21
Wereldwijde aanval met ransomware

Aan de orde is het **debat** over **de wereldwijde aanval met ransomware op vitale ICT-infrastructuur**.

De **voorzitter**:
Ik heet de staatssecretaris van harte welkom, alsook de mensen op de publieke tribune. Zij zijn niet zo talrijk, maar ongetwijfeld zijn er vele mensen die dit debat anderszins volgen. Dit debat is aangevraagd door de heer Hijink van de SP-fractie tijdens de regeling van werkzaamheden op 16 mei jongstleden. Hij is de eerste spreker. De spreektijden zijn afgesproken. Die zijn vier minuten.

De heer **Hijink** (SP):
Voorzitter. Iets minder dan een maand geleden raakten wereldwijd computers besmet met WannaCry. Dat virus — of zoals het dan heet "'ransomware"' — blokkeert je computer en gijzelt je bestanden. Binnen één dag waren er meer dan 230.000 computers geïnfecteerd in meer dan 150 landen. In Engeland werd de National Health Service getroffen, in Spanje Telefónica en in Duitsland Deutsche Bahn. Recent werd in ons land de Zonnebloem getroffen door ransomware. De medische gegevens van 4.700 mensen die meegaan op hun vakanties, zijn verdwenen. Er was een backup, maar wat met de gestolen gegevens gebeurt, weet niemand.

Het geeft aan dat er weinig bewustzijn is over de risico's van gebrekkige beveiliging van systemen en van de behoefte om steeds meer gegevens en apparaten online te koppelen. In een tijd waarin steeds meer apparaten met het internet zijn verbonden, wordt het extra belangrijk dat wij de veiligheid verbeteren. Want hoe belachelijk het ook mag klinken: het is niet ondenkbaar dat we op korte termijn te maken krijgen met digitale aanvallen vanuit gehackte koelkasten, verlichtingssystemen en beveiligingscamera's. Nu al liggen er netwerken van zulke apparaten klaar voor een mogelijke aanval. Is de staatssecretaris bekend met de kwetsbaarheid van deze apparaten? Erkent hij dat fabrikanten meer zouden moeten doen om de beveiliging te verbeteren? Is hij bereid om extra eisen te stellen aan de huishoudelijke apparatuur die nu nog slecht beveiligd is?

Hoe staat het met de veiligheid van systemen van de overheid? De Rekenkamer was daar enkele jaren geleden nog heel kritisch over. Kunnen wij ervan op aan dat de overheid voldoende offline back-upmogelijkheden heeft voor het geval het echt een keer goed misgaat? En kunnen wij erop vertrouwen dat cruciale systemen niet gekoppeld zijn aan het internet, ook niet via andere netwerken? Beschikt de overheid, zoals een bedrijf als KPN dat ook doet, over een team van ethische hackers dat permanent op zoek is naar kwetsbaarheden in de eigen systemen?

Er zijn twee keuzes voor de overheid als het gaat om onze cybersecurity. Wij kunnen alles op alles zetten om lekken te dichten en incidenten te voorkomen. Of wij willen als overheid, net als de NSA in de VS heeft gedaan, actief gebruik blijven maken van de achterdeurtjes in software, waarmee wij kwetsbaarheden juist in stand houden. Op dit moment doen wij het laatste, met WannaCry tot gevolg. Nu kwamen wij nog goed weg, maar een volgende keer hoeft dat niet zo te zijn.

De SP wil dat de informatievoorziening maar vooral ook de praktische ondersteuning aan bedrijven en burgers verbetert. Wij zien dan ook graag dat het Nationaal Cyber Security Centrum niet alleen de vitale sectoren gaat beschermen, maar ook advies en praktische ondersteuning gaat bieden aan het midden- en kleinbedrijf en aan maatschappelijke organisaties. Hoe staat de staatssecretaris tegenover dat voorstel?

Kan de staatssecretaris aangeven wie wat hem betreft de verantwoordelijkheid draagt voor de veiligheid van onze systemen? Zijn dat de mensen thuis, die moeten zorgen voor goede updates en goede software? Of is dat de overheid, die bedrijven en burgers zou moeten beschermen in plaats van zelf te hacken? Zijn het de bedrijven en particulieren die nu geld verdienen aan het kopen en verkopen van kwetsbaarheden in andermans software? Of zijn het de leveranciers van software die veel geld verdienen bij de verkoop, maar de update enkele jaren achterwege laten? Als het antwoord van de staatssecretaris luidt dat wij allemaal verantwoordelijk zijn, dan hoor ik graag hoe hij van plan is om de veiligheid van software en netwerken via al deze partijen af te dwingen.

Mevrouw **Helder** (PVV):
Voorzitter. Nederland beschikt over een van de grootste internetknooppunten ter wereld. Dat maakt ons land een belangrijke doorvoerhaven van digitale aanvallen op doelen buiten Nederland. Maar ons land is zelf ook doelwit. Statelijke actoren blijken grote belangstelling te hebben voor de innovatieve of specialistische technologie waarom Nederland bekendstaat. Door deze digitale en economische spionage van buitenlandse inlichtingendiensten komt ook de concurrentiepositie van Nederland onder druk te staan.

Recentelijk vond een wereldwijde cyberaanval plaats. Dat is ook de aanleiding voor dit debat. Een grote aanval met ransomware infecteerde meer dan 200.000 computers en ruim 10.000 organisaties in 150 landen. De kwetsbaarheid was bekend en kon ook worden gerepareerd, maar niet iedereen die verantwoordelijk is voor cybersecurity, had de update gedraaid. Naar de mening van onze fractie heeft de staatssecretaris de vragen hierover tijdens het mondelinge vragenuur op 16 mei jongstleden voldoende beantwoord. Daarom zal ik dit debat aangrijpen om de staatssecretaris een paar andere vragen te stellen over dit onderwerp.

Cyberveiligheid is van groot belang voor de nationale veiligheid. Mijn fractie wil dan ook een concreet actieplan van de staatssecretaris en niet alleen het jaarlijkse Cybersecuritybeeld Nederland. Het Cybersecuritybeeld Nederland is een jaarlijkse publicatie van het Nationaal Cyber Security Centrum en bevat inzicht in de ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity. In de laatste uitgave staat onder meer dat het economische en geopolitieke belang van onze digitale infrastructuur groeit, dat de spionage- en sabotagedreigingen toenemen, maar dat de weerstand nog steeds achterblijft. Er staat daarnaast dat de overheid en het bedrijfsleven moeten investeren en maatregelen moeten blijven treffen om de digitale veiligheid van Nederland te versterken. In dat kader

vraag ik de staatssecretaris naar een concreet actieplan in geval van nood, om het maar even zo uit te drukken.

Ik heb daarnaast nog een paar andere vragen aan de staatssecretaris. Ten eerste: na de recente aanval met ransomware is gebleken dat er al twee maanden een update van de software was om het gat te dichten. Soms is het niet tijdig dichten van een gat of het verhelpen van een kwetsbaarheid complex, omdat een update van de software het systeem kan breken. Maar soms is het ook verwijtbare dommigheid, om het maar even zo aan te duiden. Is het mogelijk om diegenen daarvoor aansprakelijk te stellen? Of is het de aangewezen weg om de makers van software aansprakelijk te stellen voor het op de markt brengen of houden van onveilige software of het niet tijdig ter beschikking stellen van updates? Ofwel: is de bestaande aansprakelijkheidswetgeving wel voldoende voor ICT-producten en -diensten?

Ten tweede: wat vindt de staatssecretaris van het eerder gedane voorstel door Fox-IT, namelijk het aanstellen van een zogenoemde "'cybercommissaris"', die vergelijkbaar is met de aangestelde commissaris voor de Deltawerken? Die laatste heeft een eigen budget en kan besluiten nemen zonder daarvoor goedkeuring nodig te hebben van de ministeries. Eenzelfde structuur zou nodig zijn voor de cybercommissaris, omdat dit sneller tot actie kan leiden wat betreft de beveiliging van digitale systemen en de bijbehorende dreigingen.

Ten derde: het ministerie heeft laten weten het initiatief van CyberSecurityKeten.NL toe te juichen. Dat is een alliantie van zes bedrijven met elk een specifieke expertise, die op individueel niveau al dan niet met de overheid samenwerken. Het doel van dit initiatief is de Nederlandse afhankelijkheid van buitenlandse internettechnologie en -kennis terug te dringen. Kan de staatssecretaris aangeven of de overheid met dit consortium in zee zal gaan?

Afrondend: het belang van een goede beveiliging van onze digitale infrastructuur kan niet overschat worden. Nu waren het ziekenhuizen, parkeer- en pinautomaten, de volgende keer ligt er weer iets anders dagenlang plat. Onze afhankelijkheid van de digitale infrastructuur wordt alleen maar groter naarmate we steeds meer dingen aan het internet gaan hangen. We weten ook allemaal dat dat de nabije toekomst is. Wat mijn fractie betreft moet de overheid dan ook vol inzetten op een sterke beveiliging van onze digitale infrastructuur.

☐

Mevrouw **Bruins Slot** (CDA):
Voorzitter. Een kleine maand geleden werd de wereld opgeschrikt door een cyberaanval die qua snelheid van verspreiding uniek genoemd kan worden. Er ontstond een sneeuwbaleffect met uiteindelijk geïnfecteerde computers in 150 landen. Daar was minder dan een weekend voor nodig. In het Verenigd Koninkrijk lagen bijvoorbeeld de ziekenhuizen stil.

Dat Nederland niet getroffen is, is meer geluk dan wijsheid, zoals de staatssecretaris al aangaf in de brief. Dat baart het CDA ook zorgen. De staatssecretaris geeft in zijn brief aan dat het Nationaal Cyber Security Centrum (NCSC) al op 14 maart gewaarschuwd heeft voor de kwetsbaarheid, waar de gijzelsoftware uiteindelijk misbruik van heeft gemaakt. Hoe monitort het NCSC wat er met een dergelijke waarschuwing wordt gedaan? Is het mandaat voor het NCSC voldoende toereikend met betrekking tot de private sector en om ervoor te zorgen dat private partijen dergelijke kwetsbaarheden dichten?

De Algemene Rekenkamer liet onlangs in haar verantwoordingsonderzoek 2016 weten dat de informatiebeveiliging bij vijf ministeries nog niet op orde is. Twee daarvan zijn Veiligheid en Justitie en Volksgezondheid, Welzijn en Sport. Met name de ontoereikende back-up- en recoverymaatregelen zijn in het licht van deze ransomware-aanval zorgwekkend te noemen. Een goede back-up zorgt ervoor dat gegevens die door de gijzelsoftware versleuteld zijn, alsnog hersteld kunnen worden. Dat is een belangrijk onderdeel van de verdediging tegen dit soort aanvallen. Kan de staatssecretaris aangeven hoe er nu wordt gewerkt aan het op orde krijgen van de back-up- en recoverymaatregelen op de ministeries?

Een aandachtspunt van de Algemene Rekenkamer, dat in dit kader ook van belang is, is de vergaande verbondenheid van systemen van de rijksoverheid, maar ook de verbondenheid van de systemen tussen de ministeries en de uitvoeringsinstellingen. Denk bijvoorbeeld aan de loonaangifteketen van het Centraal Bureau voor de Statistiek met de Belastingdienst en het UWV. De Algemene Rekenkamer schrijft in zijn rapport ook dat digitale processen die zo met elkaar versleuteld raken, in de fysieke wereld ontzettend veel gevolgen kunnen hebben. Denk maar aan het moment dat het UWV zijn diensten niet meer kan uitvoeren. Daarom wil ik graag van de staatssecretaris weten hoe wij ons zelf nu gaan beschermen tegen deze kwetsbaarheden. Hoe wordt er met het oog op deze nieuwe variant van gijzelsoftware, die zichzelf verspreidt, de komende jaren werk gemaakt van het veiliger maken van verbindingen tussen deze systemen? In dit kader is het ook van belang dat er een snelle implementatie is van de Netwerk- en informatiebeveiligingsrichtlijn. Hierin krijgen exploitanten van kritieke infrastructuur, bijvoorbeeld energiemaatschappijen en overheden, de verplichting om beveiligingsrisico's te beheren en ernstige incidenten te rapporteren. Komt dit wetsvoorstel nog steeds dit najaar? En hoeveel tijd is er na aanname van de wet nodig alvorens ziekenhuizen en energiemaatschappijen voldoen aan de in de wet verankerde eisen?

Ik kom tot een afsluiting. Onlangs heeft mevrouw Van Toorenburg in het mondelinge vragenuur aandacht gevraagd voor Nederlandse ziekenhuizen en de beveiliging van hun ICT. Begin dit jaar bleek dat ziekenhuizen hun ICT-beveiliging ook niet op orde hebben. We hebben nu net in Groot-Brittannië gezien wat de gevolgen zijn als we dat niet op orde hebben. De staatssecretaris heeft toegezegd een brief te vragen aan de minister van VWS waarin staat wanneer dit wel op orde is. De Nederlandse Vereniging van Ziekenhuizen gaf in haar eerste reactie van begin februari dit jaar aan dat zij wel een paar jaar nodig hebben voordat zij het netjes op orde hebben. We hebben niet een paar jaar de tijd. We moeten nu al proberen om het op orde te krijgen. Wanneer komt die brief? En hebben ziekenhuizen bijvoorbeeld draaiboeken klaarliggen voor het geval er zo'n geslaagde aanval is? Kortom: wij hebben geluk gehad, deze keer, maar er is werk aan de winkel.

De heer **Verhoeven** (D66):
Dat was een mooi betoog van het CDA. Dank daarvoor. Ik heb wel een vraag. Mevrouw Bruins Slot heeft het niet gehad over iets waarvan ik denk dat het heel cruciaal is in dit debat: de omgang met kwetsbaarheden in software, namelijk het al dan niet open willen laten van kwetsbaarheden in software voor de inlichtingen- en veiligheidsdiensten en de politie. Het CDA was daar de afgelopen maanden bij vorige debatten groot voorstander van. Er zijn heel veel deskundigen die zeggen: juist het openlaten leidt tot dit soort cyberaanvallen. Hoe kijkt het CDA daar nu op terug? Wat is het standpunt van het CDA op dit moment over het openlaten van die kwetsbaarheden?

Mevrouw **Bruins Slot** (CDA):
Dit gaat natuurlijk over de zero-days. De heer Verhoeven heeft die vraag al gesteld tijdens het vragenuur. Toen heeft de staatssecretaris heel duidelijk het antwoord gegeven dat dit juist een gemelde kwetsbaarheid was. Die was op 15 maart al bekend. Men heeft toen ook alle organisaties verzocht om back-ups te draaien en dat is niet gebeurd. De situatie waar de heer Verhoeven het over heeft, is dus anders dan de situatie die hier heeft plaatsgevonden.

De heer **Verhoeven** (D66):
Wij hebben het hier over een kwetsbaarheid en een patch, een reparatie, die twee weken daarvoor bekendgemaakt was. Althans, dat is wat ik gehoord heb. Ik heb de staatssecretaris dat in ieder geval nog niet anders horen zeggen. Dat hoor ik dan graag straks van hem. Je kunt niet verwachten dat wereldwijd — zoals mevrouw Bruins Slot zelf al zei — honderdduizenden systemen geüpdatet zijn als je een kwetsbaarheid gebruikt waarvan de reparatie pas zo kort bekend is. Als je kiest voor het openlaten van die kwetsbaarheden, heb je altijd dit soort problemen. Ik vraag mij af of het CDA daar nog wel oog voor heeft. Het CDA zegt altijd dat het wil dat de diensten die kwetsbaarheden kunnen gebruiken, maar dan moet het CDA ook toegeven dat dit een reëel risico is dat vaker zal gaan voorkomen.

Mevrouw **Bruins Slot** (CDA):
Dat is inderdaad de vraag die daarachter zit. Die hebben wij uitgebreid behandeld bij de Wet computercriminaliteit III en de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). De afweging van het CDA was dat je, om bijvoorbeeld de strijd tegen het terrorisme goed te kunnen voeren, in bepaalde situaties de veiligheidsdiensten gewoon de ruimte moet geven om gebruik te maken van die achterdeur. Bij beide wetsvoorstellen, dus bij zowel de Wet computercriminaliteit III als de Wiv, is een zorgvuldige afweging gemaakt waarin waarborgen zijn ingebouwd.

De **voorzitter**:
Tot slot, kort.

De heer **Verhoeven** (D66):
Dus eigenlijk zegt het CDA: we maken veel geluid over deze aanval, want het is heel erg dat dit gebeurd is en dus moeten de back-ups beter geregeld worden en moeten we veel investeren en beter organiseren. Maar over de echte oorzaak, het openlaten van kwetsbaarheden, zegt het CDA: dat laten we gewoon, want we denken nog steeds dat dat goed is. Het CDA zegt dus: wij gaan niet leren van deze aanval en blijven bij het standpunt dat we kwetsbaarheden gewoon open kunnen laten en dat we de gevaren daarvan voor lief nemen. Mag ik die conclusie trekken?

Mevrouw **Bruins Slot** (CDA):
Nee, dat mag de heer Verhoeven niet, want hij trekt het hier echt uit het verband. De heer Verhoeven weet ook dat het openlaten van een kwetsbaarheid alleen maar als een ultimum remedium wordt gebruikt, bijvoorbeeld als we terrorisme willen aanpakken. Het aanpakken van terrorisme is een van de belangrijkste dingen die wij op dit moment moeten doen. De heer Verhoeven maakt eigenlijk een vergelijking zoals: criminelen maken gebruik van een machinegeweer, maar de politie mag dat niet meer doen. Die vergelijking gaat niet op. De politie en onze veiligheidsdiensten zullen soms ook gebruik moeten maken van bepaalde instrumenten om ervoor te zorgen dat Nederland veilig is en om terroristische aanslagen te voorkomen.

De **voorzitter**:
De heer Verhoeven komt nu aan zijn eigen termijn namens D66.

De heer **Verhoeven** (D66):
Voorzitter. Dank u wel. Twee weken geleden — de collega's zeiden het al — werd de wereld opgeschrikt door een van de grootste cyberaanvallen ooit. Ransomware met de naam WannaCry infecteerde meer dan 300.000 ICT-systemen in tientallen landen. De gevolgen waren ingrijpend, soms zelfs levensgevaarlijk. In Engeland konden patiënten bijvoorbeeld geen chemokuur meer krijgen.

De aanval was zo succesvol omdat de gebruikte softwarekwetsbaarheid opengehouden was door de Amerikaanse veiligheidsdienst NSA en daar nog niet zolang een reparatie, een zogenaamde patch, voor beschikbaar was. Daardoor waren heel veel systemen op heel veel plekken nog niet geüpdatet. De aanval toont aan dat het openhouden van onbekende kwetsbaarheden reële risico's heeft voor onze cyberveiligheid. Het kabinet, maar ook partijen als de Partij van de Arbeid, het CDA en de VVD, wilden dat in ieder geval bij de behandeling van de hackwet vorig jaar en een paar maanden geleden bij de behandeling van de Wet op de inlichtingen- en veiligheidsdiensten, de Wiv, niet inzien. De inbreng van D66, die wat lang duurde, werd ofwel genegeerd, ofwel onderschat, ofwel weggelachen.

Na een aanval als deze moet het speelkwartier echter wel afgelopen zijn. We kunnen niet meer wegkijken en de gevaren van het openlaten van kwetsbaarheden negeren. Dat kan niet meer. Het is tijd voor een serieus debat over cyberveiligheid. Ik ben dus heel blij dat de SP dit debat heeft aangevraagd.

Waar is het misgegaan? Allereerst natuurlijk bij eigenaren van niet-gerepareerde systemen, zoals in Britse ziekenhuizen. D66 vraagt al jaren om het NCSC (Nationaal Cyber Security Centrum) een sterker mandaat te geven. Laat het NCSC semioverheidsinstellingen, zoals ziekenhuizen, actief helpen om hun cyberveiligheid op orde te brengen. Steeds

zei het kabinet: nee, dat is aan de instanties, de ziekenhuizen, zelf. Ziet de staatssecretaris nu ook de ernst van de zaak en is hij bereid het NCSC op dit punt alsnog een groter mandaat te geven?

De belangrijkste discussie van vandaag — ik probeerde het net in het interruptiedebat met mevrouw Bruins Slot al naar voren te brengen — gaat natuurlijk over een echte politieke keuze. We kunnen allemaal zeggen dat we meer moeten investeren, onze back-ups beter op orde moeten krijgen en er meer aandacht voor moeten hebben, maar het gaat over een politieke keuze, namelijk het gebruik en het openhouden van onbekende kwetsbaarheden door de overheid. Ja, de politie en de inlichtingendiensten moeten kunnen hacken, maar D66 heeft altijd gezegd dat dit op een verstandige manier moet gebeuren, die opsporingsbelangen aan de ene kant en cyberveiligheidsbelangen aan de andere kant naast elkaar legt. Ik vind het teleurstellend dat de staatssecretaris in zijn brief over WannaCry geen besef toont van de risico's van het openhouden van zero-days, van onbekende kwetsbaarheden. Deze ransomware-aanval laat precies zien wat er dan kan gebeuren.

Mevrouw **Bruins Slot** (CDA):
De heer Verhoeven denkt wellicht dat het over dit punt gaat, maar daarover hebben we al uitgebreid debatten gevoerd. Ik vond het interessant dat de heer Verhoeven de ziekenhuizen aanhaalde. Volgens mij is het een gedeelde zorg van CDA en D66 dat daar nog een enorme kwetsbaarheid ligt en dat we die nog lang niet opgelost hebben. Welke oplossingsmogelijkheid ziet de heer Verhoeven om ervoor te zorgen dat we die ongeveer 90 ziekenhuizen in Nederland voldoende beschermen tegen dit soort ernstige aanvallen?

De heer **Verhoeven** (D66):
Dat staat dan even los van de keuze of je kwetsbaarheden wilt openlaten. Ik geloof dat we daar vanavond niet uitkomen. Ik heb er met mevrouw Van Toorenburg, die tot mijn grote vreugde nu voorzitter is bij dit debat, al vaker discussies over gevoerd, maar ik zal dit nu parkeren. Het is inderdaad een terecht punt. We hebben er in het verleden al Kamervragen over gesteld. Ik weet niet of we dit samen met het CDA hebben gedaan, maar dat zou heel goed kunnen. Het idee om het NCSC een actievere rol te geven om dit soort semipublieke instanties te helpen zich beter te beveiligen, is volgens mij heel goed. Wij hebben dat vorig jaar ook al eens geopperd, maar toen is dat nog niet helemaal van de grond gekomen. Aangezien ik nu een cluster van Kamerleden zie die allemaal staan te knikken bij dit idee, heb ik het gevoel dat het vanavond weleens die kant op zou kunnen gaan. Daar zou ik heel blij mee zijn.

Mevrouw **Bruins Slot** (CDA):
Inderdaad, het CDA en D66 hebben het bij andere debatten met de minister van VWS al eerder over cybersecurity gehad. Het is lastig voor ziekenhuizen om die stap te zetten. De reactie in februari was dat ze nog wel enkele jaren nodig hebben. Wellicht is het een oplossingsmogelijkheid om er meer druk op te zetten. Wat verwacht de heer Verhoeven van de implementatie van de Europese richtlijn, de NIB (Netwerk en Informatie Beveiliging), die vrij binnenkort naar de Kamer komt?

De heer **Verhoeven** (D66):
Ik denk dat die een belangrijke bijdrage zal leveren. In het algemeen gaat de implementatie van Europese richtlijnen hier echter niet zo snel als we zouden willen. Ik denk dus dat een eigen nationaal initiatief, als extra laag, als extra verdedigingslinie, wel goed zou zijn. Dat moet het CDA toch aanspreken. Volgens mij zou het dus een en-enverhaal kunnen zijn. We hebben een Nationaal Cyber Security Centrum, met heel veel kennis. Dat is een bestaande organisatie, die we wat mij betreft echt goed kunnen gebruiken.

Mevrouw **Tellegen** (VVD):
Ik hoor de heer Verhoeven spreken over politieke wil. We hebben hier een uitvoerig debat gevoerd over de Wet computercriminaliteit, waarbij we heel lang naar de heer Verhoeven en zijn standpunten hebben mogen luisteren, ook als het ging om onbekende kwetsbaarheden. Het debat ging namelijk vooral over onbekende kwetsbaarheden. Zoals ik de brief lees en de informatie die we hebben gekregen over deze aanval, ging het om een bekende kwetsbaarheid. Ik vind dat dat onderscheid helder gemaakt moet worden. Ik roep de heer Verhoeven nog in herinnering dat wij hier een heel zorgvuldige politieke weging hebben gemaakt. Het waren de heer Recourt en ik die zelfs nog een amendement hebben ingediend om de omgang met die onbekende kwetsbaarheiden van nog meer waarborgen te voorzien, namelijk niet alleen een bevel door de officier van justitie maar ook nog een rechterlijke toets. Dat kan de heer Verhoeven toch onmogelijk geen zuivere politieke afweging noemen?

De heer **Verhoeven** (D66):
Dat kan ik wel. Ik herinner mij zelfs nog dat tijdens dat debat dat amendement ter sprake kwam. Ik meen dat het niet alleen van mij kwam maar dat er meerdere fracties verbaasd waren over de kwaliteit en de vergaandheid van dat amendement. Wat mij betreft behoeven wij hier de geschiedenis nu niet terug te halen, want die wet is behandeld. Ik leg de vraag voor of je misschien toch niet na moet denken over het al dan niet gebruiken van kwetsbaarheden, maar dat amendement heeft er niet voor gezorgd dat het nu ineens een zeer zorgvuldige aanpak is, waarbij alle waarborgen overeind staan. Bijvoorbeeld de CTIVD, de instantie die toezicht houdt op de inlichtingen- en veiligheidsdiensten, heeft dat onlangs benadrukt. Die heeft gezegd: er moet beter en scherper beleid komen op basis waarvan wij kunnen toetsen. Het kabinet heeft dat zelfs aangegeven, inclusief de staatssecretaris. Ik zal hem zo meteen ook vragen om echt iets met de aanbevelingen van de CTIVD te doen, want dat is tot nu toe niet gebeurd. Dus er kan nog veel meer gebeuren.

Mevrouw **Tellegen** (VVD):
Dat er nog steeds meer kan gebeuren, begrijp ik. En de hoop dat de fractie van D66 in de Eerste Kamer gaat stemmen voor deze wet die knetterhard nodig is om juist de problemen die we hier vandaag bespreken aan te pakken, heb ik niet eens meer. Ik wil echter nog wel even rechtzetten dat het beeld dat hier wordt geschetst alsof wij hier in deze Kamer bij de behandeling van die wet niets hebben gedaan om de waarborgen in die wet steviger te verankeren als het gaat om het gebruik van onbekende kwetsbaarheden, niet klopt. Sterker, er zit nu een dubbele waarborg in, waarbij

we, gelukkig maar, de opsporingsdiensten die bevoegdheden geven die ze nodig hebben om precies datgene wat we vandaag bespreken, aan te pakken en tegen te gaan.

De heer **Verhoeven** (D66):
Ik respecteer dat de VVD tevreden is met de eigen inbreng destijds en nu nog steeds. De Partij voor de Vrijheid die altijd zeer is voor het aanpakken van terrorisme heeft tegen de Wet computercriminaliteit III gestemd vanwege dit risico. Dus het komt niet alleen van mijn fractie of die van GroenLinks en de SP. Of deze wet knetterhard nodig is, daarvan weet ik niet of dat precies de goede duiding is. Wat ik wel weet, is dat iedereen in deze Kamer heel graag terrorisme wil bestrijden en verdachten wil kunnen oppakken. Mijn standpunt is altijd dat dit kan gebeuren op heel veel andere manieren en dat het openlaten van kwetsbaarheden daar niet voor noodzakelijk is en dat dit openlaten van kwetsbaarheden tegelijkertijd voor onveiligheid van het internet zorgt. Daarom ben ik er niet voor.

De **voorzitter**:
Voordat we het hele debat opnieuw doen, een slotwoord van mevrouw Tellegen en dan kunt u daarop nog reageren. En daarna sluiten we dit onderdeel af.

Mevrouw **Tellegen** (VVD):
Ter opfrissing van het scherpe geheugen van de heer Verhoeven nog het volgende. De PVV heeft naar mijn weten destijds niet op dit punt tegen de Wet computercriminaliteit gestemd, maar dat zat 'm in de straf voor een aantal delicten et cetera. Op dit punt was de PVV het in ieder geval roerend met de VVD, het CDA en de PvdA eens.

De heer **Verhoeven** (D66):
Ik zal de PVV niet meer gebruiken bij mijn standpuntinname. Dus excuus als dat tot verwarring heeft geleid.

De **voorzitter**:
In ieder geval gaat mevrouw Helder daar even op reageren, want zij is aangesproken. Mevrouw Helder van de PVV zal ons duidelijkheid geven over waarvoor zij wel of niet heeft gestemd.

Mevrouw **Helder** (PVV):
Ja, dank u wel, voorzitter. We moeten dit niet onbesproken laten want anders blijft het zo hangen. Ik heb toen niet voor niets namens mijn fractie een stemverklaring afgelegd. De waarheid ligt inderdaad in het midden. Mijn fractie heeft tegengestemd, niet omdat zij tegen het openlaten van die kwetsbaarheden is, maar omdat zij vindt dat deze vergaande bevoegdheid beperkt moet worden tot misdrijven waar een straf van acht jaar of meer op staat. Ik heb daarbij concreet genoemd terrorisme en ernstige gewelds- en zedenmisdrijven. Dus het ligt ergens in het midden.

De **voorzitter**:
Dan geef ik het woord …

De heer **Verhoeven** (D66):
Als ik nog heel kort nog een opmerking mag maken …

De **voorzitter**:
Niet in reactie op de woorden van mevrouw Helder. U mag heel kort nog een antwoord geven op de vraag van mevrouw Tellegen.

De heer **Verhoeven** (D66):
Het is echt een oprechte zoektocht naar verbinding over dit onderwerp. Mij wordt immers weleens verweten dat ik op dit punt een scherpslijper wil zijn. We hebben weleens van elkaar gezegd: als je niet voor deze wet stemt, ben je schuldig op het moment dat er een terroristische aanval plaatsvindt. Ik zou nu kunnen zeggen: als je voor dit soort wetgeving bent, ben je schuldig aan WannaCry. Dat zijn de uitersten die we natuurlijk niet moeten zoeken. Maar met de nuance, de manier waarop we omgaan met die kwetsbaarheden, welke waarborgen er zijn en welke dingen nog niet goed geregeld zijn, valt nog een hoop te winnen. Ik zou het mooi vinden als we met het CDA, de VVD en allerlei andere partijen uit de schuttersputjes kunnen komen en dat kunnen gaan regelen. Dan kunnen we tenminste stappen zetten.

De **voorzitter**:
Dank u wel. Dit was niet heel kort. Ik geef de heer Hijink de gelegenheid om te interrumperen.

De heer **Verhoeven** (D66):
Maar het was wel goed bedoeld. Daar zou u als voorzitter ook oog voor kunnen hebben.

De heer **Hijink** (SP):
Allereerst ben ik blij om te horen dat D66 het ermee eens is dat het goed zou zijn als het Nationaal Cyber Security Centrum uitbreiding en meer taken zou krijgen. Misschien kunnen we daar vanavond al een beginnetje mee maken. Dat is niet mijn vraag. Die gaat over de updates. Bij wie ligt daarvoor de verantwoordelijkheid? Je zou kunnen stellen dat iedereen uiteindelijk zelf verantwoordelijk is voor het updaten van zijn software. Maar je zou je ook kunnen afvragen of het ook niet de verantwoordelijkheid is van de ontwikkelaars van software en van de bedrijven die daar veel geld aan verdienen, om ervoor te zorgen dat zo lang hun software gebruikt wordt, die ook veilig en up-to-date is. Hoe kijkt de heer Verhoeven daarnaar?

De heer **Verhoeven** (D66):
Het is een gedeelde verantwoordelijkheid. Je kunt het niet bij één partij neerleggen. Ik denk absoluut dat de gebruiker een grote verantwoordelijkheid heeft. Daar kun je niet aan voorbijgaan. Dat zegt het kabinet ook altijd, en daar ben ik het wel mee eens. Maar je kunt ook niet zeggen dat de fabrikanten en allerlei andere spelers die in die keten een deel van het product bepalen, helemaal geen verantwoordelijkheid, geen zorgplicht zouden moeten hebben. Ik zou ook daarnaar willen kijken. Het is hier dus echt en-en. Je moet niet zeggen dat we het op één plek neerleggen, maar

je moet echt proberen om alle partijen in de keten hun verantwoordelijkheid te laten nemen.

De heer **Hijink** (SP):
Ik ben het daar van harte mee eens. Microsoft zegt bijvoorbeeld op een bepaald moment dat het stopt met de ondersteuning van XP, Vista en noem het allemaal maar op. Dan zegt de heer Verhoeven dus ook dat je tegen zo'n bedrijf zou moeten kunnen zeggen: op het moment dat jij iets op de markt hebt gebracht en er veel geld aan hebt verdiend, houd je ook een zorgplicht en een verantwoordelijkheid voor de veiligheid van dat product?

De heer **Verhoeven** (D66):
D66 heeft onlangs een initiatiefnota uitgebracht over het internet of things. Daarin hebben we veel aandacht besteed aan softwareaansprakelijkheid of een garantie op software. Ik denk dat dat een heel eind in de richting gaat van de ideeën van de heer Hijink. Ik denk dus dat we elkaar daar best wel op kunnen vinden.

De **voorzitter**:
Vervolgt u uw betoog.

De heer **Verhoeven** (D66):
De vraag aan de staatssecretaris luidt dus: ziet de staatssecretaris nu wel of niet de risico's van het openhouden van zero-days? Die vraag zou ik graag nog stellen. Daar zou ik ook graag het antwoord op vernemen.

Ook de CTIVD, de toezichthouder op de diensten, waarschuwde er onlangs al voor dat er geen goed beleid is, dat er geen duidelijk afwegingskader is voor het openhouden van onbekende softwarekwetsbaarheden. Wanneer mag een zero-day, zo'n onbekende kwetsbaarheid, opengehouden worden en wanneer moet deze gemeld worden? De verenigde Staten hebben zo'n afwegingskader met vragen als: zit de gevonden kwetsbaarheid ook in vitale infrastructuur, wat is het veiligheidsrisico als je de kwetsbaarheid openlaat en wat voor inlichtingen verwacht je te krijgen via de kwetsbaarheid? Dat soort vragen zit in dat kader.

Het kabinet heeft gezegd dat het de aanbevelingen van de CTIVD zal opvolgen. Is de staatssecretaris bereid een dergelijk afwegingskader op te stellen, zodat de CTIVD beter toezicht kan houden? Zo niet, dan hoor ik graag wat het kabinet gaat doen om de aanbevelingen toch nog op te volgen. Dat toezicht moet immers ook gelden voor de politie. Dat zou dan ook moeten betekenen dat de politie geen hacksoftware mag inkopen als de door de hacksoftware gebruikte zero-days niet getoetst kunnen worden aan het afwegingskader. Is de staatssecretaris dit met de D66-fractie eens?

☐

De heer **Krol** (50PLUS):
Voorzitter. Het WannaCry-virus was in veel opzichten verontrustend, ook al richtte het in Nederland gelukkig relatief weinig schade aan. Dat is overigens een kwestie van geluk volgens de staatssecretaris. Verontrustend is ten eerste het feit dat een ransomware-virus zich in zo'n razend tempo over een groot deel van de wereld heeft kunnen verspreiden, ten tweede het feit dat het virus slechts één computer hoefde binnen te dringen om een heel netwerk te besmetten en ten derde het feit dat het erop lijkt dat het virus is ontwikkeld door de National Security Agency, maar op de een of andere manier in verkeerde handen terecht is gekomen. Dat gegeven is op zich al schokkend. Hoe is het mogelijk dat iets binnen de NSA ontwikkeld is en op deze manier wordt gebruikt? Wat zegt dat eigenlijk over onze digitale veiligheid? Gelukkig was er een sleutel om het virus tot staan te brengen, maar tegelijkertijd is dat een groot gevaar.

Dit virus is voor degenen die er verstand van hebben en kwaad willen, makkelijk aan te passen. Ik sprak erover met de Nederlandse deskundige Brenno de Winter. Als de zwaktes eruit gehaald zijn, kunnen terroristen of misschien wel vijandige mogendheden met dit in handen vitale infrastructuur overnemen. Communicatienetwerken, ziekenhuizen, sluizen en energiemaatschappijen, eigenlijk de hele maatschappij kan worden lamgelegd. Dat is een nachtmerrie die ten koste van alles moet worden voorkomen. Een duidelijker waarschuwing kun je haast niet bedenken. Cybercriminaliteit is een van de grote bedreigingen van deze tijd. Wij moeten onder ogen zien dat het niet meer alleen individuen zijn die op een zolderkamertje proberen te hacken. Het is een groot en structureel gevaar dat als wapen kan worden ingezet door groepen, organisaties en naties die ons niet gunstig gezind zijn.

Daarom moet er nog meer ingezet worden op cybersecurity. Het is wat ons betreft nog steeds onbegrijpelijk dat het amendement van collega Verhoeven bij de afgelopen begrotingsbehandeling van Justitie geen meerderheid kreeg. Meer geld is niet alleen de oplossing, maar het wordt steeds duidelijker dat een heel grote dreiging aanwezig is voor de mondiale veiligheid. Nederland zou koploper moeten zijn in de aanpak van dit probleem. Is de regering bereid om te investeren in het proactief delen van kennis en de informatiesamenleving beveiligingsbewuster te maken? En zo ja, hoe? Welke lessen trekt de regering uit deze gebeurtenissen? Graag een reactie.

Ik dank u wel, mevrouw de voorzitter.

De **voorzitter**:
Dank u wel. Dan geef ik het woord aan mevrouw Tellegen van de VVD.

☐

Mevrouw **Tellegen** (VVD):
Voorzitter. Je moet er niet aan denken: dat je vecht voor je leven op de ic-afdeling van een ziekenhuis en het apparaat waaraan je ligt, wordt gehackt of dat een hacker erin slaagt de Deltawerken digitaal aan te vallen, met een potentiële nieuwe watersnoodramp tot gevolg. Het lijken scènes uit een film, maar het zijn scenario's die wel degelijk werkelijkheid kunnen worden. Dagelijks lopen wij risico's dat de gegevens die we op het internet achterlaten of die digitaal door bedrijven of door de overheid worden opgeslagen, worden gehackt, of het nu gaat om onze belastingaangiften of ons profiel op een datingsite. Waren wij tot voor kort voornamelijk bezig met onze veiligheid op straat, vandaag maken wij ons steeds meer zorgen over onze veiligheid in de digitale wereld.

Aanleiding voor dit debat is de wereldwijde aanval met de gijzelsoftware WannaCry. In zeker 150 landen werden honderdduizenden computersystemen gekaapt in ruil voor losgeld. In Nederland lijkt de schade beperkt gebleven en werd alleen parkeerbedrijf Q-Park getroffen. Maar de aanval doet terecht de vraag rijzen hoe het staat met de cyberveiligheid in Nederland. Doen we genoeg om onze burgers te beschermen en om onze vitale infrastructuur weerbaar te maken? Gebeurt er genoeg om het Nederlandse bedrijfsleven te beveiligen?

Allereerst gaat het erom dat onze opsporings- en veiligheidsdiensten de bevoegdheden krijgen om datgene te doen wat noodzakelijk is om ons te beschermen tegen cyberaanvallen van buitenaf en om cybercriminaliteit aan te pakken. Daar hebben zij de Wet computercriminaliteit III en de Wet op de inlichtingen- en veiligheidsdiensten hard bij nodig. Ik hoop dan ook dat de partijen die in de Tweede Kamer tegen deze wetten hebben gestemd, in de Eerste Kamer alsnog zullen instemmen.

Naast adequate wetgeving is er meer nodig. Ik noem kennis en kunde. We moeten de knapste koppen aantrekken en inzetten om onze digitale dijken optimaal te bewaken. Dat geldt voor onze vitale infrastructuur, maar ook voor de informatiebeveiliging van en door de overheid. Willen we werk maken van cyberveiligheid, dan is er ICT-expertise nodig. Dan zijn er digiprofessionals nodig die hun kennis en kunde inzetten voor een veilig digitaal Nederland. Wat is op dit punt de inzet van het kabinet? Is de Wet normering topinkomens hierbij een belemmering?

Ik kom te spreken over de coördinatie. In bijna ieder debat over dit onderwerp klinkt de roep om een stevigere coördinatie. Er is het nodige gebeurd en ondernomen om alle spelers uit het veld op structurele wijze bij elkaar te brengen. Dat gebeurt in het Nationaal Cyber Security Centrum. Dat gebeurt in de computer emergency response teams. Dat gebeurt in het Nationaal Detectie Netwerk. Dat gebeurt door de minister van Binnenlandse Zaken. Dat gebeurt door deze staatssecretaris. Maar nog altijd wordt er in alle rapporten gepleit voor een betere coördinatie. Is de kritiek op het versplinterde beeld van de aanpak en op het gebrek aan doorzettingsmacht terecht?

Ik kom op het bedrijfsleven. Met name het mkb loopt steeds grotere risico's. Er wordt werk gemaakt van de ketenaanpak, zo lezen we in de brief. Grote bedrijven nemen kleinere bedrijven onder hun hoede om hen te helpen werk te maken van digitale veiligheid, maar dat is mogelijk niet genoeg. Wordt in het Cybersecuritybeeld Nederland dat de staatssecretaris voor deze zomer nog stuurt, specifiek aandacht besteed aan het mkb en de schade die het mkb lijdt als gevolg van cyberaanvallen en cybercriminaliteit? Hoe kijkt de staatssecretaris aan tegen het advies om het NCSC in praktische zin meer te laten doen ten aanzien van het mkb?

Tot slot heb ik nog een vraag over veilige producten van ICT-leveranciers. Straks hebben ze een meldplicht als de wet in de Eerste Kamer wordt aangenomen. Maar ze hebben ook een zorgplicht. Is de aansprakelijkheidswetgeving op dit punt in orde? Of dient deze te worden aangepast?

☐

Mevrouw **Buitenweg** (GroenLinks):
Voorzitter. Eind maart, een paar dagen na mijn installatie, stond ik aan de balie van de ICT-dienst van de Tweede Kamer. Terwijl ik mij wegwijs probeerde te maken met mijn nieuwe apparatuur, ontstond ineens een heel grote drukte en moesten alle medewerkers ineens alle zeilen bijzetten. Toen was de Tweede Kamer namelijk getroffen door ransomware. De schade bleef gelukkig beperkt. Maar zo liep het op 12 mei niet af voor veel bedrijven en overheidsinstellingen in de landen om ons heen. Het is al gezegd: WannaCry-ransomware verspreidde zich toen wereldwijd, razendsnel en ongecontroleerd. Voor veel burgers, lokale overheden en bedrijven was het een wake-upcall. Zij hebben hun basisveiligheid vaak onvoldoende op orde, en dat is zorgwekkend.

Een recent rapport van het Rathenau Instituut laat zien dat met name het mkb behoefte heeft aan meer ondersteuning. Deelt de staatssecretaris dit standpunt? Vindt hij het een taak van de overheid om te investeren in bijvoorbeeld een onafhankelijk kennis- en adviescentrum voor deze bedrijven?

Hacks in vitale infrastructuur zouden natuurlijk de grootste ellende veroorzaken. Gelukkig is de weerbaarheid daar overwegend goed op orde, maar toch zijn er uitzonderingen. Een jaarlijkse stresstest zou dit aan het licht kunnen brengen. Wat vindt de staatssecretaris van het idee om bedrijven die vitale infrastructuur beheren, te vragen om jaarlijks een hacktest uit te voeren? Dat idee is door het Rathenau Instituut geopperd.

In de brief van 2 juni gaat de staatssecretaris niet in op de vraag of Nederland op dit moment voldoende opsporingscapaciteit inzet om digitale risico's het hoofd te bieden. Ik ben zelf heel erg benieuwd naar een analyse van de beschikbare mensen en de middelen die er nu zijn, afgezet tegen de capaciteit die nodig is. Die analyse is ook altijd handig als we later over middelen gaan praten.

Ik heb nog een laatste, niet onbelangrijk punt. De heer Verhoeven heeft het net al aangestipt: het wetsvoorstel inzake computercriminaliteit. Volgens de staatssecretaris biedt dit effectieve bescherming tegen ICT-dreigingen, maar GroenLinks heeft hier grote twijfels over. Na aanname van het wetsvoorstel kan de politie, simpel gezegd, terughacken. Zij zal daarvoor zogenoemde zero-days aanschaffen. Via dit soort onbewaakte achterdeurtjes in de beveiligingsprogramma's dringen hackers, dus ook de terughackers zoals de politie, computersystemen binnen. Dat is natuurlijk allemaal al besproken in het debat in december, maar toch is het ook voor vandaag relevant. Het is dus mogelijk dat de politie niet bekendmaakt dat er een veiligheidslek is. Dat is dan ook een lek dat niet gedicht kan worden als de providers en zakelijk dienstverleners daar geen weet van hebben. Mevrouw Tellegen had het net over het verschil tussen bekende en onbekende kwetsbaarheden, maar deze kwetsbaarheden blijven natuurlijk voor het grote publiek onbekend als de politie ze niet bekend maakt. Het is een beetje alsof de politie kennis heeft van de zwakte van een alarminstallatie, maar ervoor kiest om de huiseigenaren in Nederland daar niet over te informeren, zelfs niet nadat de politie zelf al heeft ingebroken bij de verdachte. Dat maakt dat burgers een stuk onveiliger zijn dan zij zich wanen. Ook de brancheverenigingvan de ICT-sector heeft vandaag nog

weer een brief gestuurd om te zeggen dat men zich daar ernstige zorgen over maakt. Mevrouw Bruins Slot maakte een vergelijking die ik erg lastig vond. Ze zei dat de politie door die zero-days over de wapens zou beschikken die terroristen nu ook hebben. Volgens mij is het punt nu juist dat je daarmee een geweer voor het grijpen legt, ook voor kruimeldieven en weet ik veel wie, waardoor de situatie echt niet veiliger wordt.

Mevrouw **Tellegen** (VVD):
Ik weet dat het aangaande de zero-days nooit meer goed komt tussen de collega van GroenLinks en mij. Desalniettemin heb ik net weer gezegd dat ik hoop dat de GroenLinks-fractie in de Eerste Kamer een verstandig besluit zal nemen, maar dat ter zijde. U noemde een voorbeeld van het openlaten van een kwetsbaarheid dat tot gevolg zou kunnen hebben dat een heleboel huiseigenaren hun veiligheidssysteem niet op orde hebben, maar dat zal natuurlijk nooit de test doorstaan die we ingebouwd hebben. Dat zou nooit de toets door de officier van justitie of de rechter doorstaan. Wil men die kwetsbaarheid open laten staan, dan moet dat altijd proportioneel zijn. Als het zoveel slachtoffers zou maken, zou dat nooit werken en zou de rechter-commissaris daar nooit toestemming voor geven.

Mevrouw **Buitenweg** (GroenLinks):
Voor individuen ...

De **voorzitter**:
Mevrouw Tellegen rondt haar vraag af en dan krijgt u het woord, mevrouw Buitenweg.

Mevrouw **Tellegen** (VVD):
U had het over huiseigenaren in brede zin. Ik zoek naar een manier om de discussie over zero days genuanceerd te voeren.

De **voorzitter**:
Wat is concreet uw vraag, mevrouw Tellegen?

Mevrouw **Tellegen** (VVD):
Is mevrouw Buitenweg het met mij eens dat het dankzij de waarborgen die wij erin gestopt hebben, nooit door die tests heen zou komen?

Mevrouw **Buitenweg** (GroenLinks):
Wat ik opmaak, ook uit de zorgen die de brancheverenigingheeft geuit, is dat er nog steeds kwetsbaarheden zijn voor individuele gebruikers. Dat zijn natuurlijk wel degelijk mensen of bedrijven die te maken hebben met schade. Er wordt een kwetsbaarheid open gelaten, en die kan volgens mij schade toebrengen en is daarom onwenselijk. Ik hoop dan ook dat de recente ransomware-aanval de staatssecretaris aan het denken heeft gezet. Mijn vraag aan hem is of hij het niet toch wenselijk vindt dat die lekken altijd kenbaar moeten worden gemaakt, zodat gebruikers die lekken zo snel als mogelijk kunnen dichten en daardoor weerbaarder zijn tegen toekomstige cyberaanvallen.

Mevrouw **Bruins Slot** (CDA):
Het beeld ontstaat nu dat er vele, vele lekken zijn die de politie en de veiligheidsdiensten gebruiken en dat zij dat naar willekeur kunnen doen, maar dat is niet zo. Er is een heel erg keurig juridisch systeem opgebouwd in de Wet computercriminaliteit en in de Wet inlichtingen- en veiligheidsdiensten om daar gebruik van te maken. Wanneer kunnen zij er gebruik van maken? Als het een belangrijk doel dient om erger te voorkomen, bijvoorbeeld om terroristische aanslagen te voorkomen. Mijn vergelijking ziet erop dat je in sommige gevallen ook een middel moet geven aan een veiligheidsdienst om erger te voorkomen, maar daar is een keurige toets op. Dat was mijn vergelijking en ik hoop dat mevrouw Buitenweg dat ook zo ziet. We moeten erger voorkomen.

Mevrouw **Buitenweg** (GroenLinks):
Ik ben het er helemaal mee eens dat terrorisme echt bestreden moet worden. Ik heb al in een ander debat eerder vandaag gezegd dat ik zeer voor gerichte bestrijding ben. U doet het alleen een beetje voorkomen alsof u ook kunt beheren wie er gebruik gaat maken van zo'n lek, maar er kunnen natuurlijk ook mensen gebruikmaken van een lek die niet de goede bedoelingen hebben die u voor ogen hebt.

De **voorzitter**:
"'U"' ben hier ik. Mevrouw Bruins Slot antwoordt.

Mevrouw **Buitenweg** (GroenLinks):
Ik denk dat u het daarmee eens bent, mevrouw de voorzitter.

De **voorzitter**:
Laat mij erbuiten, zou ik zeggen. Mevrouw Bruins Slot.

Mevrouw **Bruins Slot** (CDA):
Om uit eigen ervaring te spreken: als militair ben ik uitgezonden geweest naar Uruzgan, als peletonscommandant pantserhouwitzers, dat is een soort kanonnen. In zo'n strijd maken in de fysieke wereld inderdaad verschillende groepen gebruik van dezelfde middelen. Het verschil is alleen dat het, als het Nederlandse leger dat doet of de overheid, gebeurt op basis van rechtsregels. Soms moeten we die erge middelen gebruiken om nog erger te voorkomen. Dat gebeurt op de digitale snelweg ook. Maar dat betekent niet dat anderen daar geen gebruik van kunnen maken. Dat wordt echter alleen gedaan na de meest zorgvuldige afweging, bijvoorbeeld om een terroristische aanslag te voorkomen. Mijn vraag aan mevrouw Buitenweg is dan ook: is dit niet van belang om ervoor te zorgen dat we uiteindelijk ook ervoor kunnen zorgen dat erger voorkomen wordt en dat we dat beter goed omschreven door regelgeving doen dan dat we het vrijlaten?

Mevrouw **Buitenweg** (GroenLinks):
Ik wil helemaal niet bestrijden dat u dit met de allerbeste bedoelingen doet, om te zorgen dat dit echt een goed doel dient, namelijk het bestrijden van terrorisme. Ik ben ervan overtuigd dat u dat met die bedoeling doet. Het probleem is echter alleen dat het niet helemaal zuiver georganiseerd

kan, dat het niet helemaal zuiver dichtgeregeld kan worden en dat je dus toch bewust lekken laat ontstaan en blijft laten ontstaan; je laat ze immers staan. Die lekker zorgen voor onveiligheid en problemen. Het doet dus niets af aan de intentie waarmee dit is gedaan, maar feit is wel dat die lekken blijven bestaan en dat die kwetsbaarheden zijn waarvan mensen echt nadeel blijven ondervinden. Ik vind het van belang dat u dat ook wel erkent.

De **voorzitter**:
"'U"' is nog steeds ik. U hebt nog drie kwart minuut.

Mevrouw **Buitenweg** (GroenLinks):
Volgens mij zijn de belangrijkste punten de revue gepasseerd. Ik maak mij zorgen over die kwetsbaarheden. Verder heb ik genoemd de vitale infrastructuur en de stresstest evenals een informatiepunt voor het mkb. Dat lijken mij op dit moment de belangrijkste punten.

Mevrouw **Kuiken** (PvdA):
Voorzitter. Collega's voor mij hebben al aangegeven wat het belang is van de beveiliging van onze vitale infrastructuren. Dat gaat van groot — onze dijken, onze elektriciteit, ziekenhuizen, de Tweede Kamer — naar wat kleiner maar niet onbelangrijker leed, zoals de Zonnebloem, even los van wat voor soort ransomware het ook moge zijn. Al in 2005 hebben de PvdA, collega Martijn van Dam, en de SP een motie ingediend die erop was gericht om tot een meldplicht te komen. Organisaties zouden het moeten aangeven wanner zij gehackt werden. Partijen als CDA en VVD, maar ook de Consumentenbond waren daar toen niet enthousiast over. Ze vonden het niet belangrijk genoeg. Dit laat zien dat we, meer dan tien jaar verder, inmiddels op een ander spectrum zitten. Eigenlijk de gehele Kamer en ook het kabinet zijn ervan doordrongen dat het ongelofelijk belangrijk is. Niet voor niets gaat het kabinet, zo heb ik begrepen, regelmatig in overleg juist met al die vitale infrastructuur om cyberaanvallen te voorkomen.

Een groot aantal vragen is al door mijn collega's gesteld; het heeft ook zijn voordelen om als een van de laatsten aan de beurt te zijn. Ik vat even samen. Er is een vraag gesteld over één minister voor de digitale overheid, dus voor alle digitale informatievoorziening. Er is gevraagd of je een jaarlijkse hacktest zou moeten doen. Hoe kijkt de staatssecretaris daartegen aan? Ik wil daarnaast nog een aantal aanvullende vragen stellen.

De staatssecretaris heeft al aangegeven dat er binnenkort een update komt over alles wat er gebeurt op cybersecurity. Mijn specifieke vraag is of daar de ontwikkelingen in worden meegenomen die nu gaande zijn bij de omvorming van de nationale politie, waar men zich nog meer moet voorbereiden op cybersecurity en cyberonderzoek in brede zin en hoe dat wordt vormgegeven.

Een tweede vraag die ik heb, is wat we doen met de mens zelf. Het is heel mooi als we heel veel veiligheidssystemen optuigen, maar van een aantal mensen dat heel erg te maken heeft met beveiliging van grote en kleine organisaties heb ik gehoord dat de mens vaak de belangrijkste factor is waarom de veiligheid van systemen faalt. Op welke wijze gaan we daarop inzetten? Dat gaat natuurlijk niet alleen over mkb-bedrijven, maar juist ook over individuen die verantwoordelijk zijn voor de beveiliging van die infrastructuren. Klikken op een verkeerde mail is één klein voorbeeld, maar dat gebeurt natuurlijk ook in bedrijven. Ik krijg hier graag een reactie op van de minister.

Tot slot. Zes bedrijven hebben de handen ineengeslagen om ervoor te zorgen dat Nederland en bedrijven die in deze branche opereren, gezamenlijk optrekken om Nederland cyberproof te maken. Zij wezen er terecht op dat het belangrijk is dat we kijken naar onze eigen infrastructuur en de manier waarop wij daarmee omgaan. Ik heb daar een concreet voorbeeld van, waarover de SP ook Kamervragen heeft gesteld: de aanbesteding van onze nationale telecommunicatie. Er is wetgeving in de maak die het mogelijk maakt om wel degelijk te kijken naar de herkomstlanden bij het aanbesteden van dat soort diensten. Feitelijk is dit nog niet geregeld. Dat vind ik een gemiste kans. Hoe kijkt de staatssecretaris naar het fenomeen van herkomstlanden en de aanbesteding van onze nationale infrastructuur, zoals telecommunicatie, in het licht van onze veiligheid en cybersecurity?

De heer **Verhoeven** (D66):
Toen we het debat over de Wet computercriminaliteit III destijds hebben gevoerd, was de PvdA nog een actieve coalitiepartner en stemde zij voor. Hoe zou de PvdA-fractie vandaag de dag over deze wet stemmen?

Mevrouw **Kuiken** (PvdA):
Ik heb toen niet het woord over gevoerd, maar wij hebben hier binnen onze fractie wel uitvoerig en langdurig bij stilgestaan omdat het een belangrijk onderwerp is waar allerlei mitsen en maren aan zitten. Wij hebben serieus bekeken of we het gebruik van "'zero-days"', zoals ze geloof ik heten — ik ben wat korter woordvoerder op dit terrein — tegen zouden moeten houden. Uiteindelijk hebben we ons ervan laten overtuigen dat het in het belang van terrorismebestrijding is dat we die mogelijkheden openhouden. Daarover hebben we toen een bewust besluit genomen. Daarop zou ik op dit punt niet terug willen komen.

De heer **Verhoeven** (D66):
Dank voor dit antwoord. Mevrouw Tellegen had het in haar inbreng een paar keer over de Eerste Kamerfracties van diverse partijen, die in de Eerste Kamer misschien toch voor zouden kunnen stemmen. Het lijkt me heel ingewikkeld om als Tweede Kamerlid te gaan bepalen hoe je Eerste Kamerfractie stemt, want dat loopt nogal eens uiteen. We hebben ze niet aan een touwtje. Maar omdat we toch in die trant bezig zijn: wat gaat de PvdA-fractie in de Eerste Kamer eigenlijk doen met deze wet? Dat vind ik dan ook wel interessant. Misschien heeft mevrouw Kuiken ze wel aan een touwtje. Dan zou ik het antwoord graag meekrijgen.

Mevrouw **Kuiken** (PvdA):
Ik heb hierover nog geen overleg gehad met de Eerste Kamerfractie, dus dat weet ik niet.

De **voorzitter**:
Dank u. De staatssecretaris heeft tien minuten de tijd gevraagd om de vragen van de Kamer te kunnen beantwoorden.

De vergadering wordt van 20.22 uur tot 20.35 uur geschorst.

De **voorzitter**:
De staatssecretaris van Veiligheid en Justitie zal de vragen van de Kamer beantwoorden. Aan u het woord!

Staatssecretaris **Dijkhoff**:
Voorzitter. De aanleiding tot het debat is de uitbraak van de WannaCry-ransomware eerder deze maand. We hebben het er in het vragenuur ook al over gehad. Na het vragenuur op 16 mei zijn er geen meldingen bij het NCSC binnengekomen over besmettingen bij de rijksoverheid en vitale infrastructuur. De impact was voornamelijk buiten Nederland. Zoals een aantal Kamerleden al in herinnering heeft geroepen, durf ik dat er niet aan toe te schrijven dat wij beter zouden zijn in beveiligen. Zo'n besmetting vindt soms vrij willekeurig plaats. Het is een combinatie van ransomware met een worm die zijn weg vindt, van kwetsbaarheid naar kwetsbaarheid hopt en niet per se gericht hoeft te zijn. Je kunt dan ook niet altijd conclusies trekken uit wie er wel en niet geraakt zijn, maar alleen je zegeningen tellen.

Natuurlijk staat cybersecurity in Nederland niet pas na deze uitbraak op de agenda. Veel van de problemen die de Kamer terecht signaleert, komen ook al een tijdje voor in de verschillende cybersecuritybeelden. Je hebt liever dat dit niet gebeurt, maar laat het dan op z'n minst bijdragen aan meer bewustwording. Laat nog meer mensen wakker worden die we niet al eerder met onze bewustwordingscampagnes hebben overtuigd van het belang van cybersecurity, zodat zij hun zaken op orde gaan brengen. In Nederland is de kwaliteit van cybersecurity en het NCSC hoog. De behoefte om meer te kunnen doen is er ook. We hebben daarover al eerder met de Kamer gesproken en we hebben daartoe ook al stappen gezet, maar er is zeker ruimte om nog meer te doen, zowel in capaciteit als in wet- en regelgeving. Daarvoor hebben we de nodige wetten, die al in herinnering zijn geroepen, aan de Kamer voorgelegd en gaan we nog de nodige wetten voorleggen.

Het is een lastig probleem dat niet makkelijk te isoleren is. Het werkt niet zo simpel dat je een nieuwe overheidstak opricht die ervoor gaat zorgen dat Nederland veilig is op cybergebied. De heer Hijink vroeg wie er precies aansprakelijk is en gaf het antwoord dat hij verwachtte. Ik moet hem helaas teleurstellen qua voorspelbaarheid. Het is inderdaad iedereen, maar niet iedereen een beetje in die zin dat je een dingetje doet en dat dat dan wel genoeg is. Het is echt een keten van verantwoordelijkheden. Door jouw verantwoordelijkheid niet te nemen heb je niet alleen jezelf, maar verzwakt ook de keten waardoor je anderen in gevaar kunt brengen en risico's kunt vergroten voor ons allemaal. Dat is het ingewikkelde hieraan. Laat ik maar gewoon even wachten.

De **voorzitter**:
Mijnheer Hijink, de staatssecretaris is net met een korte inleiding begonnen en komt aan de vragen toe. Hebt u op dit punt al een vraag?

De heer **Hijink** (SP):
Ik weet niet of hij nog terugkomt op de vraag over updates en wie verantwoordelijk is. Komt hij daar nog op terug?

Staatssecretaris **Dijkhoff**:
Ja.

De **voorzitter**:
Dat was een van uw specifieke vragen.

Staatssecretaris **Dijkhoff**:
Een vraag daarvoor van de heer Hijink ging over de veiligheidsrisico's als gevolg van de toename van het aantal genetwerkte apparaten. Internet of things, het internet der dingen, betekent dat je alles online kunt zetten. Ieder ding is aan het internet te koppelen. Dat is een lastige trend. Je zou als samenleving rustig kunnen beginnen, maar zo werkt het niet. Het is allemaal heel aantrekkelijk en als het beschikbaar is, zullen mensen het ook doen. Dat brengt op zichzelf weer een nieuw risico mee, want zelfs een slowcooker kan online. Dat is handig, want dan kun je op je telefoon zien wanneer je pulled pork gaar is; dat is erg belangrijk. Daar zit software in en als het aan een netwerk hangt, is dat te hacken. Als er een kwetsbaarheid in zit, moet je ervoor zorgen dat het geüpdatet wordt. Het is misschien niet het eerste apparaat waarvan je na de aanschaf nog eens denkt dat je misschien een firmware-update moet draaien van je keukenapparatuur. Daarom is het van belang dat we daar breder beleid op hebben, het liefst internationaal, want het zijn producten die breed in de markt staan. Daarom komt het ministerie van Economische Zaken met de roadmap veilige hard- en software. Ik dring er natuurlijk steeds op aan dat het onderwerp cybersecurity daarbij een prominente plaats heeft. Je zou op internationaal niveau, maar op z'n minst op EU-niveau aan producten producteisen op dit vlak moeten stellen. Dit zou ook een plaats moeten krijgen in de EU-cyberstrategie, die we dit jaar verwachten. Nederland brengt daar ook steeds naar voren dat dit daar een onderdeel van moet zijn. Wij benadrukken dat die producten niet alleen leuke gadgets zijn, maar ook een kant hebben die zeer serieuze risico's met zich meebrengt, risico's die je moet ondervangen.

Hoe ga je bedrijven op hun aansprakelijkheid daarbij wijzen? Daarvoor kun je niet één standaard zetten, gezien de brede aard van hardware en software waarmee wordt gewerkt. Volgens mij moet de zorgplicht meerdere rollen raken, namelijk zowel die van leverancier als die van klant en van gebruiker. Mensen in al die rollen moet je wijzen op het deel van de zorgplicht dat ze hebben. We hebben een handreiking over zorgplicht voor het bedrijfsleven gepubliceerd binnen de Cyber Security Raad. Je zult dan per sector moeten aangeven hoe die zorgplicht het beste vorm kan krijgen. Ook dit is een onderdeel van de eerder genoemde roadmap van mijn collega van Economische Zaken.

Laten we eens heel concreet kijken naar de updates. De heer Hijink zegt: moet je niet verplicht stellen dat iemand die ooit een product op de markt heeft gebracht, de software in dat product altijd blijft ondersteunen? Dat vind ik een beetje lastig. Laten we concreet kijken naar de kwetsbaarheid die bij deze aanval is gebruikt. Die zat in Windows XP, en daarvan dan weer in een protocol dat niet per se heel erg nodig is voor hedendaags gebruik. Eigenlijk was het vaak al ingehaald door modernere protocollen. Je kunt bij zoiets zeggen: de producent heeft dat product op de markt gebracht, dus hij moet het blijven ondersteunen. Maar je kunt natuurlijk ook zeggen dat in sommige gevallen producten zo verouderd of zo kwetsbaar zijn dat je ze beter gewoon kunt vervangen. Dan moet je er dus bij aanschaf op letten of er op het product een soort "'niet gebruiken na"'-datum zit. Dat is bij deze software het geval. Daarbij zegt een bedrijf: we zijn inmiddels zo veel verder en er zijn inmiddels zo veel nieuwe versies dat je deze versie eigenlijk niet meer moet gebruiken. Sommigen zeggen dan: ik kan niet zonder, want ik heb vervolgapparatuur of -software gekocht die niet op nieuwere versies draait. Die kunnen dan geservicet worden, in dit geval tegen betaling. Later is de patch voor deze kwetsbaarheid in brede zin beschikbaar gesteld. Volgens mij moet je mensen dus wel verantwoordelijk houden voor de producten die ze op de markt brengen. Maar een onderdeel daarvan kan volgens mij juist ook zijn dat je zegt: dit product moet je gewoon niet meer gebruiken, dat moet je niet meer doen. Je kunt wel proberen te blijven servicen, maar in zo'n geval valt er eigenlijk niet meer tegenop te servicen. Dan kan een producent zeggen: stap over op een nieuwe variant.

Mevrouw **Tellegen** (VVD):
Ik heb hiernaar gevraagd tijdens mijn inbreng. Als ik de staatssecretaris goed begrijp, hebben we straks een meldplicht en ook een zorgplicht. Althans, bedrijven hebben die zorgplicht. Er ligt nu een protocol voor bij de raad. Dat is een soort richtlijn. Die is niet bindend. Hoe zorgen we er nou voor dat de mensen of de bedrijven die producten op de markt brengen waar mogelijk kwetsbaarheden in zitten, eigenlijk net als bij medicijnen een bijsluiter opnemen, in dit geval een digitale bijsluiter? Daarin staat dan: hier moet u rekening mee houden en dit zijn de risico's. De staatssecretaris vergeleek dit zelf net met de manier waarop dit is geregeld bij het verstrijken van de houdbaarheidsdatum bij medicijnen. Hoe kunnen we dit iets steviger maken, zodat de verantwoordelijkheid ook daar wordt gelegd waar bedrijven er ook geld aan verdienen?

Staatssecretaris **Dijkhoff**:
Ik ben het met mevrouw Tellegen eens dat dat moet. We zijn nog niet helemaal zover dat ik kan zeggen: oké, hier heb ik het malletje en zo moet het. Dit zit ook in de ontwikkeling van de roadmap van Economische Zaken die ik zojuist noemde. Het zit ook in Europese regelgeving. Je wilt dit immers het liefst breder doen dan alleen maar voor Nederland. Daarin zal je per sector tot die eis moeten komen. Het maakt natuurlijk wel wat uit waar je apparatuur voor gebruikt en waarvoor niet. Daaruit blijkt al de complexiteit. Je kunt nog wel denken per op de markt gebracht product. Maar die producten grijpen vervolgens ook weer op elkaar in. In een ziekenhuis zou men bijvoorbeeld best wel willen afstappen van Windows XP, maar het wordt moeilijker als men daarmee bepaalde apparatuur niet meer kan gebruiken omdat de leverancier van die apparatuur het niet mogelijk maakt het allemaal door te migreren naar nieuwere versies. Daar zal je ook aandacht voor moeten hebben. Het is dus iets ingewikkelder dan nu alleen maar kiezen voor die zorgplicht. Een deel zit ook in de afspraken die de klant met de leverancier maakt.

De heer **Hijink** (SP):
Ik ben het met de staatssecretaris eens dat het de vraag is waar de verantwoordelijkheid van zowel de gebruiker als de producent begint en eindigt. Iemand vertelde me net dat er nog pinautomaten in Moskou zijn die draaien op Windows 98. Nou begrijp ik dat dat een extreem geval is, maar er zijn natuurlijk wel commerciële belangen in het spel. Het is voor een softwareleverancier heel interessant om om de zoveel jaar een heel nieuw besturingssysteem te presenteren, zeker als je vervolgens stopt met het ondersteunen van het vorige. Zo houd je de business wel draaiende. Is het dan niet logisch dat je zegt: als een leverancier iets op de markt heeft gebracht, waar consumenten flink voor hebben betaald, dan mag ook van de leverancier verwacht worden dat hij dat blijft ondersteunen? Als hij stopt met de ondersteuning, moet hij dan bijvoorbeeld geen uitgeklede maar veilige versie van de opvolger overhandigen aan de gebruiker?

Staatssecretaris **Dijkhoff**:
Ik was misschien iets te theoretisch mee aan het denken. Als ik zeg dat het soms beter is om gewoon afscheid te nemen van iets wat echt verouderd is, wil ik niet zeggen dat dat je businessmodel moet worden of dat producenten vooral moeten zeggen: ja, ik vind het verouderd, koop maar een nieuwe. Maar op een gegeven moment kun je wel constateren dat het veiliger is om dat in je hele netwerk, in de samenleving niet meer te hebben, dan het te blijven oplappen. Dat neemt niet weg dat ik vind dat, als je iets levert waar een kwetsbaarheid in zit die later ontdekt wordt en die er al in zat, als je dus een product hebt geleverd waarin die opening geboden werd, je het ook moet patchen. Dan moet je het ook updaten. In de wetgeving waar wij ook voor pleiten in Europees verband zit dat ook. Als je digitale inhoud levert, om het breder te trekken dan de term "'software"', dan vallen de veiligheid, toegankelijkheid en continuïteit onder de conformiteitsplicht. Ook het aanbieden van updates valt daaronder.

De heer **Hijink** (SP):
Ja, dat valt daar dan onder, maar tegelijk zegt de staatssecretaris: een dergelijke verantwoordelijkheid is wel eindig. Of zegt hij nu: zoals wij het zien, moet die verantwoordelijkheid bij bedrijven blijven liggen? Dat gebeurt nu feitelijk niet. Nu stoppen bedrijven met het ondersteunen van bepaalde software, waardoor heel veel computers heel kwetsbaar worden. Vindt hij dat die verantwoordelijkheid moet worden uitgebreid en wil hij met voorstellen daartoe komen?

Staatssecretaris **Dijkhoff**:
Uit veiligheidsoogpunt is het soms belangrijker om te stoppen met bepaalde software te gebruiken dan die software te blijven oplappen. Verder loop je altijd het risico dat de leverancier er niet meer is, als hij failliet is gegaan bijvoorbeeld. In zo'n geval kun je er niet op rekenen dat de

oorspronkelijke leverancier updates levert. Je moet het dus breder bekijken dan alleen maar te denken: updates geven tot in het oneindige is de oplossing. Onder de conformiteitsplicht valt dat je dat wel doet, zeker als het gaat om veiligheidsrisico's die al ingebakken zaten in het product dat je op de markt hebt gebracht. Producten zijn ontelbare regels codes. Die zijn heel moeilijk onfeilbaar. Kwetsbaarheden worden er niet bewust in gezet. Je moet het dus wel blijven updaten, maar daarmee is het niet opgelost.

De **voorzitter**:
Vervolgt u uw betoog.

Staatssecretaris **Dijkhoff**:
De nodige vragen zijn gesteld over sturing en over wat ik vind van de brede roep om coördinatie. Ik vind dat ingewikkeld. Ik kan mij voorstellen dat je ervoor kiest om het anders in te richten, maar ik vind dat om twee redenen lastig.

De eerste reden is dat de roep om coördinatie vaak ophoudt bij dat punt, maar wat coördineer je dan? Het is heel fijn voor de samenleving dat je weet dat je maar bij één bewindspersoon hoeft aan te kloppen voor alle klachten die ook maar iets te maken hebben met cyber, maar dat is nog geen coördinatie. Dan moet je eerst weten wat je die persoon wilt laten doen. Je kunt niet alleen zeggen: je bent een soort überbewindspersoon op dit terrein en de rest moet naar je luisteren. Zo werkt het niet als je niet gewoon een plan hebt waar je met z'n allen aan werkt.

De tweede reden is dat het heel erg lastig los te koppelen is van primaire processen bij anderen. Het is niet iets voor erbij. Als je de digitale kant van de overheid bij één persoon legt, dan gaat hij over wel heel erg veel. Ziekenhuizen werden al genoemd. Het is niet zo dat het primaire proces in een ziekenhuis losstaat van de ICT. Dat noemen we vaak ondersteunende infrastructuur, maar het is meer en meer de kern van de zaak. Je krijgt al snel een spanningsveld, in zoverre dat je zegt "'hij coördineert"', waardoor de anderen denken "'oké, dan is het dus niet van mij"', terwijl het alleen maar werkt als iedereen op zijn eigen terrein zijn verantwoordelijkheid neemt. Je moet eerst weten welke stappen gezet moeten worden, waardoor je wellicht schotten moet doorbreken. Als je dat antwoord eenmaal vindt, kun je wellicht één persoon aanmelden die dat actief moet doen.

Ik kom daarmee meteen op de vraag of het NCSC ziekenhuizen en/of het mkb kan gaan servicen. Ik zie daarin een grote rol weggelegd voor het NCSC, maar niet zozeer als het orgaan dat zelf 1 miljoen bedrijven uit het mkb of alle ziekenhuizen in Nederland zou moeten gaan bedienen. Je kunt niet het NCSC bellen, waarna er een busje bij je komt voorrijden, de medewerkers een week bij je bezig zijn en je vervolgens veilig bent. Zo werkt het niet. Ik denk wel — dat zit ook in de plannen — dat het voor het NCSC cruciaal kan zijn om samen te werken met andere cybersecurityorganisaties, die bijvoorbeeld per branche werken of hoe je dat dan ook het liefst vanuit de samenleving zou willen inrichten. In de medische sector heb je bijvoorbeeld het Zorg-CERT, het computer emergency response team. Je kunt het NCSC via die organisaties laten werken, zodat zij daarin een rol kunnen vervullen en bij het NCSC terechtkunnen. Je kunt daarnaast decentrale clubs hebben, ingericht op een manier die bij de sector past, waar de informatie wordt gedeeld en waar tot handelen kan worden overgegaan met dienstverleners die dat voor een ander kunnen doen.

Ik denk dat zo ook …

De **voorzitter**:
Ik hoor dat u aan een nieuw stukje wilt beginnen, maar ik geef eerst het woord aan mevrouw Bruins Slot namens het CDA.

Mevrouw **Bruins Slot** (CDA):
De staatssecretaris begon zijn betoog door te benadrukken dat het van belang is om eerst een analyse te maken van de stappen die je wilt zetten om bijvoorbeeld schotten te doorbreken, voordat je iemand meer regie en coördinatie geeft. De laatste keer dat we over het Zorg-CERT spraken, was dat nog in oprichting. Mijn vraag aan de staatssecretaris is: sinds wanneer is deze organisatie actief?

Staatssecretaris **Dijkhoff**:
Het antwoord op de vraag in welk stadium van oprichting het Zorg-CERT zich bevindt of hoe operationeel het is, heb ik zo niet paraat. Ik weet wel dat er nog voor de zomer een actieplan informatiebeveiliging van het ministerie van VWS naar de Kamer komt. Ik denk dat de details hierover daarin zullen staan.

Mevrouw **Bruins Slot** (CDA):
De staatssecretaris gaf nu de indruk dat we al een Zorg-CERT hebben, dat het al is opgericht en dat het al actief aan het werk is, maar daar ligt het probleem juist. Dat is allemaal nog niet zo. Het is in oprichting en men is nog aan denken over de vraag welke stappen er precies gezet moeten worden. Is het dan niet goed om eerst de analyse te maken waarover de staatssecretaris het zelf ook heeft? Hebben we met betrekking tot private of semipublieke instellingen, waarover de heer Verhoeven het had, voldoende scherp wat we van hen moeten vragen?

Staatssecretaris **Dijkhoff**:
Volgens mij zit dat voor een deel, voor zover ze daaronder vallen, in de NIB-richtlijn waaraan we werken. Daarin staat wat we van hen gaan vragen en wat voor hen wettelijk verplicht is. Ik wilde niet de indruk wekken dat al die decentrale organisaties, sectorclubs of CERT's er al zijn. Ik wilde meer schetsen hoe ik de rol van het NCSC voor mij zie in relatie tot de samenleving, niet als directe speler die door iedereen gebeld kan worden en het vervolgens regelt, maar meer als een centraal punt.

De heer **Hijink** (SP):
De staatssecretaris zegt dat het NCSC natuurlijk niet 1 miljoen ondernemers of bedrijven gaat ondersteunen met busjes, maar volgens mij wordt dat ook niet voorgesteld. Zowel het Rathenau Instituut als VNO-NCW zegt dat het juist voor het midden- en kleinbedrijf nu ontbreekt aan een concreet aanspreekpunt waar men terechtkan, niet alleen voor informatie maar ook voor ondersteuning tegen aanvallen. Gelukkig worden er niet 1 miljoen bedrijven per dag

aangevallen, maar in extreme gevallen, zoals het eerder genoemde voorbeeld van de Zonnebloem, kan ik mij heel goed voorstellen dat men graag een adviespunt had gehad om naartoe te bellen en te vragen: wat is er aan de hand, kunnen jullie ons helpen en is dit misschien relevant voor andere organisaties of bedrijven? Die bedrijven kunnen in hun eigen ogen op dit moment nergens terecht.

Staatssecretaris **Dijkhoff**:
Ik vind het niet ingewikkeld. Aan de ene kant zou je kunnen zeggen dat zo'n sectorvertegenwoordiger zelf zou kunnen bouwen aan zo'n organisatie, aan zo'n schakelpunt. Zij zullen ook leden hebben die zeggen: dat zijn wij, je kunt ons gewoon bellen, het is ons bedrijf, het is onze corebusiness. Als de mkb'er dan zegt dat hij liever iemand heeft die het regelt zonder dat hij een factuur krijgt, wordt het ingewikkeld. Aan de andere kant wil je er duidelijkheid over scheppen wie betrouwbare partners zijn als je in de problemen zitten; je heb dus geen behoefte aan mensen die misbruik willen maken van het feit dat je daar al in zit. In die informatievoorziening kunnen we een stap zetten. We zijn al met het NCSC bezig om te bezien hoe we daar beweging in kunnen brengen, zodat je dat per sector hebt. Dat hoeft niet per se strikt gescheiden te zijn, maar het gaat erom hoe we ervoor kunnen zorgen dat het meer opkomt vanuit de samenleving. Dat is beter dan dat we nu zeggen: bel allemaal het NCSC maar. Dan mis je juist weer de focus op de kritieke en vitale infrastructuur, en dan verwatert het.

De **voorzitter**:
Mijnheer Hijink, heel kort.

De heer **Hijink** (SP):
Volgens mij hoeft dat elkaar niet te bijten. Je hebt nu een plek waar alle kennis en techniek voorhanden is. Waarom zou je er dan voor kiezen om al die ondernemers en maatschappelijke organisaties die nu geen aanspreekpunt hebben, zelf allemaal het wiel te laten uitvinden? Dat lijkt mij de omgekeerde volgorde. Er is een plek waar de kennis zit. Benut die dan ook.

Staatssecretaris **Dijkhoff**:
Er zijn meer plekken. Die mensen hoeven echt het wiel niet uit te vinden, maar ze kunnen niet allemaal in de NCSC-auto rijden. Dat is een beetje het beeld. Wij willen dus graag die kennis uitbreiden en delen, zodat zij op een ander punt beschikbaar is. Dat punt kan dan nog steeds met het NCSC schakelen als het een moeilijke zaak betreft of als men denkt dat het grote repercussies heeft voor de vitale infrastructuur. Maar als we morgen het NCSC openstellen als callcenter voor iedereen met een computerprobleem, dan komen we niet meer toe aan de kerntaak. Daarin zul je dus een slimmere verhouding moeten vinden.

De heer **Verhoeven** (D66):
Met begrip voor de manier waarop de staatssecretaris de voorstellen probeert te pareren om de NCSC een iets actievere rol te geven. Hij zegt de hele tijd "'busjes"' en "'callcenter"'. Volgens mij wil niemand busjes en een callcenter. Volgens mij willen we dat er iets meer ruimte komt voor een iets proactievere rol voor het NSCS dan nu het geval is. Dat is in het verleden lastig gebleken, want het kabinet vond en vindt dat het aan de ziekenhuizen zelf was. Wij zijn niet op zoek naar een supergroot kantoor, met busjes en een callcenter, waar iedereen naartoe kan om gratis zijn probleem op te laten lossen, maar we zijn op zoek naar een wat actievere rol voor die heel goed geëquipeerde organisatie. Daar moet toch iets te regelen zijn? Daar kunnen we toch een stap in zetten?

Staatssecretaris **Dijkhoff**:
Ik schets wat in mijn ogen het gevolg is als het NCSC vanaf nu het aanspreekpunt voor het mkb en iedereen in de medische sector zou zijn. Ik zeg niet dat de Kamer wil dat ik busjes aanschaf en een callcenter inricht, maar mijn idee is dat dat het gevolg zal zijn als je het nu zomaar openstelt. Ik wil juist dat het NCSC de opgebouwde kennis maar ook kennis over hoe je dat goed inricht, breder kan delen. Daarom is het NCSC constant actief op zoek in de samenleving naar partners om dat gestalte te geven en zeer actief in het aanjagen van initiatieven daartoe. Aan ons, aan het NCSC en de initiatieven zal dat niet liggen. Het is zaak om ze nu goed bij elkaar te brengen.

De heer **Verhoeven** (D66):
Bij het mkb is het ook weer anders; dat zijn honderdduizenden bedrijven. Bij de ziekenhuizen speelt het al langer. De ziekenhuissector is overzichtelijker in aantal en heeft een grotere overheidscomponent; dit is toch meer semioverheid, hoewel er natuurlijk ook private ziekenhuizen zijn. Hoe zit het met dat soort organisaties? Als de staatssecretaris vindt dat het NCSC daarin ook geen al te grote rol moet spelen, dan roept dat bij mij de vraag op waarom het NCSC dan überhaupt is opgericht. Hoe zit het dan met die pakweg 150 ziekenhuizen in Nederland? Ik hoor mevrouw Bruins Slot zeggen dat het er minder zijn, ongeveer 95.

Staatssecretaris **Dijkhoff**:
We moeten ervoor waken dat we door mijn terughoudendheid en het enthousiasme van de Kamer door die wisselende, op elkaar inwerkende stemmingen een onderscheid creëren dat er in die mate niet is. Ik denk dat het slim is als je voor de ziekenhuissector met zijn specifieke infrastructuur en specifieke systemen een medisch CERT hebt dat nauw in contact staat met het NCSC. Het NCSC deelt heel veel informatie met iedereen, in die zin dat het via de website beschikbare en openbare informatie is. Ik denk dat het NCSC in zo'n gelaagde, genetwerkte structuur zeker een grote rol speelt met een specialistische tak ertussen die niet alleen maar uit overheid bestaat. Dan wordt het op termijn wel een heel grote NCSC. Op die manier ontneem je de sector de broodnodige eigen verantwoordelijkheid. De sector moet daarin investeren en daaraan deelnemen.

De **voorzitter**:
U vervolgt uw betoog.

Staatssecretaris **Dijkhoff**:
Mevrouw Bruins Slot vroeg wanneer het NIB komt. Dat gaat binnen enkele weken in consultatie en komt daarna naar de Tweede Kamer.

Dan was er een vraag over het initiatief CyberSecurityKeten.NL. Ik juich dat in algemene zin toe. Het is in dit geval een aantal dienstverleners gelukt om zichzelf bekender te maken en te zeggen: wij zijn hier en dit is ons doel. Dat vind ik goed, want als er bedrijven of andere organisaties zijn die zich afvragen wie er actief zijn in het veld, kan dit helpen. Het is pril. Ik heb me niet hierover kunnen buigen. Ik weet niet of dit iets is waarvan de overheid meteen moet zeggen: dit is het. Het kan een nuttige bijdrage zijn, zeker om aan Nederlandse organisaties en bedrijven die hulp willen bij hun cybersecurity, bekend te maken dat er spelers beschikbaar zijn en dat je daarvan gebruik kunt maken.

Mevrouw Buitenweg vroeg naar de jaarlijkse stresstest die door het Rathenau Instituut is geadviseerd. Ik denk dat dit een heel nuttige functie kan zijn. Ik aarzel wat om die meteen verplicht te stellen namens de overheid. Je hebt dadelijk met de NIB-richtlijn een beveiligingsverplichting in algemene zin. Die kun je op verschillende manieren vormgeven. Ik denk dat deze optie best vaak gekozen zal worden, dus om niet alleen preventieve maatregelen te installeren, maar die ook te testen. Ik denk dat dat in het totaalpakket past. Ik aarzel er wel over om deze specifieke variant, die daar een bijdrage aan kan leveren, verplicht te stellen, omdat eerst de algemene beveiligingsverplichting nog moet worden geïmplementeerd.

Mevrouw **Helder** (PVV):
Ik meen dat de staatssecretaris net antwoord gaf op een vraag van mijn fractie over CyberSecurityKeten.NL. Dat zijn zes bedrijven. Zij willen niet fungeren als vraagbaak voor andere bedrijven. Het gaat erom dat zij de afhankelijkheid van buitenlandse internettechnologie en -kennis terug willen dringen. Ze werken al samen met individuele overheden. Dat was de reden voor mijn vraag of de landelijke overheid er ook iets in ziet.

Staatssecretaris **Dijkhoff**:
Dit is een specifiek initiatief. Ik heb niet alle deelnemende bedrijven kunnen doorlichten. Ik weet niet hoe dat zit. In algemene zin vind ik wel — dat heeft ook een beetje te maken met de discussie over aanbesteding — dat dit een onderdeel moet zijn van hoe wij daarover nadenken. Met wie doen we zaken? Wat is de impact van hun herkomst en misschien zelfs hun klantenportefeuille op de veiligheid als wij met hen in zee gaan? Dat zijn aspecten die meer en toenemend aandacht van ons krijgen.

Mevrouw **Helder** (PVV):
Ik neem voor nu genoegen met dat antwoord. Ik kan mij daar ook wel iets bij voorstellen. Mag ik de staatssecretaris vragen of hij dit te zijner tijd, als er een brief over dit onderwerp komt waar dit in past, mee kan nemen?

Staatssecretaris **Dijkhoff**:
Ja.

De **voorzitter**:
Dat is een toezegging.

Staatssecretaris **Dijkhoff**:
In het verlengde van het onderwerp dat ik net besprak, namelijk de bewustwording van de impact op veiligheid, zijn er vorig jaar extra sessies gehouden voor rijksinkopers. Zij moeten daar aandacht aan besteden. Die sessies worden voortgezet. De minister van Binnenlandse Zaken heeft een handreiking in voorbereiding met een afwegingskader van hoe je dit element bij inkoop en aanbesteding kunt meewegen.

Verder zijn er vragen gesteld over de back-up- en recoverymogelijkheden van diverse ministeries. Nou kan ik mezelf nog een pijnlijke episode herinneren waarin de back-up en de recovery tot ver terug konden gaan, zelfs met niet inmiddels meer geservicete software en hardware; maar het is wel gelukt. In enge zin is het geen cybersecuritymaatregel als het gaat om een maatregel voor nadat het met cybersecurity is misgegaan. Vandaag is er volgens mij nog een motie over aangenomen in deze sfeer. De minister van Binnenlandse Zaken zal u informeren over hoe dit verder wordt opgepakt. Ieder departement is daar zelf verantwoordelijk voor. Ik weet dus niet hoe het zit met de laatste stand van zaken van elk ministerie. Daar zal de minister van Binnenlandse Zaken u over informeren. In bredere zin hebben we vanuit cybersecurityoogpunt in eerdere dreigingsbeelden geadviseerd om niet totaal afhankelijk te worden van back-ups met hetzelfde systeem in je netwerk. Na een netwerkinvasie zijn dan ook je back-ups weg. Clouddiensten zijn wellicht ook niet altijd bereikbaar. Fysieke back-ups zijn de afgelopen jaren dus ook een aandachtspunt geweest.

Hebben wij zelf ethische hackers in dienst? Zeker, in de zin dat wij mensen hebben die de vermogens hebben en daar zeer ethisch mee omgaan. We huren ook andere partijen in om systemen te testen. We voorzien op die manier dus in de behoefte van mensen die de skills hebben en die deze voor het goede willen gebruiken. Zoals u weet stimuleren we, via de richtlijn van het OM, dat mensen met goede bedoelingen, white hat hackers, niet vervolgd worden. Als ze de procedure volgen en het netjes melden kunnen ze erop rekenen dat het gewaardeerd wordt dat ze het doen voor het goede doel, en niet voor eigen gewin of tot schade van iemand anders.

Er is gevraagd of we genoeg overige ICT-expertise kunnen vinden en of de WNT in de weg zit. Tot op heden hebben we geen moeite gehad met werven. Bij de mensen die we tot nu toe hebben aangenomen lijkt de financiële vergoeding ook niet de belangrijkste drijfveer te zijn. Sowieso zal een financiële vergoeding binnen de normen van de wet nooit kunnen concurreren met het gewin dat je met kwaadwillende zaken kunt verkrijgen, vrees ik. Het blijft elke dag hard werken om het adagium "'misdaad loont niet"' te benaderen. De uitdaging van het werk speelt wel een grote rol, net als de voldoening van het kunnen dwarszitten van kwaadwilligen. In die zin is het een spel tussen hackers. Als je voor ons komt werken, speelt los van de financiële vergoeding ook mee of je de bevoegdheden hebt om er echt werk van te kunnen maken en of je vaardigheden niet getemperd worden doordat de wetgeving je niet toestaat om terug te hacken of achter de hackers aan te gaan. Daarom hebben we natuurlijk ook het wetsvoorstel Computercriminaliteit III met uw Kamer behandeld.

De heer Krol heeft gevraagd naar het delen van kennis. Dat is een cruciaal punt. Wij hebben bijvoorbeeld de website

veiliginternetten.nl, met meer dan 1 miljoen hits. Wij besteden er ieder jaar ook aandacht aan in de NL-Alertweken, voor een specifieke doelgroep. Met veel maatschappelijke organisaties en bedrijven doen we hard ons best om ieder jaar weer meer mensen te bereiken en om hen bewust te laten zijn van de gevaren en van de zaken die ze zelf kunnen doen om de gevaren te beperken. Incidenten waarbij het wel fout is gegaan, zoals WannaCry, die de aanleiding vormde voor dit debat, dragen op zijn minst bij aan bewustwording van het probleem. Dat merken we dan ook in de aandacht die er is voor de voorlichting die wij hierover geven.

Mevrouw Kuiken vroeg — dit ligt eigenlijk in het verlengde hiervan — of de mens niet de belangrijkste factor is. Daar heeft ze gelijk in. Daarom besteden we ook zo veel aandacht aan voorlichting. In veel gevallen is de mens de belangrijkste factor. Daarom zetten we heel erg in op bewustwording. Er is een bekend acroniem, namelijk PEBCAC. Dit betekent Problem Exists Between Computer And Chair, oftewel de mens die daar zit. Die maakt vaak de verkeerde keus. Ik denk dat inmiddels iedereen weet dat je niet moet klikken op e-mailtjes met linkjes van Nigeriaanse prinsen. Net nu we iedereen daarvan overtuigd hebben, worden die pogingen echter veel slimmer. Ze komen nu niet meer van een Nigeriaanse prins of van een prins uit een ander land, maar lijken te komen van je collega, met een heel overtuigend mailtje. Dan klik je erop en zit je alsnog in de penarie. Dus ook daarbij blijft voorlichting iets permanents. Het is niet zo dat het dan ophoudt.

De Zorg-CERT is sinds deze week actief. Het NCSC helpt nu om de Zorg-CERT met expertise snel "'up to speed"' te komen. Dus daarin is ook die samenwerking te zien.

Dan kom ik op de vragen over CC III en zero-days. Zo is gevraagd of ik een ander standpunt heb over de WannaCry-episode. Het zal niet heel verrassend zijn, als ik zeg dat het antwoord daarop nee is. De wetsgeschiedenis laat zien dat de wet door het kabinet tussentijds is gewijzigd en aangescherpt op dit punt en later ook nog door de Kamer ten aanzien van de risico's die er bestaan als je een zero-day in stand houdt. Volgens mij ontkent niemand die risico's, maar het is wel een belangenafweging en niet een absolute zaak dat alles moet wijken voor het melden van een zero-day. De wet gaat ook uit van uitstel van een melding en niet van het permanent houden. Daarvoor moeten de criteria nog verder uitgewerkt worden. Dat was ook een vraag: gaat u dat doen? Ja. De criteria die genoemd worden vanuit het NSA-voorbeeld waren vrij algemeen en ook zoals we ze hier gewisseld hebben. Wat is de impact? Is het een veel voorkomend systeem waar de zero-day in gevonden wordt? Ik zou het niet zo zwart-wil willen maken, in de zin van "'het mag nooit gebeuren"', net zoals de wet nu niet toestaat: als de politie het niet wil melden, hoeft het niet. Het gaat om uitstel, dat slechts verkregen kan worden na een zorgvuldige procedure met een belangenafweging. Een kwetsbaarheid zoals deze, zou niet door de toets kunnen komen, omdat dit een systeem is dat zo veel gebruikt is en waarvan zo veel vitale zaken afhankelijk zijn, dat het belang bijna ondenkbaar is dat je het langer dan een uurtje openhoudt binnen de kaders die we hebben meegegeven. Aan de hele andere kant van het spectrum bestaan er natuurlijk criminele of terroristische organisaties, met name netwerken die zich vooral met onlinecriminaliteit of het uitwisselen van zaken bezighouden en die een eigen infrastructuur gebouwd hebben. Daarvan weet je eigenlijk: hier maakt niemand gebruik van, behalve de leden van zo'n netwerk. Mocht je daar dan al inkomen, wat wellicht met hun kennisexpertise vrij moeilijk is, dan is de enige die je moet bellen om de kwetsbaarheid te melden, degene die je probeert op te sporen. Daarom wil ik het dus ook niet zo absoluut maken en vind ik het een weging. Hoe wijdverbreider het product is waar de zero-day in zit en hoe meer vitale infrastructuur daarop rust, hoe kleiner, miniemer of tot nul de kans is dat je onder de wetgeving van CC III uitstel van melding kunt verkrijgen. Dus ik denk dat we hiervoor een zorgvuldige procedure hebben ingebouwd die stand houdt en waar ik ook volledig achtersta. Ik erken daarbij dat het openhouden van zero-days nooit goed is, maar dat het ten opzichte van andere belangen soms nodig is om tijdelijk te wijken teneinde een hoger doel te dienen.

De **voorzitter**:
De heer Verhoeven sluipt naar de microfoon. Ik kijk hem wel even indringend aan met het verzoek om niet een heel nieuw debat te voeren over de Wet computercriminaliteit III, want dat gaat de Eerste Kamer doen.

De heer **Verhoeven** (D66):
Dank u wel, voorzitter, voor de ruimte die u mij biedt op deze avond. Ik zal het echt proberen kort te doen in een serie van interrupties en dan ben ik klaar. De staatssecretaris heeft gezegd dat het niet uit te sluiten is dat de overheid hacksoftware gaat kopen bij bedrijven met daarin die kwetsbaarheden die het mogelijk maken om op basis daarvan te kunnen inbreken op smartphones, computers enz. Is het niet zo dat het bij dit soort software onmogelijk is dat de overheid dat meldt, omdat conform het businessmodel van die bedrijven je die kwetsbaarheid helemaal niet kan melden omdat je die niet kent of omdat je die niet mag melden omdat in het contract staat dat het niet mag? Oftewel: dan sluit je toch de weg af om als overheid het zo te doen als de staatssecretaris zegt?

Staatssecretaris **Dijkhoff**:
Met deze complicatie die de heer Verhoeven noemt, sluit je de weg niet af, omdat die weg speciaal ingericht is voor zero-days waar de politie zelf kennis van krijgt tijdens onderzoek. Daar stuit je op, daar stuiten onze eigen hackers op. Daar is die hele procedure voor. Vervolgens heb je dan nog het dilemma van het aankopen van hackingtools die gebruikmaken van kwetsbaarheden die je als aankoper niet kent. Daarbij loop je dus het risico om je net gedane dure aankoop zelf bij wijze van spreken de volgende dag al nutteloos te maken, doordat je toevallig zelf ook die zero-day ontdekt en hem dan meldt. Dat zal kunnen voorkomen. Het kan ook zijn dat ze bij de dienst vloeken op de politie, omdat die zo knap was om een zero-day te vinden, die gemeld is.

De heer **Verhoeven** (D66):
Dit was dus waar het met name aan het eind van het debat destijds over ging. Ik zal het niet helemaal herhalen, maar dan hebben we dus de situatie en kunnen we praten over de zorgvuldigheid, de waarborgen, over het feit dat het keurig is, dat het allemaal goed geregeld is. Maar deze weg, die de staatssecretaris niet heeft willen afsluiten en nog steeds niet afsluit, maakt het dus gewoon mogelijk dat je

software met kwetsbaarheden koopt, waarvan je als overheid gewoon weet dat je ze nooit zult kunnen melden.

Staatssecretaris **Dijkhoff**:
Tot op dit punt vind ik het nog steeds een kalme discussie die we ook voeren. Alleen hierna zal dan altijd de conclusie getrokken worden. En dan wordt die ene mogelijkheid verabsoluteerd en wordt er tegen die windmolen gevochten. Je weet ook niet welke kwetsbaarheden het zijn. Dat klopt. Maar als je ze niet koopt, weet je dat ook niet. Daar wordt het ook niet veiliger van. Als je ze niet koopt, dan zijn ze er ook nog. Dan heeft een ander ze. En dan kun je ze én niet gebruiken én ook niet melden. Het is niet zo dat je kwetsbaarheden in één keer, door ze te kopen, uitsluit van melding. Immers, als je nog steeds achterhaalt op de manier zoals ik net omschreef, dan zul je ze melden en dan zul je dus ontdekken dat die tool die je net gekocht hebt, het niet meer doet.

De **voorzitter**:
Mijnheer Verhoeven, een korte slotopmerking.

De heer **Verhoeven** (D66):
We hebben over deze wet zo lang gepraat, omdat mijn fractie bezorgd was over het openlaten van bepaalde mogelijkheden die in de praktijk tot grote problemen zouden kunnen leiden. En WannaCry is nou juist een voorbeeld van een groot probleem dat in de praktijk heeft plaatsgevonden. Dan kan de staatssecretaris zeggen: dat is het verabsoluteren van een hypothetische situatie. Maar hij zegt ook dat die kwetsbaarheden blijven bestaan. Maar er is toch wel een verschil of de overheid eraan mee moet werken om een markt voor kwetsbaarheden levend te houden door ze in te kopen en ze vervolgens niet te kunnen melden? Dat is toch wel een extra rol voor de overheid die je toch dubieus kunt noemen? Je zou toch moeten nadenken over de vraag of je als overheid de zwarte markt voor softwarekwetsbaarheden wilt stimuleren op een manier zoals de staatssecretaris nu heel luchtig schetst? Ik vind dat nogal wat, eerlijk gezegd.

Staatssecretaris **Dijkhoff**:
Er zijn twee zaken. De heer Verhoeven wekt door het gebruik van het woord "'openlaten"' de indruk dat door de andere keuze te maken, ze dichtgaan. En als dat zo was, dan zou je een andere afweging kunnen maken. Maar hier is het niet zo. Ieder voorbeeld gaat mank, dus dit ook. Er zijn heel veel dingen dual use. Die kun je voor het goede gebruiken en voor het slechte. Er zijn ook heel veel dingen waarvan we de hele samenleving verbieden om ze te doen, maar waar we de overheid als enige het monopolie op geven. We hebben in dat debat ook gewisseld dat als je de enige bent waardoor die industrie bestaat, je door ermee te stoppen ervoor kunt zorgen dat het niet meer gebeurt. In dit geval is het helaas zo dat ze verkocht worden en dat die markt er is. En die verdwijnt niet. En die stimuleer je ook niet door als Nederland in één keer te zeggen: wij stoppen ermee. Dan heb je dus de keus. Je kunt die kwetsbaarheid die je niet kunt dichten, negeren. Of je kunt die kwetsbaarheid die je niet kunt dichten, gebruiken door het aanschaffen van die tools. Het is niet zo dat door het niet meer te kopen, je ze zou kunnen gaan dichten, het probleem verhelpt en de boel veiliger maakt. Omdat we niet weet welke kwetsbaarheden het zijn, kunnen we gelukkig ook geen lijstje maken met dingen waarvan we zeggen: als we die toevallig zelf eens vinden, dan melden we ze lekker niet. Zo werkt het niet. Dan moet je ze gewoon melden en help je je eigen tool om zeep. En daar wordt het veiliger van.

De heer **Hijink** (SP):
Wat uit dit korte debat blijkt, is dat de manier waarop de overheid hiermee omgaat, cruciaal is voor de veiligheid op het internet. Als de overheid handelt, koopt en stimuleert, gaan hackers — goedwillend en kwaadwillend — wel degelijk op zoek naar deze fouten. Het is natuurlijk zo dat dit soort aanvallen vaker zullen plaatsvinden. En dus heb je veiligheidsdiensten en de overheid nodig, die ervoor zorgen dat we gaten dichten in plaats van ze open te houden, omdat het ons af en toe uitkomt om ook ergens naar binnen te kunnen komen. Mijn vraag gaat over WannaCry. De staatssecretaris zegt heel makkelijk dat het in ons geval zeker ervoor gezorgd had dat het eerder gemeld was en dus gedicht werd. Maar als dat klopt, waarom heeft dan bijvoorbeeld de NSA zo dankbaar gebruikgemaakt van deze kwetsbaarheid en heeft die waarschijnlijk nog een mand vol soortgelijke kwetsbaarheden die tot op de dag van vandaag nog niet gedicht zijn?

Staatssecretaris **Dijkhoff**:
In de hypothese dat het de NSA was, want ik kan minder makkelijk speculeren, is het simpele antwoord: omdat die niet onder CC III valt. Die valt niet onder het afwegingskader van de Nederlandse rechter-commissaris en het Nederlandse OM. Wetgeving die voor Nederland geldt, gaat niet ineens voor de Amerikaanse NSA gelden. Nogmaals, het is allemaal heel ingewikkeld. Het standpunt is dat wij veiliger af zijn als de kwetsbaarheid gedicht is. Dat is ook het uitgangspunt. Vervolgens krijg je de wollerige werkelijkheid dat je ze niet dicht kunt wensen en dat het niet kopen van die dingen ook niet ervoor zorgt dat ze dichtgaan. Ons standpunt is dat je ze meldt, tenzij andere belangen daartegen opwegen. Dan kun je de melding uitstellen. Uiteindelijk meld je ook de kwetsbaarheid waarvan je zegt dat de gevolgen voor de samenleving van die kwetsbaarheid klein zijn. Is het opsporingsbelang groot, dan kun je als de rechter-commissaris daar toestemming voor geeft en je de kwetsbaarheid hebt gevonden, uitstel van melding krijgen. Zo hebben wij de wet ingericht. Ik snap wel het ongemak van het kopen van het product dat ook gekocht wordt door anderen die daar kwaad mee willen. Dat klopt. Ik heb ook een hekel aan pistolen, andere wapens en geweren. Die worden ook gekocht door kwaadwillenden, maar ik rust de politie en het leger er wel mee uit. En het is niet zo dat door ze niet meer te kopen, ze niet meer gemaakt worden. Als je als Nederland ervoor kon zorgen dat er niet meer gehandeld wordt in zero-days door ze niet te kopen, vind ik dat een andere afweging.

De **voorzitter**:
De heer Hijink tot slot.

De heer **Hijink** (SP):
Die vergelijking gaat echt totaal mank, maar vooruit.

Staatssecretaris **Dijkhoff**:
Hij komt u niet uit. Dat is fijn, maar ...

De heer **Hijink** (SP):
Als het gaat om ...

De **voorzitter**:
Heren, de heer Hijink en dan de staatssecretaris tot slot.

De heer **Hijink** (SP):
De staatssecretaris gaat er wel heel makkelijk van uit dat de Nederlandse diensten een andere afweging zouden maken dan de Amerikaanse. Die kunnen natuurlijk heel veel profijt hebben van achterdeurtjes in software, omdat zij dan makkelijker naar binnen kunnen voor spionage of voor terrorismebestrijding of voor criminaliteitsbestrijding. Dat begrijp ik wel. Maar als dat betekent dat al die tijd dat achterdeurtje ook openstaat voor al die kwaadwillenden, vergroten wij dus de kans op aanvallen zoals wij met WannaCry hebben gezien. Het is een kwestie van tijd voordat er nog zo'n aanval komt. Dan is dus niet uit te sluiten dat een dergelijke aanval komt door een achterdeurtje waarvan onze diensten of de Amerikaanse diensten allang weten dat die openstaat, en dat dus allang gedicht had kunnen worden. Dat risico neemt u en dat is een gevaar voor de veiligheid op het internet.

Staatssecretaris **Dijkhoff**:
Dit is dus die verabsolutering of ketenredenering, die door het woordje "'absoluut"' en "'natuurlijk"' er vaak in te zetten aan kracht zou moeten winnen, terwijl die dat niet doet. Ten eerste gaat de Wet computercriminaliteit III niet over diensten. Het hele afwegingskader waarover ik het net had, gaat niet over de veiligheidsdiensten. Dat is een andere wet. Die wordt op een andere plek behandeld, met andere afwegingen. Door te zeggen "'Nederlandse diensten of de NSA"' gooi je er een paar op een hoop die onder verschillende regimes werken.

Wij hebben er belang bij dat een kwetsbaarheid gedicht wordt, als het een kwetsbaarheid is die wijdverbreid gebruikt wordt, ook bij goedwillende burgers. Dus bij een kwetsbaarheid in een systeem dat wijdverspreid is en/of vitale infrastructuur ondersteunt, ligt de lat wel heel hoog — misschien is het theoretisch dat je er overheen kunt — om te zeggen dat je in het opsporingsonderzoek van de rechter-commissaris toestemming krijgt om die niet te melden. Je hebt echter ook systemen die niet zo wijdverspreid zijn, zoals ik al eerder aangaf, systemen die ontworpen zijn en alleen maar gebruikt worden in een kleine kring, waar geen tot weinig goedwillend gebruik van wordt gemaakt. Als dan al in wetgeving staat dat een kwetsbaarheid een kwetsbaarheid is en dat we dat nooit gaan melden, onder geen enkele voorwaarde, sluit je ook de weg af om daarop door te kunnen gaan. Vervolgens wil je ook nog eens mensen kunnen pakken die in die kwetsbaarheden handelen of daarvan misbruik hebben gemaakt voor kwade doeleinden. Je kunt niet aan de ene kant zeggen dat je die kwaadwillenden wilt pakken, erachteraan wilt gaan en wilt terughacken, en aan de andere kant zeggen dat je niet wilt dat de overheid de bevoegdheden heeft om dat te kunnen doen. Ik ga overigens nergens makkelijk van uit. Ik ga er juist van uit dat het allemaal enorm moeilijke afwegingen zijn, die je niet zwart-wit kunt schetsen en vooraf heel makkelijk in absolute zin kunt beantwoorden. Daarvoor heb je een afwegingskader nodig. Dat hebben wij gemaakt. Dat moet je in de praktijk hanteren om de balans te krijgen tussen veiligheid in brede zin aan de ene kant en aan de andere kant veiligheid in het opsporingsbelang.

De **voorzitter**:
Dank u wel. Zijn er nog vragen van de Kamer die u niet hebt beantwoord?

Staatssecretaris **Dijkhoff**:
Er staat nog één vraag open. Die vraag gaat over de opsporingscapaciteit, de beschikbare mensen en middelen. Ik kan u melden dat we ook investeren in de digitale opsporing. Er werken nu 120 fte's bij het Team High Tech Crime Er gebeurt een en ander in de opbouw van het cyberteam maar ook in elke regionale eenheid van de politie. Dat is wat we nu doen. Ik kan niet zeggen dat dit genoeg is. Het zal blijvende aandacht krijgen, ook in de komende jaren. Die kennis en kunde zullen verder worden ontwikkeld, omdat ook de digitale wereld zich blijft ontwikkelen. Dat is wat we tot nu toe hebben gedaan, maar daarmee zeg ik niet dat het voor de komende jaren afdoende is.

De **voorzitter**:
Ik denk dat de vraag van mevrouw Kuiken over de nationale politie nog niet beantwoord is.

Mevrouw **Kuiken** (PvdA):
Dat is waar. Krijgen we nog een update — de staatssecretaris gaf namelijk een half antwoord — en komt het nog specifiek terug? Dan gaat het over de vraag of de plek binnen de nationale politie en de veranderingen die de heer Akerboom zelf heeft aangekondigd, niet nodig zijn. Dat lijkt mij ook voor een nieuw kabinet relevant. Daarnaast had ik een vraag gesteld over de aanbesteding van de nationale telecommunicatie.

Staatssecretaris **Dijkhoff**:
Daar ben ik op ingegaan. Dan gaat het om de aandacht die de minister van Binnenlandse Zaken daaraan heeft besteed bij de inkopers. Die aandacht is toegenomen. Ik heb gezegd dat dit een rol moet spelen, dat het een punt van aandacht is bij de inkoop en dat ook in de aanbesteding bekeken wordt of het beter verankerd kan worden. Ik heb daar nog iets anders over gezegd. Ik heb niet onthouden wat ik allemaal heb gezegd. Maar goed, ik heb het nodige hierover gezegd in mijn antwoord.

De **voorzitter**:
Ik heb het ook als antwoord genoteerd.

Ik kijk naar de Kamer. Is er behoefte aan een tweede termijn? Dat is het geval. De spreektijd is maximaal één minuut.

De heer **Hijink** (SP):
Voorzitter. Ik had vanavond niet de illusie dat wij in één keer, in een paar uur tijd de hele problematiek van ransomware en dergelijke zouden oplossen, maar ik had wel gehoopt dat we wat concrete stappen zouden kunnen zetten. Ik bemerk dat nog niet helemaal bij de staatssecretaris. Daarom dien ik drie moties in.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de digitale veiligheid van burgers in het geding is door cybercriminaliteit en -spionage;

constaterende dat de kennis over cybersecurity op dit moment bij veel bedrijven nog tekortschiet maar dat ook de systemen en data van bedrijven en instellingen buiten de vitale sectoren bescherming verdienen;

verzoekt de regering, onder de vleugels van het Nationaal Cyber Security Centrum een digital trust centre op te richten dat bedrijven en maatschappelijke instellingen informeert, adviseert én concrete hulp en ondersteuning biedt over het verbeteren van hun cybersecurity en bij het afslaan van aanvallen door hackers,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Hijink. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 465 (26643).

Haalt u rustig adem, mijnheer Hijink. We gaan het niet afraffelen. U mag …

De heer **Hijink** (SP):
Ik zie dat ik nog zestien seconden heb. Dan denk ik: dat lukt nooit.

De **voorzitter**:
Ik begrijp het, maar we willen u ook kunnen verstaan. Leest u de motie dus rustig voor.

De heer **Hijink** (SP):
Ik dien de volgende motie in.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat veel hacks en cyberaanvallen voorkomen en beperkt kunnen worden als bedrijven, burgers en de overheid gebruikmaken van de meeste recente updates van hun software;

verzoekt de regering, te onderzoeken hoe de kennis over de noodzaak van updaten bij bedrijven, burgers en de overheid kan worden vergroot en hoe de zorgplicht van ontwikkelaars van software kan worden uitgebreid zodat burgers, bedrijven en de overheid die met oudere software werken geen cruciale veiligheidsupdates mislopen,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 466 (26643).

De heer **Hijink** (SP):
De volgende motie is de laatste motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de ontwikkeling van het "'internet of things"' heeft geleid tot een verdere toestroom van slecht beveiligde apparaten bij bedrijven en burgers;

constaterende dat niemand zit te wachten op een massale cyberaanval via gehackte waterkokers of koelkasten;

verzoekt de regering, te onderzoeken welke minimale veiligheidseisen aan dergelijke apparatuur kan worden gesteld, hoe deze eisen kunnen worden afgedwongen en welke overige maatregelen nodig zijn om consumenten te beschermen tegen slecht beveiligde apparatuur,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 467 (26643).

Mevrouw **Helder** (PVV):
Voorzitter. Er zijn drie vragen van mijn fractie onbeantwoord gebleven, maar ik dacht: laat ik er een samenhangend geheel van maken. Ik heb gevraagd naar een concreet actieplan en dat was bedoeld om dreigingen en aanvallen tegen te gaan of op te treden als een dergelijk incident zich heeft voorgedaan. Ik heb gezegd: cyberveiligheid is van groot belang voor de nationale veiligheid. In dat kader vroeg ik een concreet actieplan van de staatssecretaris. Daar hangt mee samen dat ik de vraag had gesteld wat de staatssecretaris vindt van het voorstel van Fox-IT over een cybercommissaris. Dat is een commissaris voor de beveiliging van

de digitale infrastructuur. De staatssecretaris had het over een soort overkoepelende minister, maar die bedoelde ik dus niet. Ik bedoelde echt een persoon die digitale dreigingen moet tegengaan. Mijn derde vraag was of de aansprakelijkheidswetgeving nog wel afdoende is. De staatssecretaris heeft het gehad over de conformiteitsplicht, maar conformiteit is gewoon dat je als koper ervan mag uitgaan dat het gekochte voldoet aan de eisen voor normaal gebruik. Volgens mij ging dat toch een beetje voorbij aan mijn vraag, dus daar hoor ik graag nog een reactie op.

Mevrouw **Bruins Slot** (CDA):
Voorzitter. Ik wil de staatssecretaris bedanken voor zijn antwoorden. Als we terugkijken naar de effecten van de ransomware-aanval in Groot-Brittannië, dan zagen we inderdaad dat operaties in ziekenhuizen stillagen, met alle nadelige gevolgen daarvan. Daarom is het ook goed nieuws dat de staatssecretaris zegt: de zorg is inmiddels begonnen met een computer emergency response team. Dat gebeurde deze week, eindelijk, nadat in januari 2016 voor het eerst het voornemen is besproken. Dan wil ik toch nog een vraag stellen over de rol die het Nationaal Cyber Security Centrum daarin heeft. Is gegarandeerd dat alle ziekenhuizen en zorginstellingen zich ook gaan aansluiten bij die CERT, zoals die wordt genoemd? Gaat die er uiteindelijk voor zorgen dat iedereen de verstandige maatregelen gaat nemen die geadviseerd worden? En als dat niet gebeurt, welke rol heeft dan het Nationaal Cyber Security Centrum?

Mijn laatste vraag betreft de komst van de implementatie van de Netwerk- en informatiebeveiligingsrichtlijn. De staatssecretaris geeft aan dat die nu in consultatie gaat. Betekent dit nog steeds dat we in het najaar de wet kunnen verwachten? Daarachter zit een vraag waar ik nog geen antwoord op heb gehoord, namelijk dat daarna een aantal stevige maatregelen genomen moet worden om aan die richtlijn te kunnen voldoen. Wat is daarvan eigenlijk de invoeringstermijn?

De heer **Verhoeven** (D66):
Voorzitter. Dank aan de staatssecretaris. Zijn beantwoording was op de laatste vijf minuten na heel volledig. Ik vond het wel jammer dat er, toen het ging over het cruciale punt waar we de komende tijd nog verder over zullen praten, toch ook wel iets van debatvaardigheid en spiegelredenering in sloop om zijn stelling overeind te houden, terwijl ik het gevoel had dat toch wel duidelijk werd dat de overheid wel degelijk mee gaat werken aan het stimuleren van een toch wat donkere markt. Daar maakt mijn fractie zich zorgen over. Dat vind ik jammer. Voor de rest veel dank.

Ik dien twee moties in, die ik natuurlijk niet afraffel.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de CTIVD heeft vastgesteld dat de werkwijze en de relevante afwegingen voor het al dan niet melden van onbekende kwetsbaarheden intern niet zijn uitgewerkt en vastgelegd;

verzoekt de regering, een duidelijk afwegingskader op te stellen voor de inlichtingendiensten, de politie en andere overheidsdiensten aangaande de werkwijze en de relevante afwegingen voor het al dan niet melden van onbekende kwetsbaarheden,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Verhoeven. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 468 (26643).

De heer **Verhoeven** (D66):
Mijn tweede motie luidt als volgt.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de WannaCry-ransomware-aanval in het Verenigd Koninkrijk tot gevolg had dat talloze patiënten geen behandeling konden krijgen;

constaterende dat ook Nederlandse ziekenhuizen regelmatig getroffen worden door ransomware-aanvallen;

verzoekt de regering, het Nationaal Cyber Security Centrum het mandaat te geven om actief (semi-)publieke instellingen, zoals ziekenhuizen, te helpen om hun cybersecurity op orde te krijgen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Verhoeven, Hijink, Buitenweg en Krol. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 469 (26643).

De heer **Krol** (50PLUS):
Voorzitter. Dank aan de staatssecretaris. Kortheidshalve één motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat digitale veiligheid een essentieel onderdeel is van maatschappelijke veiligheid;

verzoekt de regering, materieel en immaterieel te investeren in het proactief delen van kennis om zo de samenleving structureel bewuster en weerbaarder te maken inzake digitale veiligheid,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Krol. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 470 (26643).

Mevrouw **Tellegen** (VVD):
Voorzitter. Ik dank de staatssecretaris voor zijn beantwoording. Ik sluit mij aan bij de vraag die ook ik had gesteld over de digicommissaris. De staatssecretaris heeft daar het nodige over gezegd, maar niet over de functie zelf.

Ik heb nog twee punten. Als eerste de rol van het NCSC. Zoals ik de staatssecretaris heb begrepen, is dat een aanjaagfunctie. Maar in welke richting is dat dan? We hebben enerzijds de vitale infrastructuur en anderzijds het mkb en het bedrijfsleven. Ik zoek in de beantwoording van de staatssecretaris naar wat hij voor zich ziet. Ik zie het risico van het te veel optuigen van die club. Maar anderzijds hebben we met zijn allen door dat er veel aan de hand is en dat we de vitale infrastructuur willen ondersteunen. Datzelfde geldt voor het mkb. Ik wil de staatssecretaris dus vragen om nog iets specifieker in te gaan op de vraag hoe de verhouding ligt.

Tot slot nog een vraag over die veilige producten en ICT-leveranciers. Dank voor de beantwoording op dit punt. We wachten op de roadmap. Het gaat de VVD er vooral om dat er duidelijk wordt afgesproken welke verantwoordelijkheden door wie worden gedragen, namelijk producent en/of de gebruiker.

De heer **Verhoeven** (D66):
Ik heb in eerste termijn geen vragen aan de VVD gesteld omdat het eigenlijk al met het CDA besproken was. Maar toen zei mevrouw Tellegen in een interruptie bij mevrouw Buitenweg heel veel over dat het in de wet allemaal goed geregeld is, dat het zorgvuldig is en dat er waarborgen zijn en allemaal rechtsregels. Mijn punt is nou juist steeds geweest dat een aantal zaken waarvan de intentie ongetwijfeld goed zal zijn, ook bij de VVD-fractie, juist niet goed geregeld is in de wet. Is de VVD bereid om in de toekomst, ook al omdat de behandeling van de wet nog loopt in de Eerste Kamer, er nog eens goed naar te kijken om zo een aantal gaten dat nog in de wet zit alsnog te dichten?

Mevrouw **Tellegen** (VVD):
Ik heb de heer Verhoeven net heel opgewekt horen betogen dat we in de Tweede Kamer niet gaan over wat ze in de Eerste Kamer doen, dus ik zou heel flauw kunnen zijn en zeggen: mijnheer Verhoeven, de VVD-fractie gaat in de Eerste Kamer over haar eigen afweging. Dat adviseer ik haar ook ten zeerste. Maar mijn standpunt is helder. Ik vind dat we hier een zuivere afweging hebben gemaakt en ik kom daar dus ook niet op terug.

De **voorzitter**:
En die gaan we ook niet herhalen.

Mevrouw **Buitenweg** (GroenLinks):
Voorzitter. Ik wil allereerst de staatssecretaris een welgemeend compliment maken. Hij maakt de kans dat er negatieve effecten zijn van het kopen van zero-days wel heel erg klein. Ik hoop natuurlijk van harte dat hij gelijk heeft. Maar goed, de tijd zal het leren nadat het wetsvoorstel is aangenomen.

Ik heb op een ander punt een motie, namelijk over de stresstesten. Ik heb de staatssecretaris horen zeggen dat hij die niet jaarlijks wil, maar ook dat hij er wel de noodzaak van inziet. Vandaar mijn motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat ernaar gestreefd moet worden om de vitale ICT-infrastructuur maximaal weerbaar te houden en dat een jaarlijkse stresstest daartoe een goed middel is;

verzoekt de regering, samen met de betrokken bedrijven en beheerders te voorzien in een jaarlijkse test waarin de beveiliging van de vitale ICT-infrastructuur tegen hacks wordt beproefd, en de Kamer hierover te informeren,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 471 (26643).

Mevrouw Kuiken ziet af van een inbreng in tweede termijn. De staatssecretaris heeft nog niet alle moties gekregen. Ik schors daarom even.

De vergadering wordt van 21.38 uur tot 21.46 uur geschorst.

De **voorzitter**:
De staatssecretaris heeft alle moties ontvangen en kan ze van een advies voorzien.

Staatssecretaris **Dijkhoff**:
Voorzitter. Ik begin met de moties en zal daarna ingaan op een aantal gestelde vragen.

De motie van de heer Hijink op stuk nr. 465 vraagt om een digital trust centre. Ik ben er helemaal voor dat er zo'n centrum komt en het NCSC wil het graag stimuleren, maar de motie heeft het over "'onder de vleugels"'. Dan wordt het een hiërarchie en krijgt het centrum een organisatorische inkleuring waarvan ik niet zeker weet of het de meest

optimale is. Daarom wil ik de motie in deze vorm ontraden, maar daar zeg ik wel bij dat wij nog steeds actief werken aan dit centrum of iets soortgelijks, in bredere zin.

De heer **Hijink** (SP):
Misschien begrijpen we elkaar dan verkeerd; dat zou jammer zijn. Ik heb het bewust "'onder de vleugels"' genoemd om de staatssecretaris enige ruimte te geven in de manier waarop het gebeurt. Voor mij hoeft het niet per se rechtstreeks onderdeel van het Nationaal Cyber Security Centrum te worden. Het kan ook een andere variant zijn. Als de staatssecretaris wil dat ik de motie met een paar woorden net iets anders formuleer, ben ik daar best toe bereid.

Staatssecretaris **Dijkhoff**:
Ik wil gewoon graag dat er organisaties ontstaan waarmee het NCSC een partnerschap aan kan gaan. We stimuleren ook dat ze ontstaan, dus het is niet alleen maar wachten en hopen. Maar die organisaties hoeven voor mij geen overheidsorganisaties te zijn, zeker niet in deze hoek. Ik benut liever het momentum om dit samen met maatschappelijke partners te organiseren dan dat ik zeg: hoe ze zich ook opstellen, we moeten zorgen dat er zo'n centrum komt. Dat kan ook nog eens in de weg gaan zitten bij de manier waarop de partners zich opstellen bij het verwezenlijken van dit doel, terwijl je het gezamenlijk wilt financieren en mogelijk maken. Daarom blijf ik de motie ontraden.

De motie op stuk nr. 466 wil dat we onderzoeken hoe de kennis kan worden vergroot. Ik mis even wat die motie toevoegt, want dit is gewoon onderdeel van het werk dat we doen, ook via Alert Online. In die zin vind ik de motie overbodig. Daarom ontraad ik die ook.

De motie op stuk nr. 467 zie ik als ondersteuning van beleid. Daarover laat ik het oordeel aan de Kamer. Er loopt een onderzoek hiernaar bij het ministerie van Economische Zaken. Ik zal mijn collega vragen om de Kamer na afronding van het onderzoek hierover te informeren.

De motie op stuk nr. 468 van de heer Verhoeven is op het vlak van de diensten al overgenomen in een brief aan uw Kamer. In de zero-daybrief hebben we voor de politie een vergelijkbaar kader geschetst. Bij de behandeling van de Wet computercriminaliteit III hebben we aangegeven in welke situatie welke afwegingen spelen. In mijn ogen hebben we dus al invulling gegeven aan deze motie. Het wordt misschien een beetje ingewikkeld als ik zeg dat dit met terugwerkende kracht ondersteuning van beleid is. Ik denk dat de heer Verhoeven toch verwacht dat er weer iets nieuws komt. Daarom zal ik de motie ontraden.

De **voorzitter**:
De heer Verhoeven geeft duidelijkheid.

De heer **Verhoeven** (D66):
Als er echt al een kader is, wil ik de motie best intrekken, maar dat doe ik niet nu gelijk al. Mijn vrees is juist dat dit kader er niet is, omdat de CTIVD dat nadrukkelijk gezegd heeft.

Staatssecretaris **Dijkhoff**:
Er staat hier een nummer dat ik niet helemaal kan lezen, maar in een brief is aangegeven dat de minister van BZK en Defensie de aanbeveling hierover uit CTIVD-toezichtsrapport 53 overnemen en voor hun deel zullen uitwerken. Dat geeft aan dat het al gebeurd is binnen het separate deel van de Wet computercriminaliteit III en voor de politie.

De **voorzitter**:
U ontraadt de motie en de heer Verhoeven overweegt haar in te trekken als hij nog duidelijkheid krijg op dit punt, zo concludeer ik. Gaat u verder.

Staatssecretaris **Dijkhoff**:
De motie op stuk nr. 469 van de heer Verhoeven gaat over het verbreden van het mandaat van het NCSC. Ik ontraad de motie, omdat het mandaat dan heel breed wordt en er ook sprake zal zijn van overlap. Er is bijvoorbeeld al de Informatiebeveiligingsdienst voor gemeenten, waarmee het NCSC kan samenwerken. Ik wil schakelorganisaties waarmee het NCSC kan verbinden en niet per se het NCSC zelf verbreden. Ook daarom ontraad ik de motie.

Het oordeel over de motie op stuk nr. 470 van de heer Krol laat ik aan de Kamer. De motie is ondersteuning van het beleid. In oktober dit jaar vindt Alert Online weer plaats. Ook blijven we investeren in Veiliginternet.nl.

Ik kom bij de motie op stuk nr. 471 van mevrouw Buitenweg. We hebben al gewisseld dat ik het zie als een nuttig instrument, maar dat ik het te rigide vind om het voor te schrijven. Ik ontraad de motie dan ook graag.

De **voorzitter**:
De staatssecretaris laat het oordeel over de motie van de heer Krol aan de Kamer en hij ontraadt de motie van mevrouw Buitenweg.

Staatssecretaris **Dijkhoff**:
Ja.

De **voorzitter**:
De staatssecretaris heeft nog een aantal vragen gekregen.

Staatssecretaris **Dijkhoff**:
Mevrouw Helder heeft de nodige vragen gesteld over aansprakelijkheid. Ik meende die al te hebben beantwoord, maar mevrouw Helder meende van niet. Misschien kan ik dat in een volgende brief meenemen, als we via een omweg ophelderen om welke elementen het precies gaat. Ik heb nu even geen diepgaandere kennis over datgene waar mevrouw Helder precies op doelt.

De **voorzitter**:
Ik hecht er wel aan om een termijn te kunnen noteren waarop de vraag van mevrouw Helder wordt beantwoord of de wetgeving ten aanzien van de aansprakelijkheid op dit punt voldoet of niet.

Staatssecretaris **Dijkhoff**:
Ik neem het mee in een volgende brief, maar ik weet niet wanneer die komt. Als u echt een concrete termijn wilt: het zou voor de zomer kunnen.

De **voorzitter**:
Voor de zomer. Mevrouw Helder gaat daarmee akkoord.

De andere punten waren het concrete actieplan waarnaar mevrouw Helder had gevraagd en de cybercommissaris digitale dreiging.

Staatssecretaris **Dijkhoff**:
Dat klopt. Het lijkt mij een beter moment om bij het dreigingsbeeld te bekijken of we nadere maatregelen moeten nemen ten opzichte van het lopende beleid en het lopende werk en of je dat substantieel genoeg vindt om het een heel nieuw actieplan te noemen. Zeker nu het nieuwe dreigingsbeeld er snel komt, lijkt dat mij de aanleiding om te bespreken of er meer nodig is. We hebben nu het beleid via de opsporingsaanpak. Ook hebben we net de middelen vrij kunnen maken voor het versterken van het Nationaal Detectie Netwerk. Verder doen we veel publiek-privaat. Bij het dreigingsbeeld zullen we daar verder over spreken.

Ik kom bij de vragen over de digicommissaris. Ik had het in mijn beantwoording inderdaad belegd bij een coördinerend bewindspersoon, maar er zijn natuurlijk ook andere varianten. Je moet eerst weten wat je precies wilt, omdat het logisch dat een nieuw kabinet daarvoor nieuwe plannen opstelt. Vervolgens moet je weten hoe je wilt dat het gebeurt. Wil je het bij een bewindspersoon beleggen of bij een digicommissaris? Als we nu een digicommissaris instellen, zou ik niet meteen zien hoe die grote veranderingen teweegbrengt. Het ligt er een beetje aan hoe een nieuw kabinet dat vormgeeft.

De NIB-richtlijn komt binnen een paar weken in consultatie. Daarna ligt het er ook aan hoe snel uw vragen er zijn en hoe snel onze antwoorden er vervolgens zijn. De ambitie is dat het medio 2018 van kracht zal zijn, dus door beide Kamers is. Dan zijn ook de maatregelen en het toezicht operationeel.

Dat waren de vragen die ik nog had genoteerd.

De **voorzitter**:
Volgens mij had zowel mevrouw Bruins Slot als mevrouw Tellegen nog een paar vragen, te beginnen met mevrouw Bruins Slot over de ziekenhuizen.

Mevrouw **Bruins Slot** (CDA):
Mijn vraag ging over de verhouding tussen enerzijds de rol van het Nationaal Cyber Security Centrum en anderzijds die van wat de Z-CERT voor de zorg wordt genoemd. Hoe garandeer je nou dat uiteindelijk alle zorginstellingen zich actief aansluiten bij die nieuwe digitale organisatie vanuit de zorg, waardoor je een sluitend systeem krijgt? Die vraag geldt althans als de staatssecretaris de verantwoordelijkheden inderdaad zo wil beleggen.

Staatssecretaris **Dijkhoff**:
Om die vraag volledig te kunnen beantwoorden, is van belang in hoeverre ziekenhuizen geacht worden, te vallen onder "'vitale infrastructuur"', ook straks bij de NIB. De beoordeling daarvan vindt nu plaats. Als dit door het ministerie van VWS is gedaan, kun je dat ook verder precies inkleuren.

De **voorzitter**:
Ik zie dat de vragen van mevrouw Tellegen ook beantwoord zijn. Dan zijn alle vragen beantwoord en alle moties van een advies voorzien.

De beraadslaging wordt gesloten.

De **voorzitter**:
Ik dank de Kamer en de staatssecretaris. Wij stemmen aanstaande dinsdag over de ingediende moties.