Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

28 684 Naar een veiliger samenleving

Nr. 323

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 8 juli 2011

De vaste commissie voor Veiligheid en Justitie[1] heeft op 1 juni 2011 overleg gevoerd met Minister Opstelten van Veiligheid en Justitie over:

- **de brief van de Minister van Veiligheid en Justitie d.d. 22 februari 2011 betreffende de Nationale Veiligheid (Kamerstuk 30 821, nr. 12);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 22 februari 2011 betreffende de Nationale 4Cyber Security Strategie (Kamerstuk 26 643, nr. 174);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 23 februari 2011 betreffende de kabinetsreactie op het rapport «Kwetsbaarheidanalyse Spionage Nederland» (Kamerstuk 30 821, nr. 13);**
- **de brief van de Minister van Justitie d.d. 26 juni 2009 betreffende de voortgang van de inventarisatie van de knelpunten in wet- en regelgeving bij de bestrijding van cybercrime (Kamerstuk 28 684, nr. 232);**
- **de brief van de Minister van Veiligheid en Justitie d.d. 16 november 2010 betreffende het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 (Kamerstuk 28 684, nr. 292);**
- **het EU-voorstel: De EU-interne veiligheidsstrategie (COM (2010), nr. 673);**
- **het EU-voorstel: Aanvallen op informatiesystemen (COM (2010), nr. 517).**

[1] Samenstelling:
Leden: Rouvoet (ChristenUnie), Van der Staaij (SGP), Arib (PvdA), Çörüz (CDA), Koopmans (CDA), De Roon (PVV), voorzitter, Brinkman (PVV), Vermeij (PvdA), ondervoorzitter, Van Raak (SP), Thieme (PvdD), Gesthuizen (SP), Dibi (GroenLinks), Van Toorenburg (CDA), Berndsen (D66), Van Nieuwenhuizen (VVD), Schouw (D66), Marcouch (PvdA), Van der Steur (VVD), Recourt (PvdA), Hennis-Plasschaert (VVD), Helder (PVV), El Fassed (GroenLinks), Taverne (VVD)
Plv. leden: Slob (ChristenUnie), Dijkgraaf (SGP), Bouwmeester (PvdA), Van Bochove (CDA), Sterk (CDA), Dille (PVV), Elissen (PVV), Smeets (PvdA), Kooiman (SP), Ouwehand (PvdD), Rik Janssen (SP), Sap (GroenLinks), Smilde (CDA), Pechtold (D66), Van der Burg (VVD), Dijkstra (D66), Kuiken (PvdA), De Liefde (VVD), Spekman (PvdA), Azmani (VVD), Bontes (PVV), Voortman (GroenLinks), Dijkhoff (VVD)

kst-28684-323
ISSN 0921 - 7371
's-Gravenhage 2011

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

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

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

Voorzitter: De Roon
Griffier: Van Doorn

Aanwezig zijn acht leden der Kamer, te weten: De Roon, Van Raak, Hennis-Plasschaert, Schouw, Recourt, Elissen, Dibi en Çörüz,

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

De **voorzitter**: Ik open dit algemeen overleg. Ik heet de aanwezigen welkom.

Mevrouw **Hennis-Plasschaert** (VVD): Voorzitter. We hebben een veelheid aan onderwerpen. Ik zoom eerst in op de Nationale Cyber Security Strategie. Het is voor iedereen duidelijk dat de toenemende afhankelijkheid van ICT ons kwetsbaar maakt. We moeten ons wapenen of in ieder geval adequaat kunnen reageren in geval van aanvallen, misbruik en grootschalige storingen. Ik ben me er zeer van bewust dat de Minister vaart wil maken met dit dossier. Die ambitie wordt van harte gesteund door de VVD, maar de VVD wil vooral vaart maken met een aanpak die gebaseerd is op feiten. Dat is een belangrijk uitgangspunt. Over cybersecurity horen we vaak grote verhalen, soms spookverhalen. Ook hypes spreken tot de verbeelding van velen. Structureel inzicht in de aard en omvang van de vraagstukken rondom cybersecurity is voor ons echt prioriteit nummer 1 als we tot een goed en vooral degelijk beleid willen komen. Wij vragen dus om feiten, waarbij ook de zogenoemde dringende maatschappelijke behoefte in kaart wordt gebracht. Focussen is belangrijk. Niemand zal ontkennen dat cybercrime van een andere orde is dan een cyberaanval, digitale spionage of een grootschalige verstoring door technisch, menselijk of natuurlijk falen. Mijn vrees is dat we het teveel op een hoop vegen en onvoldoende helder gedefinieerd hebben waar we ons precies tegen wapenen. Ik ontvang graag een reactie van de Minister. In dat kader hebben verschillende partijen een zogenoemde nulmeting voorgesteld. Ik sta hier positief tegenover en vraag de Minister wat zijn standpunt is in dezen.
In die notitie inzake de Nationale Cyber Security Strategie wordt verder gesteld dat toetsingsmechanismen, waaronder de bestaande toezichtfuncties, benut en waar nodig versterkt moeten worden. Wij delen dat uitgangspunt, maar de vraag is hoe de Minister dit precies wil invullen. Als hij denkt aan het bouwen van toezichtmechanismen binnen het Nationaal Cyber Security Centrum (NCSC) ben ik geheel zijn vrouw. Ik pleit voor een sterke interne toezichthouder die op basis van steekproeven controleert of alles volgens de regels verloopt. Ik pleit ook voor de totstandkoming van een jaarlijkse onafhankelijke audit. Zo hebben de Amerikanen het ook georganiseerd: «the designation of a privacy and civil liberties official to the NSC cybersecurity directorate». Dat voorbeeld wil ik graag volgen.
Aan proefballonnen die haaks staan op onze grondrechten zit de VVD niet te wachten. Ik vraag de Minister zich hier verre van te houden. Dat is kort door de bocht, maar het moet voor iedereen duidelijk zijn dat van communicatievrijheid absoluut geen sprake kan zijn als het ontvangen van informatie via internet afhankelijk wordt gemaakt van het behalen van een internetrijbewijs. Ik ontvang hiervan graag een bevestiging van de Minister.
Conform het regeerakkoord dienen maatregelen uiteraard nadrukkelijk getoetst te worden aan effectiviteit. Ook dienen de maatregelen proportioneel te zijn. Verder vindt de VVD het van belang te nadrukken dat de overheid de vrijheid bewaakt en de mensen beschermt tegen willekeur. Ofwel, bij een eventuele beperking van grondrechten moet er altijd sprake zijn van een wettelijke basis. Ik geef de Minister mee dat wij de uitgangs-

punten van de motie-Franken, zoals vorige week aangenomen in de Eerste Kamer, ondersteunen. De Eerste Kamerfractie stemde niet tegen omdat zij tegen de uitgangspunten was, maar om andere moverende redenen. De uitgangspunten van deze motie worden wel degelijk voluit gesteund door de VVD.
Dan iets over agendapunt 4. Het gaat hier om een oude brief van 26 juni 2009 over de knelpunten bij de bestrijding van cybercrime. Hierin wordt gesproken over de inrichting van een kennis- en expertisecentrum. Wat is hiervan de stand van zaken? Wat is er gebeurd met de motie-Teeven/Heerts over de noodzaak om in bepaalde gevallen gegevens heel snel veilig te kunnen stellen? Is de Minister voornemens met voorstellen te komen om criminele activiteiten door of via internet strafbaar te stellen? Er wordt ook gesproken over een jaarlijkse rapportage. Wanneer kunnen wij die verwachten?
Ik heb een paar vragen over agendapunt 7. Ik dank de staf Europese Zaken voor zijn heldere e-mail. Naar aanleiding van het voorstel voor een richtlijn over de aanval op informatiesystemen vraag ik of er in Nederland al voldoende wettelijke instrumenten zijn om daders van een aanval op een informatiesysteem te vervolgen en te berechten. Of zijn wij geheel afhankelijk van wat er in Europa gebeurt en zullen wij dit dan pas invullen? Past artikel 12 van deze richtlijn in onze bestaande civielrechtelijke regelgeving? Voor zover mijn kennis strekt, is toezicht van de rechter op rechtspersonen een onbekend fenomeen in Nederland.
Ten slotte wijs ik op de roep om meer bestuurlijk commitment van de veiligheidsregio's voor bijvoorbeeld het convenant drinkwater. Het lijkt erop dat het tekenen van het convenant een doel op zich is geworden, maar dat is het niet. Het gaat om de implementatie de uitvoering en het invullen van die afspraken. Dit schijnt nogal wat moeilijkheden op te leveren. Ik vraag de Minister om hier aandacht aan te schenken in het Veiligheidsberaad.

De heer **Schouw** (D66): Voorzitter. D66 is enthousiast over de twee ambities van deze Minister: ten eerste Nederland als digitale gateway to Europe en ten tweede Nederland in de wereldtop voor het benutten van ICT. Waar een klein land al niet groot in kan zijn. Het is goed dat wordt nagedacht over een cybersecurity strategie die ons moet beschermen. Niettemin heb ik een paar stevige bedenkingen bij de plannen die nu voorliggen. Als de zwakke plekken niet opgevuld worden, zal de security strategy straks een gatenkaas blijken te zijn.
Wat is precies de feitelijke onderbouwing van het probleem? Dat is de eerste vraag die je je moet stellen voordat je aan een beleidsnotitie begint. Hoe kwetsbaar zijn we en hoe vaak worden gegevens gestolen en van wie? Hoe vaak voeren landen een cyberoorlog met elkaar? Omdat cijfers ontbreken, is de strategie die gekozen wordt te algemeen. We lezen dat gegevens over de omvang van het probleem ontbreken. Een gevolg van het tekort aan detaillering is dat het de deur wagenwijd openzet voor ongebreidelde overheidscontrole op bijvoorbeeld het internet. Dat moeten we toch niet willen. Ik vraag de Minister de toezegging dat hij de Kamer een schriftelijke en met feiten onderbouwde precisering zendt, het liefst voor het eind van het jaar.
Mijn fractie mist het concrete juridisch kader waarbinnen maatregelen kunnen worden genomen; een juridisch kader met een rotsvaste verankering van onze grondrechten. Binnen welk juridisch kader zal er in de toekomst gehandeld worden en hoe wordt bijvoorbeeld artikel 8 van het Europees Mensenrechtenverdrag uitgewerkt, waarbij zowel de noodzaak als de proportionaliteit een rol spelen? Hoe kun je dat beoordelen als de onderbouwing van het probleem niet zichtbaar is? Wat is de legitimiteit van de overheid om op te treden in het ICT-domein en hoever mag zij gaan? Welke nationale en internationale wetten en verdragen moeten worden aangepast om deze strategie handen en voeten te geven?

Graag een overzicht hiervan en een toezegging van de Minister om daarover voor het eind van het jaar te rapporteren.
Er wordt expertise en samenwerking opgezet op verschillende fronten. Op het Ministerie van Defensie wordt zelfs 50 mln. extra vrijgemaakt voor een heus cyberleger. Niet om mensen te beschermen maar juist om hen aan te vallen. Ik vraag de Minister hoe al die initiatieven zich tot elkaar verhouden, ook tot de crisis- en rampenbestrijding die er al is. Wij willen geen versnipperde aanpak. Kan de Minister garanderen dat er geen versnipperde aanpak is door het Rijk? Hoe wordt in de samenwerking tussen de publieke en private sector gewaakt voor vermenging van belangen? Hoe kan het parlement democratische controle uitoefenen op de zelfregulering en op allerlei publiek-private samenwerkingsconstructies (pps) die het kabinet voorstaat? Kan de Minister toezeggen dat de toezichtmechanismen en -vormen nader worden uitgewerkt, liefst voor het eind van het jaar?
De D66-fractie vindt het internationale kader van de gepresenteerde strategie buitengewoon mager. De dreiging die in de Nationale Cyber Security Strategie wordt beschreven is grensoverschrijdend. Samenwerking met andere landen en EU-regulering is dus noodzakelijk, maar hoe verhoudt die zich tot de Nederlandse veiligheidsstrategie in relatie tot die Europese context? We hebben daar vaker over gesproken in de JBZ-Raad, maar ik heb het idee dat het stopcontact en de stekker niet op elkaar passen. Kan de Minister daar iets over zeggen? Hoe past de recent gestarte Benelux-samenwerking daarin?
D66 vindt dat bij de bewustwording van ICT-gebruikers winst te behalen valt. Voorlichting en eerlijke informatie bieden gebruikers de ruimte om zich op eigen kracht te weren tegen misbruik en verstoringen. Wat vindt de Minister van een privacybijsluiter bij producten die privacygevoelige gegevens bevatten om gebruikers te wijzen op de risico's van gegevensuitwisseling?
Het is goed dat er een veiligheidsstrategie wordt bedacht, maar wat D66 betreft heeft de Minister nog wel wat huiswerk te doen:
1. onderbouw het probleem met feiten;
2. geef een juridisch kader voor handelen;
3. neem privacybescherming expliciet mee in de strategie;
4. bundel de expertise en samenwerking;
5. ga in op de Europese context;
6. maak ICT-gebruikers bewust van de risico's.

De heer **Van Raak** (SP): Voorzitter. Ik heb slecht nieuws voor de Minister want ik ben het eens met de VVD en D66. De kritiek is Kamerbreed. Ook ik zie de feiten en de onderbouwing niet. Waar moeten we ons tegen wapenen? Hoe groot is het probleem? Ik mis ook een visie op de verhouding tussen veiligheid en privacy, op de verhouding tussen bescherming en toegankelijkheid en op de verantwoordelijkheid van overheid en burgers. Wel lees ik in de Nationale Cyber Security Strategie dat de regering vindt dat er meer nadruk moet komen liggen op zelfredzaamheid en eigen verantwoordelijkheid van de burger. Ik moest toen aan de Minister van BZK denken – toch een professor in de veiligheid – die zijn mobiele telefoon niet beveiligd had en daardoor afgeluisterd werd. Als die het al niet weet, hoe moeten gewone burgers het dan weten? Als burgers hun verantwoordelijkheid willen nemen en bij een ramp naar www.crisis.nl gaan, ligt de site plat. Die site doet het altijd, behalve als er een crisis is. Daarom vraag ik ook om een visie op de verantwoordelijkheid van de overheid en die van de burger. Als het gaat om individuele veiligheid mag je vrij veel vragen van burgers, maar voor de nationale veiligheid hebben we toch in eerste instantie de overheid? Daar betalen we belasting voor. De overheid moet niet te makkelijk dingen op burgers afschuiven.

Met veel interesse las ik de Nationale Cyber Security Strategie. De Minister wil het zoals altijd flink aanpakken, maar bij de allerlaatste zin op de laatste bladzijde ging ik twijfelen: «Bovenstaande activiteiten zullen binnen de bestaande begrotingen worden opgevangen». Er komt geen geld bij. Dat kan betekenen dat het geld tot nu toe niet goed is besteed, maar ook dat er geen geld voor is. Wat is er aan de hand?
Ik heb ook met veel interesse de reactie van het kabinet gelezen op de Kwetsbaarheidsanalyse Spionage in Nederland (KWAS). Dat is een onderwerp waar ik al vaker aandacht voor heb gevraagd. Een aantal jaren geleden heeft een voorganger van deze Minister een agent van de Central Intelligence Agency (CIA) uitgezet en dat geheim gehouden, maar door journalistiek onderzoek is dat toch openbaar geworden. Er is ontzettend veel spionage in Nederland, vooral economische maar ook politieke spionage uit Israël en de Verenigde Staten (VS). In Zweden zijn onlangs CIA-agenten opgepakt die spioneerden via de ambassade. Ze hebben Zweedse burger gevolgd en in de gaten gehouden zonder dat de Zweedse overheid dat wist. Dat is bekend geworden, onderzocht en veroordeeld. Ook de Noorse overheid is boos omdat CIA-agenten in Noorwegen spioneren. Dat is waarschijnlijk ook het geval in IJsland, Denemarken, Duitsland, Finland et cetera. Hoe groot is de kans dat de VS in Nederland via de ambassade mensen in de gaten houden, mensen volgen en informatie over Nederlandse burgers verzamelen zonder dat de Nederlandse overheid dat weet? Is daar contraspionage op gevoerd? Heeft de Minister enig idee van de cijfers en het soort informatie waar het om gaat? Waarom is de Minister zo stil terwijl in Zweden en Noorwegen de overheid er wel aandacht voor heeft?
Tot slot moeten we oppassen geen dingen dubbel te doen. Defensie gaat 90 mln. investeren in de bestrijding van digitale aanvallen en de Minister gaat een NCSC oprichten. De Minister zegt dat die twee dingen complementair zijn. Waarom moeten het er twee zijn? Kan het niet in één instituut? Waarom moeten Veiligheid en Justitie aan de ene kant en Defensie aan de andere kant soortgelijk werk gaan doen? We hebben ook al veel gedoe gehad over de politie tussen Binnenlandse Zaken en Justitie. Kunnen we lessen trekken voor de toekomst over de verhouding tussen Veiligheid en Justitie en Defensie?

De heer **Çörüz** (CDA): Voorzitter. De digitale snelweg biedt ongekende mogelijkheden, maar we moeten niet naïef zijn, want er zijn ook gevaren op die weg. Op grond van de nationale risicobeoordeling 2010 heeft het kabinet op dit onderdeel accenten aangebracht en dat is heel goed. Dankzij de motie-Knops is er nu sprake van een Nationale Cyber Security Strategie en komt er een NCSC. Ik vind dat de overheid in zo'n centrum moet samenwerken. Je ziet accenten bij Defensie en accenten bij Justitie. Ik zou het goed vinden als Defensie nadrukkelijk wordt betrokken bij discussies over cybersecurity, niet als concurrent maar als samenwerkingspartner. Dat geldt ook voor het bedrijfsleven. De overheid moet er samen met het bedrijfsleven in optreden. Ik zie voor het bedrijfsleven ook nog een aparte rol. We hebben het over gevaren en bescherming en over de ontwikkeling van veiligheidsconcepten. Het Nederlands bedrijfsleven moet er een uitdaging in zien om die digitale snelweg te beveiligen.
Een mogelijke oplossing voor bij de bestrijding van cybercrime is de aanpak van digitale wegmisbruikers met een zogenaamd digitaal kenteken. Net als op de gewone weg rijden we allemaal met een kenteken en hebben we 's avonds de lichten aan. De CDA-fractie is ervoor om goedwillende hackers onze eigen beveiligingssystemen te laten testen. De bewustwording en verantwoordelijkheid van de gebruikers zijn heel belangrijk. We kijken naar de overheid, het bedrijfsleven en de politiek voor het maken van wetten, maar het komt met name aan op de bewustwording van de mogelijkheden enerzijds en de gevaren anderzijds. Daar

moeten we zo jong mogelijk mee beginnen. We moeten acteren conform de rechts- en grondwetregels die wij met elkaar hebben afgesproken.
Een van de meest complicerende factoren bij de bewijsvoering van de cybercrime is de encrypties, de versleutelingen. Dat hebben we gezien in een interessant werkbezoek van deze commissie aan het Korps landelijke politiediensten (KLPD). In sommige landen zijn de criminelen zo ver dat bepaald bewijs gewoon wegloopt, omdat ambtenaren niet snel achter die versleutelingen kunnen komen. We moeten in Nederland denken aan de mogelijkheid van het zelfstandig strafbaar stellen, dan wel dit als stafverzwarende omstandigheid aan te voeren.

De heer **Recourt** (PvdA): Voorzitter. Ik heb daar de vraag over hoe zich dat verhoudt tot de onschuldpresumptie. Encryptie is op verschillende niveaus mogelijk. Je kunt daarin tot in het oneindige coderingen onderbrengen. Op welke manier zou een strafbaarstelling helpen bij het oplossen van dit probleem?

De heer **Çörüz** (CDA): Ik zie het praktisch en vergelijk het met een blaastest om vast te stellen of iemand gedronken heeft. Dat wordt een beetje lastig met dingen die in iemands hoofd zitten, maar het kan toch niet zo zijn dat door die versleutelingen het voor opsporingsambtenaren zo ingewikkeld wordt dat bewijs wegloopt? Dat willen we voor zijn. We moeten aangeven dat iemand zwaarder wordt gestraft als hij niet meewerkt. Anderzijds kan het weigeren om deel te nemen aan een onderzoek als een zelfstandig strafbaar feit in de delictsomschrijving worden opgenomen.

De heer **Recourt** (PvdA): Maar hoe weet je dat iemand weigert? Hij kan de eerste code wel geven, maar daar kan een tweede, derde, vierde of vijfde code achter zitten. Is het een effectief middel?

De heer **Çörüz** (CDA): Als je het benodigde bewijs niet boven water kunt krijgen en iemand werkt daar willens en wetens niet aan mee, kan de consequentie zijn zoals hierboven geschetst.

De heer **Çörüz** (CDA): Een ander lastig component in de bestrijding van cybercrime is rechtsmacht. Heel vaak wordt die criminaliteit internationaal opgezet. We weten niet altijd wat waar zit. Oostenrijk heeft het zo gedaan dat in de telecomwetgeving een bepaling is opgenomen dat de computer die spam of andere rotzooi ontvangt, plaats delict is. Dan vermijd je heel ingewikkelde discussies over rechtsmacht en kun je van daaruit beginnen met rechercheren. Graag een reactie van de Minister daarop.
In het kader van de rechtsmacht wil ik het hebben over het kenniscentrum cybercrime voor onze rechterlijke macht. Onze rechters en potentiële rechters worden daar via een website en via scholing en vorming op geattendeerd. Het centrum doet heel goed werk. Er zijn wat vragen over de continuering van de financiering van dit centrum. Ik ontvang graag duidelijkheid daarover van de Minister.
Tot slot sluit ik mij aan bij de oproep van mevrouw Hennis-Plasschaert over die convenanten. Van de zijde van gas-, water- en elektriciteitsbedrijven en politieregio's bereiken mij geluiden dat die convenanten nog niet zijn ondertekend. Pratend over nationale veiligheid moeten we natuurlijk ook de regels en convenanten die we hebben afgesproken, ondertekenen.

De heer **Recourt** (PvdA): Voorzitter. Voor mijn inbreng kies ik de focus van cybercrime van algemeen naar specifiek. In het algemeen heb ik mij de vraag gesteld wat we zouden doen als we onze samenleving opnieuw konden ordenen op het terrein van Veiligheid en Justitie. Zouden we het wezenlijk anders doen dan nu? Voor die vraag worden we gesteld in de

virtuele wereld. Zonder dat velen van ons het weten, is een groot deel van ons handelen al virtueel. Dit geldt voor allerlei praktische dingen als autorijden, telefoneren, e-mailen enz. en het wordt alleen nog maar belangrijker. We zullen ons steeds meer manifesteren in een virtuele hoedanigheid, niet alleen economisch maar ook in onze sociale contacten en relaties. Dat resulteert in diefstal, belediging en bedreiging tot en met terroristische aanslagen. Wat is de rol van de overheid daarbij? Er moet een balans gevonden worden tussen een big brother-achtige aanpak en volledige anarchie. Ik denk dat we moeten aansluiten bij concepten die in de oude wereld bruikbaar zijn. Immers, in die oude wereld wordt al decennialang nagedacht over de principiële benadering van briefgeheim, huisvredebreuk en computervredebreuk. Er is een mooie balans ontstaan tussen de macht van de overheid om in te grijpen en de privacy en rechtsbescherming van de burger. Waar we niet genoeg bij kunnen stilstaan, is dat strafrecht een ultimum remedium is. We moeten als overheid niet beloven virtuele veiligheid te bieden waar we dat niet kunnen waarmaken, net als dat we de veiligheid in de gewone samenleving niet kunnen garanderen.
Kortom, wat kan de burger zelf? Dat is de kern. Daar moet je als overheid primair in faciliteren door bewustwording, kennisoverdracht en praktische hulp te bieden.
Een andere vraag is of de huidige wetgeving volstaat. Wat kunnen we nu al aanpakken met de wetgeving en wat kunnen we in de toekomst aan technologie verwachten? Die vragen zijn onvoldoende uitgewerkt. Ik wijs nogmaals op het briefgeheim en op huis- en computervredebreuk. We hebben in de Kamer recent gesproken over de vraag wat aanbieders mogen doen met onze e-mails: mogen ze die lezen, volgen of afleveren? Ik verzoek de Minister de Kamer op dit punt in de toekomst concreet te informeren.
Hoe moet de overheid dat aanpakken? Niet door een topdownbenadering, maar door in netwerken te denken. Wat zo eigen is aan die virtuele samenleving, is het mondiale en het snelle. Daar moet je geen ouderwetse organisatie tegenover stellen, maar een organisatie die snel en flexibel werkt. In die zin vind ik de samenwerking met private partners prima. Enkele leden van de commissie zijn bij het Nederlands Forensisch Instituut (NFI) geweest dat samenwerkt met private partners. Ik was onder de indruk van de kennis die daar is opgedaan. Ik benadruk daarbij dat die private partners goed kennis, snelheid en efficiency kunnen inbrengen, maar dat zij er niet zijn voor het stellen van normen. Dat is aan de overheid.
Een andere goede ontwikkeling is het kenniscentrum cybercrime voor de rechterlijke macht. Dat is gefinancierd tot en met 2012. Het doel is de kennis van de digitale wereld bij alle rechters te vergroten. Hoe kun je dat structureel doen als je horizon een jaar is? Het lijkt me moeilijk om daar plannen op te ontwikkelen. De financiering lijkt te stoppen. Ik verzoek de Minister om samen met de Raad voor de Rechtspraak te zorgen voor een langere structurele financiering.
Tekort aan kennis lijkt de kern te zijn van dit dossier, zoals tekort aan kennis op de werkvloer bij de politie. Hoe moet bewijs worden veiliggesteld? Op dit moment moet de burger dat maar al te vaak zelf doen. Dat doen we toch ook niet bij een gewone inbraak? Is er voldoende kennis op de werkvloer en voldoende inzicht in het probleem? Hoe zit het met slachtofferschap, aantal daders, het profiel van daders? Hoe ontwikkelingen zich normen voor sociale media of illegaal downloaden? Dat is een taak voor de wetenschap en ik vraag me af of daar voldoende op wordt ingezet en of we überhaupt inzicht krijgen in de problematiek.
Aan het einde van de keten staat justitie. De Nederlandse justitie is door het grenzeloze karakter minimaal met één hand op de rug gebonden. Dat neemt niet weg dat een en ander mogelijk is, maar ook hier maak ik mij zorgen, niet alleen over het instrumenteel denken maar ook over de

balans tussen macht en tegenmacht. Ik las dat er plannen zijn van een officier van justitie om sites op zwart te laten zetten. Dat lijkt me een disbalans ten opzichte van hoe het zou moeten. Moet je daar niet de rechter toestemming voor laten geven, of, als het spoed heeft, de rechter-commissaris, zoals dat nu ook al werkt en in balans is?
Ik vraag de Minister ervoor te zorgen dat er geen competentiestrijd ontstaat, maar wordt samengewerkt tussen Justitie en Defensie.
De samenwerking binnen Europa is prima. Wat zorgen baart is dat als eerste de registratie van vliegtuigpassagiers op poten moet worden gezet. Is dat wel efficiënt en proportioneel? Ik denk dat Europa wel andere prioriteiten heeft.
Als afsluiting doe ik het voorstel om de burger, de consument, als uitgangspunt te nemen. Het is voor een burger onmogelijk om uit te zoeken in welk land een cybercrime is gepleegd. Zorg dat je vooruitlopend op harmonisatie van wetgeving één digitaal loket maakt, waar de burger aangifte kan doen die vervolgens door de samenwerkende Europese landen wordt doorgeleid naar het land waar de opsporing en vervolging moet plaatsvinden.

De heer **Elissen** (PVV): Voorzitter. Allereerst wil ik de Minister complimenten maken voor het ambitieniveau. Ik heb wel een vraag over de nationale risicobeoordeling waarnaar in de brief wordt verwezen. «De zorg voor een vrije en veilige samenleving is de belangrijkste taak van de overheid», zo begint die brief. Dat klinkt goed. Eerst inventariseer je de risico's en vervolgens tref je maatregelen. Ik vind het wel verontrustend dat bovenaan de lijst met thema's klimaatverandering staat. In dit kader noem ik ook het «Paper from the High Representative and the European Commission to the European Council». Dit wordt opgevoerd als bron en daarmee is direct duidelijk dat er van enige wetenschappelijke onderbouwing geen sprake kan zijn. Het stuk staat vol aannames en ontbeert iedere vorm van onderbouwing. Het heeft eigenlijk sanitaire waarde. Ziet de Minister klimaatverandering nog steeds als een van de topprioriteiten in het kader van onze nationale veiligheid? Zo nee, wil hij hieraan in komende rapportages, brieven en overige stukken zo min mogelijk aandacht besteden?
Verder maak ik uit het diagram op pagina 16 op dat links-extremisme onwaarschijnlijker is dan rechts-extremisme. Daarnaast zijn de effecten en risico's in het geval van links-extremisme beperkt, terwijl ze bij rechts-extremisme aanzienlijk zijn. Ik ontvang graag van de Minister een toelichting. Uiteraard ga ik ervan uit dat er geen sprake is van politieke kleuring door de opstellers.
Ik heb ook nog vragen over de brief van de Minister over de Nationale Cyber Security Strategie. Dit heeft als ondertitel «Slagkracht door samenwerking». Is het niet zo dat samenwerking een breed netwerk en toegang tot veel specialistische kennis kan bieden, maar dat slagkracht pas ontstaat als er een duidelijke commandostructuur wordt ingericht en een goede regie wordt gevoerd? Mijn vraag is wie het uiteindelijk op nationaal niveau voor het zeggen krijgt over de uitvoering van de Nationale Cyber Security Strategie en hoe de commandostructuur eruitziet tijdens bedreigingen van de nationale veiligheid, zowel in de operationele fase als daarna. In dit verband sluit ik me aan bij de vragen die zijn gesteld over de afstemming en samenwerking tussen Defensie en Veiligheid en Justitie.
Op pagina 5 staat dat de zorg voor de digitale veiligheid in Nederland is belegd bij veel verschillende partijen. Ik vraag de Minister om daarvan een overzicht aan de Kamer te doen toekomen.
Op pagina 6 staat dat de leveranciers een voldoende veilig ICT-product en -dienst aanbieden. Wat houdt dit precies in? Wil de Minister komen tot certificering van software en geldt dat ook voor diensten van de overheid

of voor software die aan consumenten wordt verkocht? Houdt dat ook een verbod op opensourcesoftware in? Kan de Minister hierop een toelichting geven?
Op pagina 7 wordt bij de vierde bullit ingegaan op de mogelijkheid om een elektronische Ardica te ontwikkelen. Dat lijkt mij een prima plan. Kan worden uitgesloten dat die wordt ontwikkeld door een organisatie die bewezen wanprestatie heeft geleverd? Hoe worden met malafide praktijken geassocieerde organisaties buiten de deur gehouden wanneer er op last van Europa verplicht moet worden aanbesteed? Is de Minister bereid om te bezien of we onder die verplichte aanbesteding kunnen uitkomen? Ik heb me laten vertellen dat met name Frankrijk daar bedreven in is en dat er een mogelijkheid is om met een beroep op het nationaal belang onder die Europese aanbesteding uit te komen. Dat zouden de Nederlandse ondernemers ongetwijfeld prettig vinden.
Op pagina 7 wordt verder ingegaan op de meldplicht met betrekking tot datalekken. Vindt de Minister dat er ook een registratieplicht in het leven moet worden geroepen? Welke gegevens gaan de Internet Service Providers (ISP's) vastleggen? Hoe gaat dit uitpakken in het kader van de internationale concurrentiepositie en de rechtsgelijkheid voor de grote en kleinere aanbieders, ook in het kader van de privacy? Die moet natuurlijk gewaarborgd blijven.
Op pagina 7 wordt bij de vijfde bullit ingegaan op spelregels op het internet. Wat wordt hier precies mee bedoeld? Hoe wordt voorkomen dat in Nederland Chinese toestanden ontstaan, waarbij de bevolking gecensureerd wordt terwijl criminelen vrijwel ongestoord hun gang kunnen gaan? Kan de Minister dit toelichten?
Op pagina 9 wordt onder het kopje «Financiële gevolgen» aangegeven dat de genoemde activiteiten zullen worden opgevangen in bestaande begrotingen. Komt er voor de Nationale Cyber Security Strategie een aparte financiële begroting of een overzicht waaruit blijkt hoe groot het totale budget is? Ofwel, hoe maken wij het zichtbaar en hoe kan de Tweede Kamer controleren op de efficiency en het verloop van het project?
Het volgende punt ligt wat ingewikkeld, heb ik begrepen. In het rapport «Kwetsbaarheidsanalyse Spionage Nederland» wordt geconstateerd dat economische, strategische en technisch-wetenschappelijke spionage een actuele dreiging vormen voor de nationale veiligheid. Kunnen we daaruit voorzichtig de conclusie trekken dat Nederland een risico loopt doordat niet of onvoldoende versleutelde e-mails, documenten en webconferenties kunnen worden onderschept en uitgelezen? Deelt de Minister die conclusie? Hoe verhoudt die zich tot de uitspraken van plaatsvervangend hoofdofficier van justitie mevrouw Hoogendijk op 19 april jl. dat het versleutelen van computerbestanden strafbaar moet worden gesteld? Ik ontvang graag een reactie van de Minister, vooral in het licht van de privacy van talloze burgers die hier in het geding is. Ik heb begrepen dat de heer **Çörüz** niet voor strafbaarstelling van die versleuteling is, maar het vooral zoekt in een instrument om de medewerking te stimuleren dan wel af te dwingen. Ik zou graag wat meer informatie hebben alvorens tot een definitief standpunt te komen.
De tweede doelstelling van Europa is het voorkomen van terrorisme en het aanpakken van radicalisering en werving. Die acties lijken nogal globaal en vooral gericht op voorlichting, het bemoeilijken van financiële transacties en het verhogen van vervoersveiligheid. Kan de Minister aangeven of in aanvulling hierop acties gepland staan om terroristen op te sporen en uit te schakelen, dan wel een intensivering op dit gebied?

De heer **Dibi** (GroenLinks): Voorzitter. Daar waar schurken en schorriemorrie zich vroeger uitsluitend offline manifesteerden, hebben ze dankzij een vrij en open internet een wereld aan kansen voor hun criminele doeleinden. Daar maken ze gretig gebruik van. Er is een aantal

voorbeelden genoemd, van een ronsel- en ontmoetingsplek voor bloeddorstige terroristen tot bedrijfsspionage van de opkomende wereldmachten China en Rusland. De mogelijkheden zijn even groot als grotesk. Het vraagt van Nederland, Europa en de wereld een visie hoe om te gaan met het beschermen van nationale veiligheid en de veiligheid van burgers. Het vraagt ook van overheden om niet klakkeloos op basis van angst burgerrechtelijke verworvenheden op te offeren, maar op basis van gecalculeerde risico's effectieve maatregelen te nemen die de bescherming van grondrechten waarborgen en die transparant zijn. Ik zeg dit omdat de GroenLinks-fractie parallellen ziet met de aanpak van terrorisme. Onlangs hebben we hier een debat over gehad en op basis van het onderzoek van de Radboud Universiteit Nijmegen kwamen we tot de conclusie dat heel veel van die maatregelen, hoe begrijpelijk ook, niet altijd even samenhangend en transparant zijn.
De kernvragen zijn: wat levert het op, wat is het probleem precies en waarom is het nodig.
GroenLinks beschouwt de aanpak die voorligt als belangrijk maar nog niet helemaal voldragen. Ik hoop dat de Minister openstaat voor de vragen van de Kamer. Wat is precies de onderbouwing van de aard en omvang van aan cybersecurity gerelateerde vraagstukken? Ik vraag om een duidelijke probleemanalyse. Is de Minister bereid om, nadat hij een duidelijke probleemanalyse heeft geschetst, de Kamer regelmatig te informeren over de voortgang daarvan? De digitale burgerrechtenbeweging Bits voor Freedom noemt dat een gevalideerde nulmeting, zodat we aan het eind van de rit weten of het geld dat we hierin steken, effectief en efficiënt besteed wordt. Daarnaast willen wij een duidelijke toets of de uitgangspunten van de ontworpen strategie voldoen aan het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Het kabinet zegt dat het uitgangspunt is dat de maatregelen proportioneel zijn. Het EVRM vraagt iets meer dan alleen maar proportionaliteit, namelijk ook dat de maatregelen bij wet worden voorzien en dat ze noodzakelijk zijn in een democratische samenleving. Dus dat er dringende maatschappelijke behoefte moet zijn, dat de maatregelen subsidiair moeten zijn en effectief. Is de Minister bereid om zowel die dringende maatschappelijke behoefte als de wettelijke basis toe te voegen aan deze aanpak?
De impact van de voorgenomen maatregelen op de privacy moet precies in kaart worden gebracht. De motie-Franken zou wat de GroenLinks-fractie betreft daarbij leidend moeten zijn. Is de Minister bereid om die motie centraal te stellen bij de aandacht voor privacy?
Als het om grondrechten gaat, past terughoudendheid bij het inschakelen van derden. Ik snap dat er pps moet zijn en ik ben blij dat het bedrijfsleven wil samenwerken met de overheid om te komen tot een goede aanpak, maar daar kunnen ook economische belangen prevaleren. Als een bedrijf een product maakt dat heel handig is bij de aanpak van cybercrime, levert dat veel geld op, maar dit druist tegelijkertijd in tegen allerlei grondrechten. De Kamer moet volledige inzage hebben in alle initiatieven die voortkomen uit die samenwerking. Zonder parlementaire controle kunnen wij niet weten welke initiatieven vanuit die samenwerking de burgerrechten beschadigen. Graag een toezegging van de Minister op volledige inzage in alles wat uit die samenwerking voortvloeit.
De GroenLinks-fractie realiseert zich heel goed dat wat wij hier bespreken, samenhangt met wat er in Europa besloten wordt. Heel veel zeggenschap ligt in Europa. Het is de wens van de GroenLinks-fractie dat de Minister het breed gedragen geluid in de Kamer leidend laat zijn in de onderhandelingen met zijn collega-ministers in Europa. Ik heb een specifieke vraag over de onderhandelingen die nu volop aan de gang zijn over de richtlijn voor aanvallen op informatiesystemen. Het zou wel eens de meest ingrijpende richtlijn kunnen zijn. Er is gezegd dat de Nederlandse regering positief staat tegenover het verloop van de onderhandelingen. We gaan

hier binnenkort over praten in de JBZ-Raad, maar ik ben benieuwd wat de inhoud van die positief beoordeelde onderhandelingen precies is en welk effect ze hebben op de Nederlandse wetgeving. Zal de uitkomst van de onderhandelingen invloed hebben op onze Nederlandse wetten, zodat wij ze moeten aanpassen?
Tot slot iets over de politiesterkte. De Minister zegt dat de capaciteit vergroot wordt en dat er meer aandacht van de politie komt voor cybersecurity. Ten koste waarvan gaat dat? Of gaat de Minister een blik nieuwe agenten opentrekken? Ik vraag hem heel duidelijk aan te geven hoeveel agenten erbij komen en waar ze vervolgens geen aandacht meer aan kunnen besteden.

De heer **Çörüz** (CDA): De heer Dibi heeft een punt als hij zegt dat de samenwerking tussen de overheid en het bedrijfsleven transparant moet zijn. Hij wil alles weten wat het bedrijfsleven doet, maar we willen bureaucratie toch voorkomen? Welke rapportages moeten de overheid of het bedrijfsleven leveren?

De heer **Dibi** (GroenLinks): Als het om de bescherming van grondrechten gaat, is bureaucratie voor mij ondergeschikt. Natuurlijk wil ik niet elk detail weten van wat er besproken wordt tussen bedrijven en overheid. Maar een van de conclusies bij het onderzoek naar de aanpak van terrorisme was dat het niet transparant genoeg was en dat we niet duidelijk konden maken aan de burgers waarom we wat deden. Ik zet het nu extra zwaar aan om aan te geven dat GroenLinks wil dat aan het begin van dit traject zo transparant mogelijk gecommuniceerd wordt met de Kamer. Als er belangrijke dingen afgesproken worden, moet de Kamer daarin inzage krijgen om het te controleren.

Mevrouw **Hennis-Plasschaert** (VVD): Bedoelde de heer Dibi in zijn antwoord dat de effectiviteit van maatregelen die grondrechten beperken, leidend moet zijn en dat er altijd sprake moet zijn van een wettelijke basis?

De heer **Dibi** (GroenLinks): Dat is precies wat ik bedoel. Soms schuurt iets tegen de grondrechten aan maar is het zo belangrijk voor onze veiligheid dat je het zou kunnen rechtvaardigen. Het Nederlandse legitimiteitsbeginsel moet altijd een wettelijke basis zijn voor ingrijpende voorstellen. Wij zijn het helemaal eens.

Minister **Opstelten**: Voorzitter. Dank aan alle afgevaardigden voor hun interventies. Deze strategienota is door de Kamer aangevraagd. De heer Dibi noemde het belangrijk om het hier over te hebben. Maar we zijn ook nog zoekende. Ik ben de eerste om dat te bevestigen. Ik heb ambities en zal niet nalaten om die naar voren te brengen. Ik zal niet overdrijven maar daarin de balans zoeken.
Er zijn diverse moties door de Kamerleden genoemd:
– de motie-Knops waarin wordt gevraagd om de security strategie;
– de motie-Hernandez waarin wordt gevraagd om een nationale cybersecurity strategie;
– de motie-Franken over privacyaspecten, niet alleen in verband met cybersecurity;
– de motie-Teeven/Heerts waarin wordt gevraagd om een nieuwe verkenning naar de toereikendheid van juridische instrumenten aan de hand van een inventarisatie van knelpunten in de wet- en regelgeving.

Die moties vormen een basis voor uitspraken van de Kamer – zelfs van de Eerste Kamer – en voor de strategie van het kabinet. Ik heb in de strategienota aangegeven wanneer ik met de volgende stappen zal komen. Iedereen heeft daarnaar gevraagd en dat is belangrijk.
Er zijn steeds meer incidenten. Ik heb een lijst voor me liggen. Voorbeelden daarvan zijn de accenten die gisteren in het blad Metro

werden aangebracht, huis-, tuin- en keukencriminaliteit en onrust, het afluisteren van voicemails, een gerichte aanval op de Franse overheid en de Europese Commissie ter onderschepping van gevoelige informatie en nog veel meer. Dat is de definitie van het begrip waarover wij spreken. Ik heb trouwens wel een definitie in de nota opgenomen. Die luidt kort samengevat: de kwetsbaarheid neemt toe en daarmee ook een vorm van afhankelijkheid. Dat moeten we onderkennen in een digitale, open samenleving die steeds opener wordt. De heer Recourt heeft daar heel relevante vragen over gesteld, zoals hoe we de samenleving zouden inrichten als we opnieuw konden beginnen. In ieder geval zou er dan een nationale politie zijn en een nationale risicobeoordeling. Je kunt het ook anders noemen, maar het gaat om een risicobeoordeling plus een trendrapportage.
Hoe gaat die ontwikkeling verder? Degene die het nu al precies weet, neem ik niet serieus. Inzicht is lastig, daarom zullen we een periodiek dreigingsbeeld opstellen. Sommigen hebben gevraagd om dat voor het eind van dit jaar te krijgen, maar de Kamer krijgt al op 30 juni aanstaande. het eerste dreigingsbeeld toegestuurd. Dat is de start van de cyberboard, dus overheid en bedrijfsleven samen. Ik zal de Kamer over de voortgang rapporteren. Je moet eerst weten wat precies het probleem is. Er moet een eerste dreigingsbeeld zijn waar we over kunnen spreken. Het is nog gewoon werk in uitvoering. De eerste voortgangsrapportage komt begin volgend jaar, dat zeg ik de Kamer toe.
We kunnen verschillende visies hebben maar functioneren in dezelfde rechtsstaat. We zijn het erover eens dat alles proportioneel en subsidiair moet zijn en dat er op basis van wetten wordt geopereerd. De overheid heeft in de pps een eigenstandige verantwoordelijkheid en positie. Ik ga me niet verschuilen achter een board, maar ik zal gebruikmaken van de expertise van en de samenwerking tussen publiek en privaat; onze goede mensen samen met goede mensen uit het bedrijfsleven. Ik ben uiteindelijk verantwoordelijk voor de overallpositie en als Minister ook voor het wettelijk kader en het toezicht. Dat zeg ik graag toe. Het vaststellen van een juridisch kader, zowel nationaal als internationaal, en proportionaliteit zijn noodzaak. Ik zal dat aangeven op basis van zo'n dreigingsanalyse en bekijken wat er nodig is als je iets wilt of moet veranderen. Ik zie aankomen dat dat gebeurt en ik wil dat samen met de Kamer doen op volstrekt controleerbare wijze.

Mevrouw **Hennis-Plasschaert** (VVD): Ik wil terug naar de definitie dat onze kwetsbaarheid toeneemt en daarmee ook onze onafhankelijkheid. Ik zei daarbij ook dat focussen van belang is omdat ik van mening ben dat cybercrime van een totaal andere orde is dan een cyberaanval of een grootschalige storing door technisch, menselijk of natuurlijk falen of digitale spionage. Dat wil ik graag terug horen in het betoog van de Minister over het dreigingsbeeld. Of we het nulmeting of dreigingsbeeld noemen, interesseert me niet, als maar duidelijk wordt op basis van welke feiten er beleid wordt ontwikkeld.

Minister **Opstelten**: Dat is precies wat ik aangeef. Ik ben iemand van facts and figures. Ik wil feiten hebben, anders kan ik niks. Je moet bij het creëren van draagvlak wel rekening houden met beelden, maar als je voortgang wilt maken, moeten er feiten zijn. Dan moet er iets aan de hand zijn wat we willen veranderen. Doe je dat door wetgeving, overtuigingskracht, open netwerkorganisaties, nationaal of internationaal? Die instrumenten gaan we onderzoeken.

Mevrouw **Hennis-Plasschaert** (VVD): Ik ben blij met deze toezegging. De Minister opereert slim als hij zegt dat je voor draagvlak wel beelden nodig hebt, maar we moeten ons niet laten leiden door spookverhalen en hypes, dus niet dat soort beelden alstublieft. Dat draagvlak is er wel want we zijn

ons allemaal bewust van de risico's, maar we zien ook dat de samenleving steeds meer in opstand komt door alle proefballonnen die de laatste tijd worden opgelaten.

Minister **Opstelten**: Dat ben ik met mevrouw Hennis-Plasschaert eens, maar de proefballonnen komen niet van mij. Wat ik doe is wapenfeiten noemen, maatregelen nemen of een discussie op gang brengen en een strategie met elkaar zoeken. Dat doe ik met de samenleving, het bedrijfsleven en de burgers. Dat is een uitdaging voor de Kamer en mijzelf. Communicatie is daar heel belangrijk in en zelfredzaamheid. We moeten daarin een weg vinden, ook met de collega's in en buiten Europa, want dit is iets dat bij uitstek niet door grenzen wordt bepaald. Wat dat betreft is die nationale politie misschien een stap op weg naar meer. Niet alles wordt op een hoop geveegd, dat wil ik hier benadrukken. We moeten ook geen spookverhalen vertellen, want wat er niet is, is er niet. Strafrecht is inderdaad het ultimum remedium. Er is een goede samenwerking in het kabinet tussen de verschillende Ministers die op hun eigen terrein een vanzelfsprekende verantwoordelijkheid dragen. De Minister van EL&I is verantwoordelijk voor de telecom, de digitale samenleving, de economie en het bedrijfsleven. De Minister van Defensie is verantwoordelijk voor het defensieaspect. Het is goed daar je daarin investeert als je weet dat er een dreiging is. Het kabinet heeft besloten dat ik de coördinerend bewindsman ben, dus ik moet zorgen voor de samenhang. Daar mag de Kamer mij op aanspreken. Een integrale aanpak is nodig. We hebben wel een beperkt aantal mensen en middelen. We zijn dit aan het opbouwen. Ik zal op hoofdlijnen een overzicht geven van het kader van wetten en verdragen. Over de uitgangspunten verschillen we totaal niet van mening. Het EVRM is natuurlijk een gegeven waarbinnen we ons gedragen met betrekking tot dit onderwerp. Wij zoeken de grenzen niet op. Als we iets tegenkomen in verdragen of richtlijnen op Europees niveau zullen we dat rustig met elkaar bespreken. Dan komt het via de gebruikelijke weg hier langs.

De heer **Schouw** (D66): Zegt de Minister concreet toe dat hij voor het einde van het jaar met een overzicht komt van wetten en regels die we eventueel zouden moeten veranderen, opdat het in de strategie past?

Minister **Opstelten**: Voor 1 januari aanstaande krijgt de Kamer de inventarisatie van de juridische knelpunten. Ik voorzie wel knelpunten en de Kamer krijgt dit beeld van het kabinet.

De heer **Schouw** (D66): Knelpunten definiëren het probleem, maar ik heb ook behoefte aan het juridisch vertrekpunt van het kabinet, de juridische muur die vastigheid geeft.

Minister **Opstelten**: Dat vind ik een prima bijstelling. Eerst bekijken we wat er aan de hand is, wat de feiten en het dreigingsbeeld zijn. Daarna bekijken we wat het juridisch kader is, het vertrekpunt op basis waarvan wij willen werken en wat we daarbij kunnen tegenkomen.

De heer **Elissen** (PVV): Ik hoor de Minister zeggen dat hij coördinerend bewindspersoon is. Betekent dat, in het licht van de regie en de commandostructuur, dat hij de eerstverantwoordelijke bewindspersoon is en afhankelijk van de situatie wordt bijgestaan door andere vakministers?

Minister **Opstelten**: Nee, dat gaat te ver. Ik begrijp dat de heer Elissen van commandostructuren houdt, maar we hebben een kabinet dat met één mond spreekt en waarin niemand echt de baas is behalve misschien de premier. Ik bewaak de samenhang, maar ga niet de Minister van Defensie overrulen. Als de heer Elissen vindt dat iets niet past in de

samenhang van dit verhaal, moet hij bij mij zijn. Hij mag het eerst bij de betrokken bewindspersoon aankaarten en daarna bij mij. Ik ben verantwoordelijk voor het totale verhaal. Als de premier als eerste verantwoordelijke de crisisbeheersing aan een van zijn collega's overlaat, ben ik diegene. Dan leid ik die ministerraad of dat team. Het is geen commandoteam, maar een collegiaal bestuur.

De heer **Elissen** (PVV): Ik ken de Minister als iemand die van duidelijkheid houdt, maar in crises- of rampensituaties mag er geen enkel misverstand zijn over leiderschap en regie. Later komen de vakministers pas om de hoek kijken. Ik pleit voor ontpoldering en nog meer duidelijkheid. Het slechtste wat ons kan overkomen, is discussie in de regiekamer.

Minister **Opstelten**: Daar hoeft de heer Elissen zich geen zorgen over te maken. Zelfs in een crisis is er een collegiaal bestuur. Als ik iets doe, spreek ik namens het kabinet en dan spreekt niemand mij tegen. Binnen dat collegiaal bestuur ben ik de eerst aangesprokene en voer ik de regie. Dat hebben wij al geoefend in de ministerraad.

De heer **Recourt** (PvdA): Ik begrijp uit de opmerking over de nationale politie dat de Minister gaat voor nationale cybercops. Dat ondersteun ik. Ik ben verbaasd dat hij zegt voor de cijfers te gaan en niet voor de beelden. Juist bij cybersecurity gaat het niet om wat daadwerkelijk is gerealiseerd – via de pers is ons een en ander ter ore gekomen – maar om de vraag wat wij kunnen verwachten binnen de nieuwe technologieën. Dat geldt evengoed voor de cybercrime. Het lijkt mij prettig om van de overheid die visie te krijgen en daarop te anticiperen.

Minister **Opstelten**: Ik wil voorkomen dat we actief worden omdat de beelden goed in de markt liggen. Er moet reëel iets aan de orde zijn en dat is naar mijn mening het geval. Langs die lijnen gaan we werken. Als je een visie ontwikkelt, heb je een risico- of dreigingsanalyse nodig maar ook trendrapportages over de ontwikkelingen. Ontwikkelingen zijn meer feitelijk dan beelden. Ontwikkelingen en trends die in de samenleving zichtbaar zijn, trekken we door.

De heer **Dibi** (GroenLinks): Als ik het goed begrijp, komt er binnenkort een dreigingsbeeld en daarin wordt onderscheid gemaakt tussen verschillende vormen van cybercrime, dus niet alles op een hoop. Later komt er soort juridische routekaart. Zegt de Minister dat niet alleen proportionaliteit maar ook het EVRM en de motie-Franken daarin leidend zijn?

Minister **Opstelten**: Ik kom nog op de motie-Franken. Ik zal de volle mep in beeld brengen, alleen het EVRM is te beperkt. Het is een ongelofelijk belangrijk juridisch instrument voor een regering en het is zelfs gewenst om zich daarnaar te gedragen. Als we vinden dat daarin iets zou moeten veranderen, voeren we daar een debat over voordat we een voorstel maken.

De heer **Dibi** (GroenLinks): De reden dat ik die vraag stelde, is dat het in de stukken alleen maar over proportionaliteit gaat. Blijkbaar was het EVRM bij het tot stand komen van de stukken nog niet leidend. De GroenLinks-fractie vindt dat zowel de motie-Franken als het EVRM de afbakening van de aanpak moeten zijn. Ik hoop dat de Minister die begrenzing ook aanhoudt.

Minister **Opstelten**: Ik wil het eerst over de toezichtfuncties hebben. Wij hebben heel veel toezichtfuncties: de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), het College bescherming persoonsgegevens (CBP) en diverse commissies. Wij zullen dat stelsel veranderen, zowel

intern als extern. Wij zullen dat goed uitwerken en daarover rapporteren. Er komt geen extra bureaucratie.
Mijn collega in Oostenrijk spreek ik binnenkort. Ik zal hem vragen hoe dat precies zit met die bepaling in de telecomwetgeving en hoe die werkt; ik zal dit toetsen aan de Nederlandse bruikbaarheid.
Ik denk dat ik de vragen over de huidige wetgeving in grote lijn heb beantwoord. Zo niet, dan hoor ik dat wel.
Dan de motie-Franken. Die is belangrijk en de Kamer wil natuurlijk horen dat ik daar helemaal achtersta. De vijf elementen uit de motie-Franken zijn volgens mij in het regeerakkoord opgenomen. Het kabinet moet nog reageren op die motie. Ik ken de brief van Staatssecretaris Teeven over de privacy ook. Daar zitten al die elementen in en die hanteer ik als een kader. Het doet mij genoegen dat de VVD-fractie in de Eerste Kamer deze motie steunt.
Met de heer Dibi heb ik geen discussie meer: wij zijn het eindelijk eens over de sterkte van de politie. Daarvoor worden sterktemiddelen vrijgemaakt binnen de bestaande sterkte van de politie. Wij hebben daarover gedebatteerd en de heer Dibi is het niet met mij eens. Dat is zijn goed recht, maar ik heb consistent de lijn uitgezet en het kader neergezet waarin we de komende vier jaar werken. De sterkte neemt toe als de bureaucratie afneemt. Er komt een reallocatie van sterkte. Ik heb gisteren in de Kamer gezegd dat er meer sterkte komt naar aanleiding van het Emergo-rapport en de oproep van de locoburgemeester van Amsterdam. Er komen ook een groter Openbaar Ministerie (OM) en meer rechercheactiviteiten. Van 20% pakkans voor de grote georganiseerde criminaliteit gaan we in vier jaar naar 40%.
Iedereen heeft iets gezegd over zelfredzaamheid en communicatie. Dat zullen we steunen want dat is een centraal thema, niet alleen op dit punt maar ook elders. Ik vraag wel tijd om na te denken over de vraag hoe wij dit vorm moeten geven in concrete instrumenten. Wat de heer Schouw vraagt, om bij elk wetsontwerp, maatregel of optreden een foldertje te leveren over de gevaren voor de privacy, gaat mij te snel maar ik wijs dit niet af. Dat is een instrument, maar wij moeten niet te snel conclusies trekken.
Los van de sterkte kan ik over de financiën zeggen dat we er extra geld voor hebben. Het kabinet gaat hier 4,3 mln. voor vrijmaken, afgezien van wat diverse Ministers in hun begroting doen. Ik zal voor het instrumentarium, de board en het expertisecentrum bedrijfsleven en overheid om te beginnen 4,3 mln. vrijmaken. Dat wordt als reallocatie in de begroting zichtbaar. Als de Kamer dat niet genoeg vindt, merken we dat wel bij de behandeling van de begroting.
Over de nulmeting heb ik al gesproken. Dat is een belangrijk punt.
Dan iets over het expertisecentrum voor politie, OM en zittende magistratuur (ZM). Bij het OM en ZM is reeds een centrum ingericht. Voor de politie zal worden aangesloten bij het kenniscentrum dat onderdeel zal zijn van NCSC. Daarmee is de continuïteit geborgd, ik weet alleen nog niet precies in welke vorm.
De heer Van Raak heeft gevraagd of de VS ook spioneren in Nederland. Ik ben niet verantwoordelijk voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en wil dat zo houden. Er is besloten dat de Minister die over het OM gaat, niet over de AIVD gaat. De AIVD vervolgt niemand en spoort niemand op, maar doet intelligencewerk. Het is een inlichtingendienst.

De heer **Van Raak** (SP): Het gaat natuurlijk ook om cybercrime en nationale veiligheid. Als een individu of bedrijf aan cybercrime doet, overtreedt hij de wet en moeten we daar onderzoek naar doen. Als een land dat doet komt er nog iets politieks bij. Wat vinden wij ervan als Rusland, China, Israël of de VS dat doen? Dat de CIA via de ambassades hyperactief is in het volgen van mensen moet de Minister zich aantrekken, vooral omdat de regeringen van andere landen daar wel serieus werk van

maken. Waarom deze regering en deze Minister niet? Ik vraag in het bijzonder of de Minister al inzicht heeft of cybercrimeaanvallen van bedrijven, overheden of individuen komen. Als die aanvallen van overheden komen, is de Minister dan bereid om dat niet geheim te houden en in beslotenheid een belletje te plegen, maar dat openbaar te maken? Is hij bereid er in het openbaar een politieke discussie over te voeren, omdat het niet past dat landen stiekem aanvallen uitvoeren en spioneren, zeker als het gaat om landen waarmee we samenwerken zoals Israël en de VS.

Minister **Opstelten**: Ik wil dat heel zuiver en duidelijk houden. Natuurlijk geeft de AIVD hier prioriteit aan. Ik vind niet dat ik daar antwoord op moet geven. Ik beperk me tot mijn verantwoordelijkheid. Dat is de nationale veiligheid en daarbij baseer ik mij op de informatie die wij krijgen. De NCTB krijgt informatie van de verschillende veiligheidsdiensten en zegt dan of we er iets mee moeten doen. Dat is hun verantwoordelijkheid en daar ben ik weer politiek voor verantwoordelijk. Over die spionage heb ik een convenant gesloten met voorzitter Wientjes van VNO-NCW, omdat wij samen die zelfredzaamheid van het bedrijfsleven en van burgers belangrijk vinden. Wij moeten er attent op zijn dat dit voorkomt in de samenleving en er niet te naïef in zijn. We moeten de krachten bundelen en de informatie uitwisselen. Zo moet de heer Van Raak dat zien.
De heer Van Raak heeft ook gezegd dat wij alles afschuiven op burgers als wij zelfredzaamheid willen stimuleren. Dat is niet zo. Burgers en ondernemers zijn in de eerste plaats zelf verantwoordelijk voor hun veiligheid en de overheid vult aan. Dat is de kern. We moeten dat centraal stellen in ons plan van aanpak. Daarin zet ik uiteen hoe ik de rollen van al die partijen zie. Dat plan van aanpak komt binnenkort naar de Kamer; het is het centrale punt bij de benadering van het veiligheidsbeleid. Het OM is vaak het ultimum remedium: aan de voorkant heb je weinig als je de achterkant niet waterdicht hebt geregeld. Verantwoordelijkheid begint bij de burger zelf, zodat we niet in een samenleving komen waarin iedereen naar de overheid zit te kijken en zijn verantwoordelijkheid niet neemt. Als de Kamer dat met mij eens is, hebben we een goed kader.

De heer **Van Raak** (SP): Wil de Minister definiëren wat volgens hem de verantwoordelijkheid van het individu is en wat de verantwoordelijkheid van de overheid? Het gaat hier om de nationale veiligheid. Ik noemde het voorbeeld van de Minister van BZK, omdat het om zeer gevoelige informatie gaat die van nationaal belang is. Dan blijkt uiteindelijk de nationale veiligheid afhankelijk te zijn van het feit dat de Minister van BZK wel of niet zijn code heeft veranderd. Dat kan dus niet. Met dat voorbeeld in het achterhoofd zie ik graag in de visie terug hoe dit soort dingen voorkomen zullen worden.

Minister **Opstelten**: Die vragen over de definitiepositie zijn goed, want anders is het alleen maar management by speech. Daarom duurt het even, want dat is niet zomaar een verhaal. Het is maatschappelijk ook niet alleen aan deze tafel van belang, maar het is cruciaal dat we in de hele samenleving het debat voeren over het feit dat de verantwoordelijkheid in de eerste plaats bij de mensen zelf ligt. Dat moet je scherp definiëren en je moet scherp aangeven wie welke verantwoordelijkheid draagt.
Er zijn vragen gesteld over de versleuteling en de mogelijkheden om die encryptie verplicht vrij te geven, zoals bijvoorbeeld in die zedenzaak. Die vraag is ook gesteld tijdens het algemeen overleg over kinderporno. Ik heb toen gesteld dat ik de wetgeving die in het United Kingdom (UK) bestaat, zal laten bekijken op haalbaarheid in Nederland. Ik heb wat tijd nodig om dat in beeld te brengen, maar ik hoop daar dit jaar duidelijkheid over te kunnen verschaffen.

Het voorstel voor hacking attacks door goedwillende hackers wordt door die hackers en het bedrijfsleven opgepakt. Dat kan een wezenlijke bijdrage leveren aan de beveiliging van organisaties door het uitvoeren van penetratietesten. Daar sta ik positief tegenover, mits het binnen de juridische kaders valt.
Op de vraag over de kennis bij de politie om bewijs te leveren, kan ik antwoorden dat de politie al lang investeert in kennis op digitale dragers en het veiligstellen van bewijs daarop. Daar is men op getraind en er wordt in het kader van het programma «Aanpak Cybercrime» van de politie veel nieuws voor ontwikkeld. Dat wordt gedaan met het bedrijfsleven, die over de kennis beschikt. Hoewel ik nu al onder de indruk ben, is het nog maar smal wat we hebben. De ambitie is hoog om die kennis bij de politie verder uit te bouwen. Men weet precies wat er nog moet gebeuren, dus we zijn op de goede weg. Het kan wat mij betreft niet snel genoeg gaan.

De heer **Recourt** (PvdA): Doelt de Minister op uitbouw van de nationale politie en geconcentreerde kennis of van de hele organisatie zodat er ook in de grotevolumezaken kennis is bij de lokale bureaus?

Minister **Opstelten**: Dit gaat over de top, over specialisme in grote zaken, maar ook over de hele politie. Uiteindelijk moet elke diender hiermee om kunnen gaan. Het zal in het basispakket van de kennisontwikkeling moeten komen.
Ik geef een voorbeeld van de internationale samenwerking met de wetenschap. We hebben ten eerste in Nederland de samenwerking met het bedrijfsleven en de wetenschap. Je kunt daarnaast alles in de EU aan de orde stellen. Dat gebeurt ook en dit is bij het huidige Hongaarse voorzitterschap, dat nu afloopt, een belangrijk thema. Ook in de Raad van Europa is het een belangrijk thema, in aanwezigheid van de Amerikanen. Maar we hebben ook onze eigen schaal, de Benelux. We hebben een conferentie gehad met de collega-bewindslieden van België en Luxemburg. Wij koersen op zo'n publiek-privaat kenniscentrum en zo'n board. In België heeft men de wetenschappelijke invalshoek centraal gesteld; die is vorige week vrijdag gestart in onze aanwezigheid. Zo leren we van elkaar en daarvan zal gebruik worden gemaakt om scenario's te ontwikkelen en in de toekomst de trends vast te houden.
Is de kwestie van de passagiersgegevens eerste prioriteit voor Europa? Nee. Europa is vooral strategisch bezig en ontwikkelt een interne veiligheidsstrategie en manieren om aan risicomanagement te doen. Soms is het echter nodig op Europees niveau afspraken te maken over concrete maatregelen met betrekking tot de veiligheid, bijvoorbeeld omdat landen dit niet individueel kunnen besluiten. Dat zou de effectiviteit van de maatregel ondermijnen. In dat licht moet het Europese beleid voor passagiersgegevens gezien worden. Daaraan wordt per land bilateraal gewerkt in Australië, om ervan te leren en vervolgens goedbeslagen ten ijs te komen en van daaruit de onderhandelingen met de VS en Canada goed te kunnen voeren. Het is dus geen topprioriteit, maar wel belangrijk.
Er zijn vragen gesteld over de verantwoordelijkheid van de ISP's. Dit onderwerp zit in de portefeuille van de Minister van EL&I en ik kan die vragen niet beantwoorden. Iedereen heeft zijn eigen verantwoordelijkheid. Op basis van Europese regelgeving moet dit in de Nederlandse wetgeving worden opgenomen.
Dan de klimaatverandering. In mijn nationale risicobeoordeling maak ik gebruik van meerdere bronnen en experts. Zij geven aan dat de kans van een ernstige overstroming van de Randstad zeer onwaarschijnlijk is. Ik had verwacht dat de Kamer naar aanleiding van een artikel in de Haagse Post (HP) hier vragen over zou stellen, maar dat is niet gebeurd. Ik maak een zorgvuldige analyse van dreigingen en baseer mij daarbij niet op één rapport. Op deze manier kan ik dreigingen tegen elkaar afwegen en

prioriteiten stellen. Klimaatbeheersing is een belangrijk punt, het is de werkelijkheid die zich voordoet. Daar kan de heer Elissen ook de Minister en Staatssecretaris van Infrastructuur en Milieu op bevragen.

De heer **Elissen** (PVV): We hebben een periode gehad waarin alles wat met klimaat te maken had een hype was. De strekking van mijn vraag was of de Minister het als topprioriteit ziet. Ik heb er geen moeite mee als hij zaken doet op het gebied van de waterhuishouding, een deltaplan of verhoogde dijkbewaking, maar laten we afstand nemen van al die rare dingen met betrekking tot die klimaathype. Ik vond het vreemd dat het als eerste werd genoemd in het rijtje, want de andere thema's maakten beduidend meer indruk.

Minister **Opstelten**: Als de bodem een beetje zakt, heeft dat met klimaatbeheersing te maken. Het wordt droger en het is belangrijk dat we daarover vergaderen. Ik laat me bij het onderwerp nationale veiligheid niet leiden door onderwerpen die ik meer apprecieer dan andere. Ik heb hier met feiten te maken. Gegevens die aanleiding geven om het te checken, te volgen en belangrijk te vinden. Ik hoop dat de heer Elissen dat denken waardeert en begrijpt, want het gaat om de nationale risicobeoordeling.
Dan de intensivering binnen Europa om terrorisme tegen te gaan. Wij hebben laatst een buitengewoon goed mondeling overleg gevoerd over de evaluatie van onze terrorismeaanpak en daar heldere afspraken over gemaakt. Dat is voor mij het vertrekpunt om in de Europese arena te opereren op het terrein van terrorismebestrijding en radicaliseringsaanpak. Daar spelen de AIVD en andere inlichtingendiensten ook een rol in. De Nationaal Coördinator Terrorismebestrijding (NCTb) baseert hier zijn beoordeling op. Dit onderwerp heeft ook de aandacht van de JBZ-Raad. De conclusies die hier worden getrokken, zullen mij een leidraad geven voor het optreden in de JBZ-Raad.
Wat zijn de spelregels op internet? Dat is inderdaad een gevaarlijke passage in de strategienota, want spelregels kun je met de dag veranderen. Op het world wide web zijn er geen spelregels als hiermee juridische regels worden bedoeld. De VS heeft in haar recente strategie aangegeven allereerst een debat te willen starten over gedeelde normen voor het gebruik van internet. Dat moeten we transparant en open doen. Wij volgen dit debat.

De heer **Dibi** (GroenLinks): Ik heb een specifieke vraag gesteld over de richtlijnen voor de aanvallen op informatiesystemen. De Minister is met zijn collega overeengekomen dat degene die dat doet een maximumstraf van twee jaar kan krijgen. Maar er zijn nog een aantal andere voorstellen die samenhangen met de richtlijn die heel ingrijpend zouden kunnen zijn. Ik heb begrepen dat de Nederlandse regering daar positief tegenover staat. Ik vraag de Minister waar de regering precies positief over is en welke effecten dit heeft op de Nederlandse wetgeving.

Minister **Opstelten**: Het heeft geen zin om daarop een algemeen antwoord te geven, dus ik zal dat laten nagaan en deze vraag in tweede termijn beantwoorden. Lukt dat niet, dan zal ik daarop schriftelijk antwoorden.
Dan de vragen over de convenanten met de vitale sectoren. De laatste informatie van vanochtend is dat er acht convenanten zijn afgesloten tussen veiligheidsregio's en drinkwaterbedrijven. In één regio gaat men zeer binnenkort tot ondertekening over. De convenanten zijn niet verplicht. Een convenant is een hulpmiddel, bedoeld om de samenwerking tussen vitale sectoren en veiligheidsregio's te stimuleren. Het niet hebben van een convenant betekent echter niet dat er geen aandacht voor de vitale sectoren is bij de veiligheidsregio. Het is belangrijk om structureel samen

te werken en te oefenen. De Wet veiligheidsregio's (Wvr) stelt daarom nadrukkelijk dat veiligheidsregio's de betrokken partijen minimaal een keer per jaar uitnodigen voor gezamenlijk overleg over de risico's in de regio's. Drinkwaterbedrijven en andere vitale sectoren zijn hierbij aangemerkt als crisispartners. Ik ondersteun natuurlijk het belang van samenwerking tussen deze sectoren en ik weet dat het Veiligheidsberaad daar ook zo over denkt. In mijn overleg met het Veiligheidsberaad is dit meerdere malen aan de orde geweest, onder andere naar aanleiding van het laatste AO in december jl. Ik breng dit nogmaals bij het Veiligheidsberaad onder de aandacht, met de wens dat we binnenkort 25 veiligheidsregio's hebben die een sluitend netwerk van convenanten hebben ondertekend.
Er is over links-extremisme versus rechts-extremisme gesproken. In het risicodiagram zijn de titels van de scenario's opgenomen. Achter de titel links-extremisme en rechts-extremisme gaat een specifiek scenario schuil, geen algemene stroming of groepering. De kansen en gevolgen van een scenario worden geschetst, niet van groeperingen. Daar zit dus geen enkel politiek oordeel in. De keuzes daarin zijn absoluut niet politiek van aard.

De heer **Çörüz** (CDA): Ik wil het nog even hebben over die convenanten, die afspraken over samenwerking bij rampenbestrijding en crisisbeheersing. Gelukkig zijn het er al weer meer. Ze zijn niet verplichtend, maar ze zijn er niet voor niks. Het is enerzijds het ondertekenen en anderzijds het implementeren. Ik wil de Minister als coördinerend bewindspersoon vragen de betrokkenen aan te moedigen om te tekenen.

Minister **Opstelten**: Dat doe ik via hun orgaan, het Veiligheidsberaad. Ik ga dit beraad vragen waarom het zo lang duurt. Het is niet verplichtend, omdat ik de verantwoordelijkheid daar wil laten waar hij hoort en die niet over wil nemen. Ik kan het wel stimuleren. Ik vind dit heel belangrijk, want het geeft de kern van het werk van de veiligheidsregio aan. Die is multidisciplinair en dat betekent regie over dat soort vitale sectoren. De Inspectie Openbare Orde en Veiligheid (IOOV) toetst hoe de veiligheidsregio's dit hebben gedaan. Daar komt een openbaar rapport van en dat gaat naar de veiligheidsregio's en de Kamer.

De heer **Schouw** (D66): Voorzitter. Ik bedank de Minister en zijn staf voor de adequate beantwoording. Ik heb nog een paar punten, zoals de dreigingsanalyse. De facts and figures komen nog. Het woord dreigingsanalyse stuit mij tegen de borst, want het gaat wat mij betreft over internet- en ICT-veiligheid. Daar horen zakelijk en precies de feiten op te staan. Ik zal dat toetsen en hoop dat de Minister wil bevorderen dat we het objectief en feitelijk doen. Ik wil bekijken of we die feiten in een context kunnen plaatsen, eventueel een internationale context, zodat we een beeld krijgen.
De Minister zegt dat de motie-Franken de basis vormt en belangrijk is, maar ik wil weten of hij deze motie onverkort overneemt.
In het kader van de samenhang tussen Defensie en Justitie is wat gespeeld met begrippen als regie en coördinatie. Ik ben er niet geruster op geworden, want ik ben bang dat er een mogelijkheid ontstaat dat zich twee organisaties naast elkaar ontwikkelen met dezelfde vakinhoudelijke discipline. Ik heb geen goed gevoel over de operationele units. Gaat dat wel goed met elkaar samen? Kan de Minister die ongerustheid wegnemen?
Over de zelfredzaamheid en de consumentenkracht heeft de Minister verstandige woorden gesproken: we moeten niet voor de troepen uitlopen. Maar er moet wel iets komen. Ik heb een instrument genoemd, waarbij je de consument de mogelijkheid geeft om te stemmen met de voeten, een privacybijsluiter. De Minister omarmt het niet, maar gooit het

ook niet weg. Ik vraag hem die privacybijsluiter te laten staan tot hij in de loop van het jaar met goede alternatieven komt.
In het algemeen overleg over de JBZ-Raad is over allerlei Europese ontwikkelingen op dit terrein afgesproken dat het kabinet om de vier maanden aan de Kamer zal rapporteren over de voortgang, maar dat is eenzijdig door de Staatssecretaris van Justitie veranderd in een jaar. Ik vraag de Minister om dat te corrigeren naar de eerder gemaakte afspraak.

De heer **Çörüz** (CDA): Voorzitter. Ik dank de Minister voor zijn antwoorden en voor de toezeggingen die hij heeft gedaan. Ik wacht de resultaten daarvan af, bijvoorbeeld over de telecomwetgeving in Oostenrijk en die versleutelingen. De Minister komt nog terug op dat Engelse voorbeeld. Eventueel zal inzet van goedwillende hackers plaatsvinden. Het is elke keer het zoeken naar evenwicht. Grote criminaliteit pakken we in Nederland groots aan en kleine criminaliteit op een kleine manier. Het zijn nieuwe ontwikkelingen en we zoeken naar gepaste antwoorden. Ik benadruk dat we daarbij scherp in de gaten houden dat we niet in een situatie komen dat wetgeving achter de ontwikkelingen aanholt, maar dat we onze politiemensen en zittende en staande magistratuur de instrumenten en kennis geven om altijd adequaat te kunnen ageren.
Ik heb de woorden van de Minister over de samenwerking met Defensie begrepen als niet naast elkaar maar met elkaar. Ik krijg daar graag nog een bevestiging van.
Naast wetgeving en mogelijke wetgeving hebben mijn collega's en ik de bewustwording nogmaals onderstreept. Zo jong mogelijk, want ik sta er soms versteld van hoe jong kinderen al iets in de virtuele wereld kunnen. Ik ontvang graag een reactie van de Minister op een bericht in de Wall Street Journal van gisteren, waarin de VS een cyberaanval bestempelen als een oorlogshandeling. Stel dat een aantal Nederlandse jongeren uit Nederland een aanval doet op bijvoorbeeld het elektriciteitsnet in de VS, dan is de Amerikaanse stellingname heel helder.

De heer **Recourt** (PvdA): Voorzitter. Ik dank de Minister voor de beantwoording en voor zijn toezeggingen. Ik hoor hem zeggen dat het werk in uitvoering is en dat er wordt nagedacht. Samenvattend, dit overleg blinkt uit in denken en niet in concrete uitspraken. We zijn nog niet geland. Ik denk dat we later moeten terugkomen met meer concrete maatregelen en debatten. Ik heb de indruk dat we nog niet ver genoeg zijn met het doordenken hoe we ons juridisch stelsel moeten aanpassen aan toekomstige technologische ontwikkelingen. Ik zal een voorstel voor een procedurevergadering doen om de Kamer beter te laten informeren. Ik heb het idee dat we te veel vanuit ons huidige instrumentarium kijken wat er op ons afkomt, maar dat was voor gisteren en niet voor morgen. Ik ga ervan uit dat we erop terugkomen.
Ik vraag de Minister of consumentenbescherming voorop moet staan op Europees niveau. De overheden moeten de consumenten niet het bos insturen waar het de rechtsmacht betreft. Dat trekken we naar ons toe door het voor de consument uit te zoeken.
Ik ga ervan uit dat we het principiële debat over encrypties voeren als technisch uitgezocht is hoe dat in Engeland gaat.

De heer **Elissen** (PVV): Voorzitter. Ik dank de Minister voor zijn geruststellende antwoorden. Wij hebben wat zorgen geuit en de Minister heeft duidelijke antwoorden gegeven over proportionaliteit, waarborgen en privacy. Hij zei zelfs «de volle mep», dus veel meer dan alleen de EVRM. Dat stelt ons gerust.
Ik ben benieuwd naar de kabinetsreactie op de motie-Franken, maar ik ben tevreden omdat de Minister aangeeft dat hij die als kader hanteert.

Mijn complimenten aan de opstellers van de Nationale Risicobeoordeling Bevindingenrapportage 2010. Die roept wel wat vragen op, maar het is een stap in de goede richting en zal doorontwikkeld worden.
We kijken uit naar het eerste dreigingsbeeld op 30 juni, evenals naar de presentatie van de cyberboard.
Waar ik wel mee worstel, is de afbakening. Ik vind het lastig om een goede afbakening te hebben van wat hier ter sprake te brengen. Dat heeft te maken met de recente algemeen overleggen over terrorismebestrijding, de JBZ-Raad en de brandweer. Ik heb het gevoel dat de onderwerpen door elkaar heenlopen. Het is ook een opdracht aan onszelf om daar kritisch naar te kijken om het wat efficiënter te organiseren.

De heer **Dibi** (GroenLinks): Voorzitter. Ik dank de Minister voor de beantwoording en zijn open houding om samen met de Kamer, het bedrijfsleven en iedereen die er verstand van heeft, te zoeken naar de meest effectieve bestrijding van alle vormen van cybercrime. Ook dank voor de toezegging dat zowel de motie-Franken als het EVRM leidend is in het zoeken naar oplossingen. Ik sluit me aan bij de opmerking van de heer Schouw en neem aan dat het onverkort het kader wordt voor de aanpak.
Ik heb geen toezegging gehoord dat de Kamer inzage krijgt in alle initiatieven die voortvloeien uit de pps. De Kamer wil wel de parlementaire controle houden op initiatieven die mogelijk indruisen tegen grondrechten of ertegenaan schuren.
Ik heb een vraag over de politiesterkte. Begrijp ik goed dat de Minister zegt dat het een reallocatie van middelen is, dus dat het wordt gevonden binnen de huidige capaciteit, maar dat het door de aanpak van de bureaucratie niet ten koste gaat van iets anders? Is dat reëel of gaat het wel ten koste van iets anders en zo ja, wat dan?
Mijn laatste vraag is de belangrijkste en gaat over het startpunt van de dreigingsanalyse. Ik ga ervan uit dat het niet een opsomming van het departement wordt van allerlei incidenten, maar dat het een onafhankelijk en wetenschappelijk onderbouwd onderzoek is. Dat is voor de GroenLinks-fractie een harde voorwaarde voor die analyse.
Tot slot dank ik de Minister voor de opmerking dat hij de mate van dreiging niet afhankelijk maakt van politieke opvattingen, maar van feiten.

Minister **Opstelten**: Voorzitter. Bij de dreigingsanalyse zal ik natuurlijk aangeven hoe ik daartoe kom. Ik wil er ook verantwoordelijk voor zijn. Met het bedrijfsleven, de wetenschap en iedereen die er verstand van heeft, wordt erover gesproken. Het zal objectief zijn. De Kamer kan bekijken of het een goed instrument is om verder uit te bouwen.

De heer **Dibi** (GroenLinks): Ik vind het lastig dat het van een departement komt. Ik heb alle vertrouwen in de Minister en zijn ambtenaren, maar het gaat erom dat we een goed, onafhankelijk startpunt hebben. Niet gemaakt door mensen die er misschien ook eigenbelang bij hebben, maar door wetenschappers die vaststellen wat de aard en omvang van cybercrime is. Het moet echt wetenschappelijk en onafhankelijk gebeuren, anders overweeg ik een initiatief hierop.

Minister **Opstelten**: De analyse op het terrein van de NCTb en de nationale veiligheid doen we zelf. De heer Dibi mag van mij vragen dat ik daarbij de kennis van anderen gebruik. Ik vraag hem dringend eerst af te wachten waar we mee komen. Hij zal verrast zijn door de kwaliteit. Ik heb genoteerd: objectiviteit, in een context plaatsen en dat het gaat over kwetsbaarheden. Dat zullen we zichtbaar maken. Dat is voortdurend aan ons gevraagd en daarin hebben we geïnvesteerd. Dat gaan we presenteren bij de start van de pps op 30 juni.

De heer **Dibi** (GroenLinks): Ik ben bang dat we enigszins van mening verschillen. Een goed begin is het halve werk. Als ik de Minister beluister, is waar hij mee zal komen niet onafhankelijk en wetenschappelijk.

Minister **Opstelten**: Het is wel wetenschappelijk. Ik zal alle topmensen die hier verstand van hebben, zowel nationaal als internationaal, hierbij betrekken. Het moet de toets der kritiek kunnen doorstaan. Daarom voeg ik ook het woord kwetsbaarheden toe. Ik vraag de heer Dibi om mij het voordeel van de twijfel te gunnen. Daarna voeren we er weer een debat over.

De heer **Dibi** (GroenLinks): Ik gun de Minister het voordeel van de twijfel. Ik ga met mijn collega-Kamerleden overleggen of we de Minister een handje moeten helpen of dat wij moeten wachten tot 30 juni. Maar dan moet de Minister toezeggen het opnieuw te doen als de Kamer ontevreden is over het beeld.

Minister **Opstelten**: Het antwoord is ja. Het is belangrijk dat onze veiligheidsdiensten ook meedoen. Als je het aan een wetenschapper geeft, zal dat niet gebeuren. Ik heb als Minister de mogelijkheid om alle gegevens te krijgen en een wetenschapper niet. Dit wordt een eerste proeve van bekwaamheid en als de Kamer er anders over denkt, sta ik daar open voor.

De heer **Schouw** (D66): De Minister krijgt natuurlijk het voordeel van de twijfel, maar ik wil hem ten overvloede voorhouden dat dit gevoel Kamerbreed heerst en dat het jammer zou zijn als er op dat punt een valse start wordt gemaakt. Als de Minister meer tijd nodig heeft, krijgt hij die wat mij betreft.

Minister **Opstelten**: Dat waardeer ik zeer, want dat is precies wat we nodig hebben. Het gaat om kwaliteit en zowel de Kamer als ik wil een goede start. De elementen zijn duidelijk aangegeven.
Het antwoord op de vraag over de motie-Franken is ja. In de Eerste Kamer is ook sympathiek gereageerd op de motie.
De samenwerking met mijn collega's is uitstekend. In die board zit ook Defensie. Het is een eenheid en ook in de operationele situatie is er samenwerking. Er is geen risico dat hier zaken uit elkaar zouden lopen. Wij hebben in eendrachtige samenwerking deze strategienotitie tot stand gebracht. Ik kan elke twijfel wegnemen. Defensie is natuurlijk Defensie, maar wij werken schouder aan schouder. Daar mag de Kamer mij aan houden.
De privacybijsluiter voer ik niet af, maar ik wil nadenken of er wellicht nog andere mogelijkheden zijn.
Ik zal nagaan of er een misverstand is over de toezegging dat er na vier maanden wordt gerapporteerd of na een jaar. Wat ik toen heb gezegd, geldt.
Ik heb kennisgenomen van het verzoek om de bewustwording zo jong mogelijk te laten plaatsvinden. Dat moeten we vasthouden.
De Wall Street Journal heb ik niet gelezen en ik weet niet in welke context het staat, maar de Amerikanen zeggen het anders dan wij. Ik weet niet of de Amerikanen oorlog bedoelen als ze over de «war on drugs» spreken. Wij hanteren dat begrip niet en dat moeten we ook niet overnemen. Als de Kamer wil, ben ik bereid om het artikel te lezen en er een column met mijn commentaar of een recensie over te schrijven.

De heer **Çörüz** (CDA): Het lijkt een beetje irreëel, maar het artikel heeft betrekking op de formele cyberstrategie van het Pentagon. Het kan gaan spelen als Nederlanders bepaalde dingen ondernemen. De reactie kan dan

vrij verstrekkend zijn. Ik vraag de Minister te bekijken wat dit eventueel kan betekenen voor de Nederlandse situatie.

Minister **Opstelten**: Ik zal het artikel laten analyseren en dit betrekken bij onze eigen werkzaamheden.
Ik ben het met de heer Recourt eens dat wij nog niet veel concrete maatregelen hebben, maar we hebben wel concrete acties. Ik kom voor 1 januari 2012 met een rapportage over het juridisch instrumentarium. We gaan dat van verschillende kanten in kaart brengen. We zullen nog bekijken waar dat debat gevoerd moet worden.
Over de afbakening hebben wij al gesproken en ik heb daar weinig aan toe te voegen.
Bij de politie zijn de prioriteiten voor ons leidend. Die zijn bij de Kamer bekend en we rapporteren daar voortdurend over. We werken ze per prioriteit uit in concrete resultaten en ze zullen zichtbaar zijn in de begroting. Daar zal de sterkte met name op gericht worden. Vervolgens is er een lokale prioriteitsstelling door burgemeesters en officieren van justitie. Zij bepalen wat in Zaltbommel, Genemuiden of Urk de politie-inzet moet zijn. Daar wil ik het bij houden en we gaan geen debat voeren over wat er allemaal niet gaat gebeuren. Dat betekent niet dat alleen maar die prioriteiten plaatsvinden: dagelijkse dingen gebeuren natuurlijk ook. Dit is de inzet en het is mijn taak om de resultaten te laten zien.
De grootschalige aanpak van aanvallen op informatiesystemen is in Nederland al aardig op orde, zowel in strafrechtelijke als in materiële en formele zin. Nederland heeft het Cybercrimeverdrag van de Raad van Europa tien jaar geleden bekrachtigd. Dat hebben we laatst herdacht en gevierd in Boedapest. Het verdrag is nationaal vertaald. Op het EU-niveau is Nederland betrokken bij de daar spelende activiteiten in de hele critical information infrastructure protection (CIIP). We hebben daar een internationale oefening mee gehad, genaamd Cyberstorm. Op 30 september is het ontwerp van de Europese Commissie voor een richtlijn voor aanvallen op informatiesystemen verschenen. De ontwerprichtlijn strekt tot verbetering van de justitiële samenwerking tussen lidstaten door onderlinge aanpassing van het strafrecht via vaststelling van minimumregels inzake aanvallen op informatiesystemen. De ontwerprichtlijn vervangt het bestaande kaderbesluit van 2005, maar neemt daar veel van over. Daarnaast bevat de ontwerprichtlijn ten opzichte van het kaderbesluit enkele aanvullingen. Het kabinet staat positief tegenover het voorstel. De aanpak van de cybercriminaliteit op het niveau van de EU is een uit het Stockholm Programma voortvloeiende prioriteit. Ondersteuning daarvan ligt in het verlengde van de in het regeerakkoord opgenomen ambitie op het gebied van cybercrime.
Tot slot heb ik een uitnodiging. De afgelopen periode heeft een aantal Kamerleden een bezoek gebracht aan het Nationaal CrisisCentrum (NCC). Het NCC fungeert als rijksbreed crisiscentrum en bereidt de besluitvorming op politiek-bestuur niveau voor bij ernstige incidenten en dreigende crises. Ik nodig belangstellende Kamerleden uit voor een werkbezoek aan het NCC om te zien hoe dat werkt en om voorlichting te krijgen over wie op welk moment wat doet. Dat is ook de plaats waar het kabinet of een delegatie van het kabinet vergadert als er een crisis is. Alle thema's die hier spelen, komen daar interdepartementaal bij elkaar.

De **voorzitter**: Ik noteer de volgende toezeggingen:
– De Kamer kan op of rond 1 juli het periodieke dreigingsbeeld cybersecurity tegemoet zien.
– De Minister legt voor het eind van dit jaar aan de Kamer zijn visie voor op het breed juridisch kader met betrekking tot cybersecurity en de inventarisatie van de juridische knelpunten.

– De Kamer ontvangt van de Minister informatie over de wetgeving in Oostenrijk met betrekking tot cybercrime, met name over de rechtsmachtkwestie.
– De Minister komt terug op de inzet van goedwillende hackers.
– De Minister komt terug op het kenniscentrum cyber.
– De Minister doet de Kamer de nota over zelfredzaamheid toekomen.

Tot slot danken wij de Minister voor de uitnodiging voor een bezoek aan het NCC.

De heer **Recourt** (PvdA): Ik zou graag nog noteren de harde garantie van de Minister voor financiering van het kenniscentrum rechterlijke macht.

Minister **Opstelten**: Ik heb gezegd dat de inzet van het expertisecentrum voor de zittende magistratuur en het OM wordt gecontinueerd.

De **voorzitter**: Ik sluit dit algemeen overleg. Ik dank de Kamerleden voor hun inbreng, de Minister voor de beantwoording en de anderen voor hun belangstelling.