequenties van ondervinden,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Hachchi en El Fassed. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 196 (26643).

☐

Mevrouw **Hachchi** (D66):
Voorzitter, ook het opdrachtgeverschap van de overheid ...

De **voorzitter**:
U bent al over uw tijd heen.

Mevrouw **Hachchi** (D66):
In dat geval beperk ik mij tot het indienen van de volgende motie over het opdrachtgeverschap.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de overheid op het gebied van ICT sterk afhankelijk is van externe partijen;

overwegende dat goed opdrachtgeverschap essentieel is voor de kwaliteit van de digitale dienstverlening van de overheid;

overwegende dat ICT-kennis in onvoldoende mate aanwezig is bij de overheid en dat zij daarom achterloopt bij het bedrijfsleven;

overwegende dat dit ten koste gaat van de kwaliteit van ICT-aanbestedingen en het bijbehorende contractmanagement;

verzoekt de regering, de ICT-kennis binnen de overheid te verbeteren zodat zij meer gelijkwaardige contractpartners zijn en de Kamer hierover voor de voorjaarsnota te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Hachchi en Elissen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 197 (26643).

Hachchi

☐

Mevrouw **Hachchi** (D66):
Ik heb nog twee moties.

De **voorzitter**:
Leest u die dan heel snel voor. U had nog een interruptie te goed, dus u leest de moties voor en ziet u af van uw interruptie. Dat lijkt mij een prima oplossing.

Mevrouw **Hachchi** (D66):
Dank u wel, voorzitter.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat er sprake is van een intensieve opslag van privacygevoelige gegevens door de overheid;

overwegende dat het opslaan van privacygevoelige gegevens inherent is aan risico's voor de privacy en daarmee de veiligheid van mensen;

verzoekt de regering, de overheden en bedrijven op te roepen niet meer privacygevoelige gegevens digitaal op te slaan dan strikt noodzakelijk is,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Hachchi en El Fassed. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 198 (26643).

Mevrouw **Hachchi** (D66):
De minister is te kort ingegaan op de internationale inzet van het kabinet. Daarom dien ik de volgende motie in.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat op internationaal niveau gebruik wordt gemaakt van certificaten om de veiligheid van de digitale communicatie te waarborgen;

constaterende dat certificaten niet kunnen voorkomen dat onbevoegden de digitale communicatie afluisteren, waardoor zij zich toegang kunnen verschaffen tot privacygevoelige gegevens;

overwegende dat dit verstrekkende gevolgen kan hebben voor de privacy en daarmee ook voor de veiligheid van mensen in binnen- en buitenland;

overwegende dat een alternatief voor het certificatensysteem niet op korte termijn voorhanden is;

verzoekt de regering, op internationaal niveau de urgentie van herziening van het certificaatsysteem aan te kaarten, en een onafhankelijk wetenschappelijk onderzoek te doen naar alternatieven voor een certificaatsysteem,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Hachchi en El Fassed. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 199 (26643).

☐

De heer **El Fassed** (GroenLinks):
Voorzitter. Ik dank beide bewindslieden voor de beantwoording. Net als velen hier, zijn wij toch niet helemaal gerust. Vandaar dat sommigen een stok achter de deur willen hebben, omdat wij weten en ook tijdens de hoorzitting bleek dat wij niet zomaar kunnen overgaan tot de orde van de dag.
Ik dank de minister voor de toezegging inzake de Wetenschappelijke Raad voor het Regeringsbeleid. Ik dien twee moties in.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de minister van Volksgezondheid, Welzijn en Sport in 2004 een speciaal gezant heeft benoemd om te onderzoeken hoe logistieke processen in de gezondheidszorg beter georganiseerd kunnen worden;

constaterende dat banken een hoger beveiligingsniveau hanteren op ICT-gebied dan veel overheidsinstanties;

constaterende dat de Wetenschappelijke Raad voor het Regeringsbeleid concludeert dat in de dagelijkse digitale praktijk een iOverheid is ontstaan die volop draait op nieuwe informatiestromen die door ICT mogelijk zijn gemaakt en dat die nieuwe iOverheid flink uit de pas loopt met de bestaande structuur en de verantwoordelijkheden van de overheid;

van mening dat het proces van voortgaande digitalisering meer onderzoek vereist waardoor de overheid onvoldoende het belang van privacy en veiligheid kan waarborgen;

verzoekt de regering, op korte termijn een speciaal gezant, bijvoorbeeld uit de financiële sector, te benoemen, om de overheid door te lichten op basis van de vraag in hoeverre een cultuuromslag nodig is op het gebied van ICT, veiligheid en privacy en aanbevelingen te doen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid El Fassed. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 200 (26643).

El Fassed

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat het Genootschap van Informatiebeveiligers al in 2006 kritiek heeft geuit op het lage beveiligingsniveau van DigiD;

constaterende dat banken een hoger beveiligingsniveau hebben gekozen en veel overheidsinstanties een lager niveau acceptabel vinden;

van mening dat het beveiligingsniveau voor de uitwisseling van persoonsgegevens hoger moet;

verzoekt de regering, op korte termijn te onderzoeken of het mogelijk is het beveiligingsniveau van transacties of mutaties via DigiD te verhogen naar eenzelfde niveau als banken hanteren bij internetbankieren, bijvoorbeeld door het gebruik van een e-identifier,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden El Fassed en Hachchi. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 201 (26643).

☐

Mevrouw **Hennis-Plasschaert** (VVD):
Voorzitter. Eigen verantwoordelijkheid maar geen vrijblijvendheid. Als de verantwoordelijkheid niet wordt gedragen, moet worden ingegrepen. Regie dus. Mooie woorden van de minister, waaraan ik hem graag zal houden.
Wat betreft de meldberichten bij inbreuk op het systeem raakte ik de minister even kwijt in zijn beantwoording. Wel stel ik vast dat een Kamerbrede meerderheid zeer veel waarde hecht aan de zogenoemde security breach notification. Om die reden dien ik mede namens alle collega's hier aanwezig de volgende motie in.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat er op dit moment geen sprake is van een wettelijke verplichting tot het melden van een security breach;

overwegende dat het niet melden van een security breach verstrekkende gevolgen kan hebben;

verzoekt de regering, over te gaan tot een wettelijke meldplicht, de zogenaamde security breach notification, waarbij het melden van een security breach verplicht wordt gesteld, zo spoedig mogelijk na ontdekking van de inbraak, voor organisaties betrokken bij voor de samenleving vitale informatiesystemen;

verzoekt de regering tevens, daarbij zo min mogelijk drempels in te bouwen voor een melding en de te bieden hulp voorop te stellen;

verzoekt de regering voorts, ervoor te zorgen dat de melding bij het Nationaal Cyber Security Centrum (NCSC) wordt gemaakt en het NCSC vervolgens ook aan te wijzen als verantwoordelijke voor de coördinatie van de opvolging van de melding,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Hennis-Plasschaert, Van der Steur, Koopmans, Elissen, El Fassed, Hachchi, Heijnen en Gesthuizen.
Zij krijgt nr. 202 (26643).

☐

De heer **Koopmans** (CDA):
Voorzitter. Voor nu ben ik tevreden over de aanpak en over het feit dat de OnderzoeksRaad Voor Veiligheid wordt ingezet om een onderzoek te doen.
In de antwoorden van beide ministers hoor ik "een lerende Rijksoverheid" die hiervoor openstaat en de zaken op een goede manier wil aanpakken. Ik zie echter ook dat er nog bergen werk zijn te verzetten. Beide ministers hebben nogal wat toezeggingen gedaan die in de komende periode door hun diensten moeten worden uitgevoerd. Betrek ik daar nog bij dat ook de Kamer door een aantal uitspraken de regering een stapel beleid meegeeft, dan is het wel de vraag of wij qua prioriteitstelling de juiste volgorde kiezen. Vanuit dat oogpunt gezien, verzoek ik de ministers om daar kritisch in te blijven. Kernpunt moet zijn dat deze regering en deze bewindslieden de veiligheid van het internet voor de rijksoverheid en voor de inwoners van Nederland zo veel mogelijk borgen. Dat moet eerst gebeuren en daarna komen alle andere belangwekkende zaken aan de orde.

☐

De heer **Elissen** (PVV):
Voorzitter. Ik dank de bewindlieden voor de antwoorden en de toezeggingen. De belangrijkste vraag op dit moment is natuurlijk hoe we voorkomen dat we na "lektober" een "noodvember" krijgen en een "lDecember". Om die reden dien ik de volgende motie in.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat er bij ICT-projecten van de overheid te weinig aandacht is voor de bescherming van privacy en er te weinig aandacht is voor het voorkomen van misbruik van deze systemen;

overwegende dat privacy van burgers niet verder aangetast dient te worden dan strikt noodzakelijk is en dat onveilige systemen privacy in gevaar brengen;

overwegende dat systemen die gemakkelijk gekraakt kunnen worden het aanzien van de overheid ernstig aantasten;

overwegende dat achteraf systemen aanpassen om privacy te waarborgen en veiligheid te verhogen in de regel duurder is en vaak tot een lager beschermingsniveau leidt dan wanneer privacy en veiligheid aan het begin van een project randvoorwaarden zijn;

verzoekt de regering, bij de ontwikkeling van alle nieuw te starten ICT-projecten privacy by design en safety by design toe te passen zodat nieuwe ICT-systemen veiliger zijn en beter berekend op misbruik en slechts privacygevoelige gegevens bevatten als dat strikt noodzakelijk is,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Elissen en Gesthuizen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 203 (26643).

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat databeveiliging belangrijk is voor het beschermen van privacy maar ook voor het beschermen van bedrijfs- en staatsgeheimen;

overwegende dat datalekken het aanzien van de Nederlandse overheid in binnen- en buitenland ernstig schaden;

overwegende dat veel huidige methoden, zoals audits waarbij slechts naar procedures en managementsystemen wordt gekeken, geen garanties bieden voor de daadwerkelijke veiligheid van een systeem;

overwegende dat de overheid zelf kennis over ICT en beveiliging in huis dient te hebben om een goede opdrachtgever te kunnen zijn en om haar onafhankelijke positie veilig te stellen;

verzoekt de regering om jaarlijks te onderzoeken, onder andere met behulp van penetratietesten, hoe goed verschillende overheidsonderdelen gegevens van burgers beveiligen en de resultaten van het onderzoek naar de Tweede Kamer te sturen, zodat deze een adequaat beeld van gegevensbescherming in Nederland krijgt,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Elissen, Koopmans, Hennis-Plasschaert, Heijnen, Hachchi, El Fassed en Gesthuizen.
Zij krijgt nr. 204 (26643).

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de Nederlandse overheid geen direct toezicht houdt (thans deels tweedelijnstoezicht) op alle kritische ICT-systemen en op de organisaties die werken met deze kritische ICT-systemen;

overwegende dat gebleken is dat het huidige toezicht tekortschiet;

verzoekt de regering om eerstelijnstoezicht in te stellen voor alle kritische ICT-systemen en de betrokken bedrijven en organisaties;

verzoekt de regering tevens om jaarlijks een overzicht van deze systemen en organisaties naar de Kamer te sturen, zodat helder is welke bedrijven, organisaties en systemen onder dit strengere toezicht vallen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Elissen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 205 (26643).

☐

De heer **Elissen** (PVV):
Het heeft misschien wel iets weg van speeddaten, maar zo houden we het tempo erin.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat onzorgvuldig omgaan met gegevens, het verkeerd gebruiken van gegevens en het onderschatten van de noodzaak om goede beveiligingsmaatregelen te treffen, kunnen leiden tot aantasting van de privacy;

overwegende dat privacybescherming altijd een rol dient te spelen wanneer de overheid gebruik maakt van gegevens van burgers;

overwegende dat er aan de kant van de overheid over de gehele linie een bewustwording dient plaats te vinden dat privacybescherming belangrijk is;

overwegende dat een ketenbenadering kan helpen bij het beschermen van de privacy;

verzoekt de regering om een beleid te ontwikkelen dat toeziet op de integrale bescherming van privacy, te beginnen met een notitie integrale privacybescherming waarin, analoog aan hoe dat binnen de crisisbescherming gebruikelijk is, gebruikgemaakt wordt van een keten van proactie, preventie, preparatie, repressie en nazorg, zodat ge-

gevens van Nederlanders nu en in de toekomst beter beschermd blijven,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Elissen en Hachchi. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.
Zij krijgt nr. 206 (26643).

De vergadering wordt van 0.15 uur tot 0.25 uur geschorst.

□

Minister **Donner**:
Voorzitter. Ik neem mij voor om vooral in te gaan op de moties en een paar gerichte vragen, zoals die van de heer Heijnen.
In de motie-Gesthuizen/El Fassed op stuk nr. 194 richten de indieners zich strikt genomen tot het Presidium, maar ik wil deze motie toch ten stelligste ontraden. Anders gaan immers op hetzelfde moment allerlei onderzoeken langs en naast elkaar lopen. Het gaat ook om onderzoeken van geheel verschillende soort. Een onderzoek van de Kamer zal altijd meer gericht zijn op het horen en het lezen, terwijl de bedoeling van ons verzoek aan de Raad voor Veiligheidsonderzoek juist is om breed te kijken naar de bestaande systemen. Daarnaast zal de wijze waarop zaken nu zijn aangepakt voorwerp zijn van de inspectie. Derhalve zou ik deze motie willen ontraden, hoewel zij niet aan de regering is gericht.
Op de motie-Gesthuizen op stuk nr. 195 zal mijn collega ingaan.
De heer Heijnen kwam terug op de problematiek van en het onderzoek naar de verklaring. Dat je op een gegeven moment dit soort certificaten krijgt, dat je de verklaringen krijgt en dat desondanks bij DigiNotar blijkt dat de zaak niet op orde is, betekent dat er op dat punt iets mis is. Dat ben ik met de heer Heijnen eens. Daarom vindt er onderzoek plaats naar wat er gebeurd is. Maar ik wil bestrijden dat het hele systeem zoals het functioneert, niet goed is want dan zouden wij de signalen moeten hebben dat het bij de andere certificatiesystemen ook niet op orde is. Dat laat onverlet dat uit het onderzoek kan blijken dat er op bepaalde punten onvoldoende gecontroleerd is, maar evenzeer kan blijken dat een en ander heel gericht het gevolg is van de wijze waarop DigiNotar is omgegaan met de controles.

De **voorzitter**:
De heer Heijnen begint nu aan zijn derde interruptie.

De heer **Heijnen** (PvdA):
Dat is minder dan wat de minister schreef in zijn antwoorden op vragen: "In het licht hiervan voert het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoek uit naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop."

Minister **Donner**:
Dat neem ik ook niet weg. Ik zeg juist dat er een probleem is. Ik sta hier niet iets anders te beweren. Ik geef alleen tegelijkertijd aan dat bij andere certificatie-instituten niet dezelfde problemen zijn geconstateerd. Juist in het kader van de aanpak van de DigiNotar-problematiek is van alle andere certificatieorganisaties in Nederland, onmiddellijk voordat men daarop aangewezen was, individueel gecontroleerd of hun beveiliging op orde was.

De heer **Heijnen** (PvdA):
Ik kan moeilijk bestrijden dat zich incidenten hebben voorgedaan bij de andere instituten of bedrijven, maar ik mis de erkenning dat het systeem van toezicht in de casus-DigiNotar volstrekt heeft gefaald en dat er sprake bleek te zijn van een papieren auditing op het proces. Daarvan zal de minister blijk moeten geven voordat hij tegen zijn medewerkers kan zeggen: dat was eens maar nooit weer.

Minister **Donner**:
Dat is precies wat ik de heer Heijnen gezegd heb. Aan de ene kant krijg je de certificaten en de rapporten. Aan de andere kant blijkt een en ander vervolgens onvoldoende. Daarom laten wij het systeem onderzoeken. Dat is niet alleen op dit incident gericht maar breder. Ik wil het beeld wegnemen dat ieder van die instituten niet deugde, omdat dit gebeurde.
In de motie-Hachchi/Elissen op stuk nr. 197 verzoekt mevrouw Hachchi de regering de ICT-kennis binnen de overheid te verbeteren zodat zij meer gelijkwaardige contractspartners zijn en de Kamer hierover voor de voorjaarsnota te informeren. De strekking van de motie is ondersteuning van het beleid.
Ik zou alleen willen verzoeken om het tijdstip te wijzigen waarop de Kamer geïnformeerd moet worden, want ik kan dan toezeggen dat ik dit punt mee zal nemen in de jaarrapportage over de bedrijfsvoering van het Rijk, die in mei bij de Kamer ligt in het kader van de algehele – ik weet niet precies hoe het heet – kwijting.
In de motie-Hachchi/El Fassed op stuk nr. 198 wordt de regering verzocht om de overheden en bedrijven op te roepen, niet meer privacygevoelige gegevens digitaal op te slaan dan strikt noodzakelijk is. Naar mijn mening is dat toepassing van de wet. Daarin wordt geëist dat persoonsgegevens alleen worden opgeslagen als dat proportioneel nodig is. Anders is het strijdig met de wet. Derhalve is deze motie zonder meer ondersteuning van beleid, maar overbodig.
In de motie-Hachchi/El Fassed op stuk nr. 199 wordt de regering verzocht, op internationaal niveau de urgentie van herziening van het certificaatsysteem aan te kaarten. Deze motie is ondersteuning van beleid. Dat is al gedaan. Ik wijs erop dat dit geen garantie is voor aanpassing van het internet. Daarnaast wordt de regering in de motie verzocht, een onafhankelijk wetenschappelijk onderzoek in te stellen naar alternatieven voor certificaatsystemen. Dat punt zou ik na willen gaan. Immers, om nog een onderzoek op dit punt te starten, ook als blijkt dat er internationaal weinig gevoeligheid bestaat voor verandering, is minder zinvol. Ik meen dat er op dit moment al een onderzoek loopt in Nederland bij TNO, maar ik zal na moeten gaan in hoeverre er al onderzoek op dit punt loopt. Als mevrouw Hachchi het laatste deel schrapt, dan zeg ik toe dat ik de Kamer daar zo snel mogelijk over zal inlichten.
Mevrouw Hachchi vroeg of ik de Kamer wil informeren over het AIVD-onderzoek. Dat zal ik doen. Waar dat niet in het openbaar kan gebeuren, zal ik de commissie voor de Inlichtingen- en Veiligheidsdiensten daarover rapporteren voor zover dat nog niet is gedaan.
Mevrouw Hachchi ging in tweede termijn opnieuw in op de inzet van hackers. We hebben een- en andermaal aangegeven dat ethische hackers worden ingezet. De mo-

tie op dit punt van mevrouw Hachchi wordt door mijn collega van Veiligheid en Justitie behandeld, juist omdat in die motie wordt gevraagd om strafrechtelijke immuniteit.

Mevrouw **Hachchi** (D66):
Voorzitter. Mijn motie op stuk nr. 196 trek ik in.

De **voorzitter**:
Aangezien de is ingetrokken, maakt zij geen onderwerp van beraadslaging meer uit.

Minister **Donner**:
Voorzitter. Ik kom op de motie-El Fassed op stuk nr. 200, waarin hij de regering verzoekt, een speciale gezant te benoemen om de overheid door te lichten. Deze motie moet ik ontraden. Dit zou weer een andere vorm zijn waarop de overheid wordt doorgelicht naast het onderzoek dat zal worden gedaan door de raad voor de veiligheid. Naar mijn mening moet eerst een nadere analyse plaatsvinden van de vraag of de cultuur het probleem is of dat dit elders zit. Als de cultuur het probleem is, meen ik dat een gezant niet de oplossing is. We moeten niet omdat we de discussie over DigiNotar hebben, heel Nederland met allerlei commissies, onderzoeken et cetera belasten. Ik meen dat wij de richting aangeven met één centraal onderzoek.

In de motie-El Fassed/Hachchi op stuk nr. 201 wordt de regering verzocht, op korte termijn te onderzoeken of het mogelijk is om het beveiligingsniveau van transacties of mutaties via DigiD te verhogen. Op dit moment wordt gewerkt aan een nieuwe versie van DigiD. Ik zal de Kamer inlichten over de wijze waarop het veiligheidsniveau wordt aangepast. Ik stel voor dat de heer El Fassed de motie aanhoudt totdat ik de Kamer daarover heb ingelicht. Dan kan er altijd nog gekeken worden of verdere maatregelen moeten worden genomen.

Ik kom op de motie-Elissen/Gesthuizen op stuk nr. 203 over de ontwikkeling van privacy by design en safety by design voor nieuwe ICT-systemen. Deze motie is overbodig, omdat dit al kabinetsbeleid is. Voor safety by design zijn de beveiligingskaders van het Rijk verplicht uitgangspunt voor ieder informatiesysteem. Deze kaders zijn gebaseerd op de code voor informatiebeveiliging. Dat is een internationale standaard die ook in de markt veelal de basis vormt voor de eigen informatiebeveiliging van de organisatie. Voor de safety zal via het instrument van DigiD gebruik worden gemaakt van jaarlijkse beveiligingsassessments. Dit element is betrokken bij het beleid.

De motie-Elissen c.s. op stuk nr. 204 ging over onderzoeken met behulp van penetratietesten. Ik verwijs wederom naar de brief die ik gisteren aan de Kamer heb gestuurd. Daarin is voor de DigiD-dienstverlening aangekondigd op welke wijze er gereageerd zal worden. Uitbreiding van dergelijke jaarlijkse onderzoeken sluit ik niet uit. Als ik de motie, zoals deze nu luidt, letterlijk interpreteer, wordt het een enorm project. Als ik haar zo lees dat de heer Elissen er vooral op doelt om steekproefsgewijs onderzoek te doen, ook met de penetratietesten, ligt het in de lijn van de brief van gisteren dat dit soort onderzoeken ook bij de gemeenten worden gedaan. Dan zie ik de motie als ondersteuning van beleid.

De heer **Elissen** (PVV):
Ik geef nog een korte toelichting op mijn motie. De minister ziet de motie als ondersteuning van beleid. Ik juich het toe dat de minister voor DigiD al voor deze koers heeft gekozen. De motie heeft echter een bredere strekking: zij ziet op een bredere toepassing en ook op de privacy. Ik dank de minister voor zijn toezegging dat het ondersteuning van beleid is.

Minister **Donner**:
Ik geef aan dat wij een en ander uitbreiden, maar dat kan niet nu in een klap systematisch. Daarom doen wij die penetratietest steekproefsgewijs.

In de motie-Elissen op stuk nr. 205 wordt de regering verzocht om eerstelijnstoezicht in te stellen voor alle kritische ICT-systemen. Het eerstelijnstoezicht ligt bij de verantwoordelijke organisaties; dat heb ik uitgelegd. Uitgangspunt daarbij is dat de verantwoordelijkheid voor de veiligheid en het beheer in een hand moeten zijn. In de brief die ik gisteren heb aangekondigd, heb ik aangegeven op welke wijze de rapportageplicht van organisaties aan Logius inzake DigiD-dienstverlening wordt uitgebreid. Ik sluit niet uit dat ik dit ook doe ten aanzien van andere ICT-systemen. Mijn advies aan de heer Elissen is om deze motie aan te houden; dan kunnen wij eerst nagaan welke systemen er zijn en wat daarvoor nodig zou zijn. Dat is ook in lijn met de vorige notitie.

In de motie-Elissen/Hachchi op stuk nr. 206 wordt de regering verzocht om de integrale bescherming van privacy op te nemen. Er is een actief privacybeschermingsbeleid met het College bescherming persoonsgegevens als actief toezichthouder. Er worden kwetsbaarheids- en afhankelijkheidstoetsen uitgevoerd. Ik zal de Kamer een overzicht doen toekomen van wat er op dit moment onder het integrale privacybeleid valt. De motie zie ik dus als ondersteuning van beleid.

Mevrouw **Hachchi** (D66):
Ik wil een correctie van mijn kant doorgeven. Ik wil de motie op stuk nr. 198 intrekken; de motie op stuk nr. 196 wil ik wel in stemming brengen.

De **voorzitter**:
Aangezien de is ingetrokken, maakt zij geen onderwerp van beraadslaging meer uit.

□

Minister **Donner**:
Ik slaakte al een zucht van opluchting dat de motie op stuk nr. 196 was ingetrokken.

De **voorzitter**:
Ja, men moet nooit te vroeg juichen.

De heer **El Fassed** (GroenLinks):
Ik houd mijn beide moties aan.

De **voorzitter**:
Op verzoek van de heer El Fassed stel ik voor, zijn moties op stuk nrs. 200 en 201 (26643) aan te houden.

Daartoe wordt besloten.

□

Minister **Opstelten**:
Mevrouw de voorzitter. De motie-Gesthuizen op stuk nr. 194 is uiteraard ter beoordeling van de Kamer. Ik wil wel benadrukken dat wij twee onderzoeken doen naar de

gang van zaken, door de Inspectie Openbare Orde en Veiligheid en de Onderzoeksraad voor de Veiligheid. Dat zal natuurlijk op de toekomst gericht zijn. Ik heb ook gezegd dat de dreigingsanalyse die een duidelijk beeld geeft van hetgeen in ons land op het terrein van cyber security aan de hand is, dan door alle deskundigen in Nederland wordt bekeken, inclusief het juridisch instrumentarium en de knelpunten die zich daarbij voordoen. Dat moet toch voldoende zijn. Daar leggen wij onze prioriteiten.

Dan de motie-Gesthuizen op stuk nr. 195. Ik refereer aan hetgeen ik heb gezegd over de crashteams en de manier waarop wij omgaan met de ontwikkeling van het Nationaal Cyber Security Centrum, over de positie van GOV-CERT-centrum en zijn internationale reputatie, over de hele crisisstructuur waarin men opereert en de ICT-respons. Ik heb ook aangekondigd dat zij een duidelijke positie krijgen in het Nationaal Cyber Security Centrum en dat ook het juridisch instrumentarium van doorzettingsmacht zal worden bekeken. Het zal dan ook niet verrassen dat ik deze motie wil ontraden.

Dan ga ik in op de motie-Hachchi/El Fassed op stuk nr. 196. Ik was net als collega Donner zeer opgelucht toen ik hoorde dat zij werd ingetrokken, maar dat is kennelijk een klein misverstand. Ik moet nadrukkelijk zeggen dat het aannemen van deze motie door ons wordt ontraden omdat het niet kan. Wij maken graag gebruik van hackers, maar binnen de grenzen van onze rechtsstaat en binnen de grenzen die de wet ons toelaat. Ik heb dat ook in de eerste termijn gezegd. Mevrouw Hachchi en de heer El Fassed zullen begrijpen dat wij van mening verschillen.

De motie-Hennis c.s. op stuk nr. 202 is ons uit het hart gegrepen. Daarin staat ongeveer wat ik zelf in eerste termijn heb gezegd. Het is een krachtige en brede ondersteuning van ons beleid op een heel belangrijk punt. Op de uivoering van de motie zal ik ingaan in de brief aan de Tweede Kamer over de inrichting van het Nationaal Cyber Security Centrum. Dat zal voor het eind van het jaar gebeuren.

Mevrouw de voorzitter. Dit zijn mijn antwoorden.

De **voorzitter**:
Ik dank de minister. Hiermee zijn wij gekomen aan het eind van dit debat. Over de moties zal spoedig na het herfstreces worden gestemd.

De beraadslaging wordt gesloten.

Sluiting 0.43 uur.