Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 551

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 18 juli 2018

De vaste commissie voor Justitie en Veiligheid heeft op 28 juni 2018 overleg gevoerd met de heer Grapperhaus, Minister van Justitie en Veiligheid, over:

- **de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 21 juni 2017 inzake cybersecuritybeeld Nederland 2017 (CSBN 2017) (Kamerstuk 26 643, nr. 477);**
- **de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 20 september 2017 inzake reactie inzake cyberaanval met ransomware en voortgang moties uit Wannacry-debat (Kamerstuk 26 643, nr. 487);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 14 mei 2018 inzake voorzorgsmaatregel ten aanzien van gebruik Kaspersky antivirussoftware (Kamerstukken 30 821 en 26 643, nr. 46);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 20 april 2018 inzake integrale aanpak cybercrime (Kamerstuk 28 684, nr. 522);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 20 april 2018 inzake Nederlandse Cybersecurity Agenda (NCSA) (Kamerstuk 26 643, nr. 536);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 13 juni 2018 inzake Cybersecuritybeeld Nederland 2018 (Kamerstuk 26 643, nr. 540);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 26 juni 2018 inzake aanpak Cybersecurity kennisontwikkeling en onderzoeksinvesteringen (Kamerstuk 26 643, nr. 544).**

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

De voorzitter van de commissie,
Van Meenen

De griffier van de commissie,
Hessing-Puts

kst-26643-551
ISSN 0921 - 7371
's-Gravenhage 2018

Voorzitter: Van Meenen
Griffier: Verstraten

Aanwezig zijn zes leden der Kamer, te weten: Alkaya, Buitenweg, Van Dam, Van Meenen, Arno Rutte en Verhoeven,

en de heer Grapperhaus, Minister van Justitie en Veiligheid.

Aanvang 14.01 uur.

De **voorzitter**:
Van harte welkom bij het algemeen overleg van de commissie voor Justitie en Veiligheid, met als onderwerp cybersecurity. Het aantal leden is nog enigszins beperkt, maar ik verwacht er nog wel een paar. Ik heet de Minister en zijn ambtenaren van harte welkom, zo ook de leden, de griffier en u allen op de publieke tribune, de ondersteuning en de mensen die dit elders volgen. We hebben een spreektijd van vier minuten. Gezien het aantal leden zou ik zeggen dat u met vijf interrupties vooruit kunt, maar zo veel hoeven het er niet te worden. Ik meld alvast dat ik om 14.12 uur even weg moet naar de regeling, zoals dat hier heet. Dan zal de heer Rutte het voorzitterschap tijdelijk overnemen en daarna zal ik terugkeren, hopelijk. Ik geef als eerste het woord aan de heer Rutte van de VVD.

De heer **Arno Rutte** (VVD):
Voorzitter, dank u wel. Als je de deur van je huis niet op slot doet en je raam open laat staan, is de kans dat er een inbreker binnentreedt en kostbare spulletjes steelt, groot. Iedereen begrijpt dat en daarom is de fysieke beveiliging van huizen en bedrijfspanden in ons land doorgaans goed in orde. Er is inzicht in welke beveiligingsmaatregelen nodig zijn om een gewenste mate van beveiliging te bereiken. Die middelen voldoen aan de kwaliteiten die de koper daarvan mag verwachten. Een slot breek je niet zomaar open, een hek valt niet zomaar om, zodra iemand er een duwtje tegenaan geeft, een alarm gaat doorgaans ook wel af als deuren of ramen ongewenst geopend worden. Als die producten niet de te verwachten veiligheid opleveren, dan is de leverancier aansprakelijk voor de geleden schade. Dankzij die kennis en kunde kun je je huis of bedrijf ook adequaat verzekeren tegen fysieke dreigingen.
Was het in de wereld van de digitale veiligheid maar net zo helder. Helaas is dat nog niet het geval. Bedrijven, en ook particulieren, betalen veel geld voor cyberbeveiliging die in de praktijk niet of nauwelijks blijkt te werken. Ik sprak uitgebreid met een ondernemer uit Vriezenveen, die zijn internationaal opererende mkb-bedrijf met 60 medewerkers totaal op slot zag gaan door een ransomware-aanval. Hij dacht dat hij het goed voor elkaar had, maar zijn digitale beveiliger had het uitbesteed aan iemand die er verstand van had en die gaf juist op het moment dat het het hardste nodig was, niet thuis. Het beveiligingsbedrijf gaf toe dat het niets kon doen en dat het ook al acht andere klanten overkomen was. De ondernemer heeft uit arren moede de hacker de gevraagde bitcoins betaald en samen met de helpdesk van de hacker stap voor stap de vergrendeling van de computers ongedaan gemaakt. Het beveiligingsbedrijf, dat kennelijk geen beveiliging bood voor een bekend soort aanval, werd aan de dijk gezet, maar datzelfde bedrijf kan probleemloos verdergaan met geld verdienen aan inferieure beveiliging.
In de uitstekende Nederlandse Cybersecurity Agenda – complimenten daarvoor aan de Minister en aan iedereen die daaraan meegewerkt heeft – staat dat het kabinet met stakeholders en wetenschappers in gesprek is over de uitgangspunten voor aansprakelijkheid bij onveilige hard- en software. Dat is een uitstekend idee. Wat de VVD betreft moet ook de aansprakelijkheid bij inferieure digitale beveiligingsproducten en -diensten verhelderd en verbeterd worden. Het is immers in ons aller

belang dat digitale beveiliging net zo betrouwbaar is als fysieke beveiliging. Producten en diensten moeten doen wat ze beloven. Als de te verwachten beveiliging schromelijk tekortschiet, moet de leverancier aansprakelijk zijn voor de geleden schade. Ik hoor hierop graag een reactie van de Minister.
Voorzitter. Ik ga over op een ander punt. Het kabinet heeft besloten dat de rijksoverheid uit het oogpunt van nationale veiligheid stopt met het gebruiken van Kaspersky Antivirus. De VVD steunt dit, al roept dit besluit ook heel veel vragen op. Zijn er eigenlijk wel adequate vervangers voor Kaspersky? Krijgen we die wel voldoende en voldoende snel geïmplementeerd? Ook een specifieke vraag: mogen cruciale toeleveranciers van de overheid Kaspersky nog wel gebruiken? Als dat niet zo is, hoe zien zij dat dan terug in afspraken met diezelfde overheid?
Daarnaast roept dit besluit vragen op over eventuele vervolgstappen. Uit het oogpunt van nationale veiligheid komen ook zeer ongemakkelijke internationale cybervraagstukken naar voren, denk aan de Amerikaanse Cloud Act, die regelt dat de Amerikaanse overheid inzage heeft in alles wat op een Amerikaanse cloud verschijnt. Dat klinkt ver weg, maar dat raakt direct de overheid, die intensief gebruikmaakt van diensten als Office 365 en iCloud, zoals in mijn telefoon. Denk aan het feit dat vrijwel al onze communicatiesystemen worden gebouwd met Chinese infrastructuur. Hoe verhouden deze dingen zich tot het beschermen van de nationale veiligheid? Gaan er meer verboden volgen? Zo ja, hebben we dan betrouwbare alternatieven voorhanden? Graag een reactie.
Tot slot. Zoals heel terecht in de Nederlandse Cybersecurity Agenda naar voren komt, is cybersecurity bij uitstek een stelsel van publiek-private samenwerking. Vanuit dat perspectief heb ik een aantal weken geleden het initiatief gelanceerd om cyberdeskundigen uit het bedrijfsleven op forse schaal als cybervrijwilliger in te zetten bij de politie. Betrokken bedrijven zijn enthousiast en staan echt te popelen en te springen. Ook de Minister was heel enthousiast en dat is mooi. Ik ben benieuwd in hoeverre dat enthousiasme al tot gerichte actie bij de politie heeft geleid.
Voorzitter, dank.

De **voorzitter**:
Dank u zeer. Dan geef ik het woord aan de heer Van Dam van het CDA.

De heer **Van Dam** (CDA):
Dank u wel, voorzitter. Een belangrijk overleg vanmiddag over cybersecurity, een belangrijk punt in een land waar digitalisering en digitale dienstverlening zich op een hoog niveau bevinden en waar wij ook in hoge mate kwetsbaar zijn voor die dreiging. Complimenten voor de stukken die voorliggen; complimenten voor de aanpak en de agenda. We hebben van de week ook nog een briefing gehad op het ministerie. Die was ook zeer verhelderend. Veel dank daarvoor.
Uit de aard van mijn werkzaamheden word ik ook geacht wat kritische opmerkingen bij het geheel te maken en daar kom ik nu op. Tussen alle stukken raak ik door de bomen het zicht weleens kwijt. Om dat heel concreet te maken; er is een brief van 20 april «Naar een veiliger samenleving», met een viertal lijnen: preventie, opsporing en nog wat andere dingen. Maar er is ook een heel rapport, de Nederlandse Cybersecurity Agenda, ook van 20 april, met zeven lijnen. Het lijkt wel alsof de beleidsstukken elkaar wat overtuimelen. Kan de Minister nog eens aangeven wat de verhouding is tussen die twee documenten, welk stuk leidend is en wat zijn rol als coördinerend Minister daarin is?
Een ander punt bij die Cybersecurity Agenda is de smartheid van die agenda. Er staat een lawine aan maatregelen in, op zeven thema's. Ik ga die niet allemaal uitlichten, maar bij sommige dingen vraag je je af: dat zijn prachtige intenties, mooie vergezichten, maar hoe gaan wij als Kamer

op een later moment nog eens checken tot wat voor acties, producten, effecten al die miljoenen die daaraan vasthangen, hebben geleid?
Ik wil de Minister op dit moment helemaal niet vasttimmeren op exact zoveel van dit en zoveel van dat, maar het kent wel een hoge mate van abstractie en vaagheid; veel ambitie maar hoe gaat die landen? Hoe gaat de Minister zijn rol als coördinerend Minister naar al die ministeries waarmaken? Hoe kunnen wij als Kamer de vinger erbij leggen of die ambities waargemaakt worden?
Voorzitter. Een ander punt is het cybersecuritybeeld. Daar ben ik eens wat ingedoken. De hoofdconclusie is dat wij ons vooral zorgen moeten maken over statelijke actoren en over criminele boeven die zich tot ons wenden. Dat staat in het cybersecuritybeeld van 2018, maar in 2017 staat als kernbevinding: beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan. In 2016 was het: statelijke actoren en beroepscriminelen vormden het afgelopen jaar de grootste dreiging. In 2015 is het eigenlijk exact dezelfde formule.
Ik vind dat hele cybersecuritybeeld, ook als ik het vergelijk met andere criminaliteitsbeelden, wel een hoge mate van abstractie in zich hebben en ook regelmatig dezelfde open deuren intrappen die kennelijk al jaren openstaan. Dan denk ik bij mezelf: oké, welke landen dan, welke statelijke actoren? Ik ga geen land noemen, want dat levert weer allerlei gedoe op, maar moeten we dan niet eens een diplomatieke oorlog beginnen met een land dat daarin doet? Ik vind het een beetje abstract en opendeur-achtig. Hoe gaat dat concreter worden? Dat is mijn algemene vraag en daar sluit ik mee af: het mag wel een tikje concreter gaan worden, de komende jaren. Wat gaan we concreet doen? Dat is mijn ambitie.
Een ander punt waar ik echt behoefte aan heb, is een verhaal eroverheen. We hebben een rondetafel gehouden over cybersecurity en daar had iemand het prachtige beeld van Nederland in de strijd tegen het water. Wij liggen allemaal grotendeels onder zeeniveau en de bedreiging die het water voor ons vormt, hebben wij inmiddels weten om te buigen naar een soort exportproduct. Waar ook ter wereld het water een dreiging is, gaan Nederlandse ingenieurs de wereld redden. Bij cybersecurity zou ook onze ambitie moeten zijn dat we van ons nadeel ons voordeel maken. Dat mis ik een beetje in die stukken; een narrative, een verhaal eroverheen, dat ook effectief zou kunnen zijn omdat een heel groot aantal mensen in dit land toch naar datzelfde verhaal toe moeten roeien.
Dank u wel.

De **voorzitter**:
Dank u wel. Er is een interruptie van de heer Verhoeven, maar voor ik hem het woord geef, draag ik het voorzitterschap even over aan de heer Rutte, zodat ik rustig naar de regeling van werkzaamheden kan. Ik ben zo terug.

Voorzitter: Arno Rutte

De heer **Verhoeven** (D66):
Voorzitter. Ik wil de heer Van Dam danken voor zijn mooie betoog. Hij zegt dat het allemaal wel een stukje concreter mag. Ik vind dat een terechte opmerking. Het is altijd lastig om aan het begin van een document met een bepaalde richting heel concreet te zijn, maar die ambitie deel ik. Wat zou dan vanuit de CDA-fractie het idee zijn over concretisering? Op welke vlakken ziet de CDA-fractie voorstellen om het cybersecuritybeleid in Nederland te concretiseren? Want ik ben het geheel met de heer Van Dam eens dat het nodig is, alleen ik denk ook dat het zaak is dat de fracties in de Tweede Kamer daar zelf ook intensief over nadenken.

De heer **Van Dam** (CDA):
Nou, ik zal eens een drietal dingen noemen. In de eerste plaats, en dat heb ik al genoemd: als die statelijke actoren al meerdere jaren een wezenlijk

onderdeel vormen van ons probleem, wat is dan bij wijze van spreken de actie naar landen toe die wij in Nederland ondernemen? Ik heb ook gelezen dat er een uitbreiding in het diplomatennetwerk is. Ik kan me voorstellen dat als we helderder in beeld hebben bij welke landen we een probleem hebben, dan ook helderder in beeld is waar die diplomaten het eerst naartoe moeten. Dat is één ding.
Een tweede ding is dat het voor heel veel burgers toch nog best lastig is. Als jij slachtoffer bent van cybercrime, en je computer doet het bijvoorbeeld ineens niet meer, waar ga je dan naartoe en wie gaat je helpen? Als je daarmee bij het gemiddelde politiebureau komt, denk ik toch dat ze je over het algemeen vrij ongelukkig aankijken. Daar is gewoon een heel concrete verbetering te maken in de bescherming van burgers.
Een laatste element. Collega Rutte had het al even over Kaspersky. Als ik die brief lees, klinkt het mij toch wat willekeurig in de oren dat dat gebeurt. Ik denk dat er voor aanbieders van zulke wezenlijke producten ook wel iets meer concreetheid mag zijn: waarom is hiervoor gekozen? Zijn er niet andere aanbieders die daar dingen in doen? Want het gaat om software die iedere Nederlander gebruikt om zelf veilig te blijven.
Ik hoop dat ik de heer Verhoeven hiermee enige concrete punten heb gegeven. Let wel, ik ben het er volkomen mee eens als u zegt: laten we het nu niet helemaal dichttimmeren. Ik zie in deze cyberagenda de ambitie om vanuit Justitie en Veiligheid het vuur aan te steken om al die ministeries aan de slag te laten gaan. Dus laten we nu niet een soort beperking opleggen. Nee, juist het voortschrijdend inzicht is ontzettend belangrijk. Maar uiteindelijk gaat het er wel om dat wij ook kunnen controleren waar de centen aan uitgegeven zijn.

De **voorzitter**:
Misschien heeft de heer Verhoeven nog een vervolgvraag? Ik begrijp van niet. Anders krijgen we ook interrupties die lijken op een tweede of derde termijn. Maar goed, daar werd ook uitgebreid naar gevraagd.
Dan geef ik het woord aan mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
Ik denk dat de heer Verhoeven niet nog meer zendtijd wilde weggeven, maar ik was het wel eens met de opmerking van collega Van Dam dat het een ambitieuze agenda is. Ik wil de Minister ook van harte danken voor het uitleggen van deze agenda.
Het onderwerp heeft inderdaad nog niet altijd alle handen en voeten die je wilt. Het is soms ook nog wel wat verwarrend, althans voor mij. Je denkt: er is een National Cyber Security Center. Er is een Digital Trust Center. Er komt een informatieknooppunt en een Global Forum on Cyber Expertise. Ik vraag me wel af, en misschien kan de Minister daar nog iets over zeggen, op welke wijze ervoor gezorgd wordt dat alle kennis en informatie goed gedeeld wordt. Er moet geen enorme overlap bestaan en het moet helder zijn voor mensen waar ze heen moeten. Dat Digital Trust Center is er pas redelijk recent, meen ik. Weten mensen dat dan ook te vinden?
Laat ik een paar dingen zeggen. Een goed punt vond ik de kennisontwikkeling die in de Cybersecurity Agenda onder nummer 6 werd aangekondigd. Ik heb er wel een aantal vragen bij. Het is goed om kennis te vergaren, maar de bedoeling is natuurlijk dat die ook wordt toegepast in producten. Tegelijkertijd zie je het volgende. Wanneer de in Nederland vergaarde kennis en kunde vermarkt moet worden in investeringen, en die investeringen daarna ook echt in de markt moeten worden gezet, dan gaat er heel veel kennis en kunde weg. Dat komt doordat het investeringsklimaat in Nederland toch wat conservatiever is. Je ziet dat de investeringsbereidheid bij Amerikaanse partijen vaak veel groter is, met als gevolg dat zaken die wij híér allemaal aan het opbouwen zijn, uiteindelijk dáár in de markt worden gezet. Vervolgens vallen die ook weer onder de regels die gelden in Amerika.

Je zag het ook gebeuren met kwantumcomputingonderzoek in Delft, waarbij Microsoft en Intel wel bereid waren om hier in te investeren, en niet een partij uit Nederland. Ook nu is er een bedrijf dat een techniek heeft geprofessionaliseerd, met name om de infrastructuur van internet beter te beveiligen, maar er niet in slaagt om dat ook te vermarkten.
Wat is dan de rol van de overheid? Ik wil niet zomaar zeggen dat wij daar als overheid allemaal een rol in hebben, maar ik ben wel zoekende. Wat is nu de rol van Nederland om wat meer durfinvesteringen te stimuleren? Hoe ziet de Minister dat, in Nederlands verband, maar misschien ook in Europees verband? Ik heb natuurlijk weleens vaker gezegd dat ik mij er grote zorgen over maak dat wij accepteren dat in Amerika de grote datagiganten het speelveld voor zichzelf houden. Ik vraag me af wat vanuit Europa de strategie is om ervoor te zorgen dat er een soort eigen basis wordt ontwikkeld.
Dan ten opzichte van de opmerkingen die een aantal collega's maakten over Kaspersky en de lijn die Nederland daarin gekozen heeft, namelijk dat we eigenlijk een soort launching consumer zijn: we moeten ergens een grens trekken en we vinden dat er nu een te groot risico is bij het gebruik van dit product. De vraag is: wat is dan de lijn? We willen niet dat het hapsnap of een soort willekeurigheid is. Ik wil best geloven dat het logisch was om het hier te doen. Ik weet dat niet, maar daar zal vast een goede reden voor zijn. Maar waar ligt dan de lijn? En moeten andere bedrijven dan ook volgen? Want klopt het ook dat C2000 ontwikkeld is door een bedrijf dat in Chinese handen is? En wat vinden we daar dan van? De VVD gaf dat ook al aan rond de Amerikaanse Cloud Act. Ik denk dus dat het van belang is dat het beleid dat Nederland gaat uitvoeren echt begrijpelijk is. Daarom heb ik behoefte aan een beleidslijn. Ik heb die in een eerder debat ook gevraagd. Ik heb die nog niet gekregen, maar bij dezen vraag ik het nog een keer.
Mijn collega de heer Van der Lee heeft in een eerder debat, waar ook de heer Verhoeven aan deelnam – bij het vragenuur, geloof ik – gevraagd om een digitaal keurmerk. Toen heeft de heer Verhoeven een parallel getrokken met het Keurmerk Veilig Ondernemen, zodat helder is wat eigenlijk de standaard is voor veiligheid. Staatssecretaris Keijzer heeft toen toegezegd te gaan kijken naar het plan van de heer Verhoeven, dat een geamendeerd voorstel was van mijn collega Van der Lee. Dan is mijn vraag aan de Minister: hoe staat het ten aanzien van een digitaal keurmerk veilig ondernemen?
Ik denk dat ik dan de belangrijkste punten... De tijd is ook al om, dus dat is dan vanzelf opgelost.

De **voorzitter**:
Mevrouw Buitenweg hoopt op heel veel interrupties of anders op een mooie tweede termijn. Er zijn altijd kansen, maar niet meer in de eerste termijn. U was 32 seconden buiten de tijd. Ik zie de heer Alkaya al ongeduldig op z'n stoel draaien. Hij krijgt bij dezen het woord van mij.

De heer **Alkaya** (SP):
Heel veel dank, voorzitter. Laat ik beginnen met excuses. Het zijn drukke dagen, dus ik hoop de tweede termijn ook mee te kunnen pakken, maar ik heb ook een overlappend AO, dus misschien dat ik de zaal uit moet rennen.
Maar eerst dit belangrijke onderwerp. De dreigingen in het digitale domein zijn de afgelopen jaren alleen maar toegenomen. Het kabinet bevestigt dit ook in het Cyber Security Beeld en in de Cybersecurity Agenda. Complimenten en dank daarvoor.
Niet alleen bij de overheid en de vitale infrastructuur, maar ook bij consumenten en het mkb, neemt het belang van cyberveiligheid toe. Ik ben blij dat er, naar aanleiding van een motie van onder andere de SP, een Digital Trust Center is gekomen dat het mkb moet ondersteunen bij het op

orde brengen van hun cyberveiligheid. Ik heb hier hooggespannen verwachtingen van.
Ook goede cyberveiligheidbedrijven zijn hierin van groot belang. Het is al door een aantal collega-Kamerleden van mij genoemd, en ook ik was een beetje verbaasd door het in de ban doen van Kaspersky. Aan de andere kant snap ik het als we kijken naar de vermeende rol van Rusland in het digitaledreigingsbeeld.
Tegelijkertijd is onze grootste bondgenoot medeveroorzaker van de problemen die de basis van dit algemeen overleg vormen. Het Amerikaanse National Security Agency heeft bijvoorbeeld de cyberwapens ontwikkeld die door kwaadwillende hackers zijn omgevormd tot WannaCry, de gijzelvirussoftware die verschillende landen en ziekenhuizen lamlegde en in Nederland leidde tot problemen bij bedrijven.
Voorzitter, ik bespeur een interruptie.

De **voorzitter**:
Ja, de voorzitter was even vergeten dat hij voorzitter was. Het is wat.
Ik geef het woord aan de heer Verhoeven, die u een vraag wil stellen.

De heer **Verhoeven** (D66):
Nou, het is niet zozeer weer allemaal interruptie en scherp slijpen – alhoewel ik dat ook heus weleens doe – maar gewoon even een vraag. Ik vind het namelijk leuk om te horen dat vier sprekers toch vragen hebben bij de Kasperskycasus. Ik zal dat zelf dadelijk ook doen. Dat is van VVD tot SP en van GroenLinks tot CDA, dus dat is toch interessant. De heer Alkaya zei net dat de Russische dreiging ergens wel een logische aanleiding is. Dat zie ik zelf ook zo, maar stel nou dat we bijvoorbeeld eens kijken naar het bedrijf Huawei uit China? Hoe ziet de heer Alkaya het dan?

De heer **Alkaya** (SP):
Daar geldt exact hetzelfde voor. Verderop in mijn betoog kom ik ook op een aantal Amerikaanse producten die worden gebruikt. Mijn vraag is eigenlijk vergelijkbaar met die van een aantal collega-Kamerleden: is hier sprake van willekeur of zijn we aan het toewerken naar een soort raamwerk, een soort kader, waarbij we uit voorzorg een aantal bedrijven weren uit het overheidsapparaat, hoewel we niet kunnen pinpointen waar de cyberdreiging in die landen vandaan komt? Het land waar die dreigingen vandaan komen maakt dan wat mij betreft niet uit.

De **voorzitter**:
Had u nog een vervolgvraag, meneer Verhoeven? Nee? Dan vraag ik de heer Alkaya zijn betoog voort te zetten.

De heer **Alkaya** (SP):
Dank, voorzitter. Ik zat midden in het punt dat ik wilde maken en ga daarmee verder. De Verenigde Staten hebben vergelijkbare wetgeving met Rusland om hun bedrijven aan te sturen als het om veiligheid gaat. We kennen allemaal de casus waarin de FBI naar aanleiding van een terroristische aanslag een rechtszaak heeft aangespannen tegen Apple om inzage te krijgen in hun systemen. Is de Minister aan het overwegen om McAfee, Symantec en andere Amerikaanse bedrijven ook uit voorzorg in de ban te doen, omdat we daar ook onze bedenkingen bij hebben? Daar kan ik Huawei aan Chinese kant zo bij noemen. Welke criteria worden hierbij gehanteerd, om willekeur bij dit soort overheidsinterventies te voorkomen?
Voorzitter. Een van de grootste risico's op het gebied van cybersecurity is inmiddels het internet of things geworden, het netwerk van gewone apparaten zoals thermostaten en stofzuigers. Van vrijwel alle apparaten is inmiddels een variant verkrijgbaar die ook toegang heeft tot het internet. Voor veel mensen is het al moeilijk genoeg om een gewone computer

up-to-date en beveiligd te houden, laat staan apparaten waarvan de functie niet eens is dat ze op het internet kunnen. Toch bestaat er voor fabrikanten geen verplichting om te zorgen voor adequate software-updates. Al eerder heeft de Kamer de regering opgeroepen om maatregelen te nemen tegen onveilige internetapparaten, maar wat gaat er nu gebeuren? Bovendien valt de beveiliging niet onder de garantieregels, terwijl de levensduur van een product toch mede wordt bepaald door hoe goed de software wordt bijgehouden. Samsung heeft recent gelijk gekregen van de rechter in de stelling dat het toestellen ouder dan twee jaar niet meer hoeft te ondersteunen. Hiermee is de levensduur van telefoons van Samsung dus de facto twee jaar geworden, maar zo'n product blijft het natuurlijk na twee jaar prima doen. Het risico voor de samenleving als mensen deze producten na twee jaar blijven gebruiken, is eigenlijk net zo groot als voor de gebruiker zelf. Denk aan de ddos-aanvallen op banken waarbij gebruik is gemaakt van gehackte apparaten. Voorzitter, mijn vraag aan de Minister is: hoe moet een persoon of bedrijf erachter komen dat zijn netwerk openstaat voor hackers omdat bijvoorbeeld zijn thermostaat al een paar maanden niet is bijgewerkt? Is diezelfde burger of datzelfde bedrijf dan niet eigenlijk gedwongen om telkens weer een nieuw product aan te schaffen omdat er geen updates meer worden geleverd, terwijl het product het gewoon doet? Niet iedereen heeft het geld om iedere twee jaar nieuwe producten aan te schaffen. Bovendien is dat zonde van het geld en zonde van het milieu.
Voorzitter. Het lijkt mij helder wat hier moet gebeuren. Digitale veiligheid als optioneel beschouwen is geen optie meer. Consumentenbescherming valt weliswaar onder de Staatssecretaris van Economische Zaken en Klimaat, maar ik ben van mening dat het risico van een onveilig internet of things voor de rest van de samenleving te groot is om het alleen in het kader van consumentenbescherming te beschouwen. Is de Minister bereid om samen met de Staatssecretaris van Economische Zaken en Klimaat te bekijken hoe de garantiewetgeving aangepast kan worden zodat ook het up-to-date houden van beveiligingssoftware onder de garantiewetgeving valt?

De **voorzitter**:
Ik moet streng zijn met de spreektijd. Hoorde ik daar een punt?

De heer **Alkaya** (SP):
Dat was een punt, ja.

De **voorzitter**:
Heel goed. Dank u wel. Dan geef ik het woord aan de heer Verhoeven namens D66.

De heer **Verhoeven** (D66):
Dank u wel, voorzitter. Fijn dat het kabinet de toenemende dreiging van cybercrime en het belang van cybersecurity in een agenda heeft gevat. Ook ik zal proberen om de agenda op een aantal punten nog wat aan te scherpen.
Allereerst ethische hackers. Die zijn essentieel voor onze veiligheid, want zij vinden heel veel kwetsbaarheden en fouten. Nederland had als eerste een richtlijn voor responsible disclosure. We hebben ook prachtige bedrijven als HackerOne, die wereldwijd ethische hackers koppelen aan bedrijven en overheden. Ik ben alleen benieuwd welke rol de Minister weggelegd ziet voor ethische hackers in zijn cybersecurityagenda. Wil hij daar wat over zeggen? En is hij bereid om met partijen als HackerOne samen te gaan werken om bug-bountyprogramma's van ministeries en overheidsinstanties op te zetten? Dat is ook een van de aanbevelingen uit een van de rondetafels hierover: geef ethische hackers een serieuze plek in het cybersecuritybeleid.

Dan het NCSC. Dat is een mooi voorbeeld van publiek-private samenwerking, waarmee wij andere landen een goed voorbeeld geven. Alleen spelen zij onbekende kwetsbaarheden, zero-days, nog niet gemelde kwetsbaarheden, door aan de AIVD. Ik heb de Minister daar al eerder op aangesproken. Ik heb er zelfs een motie over ingediend, die toen verworpen is. Toch wil ik de Minister vragen om zorgvuldig om te gaan met de positie van het NCSC, dat van grote waarde is voor de cyberveiligheid. Het NCSC moet voor iedereen een betrouwbare plek zijn om dingen te melden. Hoe wil de Minister ervoor zorgen dat ethische hackers iets kunnen melden zonder dat het terechtkomt bij de inlichtingendiensten, of in ieder geval zonder dat het daar op een verkeerde manier terechtkomt?

De **voorzitter**:
Volgens mij is er inmiddels een officiële voorzitter gearriveerd. Ik hoop dat die de hamer van mij over kan nemen, zodat ik een vraag kan stellen aan de heer Verhoeven.

Voorzitter: Van Meenen

De **voorzitter**:
De heer Verhoeven is al aan het woord? Het gaat snel. Meneer Verhoeven, u hebt een interruptie van de heer Rutte, als ik het goed begrepen heb.

De heer **Arno Rutte** (VVD):
Soms heb je een heel ingewikkeld pettenprobleem! Het is wat.
Op een goede manier omgaan met informatie over dit soort kwetsbaarheden, bijvoorbeeld zero-days. Hoe ziet de heer Verhoeven dat voor zich in het kader van wet- en regelgeving, ook binnen het kader van de net aangenomen Wet computercriminaliteit III?

De heer **Verhoeven** (D66):
Sowieso vindt mijn fractie dat dit heel beperkt zou moeten zijn. Het liefst ziet mijn fractie dat het helemaal niet gebeurt, maar we hebben te maken met een ruime meerderheid in de Kamer die vindt dat het wel moet kunnen. In het regeerakkoord staan heel goede dingen over de Wet computercriminaliteit III. Ik denk dat er voor het doorspelen van onbekende kwetsbaarheden naar de AIVD een duidelijk kader zou moeten zijn. Laat dat ook een openbaar of transparant kader zijn, zodat we weten hoe we dat in dit land aanpakken. Dat ontbreekt nog. Er is dus nog geen duidelijke richtlijn voor. Die zou er wat mij betreft wel moeten komen.

De heer **Arno Rutte** (VVD):
Ik weet dat de heer Verhoeven en D66 wat terughoudender dan de VVD denken over hoe we met dit soort informatie zouden moeten omgaan. Tegelijkertijd is die Wet computercriminaliteit nu wel aangenomen, ook in de Eerste Kamer, dus die gaat gelden. Het kan wel degelijk in het belang van de nationale veiligheid zijn dat dit soort kwetsbaarheden worden doorgespeeld aan de AIVD. Hoe ziet de heer Verhoeven zo'n restrictief kader voor zich? Welke toets hebben we dan? Als de nationale veiligheid het toetsingskader is, is dat toch een redelijk helder kader? Dan moet het toch juist bij de AIVD landen?

De heer **Verhoeven** (D66):
Ja, maar «nationale veiligheid» is geen helder kader. «Nationale veiligheid» zijn twee woorden die vaak, soms zelfs te pas en te onpas, worden gebruikt om allerlei keuzes mee te onderbouwen. Ik vind het absoluut een dilemma. Aan de ene kant wil je de nationale veiligheid beschermen en zou je dus onbekende kwetsbaarheden moeten melden zodat ze gebruikt kunnen worden om bepaalde verdachten of criminelen

dieper te kunnen volgen. Aan de andere kant – dat zei de heer Alkaya net al heel goed, en daar hebben wij de afgelopen jaren ook vaak aandacht voor gevraagd – is de nationale veiligheid juist in het geding als we onbekende kwetsbaarheden op allerlei plekken gaan delen en gebruiken. Dat geldt zeker als we dat als overheid doen, omdat we dan ook de markt voor onbekende kwetsbaarheden gaan stimuleren. Denk aan een zero-day die gebruikt wordt om kerncentrales, havennetwerken of andere zaken plat te leggen. Dat is ook niet in het belang van de nationale veiligheid. Het is dus niet zozeer de oude discussie van privacy versus veiligheid. Het is hier de discussie veiligheid versus veiligheid. Daarom vind ik dit zo belangrijk en daarom moet er een kader komen.

De **voorzitter**:
Gaat u verder.

De heer **Verhoeven** (D66):
Dat doe ik.
De vraag was ook nog of de Minister stappen neemt om het NCSC als aanspreekpunt voor alle search in sectoren te gaan gebruiken.
Dan over die zero-days. Een belangrijk element is een duidelijk kader voor de omgang van de overheid met zero-days. Voor de AIVD en de MIVD ligt dat er; de Minister van Binnenlandse Zaken heeft dat op verzoek van VVD en D66 geregeld. Maar de Minister van Justitie en Veiligheid vindt het waarschijnlijk – of blijkbaar – nog niet nodig dat de politie ook zo'n kader heeft. Kan de Minister daar nog eens op ingaan? En is de Minister het met mij eens dat zo'n afwegingskader eigenlijk ook voor de hele overheid zou moeten gelden, dus ook voor de politie en de opsporingsdiensten?
Ik ben heel blij dat het kabinet investeert in cybersecurityonderzoek. Dat moet nog wel wat beter gebundeld worden. Daarom is het heel goed dat er nu een verkenning komt om een instituut op te zetten. Is de Minister bereid om die verkenning voor de begrotingsbehandeling naar de Kamer te sturen?
Ik sluit mij aan bij het punt over het internet der dingen. Verplichte standaarden voor apparaten zijn belangrijk, maar een apparaat met een levensduur van meer dan een aantal jaar, dat niet meer voldoet aan de standaard nadat het een tijd geleden is aangekocht, is natuurlijk ook kwetsbaar. Daarmee is softwareaansprakelijkheid die langer duurt dan het moment van aankoop ook van belang. De Minister geeft aan dat hij met stakeholders en wetenschappers in gesprek is. Wanneer kan de Kamer de resultaten van die gesprekken tegemoetzien? Ik denk dat softwareaansprakelijkheid een heel belangrijk punt is voor de toekomst, voor de nationale veiligheid en voor al die apparaten die op het internet zijn aangesloten.
Ik zou willen afsluiten met een korte opmerking over de situatie rondom het bedrijf Kaspersky. Volgens mij hebben we daar allemaal vergelijkbare dingen over gezegd. Ook daar zou een kader voor moeten komen. De Minister kan flink aan de slag met het maken van een aantal goede kaders. Ik denk overigens dat dat een logische aanpak is, want je hebt een soort van meetlat nodig op het moment dat er een internationale dimensie op je afkomt en je wilt weten hoe je daar objectief mee omgaat.
Ik zou de Minister ook nog het volgende willen vragen. Kaspersky nu van de Nederlandse markt weren – of zelfs van de Europese markt, want ook daarover wordt gesproken – is één kant, maar laten we ook eens denken aan het bedrijf ASML, uit Nederland. Dat is een van de wereldwijde monopolisten die overal chipmachines maken. Als Rusland nu eens zou zeggen dat het ook ASML-producten van zijn markt gaat weren? Is daar ook over nagedacht? Zijn dat soort signalen er? Kortom, ziet het kabinet de wederkerigheid van dit soort maatregelen? Zijn die voldoende afgewogen? We hebben in deze markt zelf ook heel veel te exporteren en te winnen.

De **voorzitter**:
Dank u wel. Er is nog een interruptie van de heer Van Dam.

De heer **Van Dam** (CDA):
Ik hoor de heer Verhoeven zeggen dat hij van de Minister voor andere diensten dan de AIVD en de MIVD ook een soort van richtlijnen wil voor de omgang met zero-days. Dat heb ik toch goed begrepen? Dan zou ik van de heer Verhoeven, nu onlangs de Wet computercriminaliteit III is aangenomen, toch weleens willen weten wat de ambitie van D66 in dezen is. Wat uw standpunt was is overhelder. Is het de bedoeling om elke keer weer te proberen om in dezen terrein terug te winnen? Of is de norm die nu in de Wet computercriminaliteit III is benoemd, ook uw uitgangspunt voor de richtlijnen voor andere overheidsdiensten?

De heer **Verhoeven** (D66):
Dit is een begrijpelijke vraag. O, excuus, voorzitter: u wilde mij nog het woord geven, maar ik had het al.

De **voorzitter**:
Nou, we krijgen vragen uit het land wat zero-days zijn. Misschien wilt u dat eerst nog even voor de luisteraars uitleggen. De heer Van Dam mag het ook doen. Het maakt niet uit wie het doet; als ik het maar niet hoef te zijn.

De heer **Van Dam** (CDA):
Ik heb in de politiek geleerd dat je het eigendom vooral daar moet laten liggen waar het is, dus ik laat dat graag aan meneer Verhoeven over.

De **voorzitter**:
Misschien kunt u dat nog even kort toelichten.

De heer **Verhoeven** (D66):
Voor de zekerheid zeg ik dan wel dat ik zelf geen zero-days bezit, voorzitter. Een zero-day is wat mij betreft het best samen te vatten als een onbekende kwetsbaarheid, een kwetsbaarheid in software die nog niet ontdekt of gemeld is, waardoor die ook nog niet gedicht is. Waarschijnlijk krijg ik op Twitter nu allemaal mensen die mij wat aanvullingen geven voor de precisie, maar dit is het in grote lijnen, voor de kijkers thuis.
De heer Van Dam vroeg: wilt u terrein terugwinnen? Als D66 meer zetels zou hebben en wij de mogelijkheid zouden zien om een Kamermeerderheid te creëren om het benutten of gebruiken van onbekende kwetsbaarheden – of het door de overheid stimuleren van de markt voor onbekende kwetsbaarheden – terug te draaien, dan zullen wij dat niet nalaten. Ik geloof dat ik heel duidelijk ben geweest over het feit dat ik het zelf een maatregel vind met grote nadelen in het kader van de nationale veiligheid. Alleen, op een gegeven moment word je gewoon geconfronteerd met een ruime Kamermeerderheid die wat anders doet; dat hebben we ook gezien bij de Wet op de inlichtingen- en veiligheidsdiensten en dat zien we ook bij andere onderwerpen. Dan heb ik als Kamerlid de edele plicht om voortdurend te kijken welke stappen de overheid, het kabinet zet in een bepaalde richting die ik niet wenselijk vind. Ik zie dat die wet aangenomen is en dat accepteer ik ook. Hij wordt uitgevoerd. In het regeerakkoord wordt ook nog geld aan de politie gegeven om zelf onderzoek te doen naar die kwetsbaarheden in plaats van ze in te gaan kopen. Ik ben daar blij mee, want dat vermindert het probleem al wat, maar ideaal is het nog niet. En elke keer als er nu weer stappen gezet worden, in dit geval dat de AIVD en de MIVD kwetsbaarheden aangereikt krijgen van het NCSC, zal ik daar vragen over stellen. Maar ik accepteer wel dat een wet aangenomen is, absoluut. Ik ben een redelijk mens.

De heer **Van Dam** (CDA):
Ik ben heel blij om te horen dat een Kamerlid accepteert dat een wet is aangenomen. Dat is winst. Het punt is dat ik denk dat het jammer zou zijn als we elke keer weer die strijd moesten strijden, hoezeer ik me dat politiek ook kan voorstellen. Ik hoop namelijk heel erg dat de markt gaat anticiperen en op een gegeven moment zelf weet hoe de Nederlandse overheid met dat soort dingen omgaat. Dat is mijn punt. Ik zou het jammer vinden als we dat hier elke keer weer als een soort discussie hadden.

De heer **Verhoeven** (D66):
Dat begrijp ik. Volgens mij is er nu duidelijk beleid. Op een aantal punten zijn er ontwikkelingen en vraag ik om verdere verduidelijking van het beleid, juist in het belang van wat de heer Van Dam zegt. Daar vinden we elkaar heus wel, maar politiek is ook altijd wel een beetje blijven strijden voor je idealen. Ik herinner me nog een debat over de wet op de majesteitsschennis. Toen was de heer Van Dam aan alle kanten in alle staten omdat er iets gebeurde wat hij niet wilde. Toen heeft hij zich ook niet even neergelegd bij het feit dat er iets gebeurde wat hij niet wilde. Een beetje volhouden en doorzetten voor je idealen is dus ook wel iets wat erbij hoort, maar ik zal dat binnen de kaders van het redelijke doen, zodat het beleid dat er nu is duidelijk op internationaal gebied vervolgd kan worden.

De **voorzitter**:
Ik dank u zeer. Daarmee komt er een einde aan de eerste termijn van de zijde van de Kamer. De Minister heeft verzocht om een korte schorsing.

De vergadering wordt van 14.37 uur tot 14.50 uur geschorst.

De **voorzitter**:
We gaan verder met dit algemeen overleg. Ik geef de Minister van Justitie en Veiligheid het woord voor zijn eerste termijn.

Minister **Grapperhaus**:
Dank, voorzitter. Voordat ik inga op de vragen, denk ik dat het goed is om iets te zeggen over de veiligheid in het digitale domein in het algemeen. Die is voor dit kabinet een topprioriteit. We hebben daarom ook in het regeerakkoord een structurele aanvullende investering van 95 miljoen euro in cybersecurity vastgelegd. Met de Cybersecurity Agenda wordt een belangrijke en noodzakelijke stap gezet om Nederland digitaal veilig te houden. We willen op een veilige wijze de economische en maatschappelijke kansen van digitalisering verzilveren en onze nationale veiligheid in het digitale domein beschermen. We werken daaraan langs de lijn van die zeven ambities die al eerder door enkelen van u zijn genoemd, en daarbij aan een groot aantal concrete maatregelen die cyberdreiging het hoofd bieden en Nederland digitaal veilig gaan maken.
Het voert te ver om alle maatregelen hier te noemen, maar ik geef een aantal voorbeelden van waar we nu mee aan de slag zijn. Ik noem de capaciteiten van onder meer de inlichtingen- en veiligheidsdiensten, Rijkswaterstaat en het NCSC, die structureel worden versterkt. Zo krijgen we inzicht in dreigingen en kunnen we digitale aanvallen signaleren en verstoren, en zo verhogen we ook de weerbaarheid. Met de extra middelen voor cybersecurity die dit kabinet vrijmaakt, kunnen de komende jaren ongeveer 350 fte structureel extra aan de slag bij de betrokken organisaties. Het landelijk situationeel beeld wordt versterkt en er komt een samenwerkingsplatform om informatie en handelingsperspectief met belanghebbende organisaties te delen. De Wet computercriminaliteit III, deze week aangenomen in de Eerste Kamer, breidt ook de opsporingsmogelijkheden van politie en justitie uit. We investeren ook structureel in kennisontwikkeling, onder meer met de Nationale Cyber

Security Research Agenda voor fundamenteel en toegepast cybersecurity-onderzoek. We werken aan veilige hard- en software door onder andere het inrichten van testfaciliteiten, verkenningen naar standaarden, certificeringsmogelijkheden, veiligheidslabels en aansprakelijkheid.
Maar dat redden we als overheid niet alleen. We willen de partijen ook zo veel mogelijk helpen om hun eigen verantwoordelijkheid te kunnen nemen. Publiek-privaat wordt met het opzetten van de cybersecurityalliantie op diverse terreinen samengewerkt, onder andere aan cybersecurity-standaarden voor ketens, maar ook door gebruik te maken van het groot-helpt-kleinprincipe. Het landelijk dekkend stelsel en het Digital Trust Center zijn goede voorbeelden van hoe we alle partijen in staat willen stellen hun eigen cybersecurity te verstevigen. Sectorale toezichthouders gaan ook meer toezien op de cybersecurity in sectoren in de vitale infrastructuur waar dat tot nu toe niet gebeurde. Met private partijen wordt bovendien de ontwikkeling verkend van een certificeringsstelsel voor cybersecuritydienstverleners bij wie veilig dienstverlening kan worden afgenomen.
Het onlangs uitgebrachte Cybersecuritybeeld Nederland laat opnieuw zien dat de dreiging aanzienlijk is en steeds in ontwikkeling. Dat vraagt om een continue, dynamische, meerjarige cybersecurityaanpak. Daarom wordt met de agenda de koers uitgezet en houden we ruimte om bij te sturen waar nodig. Jaarlijks wordt aan de hand van het Cybersecuritybeeld Nederland en relevante technologische en maatschappelijke ontwikkelingen bezien of we onze aanpak moeten bijstellen. Ik wil hierbij alvast zeggen dat ik daarover graag met uw Kamer in dialoog blijf.
Voorzitter. Ik heb een aantal vragen gekregen die eigenlijk allemaal zien op certificering en aansprakelijkheid; daar wil ik eerst op ingaan. Ik heb al gewezen op die digitaal veilige hard- en software. Door de opmars van het internet of things worden steeds meer dingen met het internet verbonden; de heer Alkaya refereerde er al aan. Dan moeten ze digitaal veilig zijn. Je moet ze veilig en vertrouwd kunnen gebruiken, niet alleen voor de digitale veiligheid van de gebruiker zelf, maar voor de samenleving als geheel. Door kwetsbaarheden in hard- en software van een apparaat kunnen kwaadwillende partijen zich eenvoudig toegang verschaffen tot een apparaat en via dat apparaat tot het netwerk waar het deel van uitmaakt, met alle gevolgen van dien, bijvoorbeeld het misbruik van dat apparaat voor ddos-aanvallen, het manipuleren van de werking van het apparaat of de diefstal van informatie.
Digitale veiligheid van hard- en software komt niet vanzelf tot stand. De aanbieders lossen niet altijd alle digitaleveiligheidsrisico's die gepaard gaan met hun processen en producten op. Gebruikers hebben nauwelijks middelen om een goede inschatting te kunnen maken van wat het digitale veiligheidsniveau is van het apparaat dat zij gebruiken en dat aan internet is verbonden. Om die digitale veiligheid van hard- en software te bevorderen, hebben de Staatssecretaris van Economische Zaken en ikzelf een roadmap opgesteld voor het gebruik van die hard- en software. Die roadmap bevat een samenhangende set van maatregelen die nodig zijn om de digitale veiligheid op een gebalanceerde wijze te bevorderen en maakt ook integraal deel uit van de Nederlandse Cybersecurity Agenda 2018. Ik wil u hierbij zeggen dat het voornemen is om uw Kamer jaarlijks te informeren over de voortgang en de doorontwikkeling en uitvoering van die roadmap, want de ontwikkelingen gaan natuurlijk snel.
Een vraag van de heer Alkaya die hierop aansluit, was of deze Minister bereid is om de garantiewetgeving aan te passen in het kader van de problematiek van het internet of things. Welnu, de wijze waarop wordt omgegaan met aansprakelijkheid en garantie is een heel belangrijk onderwerp in die roadmap. Ik zal deze suggestie meenemen naar de Staatssecretaris van Economische Zaken om verder te bekijken bij de uitwerking van de roadmap. Om echt volledig te zijn wil ik er nog aan toevoegen dat die aansprakelijkheid een van de maatregelen is om

veiligheid te bevorderen. Stakeholders en wetenschappers geven aan dat het Nederlandse aansprakelijkheidsrecht op dit moment goede handvatten biedt voor schadeverhaal bij onveilige software. We zijn daar in EU-verband ook volop mee bezig. Maar we moeten ons ook realiseren dat absolute veiligheid niet bestaat. Dat neemt niet weg dat we dus werken aan regels om de softwareveiligheid te bevorderen. Daarbij wordt in EU-verband zowel gesproken over productaansprakelijkheid alsook over contractuele verplichtingen van verkopers om updates aan consumenten te leveren. Het kabinet zal uw Kamer verder informeren over de uitkomsten van de gesprekken die we op nationaal en EU-niveau voeren, ook weer over de doorontwikkeling van die roadmap. Dat gebeurt dus zowel nationaal als internationaal. Verder wil ik op dit punt nog melden dat het Centrum voor Criminaliteitspreventie en Veiligheid, het CCV, is begonnen met gesprekken met verzekeraars. Dat zou moeten resulteren in een cybersecurityrisicomodel voor bedrijven en moet ook leiden tot een keurmerk voor aanbieders van cybersecuritydienstverlening.

Mevrouw **Buitenweg** (GroenLinks):
De Minister gebruikt veel woorden. Alles moet integraal en het is allemaal heel erg jargon. Ik vraag me wel af wat de Minister nou eigenlijk zegt. Als het over productaansprakelijkheid gaat, zegt hij dat alles zal worden meegewogen. We hebben ook nog Europese samenwerking. Wat is nou de inzet van de Minister in Europa op dit specifieke punt? Mijn collega had ene heel specifiek punt ten aanzien van de softwareaansprakelijkheid, die soms maar voor een heel korte periode van zo'n twee jaar wordt geaccepteerd. Wat zegt de Minister daarvan? En wat is zijn inbreng in Europa? Want er komt niet ineens iets uit Europa; we stoppen er ook iets in.

Minister **Grapperhaus**:
Ik heb daarnet juist concreet op de heer Alkaya geantwoord en gezegd dat ik zijn suggestie om de Nederlandse garantiewetgeving nog eens goed tegen het licht te houden omarm. Hij noemde een goed voorbeeld van de problematiek van ondersteuning gedurende een bepaalde periode voor apparaten die in wezen veel langer gebruikt worden. De discussies in Europees verband zijn, zo blijkt ook uit de roadmap voor soft- en hardware, hoe je de doorontwikkeling van dit soort producten en diensten, die voortdurend plaatsvindt, zodanig kunt laten begeleiden met goeie regelgeving op het gebied van aansprakelijkheid en veiligheid dat de gebruiker bij iedere volgende ontwikkeling nog steeds eenzelfde veiligheidsniveau kan verwachten van zijn apparaten, respectievelijk eenzelfde aansprakelijkheid van de producent of de dienstverlening. Ik denk dat dat helemaal niet zulke algemene termen zijn, want dit is nou juist de kern van de problematiek die ook in de roadmap wordt beschreven.

Mevrouw **Buitenweg** (GroenLinks):
Toch probeer ik even een vertaling te maken, want ik ben een simpele vrouw. Zegt u nou: ik vind het slecht dat die productaansprakelijkheid zo kort is en daar wil ik wat aan doen?

Minister **Grapperhaus**:
Nee hoor, dat zeg ik helemaal niet. Ik neem de gedachte van de heer Alkaya, die ik ook ga bespreken met de Staatssecretaris, over dat we goed moeten kijken of de wetgeving die we in Nederland op het gebied van garanties hebben, wel helemaal aansluit. Zien we aanleiding om die aan te passen in het licht van het feit dat die internet-of-thingsproducten zich almaar doorontwikkelen in een zeer snel tempo en telkens bij iedere doorontwikkeling mogelijk nieuwe issues op het gebied van veiligheid en gebruik geven?

De heer **Alkaya** (SP):
Ik heb die toezegging genoteerd. Dank daarvoor. We moeten ook niet op alle punten van de roadmap apart terugkomen, maar dit lijkt me wel een belangrijke, vooral omdat de rechter recent een uitspraak heeft gedaan over een specifiek geval van Samsung. Enerzijds gaat het over producten waarbij consumenten er redelijkerwijs van uit kunnen gaan dat ze veilig worden gehouden door de fabrikant, zoals smartphones. Anderzijds gaat het inderdaad over producten die meer in de sfeer van the internet of things zitten. Ik ben benieuwd wat de uitkomst van die gesprekken zal zijn. Ik wil mijn linkerbuurvrouw hierin ondersteunen: ik vind twee jaar wel te kort voor een smartphone. Het is zonde van het geld en van het milieu als consumenten worden gedwongen om iedere twee jaar een nieuwe telefoon aan te schaffen omdat de beveiliging anders niet op orde is. Nadat die gesprekken met de Staatssecretaris hebben plaatsgevonden, zou ik in een brief graag meer informatie ontvangen over wat we in dezen kunnen verwachten. Kan de Minister dat toezeggen? De roadmap is in april uitgekomen, dus we moeten bijna een jaar wachten op de voortgang met betrekking tot die roadmap.

Minister **Grapperhaus**:
Zoals ik heb aangegeven, ga ik deze suggestie bespreken met de Staatssecretaris. Zij is hier natuurlijk in de lead, zoals u in eerste termijn ook al zei. De expertgroep in EU-verband komt komend jaar nog een aantal keren bijeen, en ik ben het met u eens dat het goed is om elkaar van de voortgang op dit onderwerp op de hoogte te houden. Ook dat heb ik bij dezen toegezegd.

De heer **Arno Rutte** (VVD):
Ik had een iets afwijkende vraag gesteld over aansprakelijkheid rondom beveiligingssoftware. Gaat de Minister daar nog specifiek op in? Hij noemde wel iets in het kader van CCV. Als hij daar nog specifiek op ingaat, heb ik nu nog geen vraag, maar anders zou ik daar nu een vraag over willen stellen.

Minister **Grapperhaus**:
Ik zal nog even de punten met betrekking tot software afmaken. Er was ook een vraag over het keurmerk voor digitaal veilig ondernemen. In het vragenuur van 5 juni met de Staatssecretaris heeft de heer Verhoeven die optie voor een keurmerk voor digitaal veilig ondernemen benoemd. De collega, de Staatssecretaris van Economische Zaken, is dat op dit moment in overleg met private partijen aan het bezien.
Voor de certificering is op dit moment veel aandacht vanwege de groei van het aantal internet-of-thingsproducten en de zorg dat daar veel onveilige producten bij kunnen zitten. Laat ik vooropstellen dat het heel goed is dat we daar heel veel aandacht voor hebben. Dat is dan ook de reden dat die digitaal veilige hard- en software een van de ambities uit de Cybersecurity Agenda is. Voor de heer Alkaya wil ik nog benadrukken dat wij er in Brussel ook op aandringen om in de onderhandelingen de verordening voor cybersecurity snel vastgesteld te krijgen, juist omdat we bedrijven de mogelijkheid willen bieden om Europese standaarden en certificaten te ontwikkelen. Daar ontbreekt het nu natuurlijk nog aan.

De heer **Verhoeven** (D66):
Ik vind dat al best een mooie ontwikkeling, maar uiteindelijk helpt er maar één ding: een Europees verkoopverbod, gekoppeld aan heel duidelijke eisen. Nederland mag dat niet zelf doen, want we zijn lid van een Europese interne markt en kunnen niet onze verkoopverboden opstellen. Daarom zoeken we het nu in wat meer onderliggende wetgeving, certificering enzovoort. Heel goed; dan kunnen we ook een koploper zijn. Wordt er in Europa ook gesproken over die serieuze maatregel? Want dat

is echt dé manier om als Europa het verschil te maken in de mondiale economie, als het gaat om allerlei producten op het gebied van digitalisering en cybersecurity. Wij kunnen gewoon gebruikmaken van onze sterke, grote afzetmarkt.

Minister **Grapperhaus**:
Ja, dat is eigenlijk wat ik net al aangaf: daar wordt in Europa over gesproken. De heer Verhoeven heeft dit punt overigens al bij een eerdere gelegenheid aan de orde gesteld, ik denk terecht. Daarom dringt Nederland er mede op aan om vooral vanuit Europa met standaarden te komen. Dat geeft ons een veel grotere positie dan wanneer we dat als land alleen zouden doen. Intussen moeten we ervoor zorgen dat we in Nederland zelf digitaal zo veilig mogelijk worden, waar het nog niet Europees is. Een koploperpositie, zoals de heer Verhoeven dat noemt, kan geen kwaad, hoewel ook andere landen daar zeer sterk in zijn.

De heer **Verhoeven** (D66):
Helemaal eens. Is aan die standaarden en criteria ook de consequentie van een verkoopverbod verbonden? Wordt er op dat niveau over gesproken en is dat de Nederlandse inzet?

Minister **Grapperhaus**:
Het is niet zo dat Nederland nu als harde inzet heeft om in die standaarden op te nemen dat producten hoe dan ook van de markt moeten worden gehaald, maar Nederland heeft wel een inzet die erop neerkomt dat standaarden en de certificering op basis van die standaarden een zeer belangrijke, zo niet harde eis worden. Uiteindelijk moet die certificering natuurlijk hoe dan ook als uitkomst hebben dat onveilige producten uit de markt raken, of in ieder geval bij de consument weg raken.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Er waren een aantal vragen rondom Kaspersky.

De heer **Arno Rutte** (VVD):
Ik heb een heel verhaal verteld over mijn grote zorgen over mensen die beveiliging aanbieden, beveiligingsdiensten en beveiligingsproducten. Dat was een iets andere vraag dan de vraag of de software veilig is. Nee, het gaat om de dienst die bedrijven aanbieden om je bedrijf of computer te beveiligen. Daarbij gebeurt alles maar naar best effort, maar als er ellende van komt, loopt iedereen daar gillend van weg en zegt: daar kan ik ook niks aan doen. Hoe kan ook daar de aansprakelijkheid verbeterd worden? Welke eisen mag je aan dit soort producten en diensten stellen? Mag ik de Minister zo begrijpen dat hij dat ook wil meenemen in het hele verhaal over softwareaansprakelijkheid? Ik vraag dat specifiek omdat dat wel een iets ander vraagstuk is dan alleen de vraag of de geleverde software inherent onveilig was.

Minister **Grapperhaus**:
Even terugkomend op een paar dingen. Ik heb net al gewezen op de verkenning die het CCV, het Centrum voor Criminaliteitspreventie en Veiligheid, is begonnen met verzekeraars om een cybersecurityrisicomodel te maken. Dat moet ook leiden tot een keurmerk voor aanbieders van cybersecuritydienstverlening. Ik geef het punt van de aansprakelijkheid mee aan de Staatssecretaris van Economische Zaken. Zij zal daar in het kader van de behandeling van de roadmap bij u op terugkomen. Dat ligt net buiten het bereik van waar ik hier over spreek en kan spreken. Het

punt van de aansprakelijkheid van de dienstverleners is door u gemaakt en zal bij de behandeling van de roadmap terugkomen.

De heer **Arno Rutte** (VVD):
Het is heel verstandig dat de dingen worden opgepakt door het CCV samen met verzekeraars. Dat helpt, want dan krijg je inzicht. Dat gebeurt ook bij sloten, bij hekwerk en al dat soort zaken. Dat helpt om de verzekerbaarheid vooruit te brengen. Ik vind het heel belangrijk, en ik hoop ook dat de Minister dat indringend doet, dat het niet alleen maar gaat over de aansprakelijkheid voor je product, de software die je levert, maar ook over de aansprakelijkheid voor de dienst, de belofte die je doet met je dienst. Wij zouden het ook niet accepteren als een beveiligingsbedrijf twee slapende beveiligers stuurt en bij een inbraak zegt: sorry, het was best effort, dit waren de besten die we konden krijgen.

Minister **Grapperhaus**:
Ja, maar ik kan alleen maar herhalen wat ik net gezegd heb. De risicoanalyse van het CCV moet leiden tot certificering. De kwestie van de eventuele aansprakelijkheidsissues komt bij de roadmap aan de orde. Daar komt de Staatssecretaris bij u op terug.

De **voorzitter**:
Dank u wel. Gaat u verder.

Minister **Grapperhaus**:
Kaspersky. Een aantal leden heeft gevraagd of er een kader is geweest aan de hand waarvan de beoordeling heeft plaatsgevonden en, zo ja, wat dat kader is geweest. Inderdaad, dat kader is er geweest. Dat heb ik ook in de brief inzake Kaspersky aan uw Kamer aangegeven. Er zijn een drietal factoren die in combinatie met elkaar hebben gezorgd voor dit besluit. Het eerste punt is het feit dat de antivirussoftware van Kaspersky diep in systemen zit. Dat geeft een risico. Als op enig moment na een verplichte instructie – daar kom ik zo op – van de Russische overheid daarmee gemanipuleerd wordt, dan kan dat heel diep in de systemen ernstige gevolgen hebben. Het eerste toetspunt is dus: over wat voor software spreken we hier? Het tweede punt is de Russische regelgeving die bedrijven verplicht mee te werken met de Russische inlichtingendienst. Het derde toetsingspunt is dat in dit geval de Russische overheid een offensief cyberprogramma heeft dat gericht is op Nederland en Nederlandse belangen. Dat laatste is gebaseerd op vertrouwelijke inlichtingen van de diensten.
Daarmee kom ik meteen bij het punt van de heer Alkaya, die terecht erop wijst dat er ook andere landen zijn waar die verplichting bestaat voor bedrijven die in die landen zijn gevestigd, die in voorkomende gevallen gedwongen zijn mee te werken met overheden. Maar in die landen, bijvoorbeeld de Verenigde Staten, speelt in ieder geval dat derde punt niet.

De heer **Alkaya** (SP):
Een informatieve vraag hierover. De heer Van Dam en ik hebben inderdaad een technische briefing hierover gehad. Het is heel moeilijk om vast te stellen waar de dreiging precies vandaan komt, of het de overheden in die landen zijn, aan de overheid gelinkte organisaties of gewoon criminelen in die landen. Hoe gaat de afweging op dat derde punt in de praktijk in zijn werk? Maakt uiteindelijk de Minister op basis van vertrouwelijke informatie persoonlijk die afweging: ja, hier wordt voldaan aan die derde optie? Kunnen wij hem dan ook daarop aanspreken?

Minister **Grapperhaus**:

Dit is een afweging die door mij verantwoord wordt in de Raad voor Veiligheid en Inlichtingen. Via dat kader vindt ook de toetsing door de Kamer plaats.

Mevrouw **Buitenweg** (GroenLinks):
Ik denk dat het van belang is dat bedrijven weten voor wie dit zal gelden. Anders worden zij ineens geconfronteerd met het feit dat bepaalde software in de ban gaat, terwijl zij daarin geïnvesteerd hebben. Laten we een concreet land noemen. Geldt dit ook voor Chinese producten? Hoe bereidt u voor dat bedrijven weten of kunnen verwachten dat die software in de ban gaat?

Minister **Grapperhaus**:
Er is gewerkt aan een aanbestedingsprotocol waarmee bij een toekomstige aanbesteding in diverse fasen kan worden getoetst in hoeverre deze drie elementen een rol spelen c.q. in de toekomst een rol zouden kunnen spelen. Verder kunt u zich voorstellen dat het heel nauw luistert en dat het uiteindelijk een case-by-casebeslissing zal moeten zijn. Dat is natuurlijk heel lastig, maar ik heb deze drie concrete criteria genoemd. Vandaar dat het goed was om even te benadrukken dat dit geen beslissing is van alleen deze Minister waarop geen toetsing plaatsvindt. Die beslissing wordt in den brede getoetst binnen de RVI en daarnaast ook in het kader waarbinnen de RVI parlementair wordt getoetst.
Maar ik wilde toch nog even doorgaan op het punt dat mevrouw Buitenweg terecht maakt. Laten we dan ook even gaan naar de punten die door u en de heer ...

De **voorzitter**:
We zijn nog steeds met de beantwoording van een interruptie ... Nee?

Minister **Grapperhaus**:
Ik wilde namelijk zeggen: het punt van de Chinese bedrijven.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Het gaat om de Chinese bedrijven. Dan hebben we het over Huawei en C2000; laten we het allemaal bij de naam noemen. De Nederlandse overheid beziet de risico's die verbonden kunnen zijn aan digitale producten en diensten, ook van dergelijke Chinese bedrijven. Dat gebeurt echt heel zorgvuldig case by case op basis van de drie criteria die ik noemde. Nogmaals, die staan in mijn wat ik maar even noem Kaspersky-brief. Voor degenen die dat in alle rust nog willen nalezen, staan ze uitvoerig beschreven. In het geval van Kaspersky heb ik toegelicht en verantwoord dat de combinatie van de toets op die drie punten ertoe heeft geleid dat er is geoordeeld dat er sprake is van risico's voor de nationale veiligheid. Ten aanzien van de antivirussoftware wil ik overigens benadrukken dat dat bij andere producten niet het geval was. Gezien de nationale veiligheidsbelangen en ook de belangen van het bedrijfsleven, is het onmogelijk om met elkaar vooruit te lopen op of te speculeren over al dan niet toekomstige maatregelen. U zult iedere keer zien dat ik aan uw Kamer een brief zal sturen waarin ik een dergelijke beslissing verantwoord. Die beslissing is daarvoor getoetst op de wijze zoals ik naar aanleiding van de vraag van de heer Alkaya heb omschreven. Ik vind de vraag van mevrouw Buitenweg volkomen begrijpelijk, maar de transparantie is er in ieder geval achteraf in de verantwoording aan uw Kamer en aan de hand van deze drie gehanteerde criteria. Nogmaals, er wordt bij toekomstige aanbestedingen ook gewerkt met een aanbestedingsprotocol

waarin de toetsstenen voor en tijdens het aanbestedingsproces ook benoemd zijn.

De heer **Verhoeven** (D66):
Ik wil nog weten of dezelfde drie eisen gelden voor eventuele alternatieve aanbieders. Heeft hun land een offensieve cyberstrategie? Heeft hun land de plicht om die bedrijven te laten samenwerken met de betreffende binnenlandse veiligheidsdiensten? En leveren die bedrijven ook software die diep in de systemen gaat? Dat eerste criterium snap ik wel. Maar ja, dat maakt nou juist de antivirussoftware zo goed. Eigenlijk zeg je: we gaan voor zwakkere spelers omdat ze dan minder diep erin zitten. Dan zit je alweer in een soort van dilemma tussen veiligheid en veiligheid.

Minister **Grapperhaus**:
Het antwoord aan de heer Verhoeven is ja. Die drie criteria zijn consistente criteria, die dus ook voor alternatieve aanbieders in het kader van een aanbesteding zouden worden gehanteerd. Nogmaals, we moeten benadrukken dat, zoals ik ook in de brief heb aangegeven, het ook gaat om een afweging ter voorkoming van verwezenlijking van grote risico's voor de nationale veiligheid.

De heer **Verhoeven** (D66):
Oké. Dat derde punt vat de Minister waarschijnlijk wel samen en het zal iets genuanceerder zijn opgeschreven. Maar een offensieve cyberstrategie moet dan wel tegen Nederland gericht zijn, want er zijn natuurlijk tal van landen met een offensieve cyberstrategie. Het moet dan ook echt onderbouwd zijn door de diensten dat daar sprake van is, enzovoorts.

Minister **Grapperhaus**:
Het antwoord is helaas ja. Ik zeg «helaas», omdat deze beslissing een heel zorgvuldige afweging is geweest die genomen moest worden in het belang van de nationale veiligheid. Alle drie de criteria die ik genoemd heb zijn zorgvuldig nagelopen en hebben tot die beslissing geleid.

De heer **Arno Rutte** (VVD):
Is daarmee het hele kopje Kaspersky voor de Minister klaar, of komt er nog iets?

Minister **Grapperhaus**:
Ik heb nog wel een aantal antwoorden. Die zal ik doorlopen.
Een vraag van CDA, GroenLinks, D66 en SP is: hoe zorgt u als kabinet nu voor een consistent en voorspelbaar beleid voor bedrijven? Ik heb daar al iets over gezegd, ook over dat aanbestedingsprotocol. Ik zal daar niet lang meer bij stilstaan. Maar waar het natuurlijk toch om gaat, is dat nationale veiligheidsbelangen en economische belangen hier zij aan zij staan. Ik ben me ervan bewust dat de helemaal eenduidige aanpak die het nationale veiligheidsperspectief geeft, er nog niet voor de volle 100% is. Die moeten we juist in het kader van die Cybersecurity Agenda verder ontwikkelen. We hebben hier echt te maken met een nieuw terrein, dat we ook in samenspraak met private partijen goed willen inrichten. Daar spelen gewoon een aantal heel belangrijke dilemma's. Ook dat wil ik hier niet verhullen. De heer Verhoeven hintte daar al een beetje op, want je wilt uiteindelijk niet, bijvoorbeeld als het om antivirussoftware gaat, met een partij zakendoen die nou juist weer níét diep in die systemen gaat. Dan doet die software namelijk niet het werk waar die nou juist voor bestemd is, althans niet optimaal. Maar in ieder geval, een van de prioriteiten, die u ook terugvindt in de Cybersecurity Agenda, is om erop in te zetten dat we hier echt een steeds verdergaande, beleidsmatige aanpak op hebben.
De heer Rutte stelde ook nog de vraag wat nou de consequenties zijn en hoe het zit met adequate alternatieven. In de markt zijn meerdere

alternatieven beschikbaar. De consequenties van de maatregel zijn van tevoren afgewogen. De maatregel geldt voor de rijksoverheid en voor de vitale infrastructuur op basis van een risicoafweging, waarbij bijvoorbeeld ook KPN als vitale aanbieder wordt gezien. Dit is dus ook van toepassing op diensten en systemen die partijen leveren aan de rijksoverheid.
De heer Rutte en mevrouw Buitenweg hadden nog vragen naar aanleiding van de Cloud Act. Ik ben daar natuurlijk mee bekend. Wat mij betreft is dat een andere situatie dan die ten aanzien van de tegenover Kaspersky getroffen voorzorgsmaatregel. Daar is sprake van de combinatie van de drie factoren die ik al genoemd heb, die ga ik niet voor u herhalen. Daar is dus op gehandeld zoals aan de hand van die drie criteria is gehandeld.

Mevrouw **Buitenweg** (GroenLinks):
Ik probeer het verschil duidelijk te maken. Het verschil is dat in het geval van de Cloud Act een deel van de criteria er natuurlijk alsnog aan voldoet, maar dat het offensieve programma niet specifiek op Nederland gericht is. Er is dus wel sprake van een offensief programma, er is wel sprake van antivirussoftware die diep in de systemen zit, er is sprake van dat van bedrijven geëist wordt dat ze aan dat offensieve programma meedoen. Maar het verschil is dat dit moment de regering dat niet op Nederland richt.

Minister **Grapperhaus**:
Ja, zo is het. Ik wil benadrukken dat de diensten op dit punt alert zijn, ongeacht de landen die het betreft. Waarbij op 1 en 2 een ja is gegeven dat dat speelt.

Mevrouw **Buitenweg** (GroenLinks):
Ik snap heel goed dat het politiek gezien niet op Nederland zit, maar er is natuurlijk ook vaak sprake van bedrijfsspionage, die ook vaak door overheden wordt gestimuleerd, ook voor de economische groei en bloei ergens anders. Hoe wordt dat meegewogen?

Minister **Grapperhaus**:
Als van overheidswege sprake is van een offensieve bedrijfsspionagecampagne – het kan ook zijn dat er bewijzen zijn dat die campagne via het bedrijfsleven loopt van een betreffend land maar dat de overheid daar heel actief bij betrokken is – dan geldt daar in beginsel ook hetzelfde derde criterium voor, want dan is er sprake van een offensieve campagne. Maar dat is dan van overheidswege van het betreffende land, want dat heeft weer te maken met de combinatie met het tweede criterium, de vraag of dit land wetgeving heeft die bedrijven uit het land, dus ook softwareproducenten, dwingt om mee te werken met de overheidsdiensten van dat land om bijvoorbeeld te manipuleren?

De heer **Arno Rutte** (VVD):
Het is heel goed dat de Minister hier zo uitgebreid op ingaat. Dat geeft ook wel wat handvatten om in de toekomst te kijken hoe dit werkt. Dat is heel inzichtelijk. Dank daarvoor. Mijn vraag, voor zover de Minister daar antwoord op kan geven, gaat over twee landen waar op het gebied van digitale infrastructuur en software heel veel zaken mee moet worden gedaan. Het ene zijn de Verenigde Staten en het andere is China. Dat zijn toch ook allebei landen waar deze problematiek in ieder geval op nummer 1 en 2 staat, van wat de Minister net omschrijft. Het zijn op zich bevriende landen en tegelijkertijd voel je ook het ongemak. Als het nu gaat om virussoftware, is dat lastig, want dat zit diep in systemen, daar hebben mensen ongemak van. Maar stel nu dat in China wel in één keer die offensieve strategie komt, die onze hele digitale infrastructuur raakt. Bijna elke zendmast is een Huawei-zendmast, om eens wat te noemen. Dan kom je er toch niet als je zegt: «die mag niet meer»? Dan hebben we

namelijk helemaal geen zendmast meer staan. Andersom, als de overheid als bedrijfssoftware Office 365 gebruikt, en we vinden dat de Verenigde Staten toch wel een erg offensieve strategie heeft, dan kun je niet zomaar zeggen «dat doen we niet meer», want dan valt de hele rijksoverheid om, en alle gewone kantoorautomatisering. Een lange vraag, maar de vraag is eigenlijk: denken we daarover na? Zijn we daarop voorbereid, ook om eventueel alternatieven te hebben?

Minister **Grapperhaus**:
Laat ik nog even het eerste criterium pakken, over het diep in de systemen zitten. Dat is natuurlijk een heel belangrijk punt. Op het moment dat we te maken hebben met een leverancier die met zijn producten of diensten diep in onze systemen zit en die daarnaast uit zo'n land komt waar die dwangwetgeving bestaat om mee te werken met overheidsdiensten en dan dus mogelijk te manipuleren, en we weten vervolgens dat ze offensief gericht zijn, dan is er in het kader van de nationale veiligheid helaas geen andere afweging mogelijk. Want daarom heb je die drie criteria om te concluderen: met deze leverancier van dit product – zo is het ook gegaan ten aanzien van Kaspersky – kunnen we geen risico nemen in het kader van de nationale veiligheid. Dat betekent dat wij – daar mag u inderdaad ook op rekenen – natuurlijk van tevoren ook hebben meegewogen, erop hebben geanticipeerd dat er ook daadwerkelijk alternatieven en uitwijkmogelijkheden zijn. Dat hebt u mij ook horen antwoorden bij Kaspersky.

De heer **Arno Rutte** (VVD):
Dat laatste is van belang. En ik geloof ook direct dat dat bij antivirussoftware het geval is, hoewel ook dat best ingewikkeld is, zoals ik van deskundigen begrijp.
Ik heb er begrip voor dat de Minister niet tot in alle punten en komma's kan antwoorden, want dit gaat over nationale veiligheid, dat is lastig. Maar het is niet een geheel theoretische gedachtenkronkel dat we ons ten aanzien van dingen die in China gebeuren op een bepaald moment ook ernstig zorgen gaan maken. Dan hebben we het niet meer over iets wat antivirussoftware heet, maar inderdaad bijvoorbeeld over de hele infrastructuur aan zendmasten op het gebied van gsm. Dan kun je zeggen dat het niet diep in je systeem zit, maar het kan wel om heel kwetsbare informatie gaan. Hebben we op zo'n moment ook echt van tevoren al, nu al strategisch nagedacht of kunnen we nadenken over alternatieven? Hoe vullen we dat in? Voor zover de Minister daar wat over kan zeggen, denk ik wel dat dat relevant is.

Minister **Grapperhaus**:
Daar wordt voortdurend over nagedacht, want we moeten ons realiseren dat dit een van de kernonderwerpen is van cybersecurity. De heer Van Dam heeft de vergelijking gemaakt met, als ik het goed mag zeggen, digitale dijkbewaking. Dat is een gegeven waar onze regelgeving in de toekomst helemaal op moet zijn ingericht. Vandaar ook zo'n aanbestedingsprotocol. Het is ook een gegeven waar we ons beleid op moeten inrichten. Dat betekent dus niet alleen maar zeggen: we toetsen langs die drie criteria en we kunnen die zendmasten niet meer gebruiken, want de leverancier voldoet niet aan die drie criteria. Nee, we moeten ook anticiperen en kijken hoe we het mogelijke probleem dat daardoor ontstaat gaan oplossen. Blijft nog steeds – dat wil ik hier voor alle aanwezigen benadrukken – dat, als je cybersecurity echt heel goed wilt invullen, je dat case-by-case en met maatwerk zult moeten doen. Maar ik blijf ten slotte ook verantwoorden aan uw Kamer – want dat heeft uw Kamer gezien – wat ik beslist heb en waarom. De heer Alkaya heeft antwoord gehad op de vraag of dat een beslissing was die ik in mijn eentje heb genomen. Nee, deze beslissing is wel degelijk getoetst, zowel binnen het kabinet als binnen een kleine groep van de Kamer.

De heer **Van Dam** (CDA):
Voorzitter, excuus dat ik nog even doorvraag op dit punt. Toen ik die berichtgeving over Kaspersky las, dacht ik: waarom nou Kaspersky? Maar tot mijn genoegen kom ik erachter dat er beleid achter zit. Het is toch prachtig dat er een soort criteria zijn die erachter zitten. Maar hoe kunnen Nederlanders nou kennis nemen van dat beleid dat erachter zit bij hun eigen afweging of hoe kan een ministerie dat een nieuw systeem aanschaft dat? Daar zijn twee opties voor: of ze gaan deze brief over Kaspersky lezen – de kans dat de gemiddelde Nederlander dat doet is niet groot – of ze gaan de uitzending van dit AO nakijken, waarop de kans ook niet heel groot is. Dus zou de Minister nou niet bereid zijn om dat beleid nog eens apart te formuleren en ook bekend te maken? Ik kan me ook heel goed voorstellen dat dat een soort groeimodel is, maar ik denk dat dit echt een wezenlijke bijdrage zou kunnen leveren aan het veiliger worden van Nederland.

Minister **Grapperhaus**:
De brief? Inderdaad, daar heb ik de Kamer over geïnformeerd. Ik heb de drie punten die ik nu steeds herhaal dezelfde ochtend op radio 1 uiteengezet op de korte manier die, naar ik stellig verwacht, door alle luisteraars is begrepen. Ik heb het ook voor de NOS-televisie nog een keer uitgelegd, want ik realiseer me terdege dat het goed is dat burgers van Nederland weten wat de afwegingen zijn en hoe dat kader werkt. Het staat ook in het persbericht, maar ik wil zeker wat de heer Van Dam zegt nog eens meenemen en benadrukken dat wij ervoor zullen zorgen dat dit soort beslissingen en vooral dat afwegingskader zo veel mogelijk bekend worden, zodat mensen weten waar ze aan toe zijn.
Daar wil ik nog het volgende over zeggen. De heer Van Dam vroeg nog – ik begrijp dat de voorzitter het goed vindt dat ik daarop in aansluiting op de interruptie van de heer Van Dam nog even inga – hoe burgers en bedrijven buiten de vitale infrastructuur op de maatregel moeten reageren. Welnu: die moeten natuurlijk hun eigen afweging maken, want het risico dat ten aanzien van die maatregel is genomen, gaat over de nationale veiligheid. Dat richt zich op het voorkomen van cyberspionage en cybersabotage bij de rijksoverheid en de Nederlandse vitale infrastructuur. Het overgrote deel van onze samenleving is natuurlijk geen doelwit van die dreiging. Die moeten zich eerder vooral richten op het waken tegen vormen van cybercrime. Eenieder kan daarin zijn eigen afweging maken. Maar ik benadruk het punt van de heer Van Dam dat het afwegingskader wat de overheid hier heeft gehanteerd zo veel mogelijk bekend moet zijn.

De heer **Van Dam** (CDA):
Ik heb in eerste termijn al gezegd dat ik erg veel waardering heb voor alle plannen die er liggen. Soms vind ik ze in hun formulering nogal vaag en abstract. Ik had net met mevrouw Buitenweg daarover een gesprekje, waarin ik een woord gebruikte dat zich niet leent voor de parlementaire microfoon. Dit lijkt mij nou juist zo'n kans om het concreter te maken, om ook mensen iets in handen te geven. Ik zou er erg op aan willen dringen dat er een soort beleidskader veilige software komt, wat dan misschien ook kan oplossen dat die statelijke actoren iets beter en concreter in beeld komen, dat mensen, bedrijven en overheidsorganisaties daar zelf hun gedrag op af kunnen stemmen.

Minister **Grapperhaus**:
Echt even voor de mensen die kijken, voor de gewone burger: we moeten twee dingen heel goed uit elkaar blijven houden. De veilige soft- en hardware zit hem vooral in het verder ontwikkelen van de roadmap. Dat is primair een taak van de Staatssecretaris van Economische Zaken. Daar wil ik niet te zeer in treden. Dan hebben we het echt over de gewone,

alledaagse dingen die je gebruikt en waarvan je wilt dat ze digitaal veilig zijn. Dit gaat over softwareproducten en – diensten die een heel belangrijke rol kunnen spelen in overheidssystemen, die daar diep ingaan. Daar heeft de overheid een driepuntstoets, die ik zoals gezegd uiteen heb gezet in de brief en in de persmomenten daaromheen. Die driepuntstoets, herhaal ik toch nog even heel snel, want dat is altijd goed, bestaat uit punt 1: is dit hele wezenlijke, indringende software? Punt 2: is de leverancier een bedrijf dat gevestigd is in een land waar de overheid volgens wetgeving dat bedrijf kan dwingen om mee te werken aan oneigenlijk gebruik van die software? Punt 3: is dat land wat die wetgeving heeft bij onze diensten op dat moment bekend als een land dat een offensieve binnendringingsstrategie voert ten opzichte van Nederland? Is aan die drie criteria voldaan, dan moeten wij niet het risico nemen voor de nationale veiligheid. En nogmaals: dat is dat de gewone burger niet verward raakt. Dat is dus iets anders dan of je thermostaat thuis als internet of things veilig is.

De **voorzitter**:
Korte vervolgvraag van meneer Van Dam.

De heer **Van Dam** (CDA):
Wat mij betreft gaan deze criteria verder als de Grapperhaustoets door het leven. Ik begrijp ook heel goed dat dat niet om de kleine dingen gaat, maar een heel concreet voorbeeld: onlangs is er in de Defensiekring gesproken over het aanschaffen van een heel nieuw ICT-systeem. Volgens mij is dat een miljardenopdracht. Het lijkt me wezenlijk dat die Grapperhaustoets daar ook op wordt losgelaten. Ik vind het gewoon heel erg van belang dat dat een kenbare toets is binnen de overheid.

Minister **Grapperhaus**:
Er wordt mij nu te veel eer aangedaan. Ik merk dat het lid Verhoeven het heel prettig vindt dat ik dat nu even hardop uitspreek. Deze criteria worden evenzeer bij de systemen waar de heer Van Dam het over had gehanteerd.

De **voorzitter**:
Dank u wel. Gaat u verder.

Minister **Grapperhaus**:
Ik wilde nog even dat punt van de wederkerigheid van de heer Verhoeven aanstippen. Dat is een terecht punt. Wij hebben de mogelijkheid van een dergelijke reactie inderdaad meegenomen bij de afwegingen en de besluitvorming. Maar het kabinet heeft daar geconcludeerd dat met het oog op de nationale veiligheid en gezien de op het spel staande belangen het risico van digitale spionage en sabotage zo veel mogelijk moet worden voorkomen. Het heeft die maatregel daarom genomen. Via u nog tegen de heer Verhoeven: ik benadruk dat dat alleen gold voor dit type antivirussoftware en niet voor alle producten en samenwerkingen die er bestaan met Kaspersky. Daarmee wil ik alleen maar aangeven dat het absoluut geen soort algehele bedrijfsboycot is geweest. Niet.
Dan kom ik op een ander onderwerp dat de heer Rutte noemde, namelijk de politievrijwilligers. Hij vroeg naar de stand van zaken. Er is met de politievakorganisaties overeenstemming bereikt over het zogenaamde inzetkader politievrijwilligers en het sturingsconcept politievrijwilligers. Dat zijn twee wezenlijke onderdelen van het uniforme vrijwilligersmanagement. Er zijn ook allerlei stappen gezet over de rechtspositie, want dat is in dit kader echt van groot belang. Ten aanzien van het werven van nieuwe politievrijwilligers wordt er nog deze zomer een conceptplan werving en selectie besproken met de bonden en de LOPV. In dat kader wordt komend jaar al in dienst zijnde politievrijwilligers de gelegenheid

gegeven om doorstroomonderwijs te volgen. Op dit moment draaien bij de politie al vrijwilligers mee die zijn ingezet en deskundig zijn op het gebied van bestrijding van cybercrime, onder andere bij de landelijke eenheid, waarin zoals u weet ook extra wordt geïnvesteerd.

De heer **Arno Rutte** (VVD):
Dat klinkt heel goed. Waarom ik er toch even op terugkwam, is omdat ik weet dat een aantal bedrijven, mede naar aanleiding van het initiatief, echt klaar zit en min of meer wacht op dat contact met de politie. Dat is wat anders dan werven, waarbij je zegt: kom bij ons. Maar de vraag is: kom als bedrijf bij ons en wij denken graag met u mee over hoe we dat vorm kunnen geven. Ik geloof dat Defensie dat ook doet bij de Nationale Reserve. Zou zo'n stap onderdeel kunnen zijn van het wervingsbeleid? Dat zou bij de cybervrijwilligers enorm kunnen bijdragen.

Minister **Grapperhaus**:
Ik geef dat mee aan de korpsleiding, om dat in te brengen bij de LOPV.

De **voorzitter**:
Dank u wel.

Minister **Grapperhaus**:
Ik wil nog even naar de concretere aanpak op statelijke actoren, een vraag van meneer Van Dam. Ongewenste buitenlandse inmenging betreft inderdaad activiteiten van statelijke actoren. Er is een brede aanpak, die begint met een goede informatiepositie van de overheid en samenwerking tussen departementen en het lokale bestuur. We hebben ook allerlei diplomatieke instrumenten om die landen aan te spreken. Dat varieert van het vroegtijdig signaleren en bespreekbaar maken via diplomatieke kanalen tot het betreffende land publiekelijk aanspreken op inmengingsactiviteiten. Daarbij maken de betrokken diensten en departementen bij dreigende incidenten ook gebruik van maatregelen in het kader van openbare orde en veiligheid. Het kabinet neemt doorlopend maatregelen die bijdragen aan de weerbaarheid tegen ongewenste buitenlandse inmenging. Samen met de collega van BZK heb ik daarover een brief gestuurd. Dan hebben we het over maatregelen rondom het berekenen van verkiezingsuitslagen en gesprekken met sociale media over het tegengaan van desinformatie. Dat laatste – via u tegen de heer Verhoeven – is ook in Europees verband aan de orde. De collega van BZK is daar absoluut in the lead, net als bij het vergroten van de weerbaarheid van politieke ambtsdragers. Verder investeert het kabinet in de digitale weerbaarheid. Dat varieert van het weerbaarder maken van mensen op het punt van cybercrime tot en met het stimuleren van de cybersecuritybewustheid en investeringen bij bedrijven.
De heer Van Dam vroeg naar het dreigingsbeeld. Hij ziet daar ieder jaar dezelfde zin, met telkens twee woorden omgedraaid, als ik zijn betoog mag samenvatten. Gisteren heeft in het AO over de NAVO mijn collega van BZ toegezegd, nog dit jaar een brief aan de Kamer te zullen doen toekomen over attributie- en responsvraagstukken. Ik denk dat het goed is dat die brief er eerst komt en dat we dan concreter over dit onderwerp, voor zover het cybersecurity betreft, verder praten met elkaar.

De heer **Van Dam** (CDA):
Wat bedoelt u met die attributie en dat andere woord dat ik alweer kwijt ben?

Minister **Grapperhaus**:
Attributie is het toewijzen aan landen van bepaalde acties, op een bepaalde schaal, van onwaarschijnlijk naar zeker. Dat laatste is het

overigens bijna zelden, maar goed. Ik denk dat het goed is om aan de hand van die brief dat onderwerp verder te bespreken.
Mevrouw Buitenweg had...

De heer **Van Dam** (CDA):
Dan toch: heel goed dat dat gebeurt, maar ik zou de Minister willen oproepen om in de volgende criminaliteitsbeeldanalyse – er zijn er genoeg op andere terreinen – iets meer concreet te worden. Dat biedt onze diensten namelijk de gelegenheid om ook concretere handelingen te ondernemen. Ik zou toch hopen dat in de loop der jaren dat beeld zich wat concreter ontwikkelt.

Minister **Grapperhaus**:
Die oproep neem ik mee.

De **voorzitter**:
Helder. Gaat u verder.

Minister **Grapperhaus**:
Mevrouw Buitenweg had een vraag over het investeringsklimaat. Hoe voorkomen we dat kennis en techniek uit Nederland wegvloeien en wat is de rol van de overheid daarbij? Welnu, ik heb u daarover op 26 juni een brief gestuurd, met daarin een duidelijke uitwerking van de rol van de overheid en het inderdaad stimuleren van de kennisontwikkeling. De brief is ook namens de collega's van EZK en OCW gestuurd. Ik zal zo bij de beantwoording van een paar vragen van de heer Verhoeven daar nog wat nader op ingaan. Maar die brief geeft, denk ik, heel duidelijk het kader aan.
Verder...

Mevrouw **Buitenweg** (GroenLinks):
Het punt was juist niet de kennisontwikkeling – daarvoor is voldoende aandacht – maar hoe zaken en producten die ontwikkeld zijn op de markt worden uitgerold. Nederland is daar vaak slecht in. De kennis die opgebouwd is in Nederland, vertrekt vervolgens naar een buitenland. Dus de kennisontwikkeling, dat zit wel goed, maar het punt zit hem meer in het vermarkten. Daar zijn vaak onvoldoende mogelijkheden voor Nederland. Wil de regering de gevolgen daarvan bekijken?

Minister **Grapperhaus**:
Daar wordt natuurlijk ook in dit kader naar gekeken. Daarbij moeten we ons natuurlijk wel realiseren dat de thuismarkt en de investeringsmarkt van Nederland in eerste instantie geringere slagkracht hebben dan die van Microsoft. Aan de andere kant laat de ontwikkeling in Nederland zien dat bedrijven als het door de heer Verhoeven al genoemde ASML een heel grote omvang en een globale marktpositie hebben. Maar zij hebben ook een heel sterke positie in de eigen deelmarkt. Daarnaast – maar dan ga ik echt toe naar het terrein van Economische Zaken – heeft Nederland natuurlijk een sterk stimulerend beleid op het gebied van bedrijven die juist dit soort producten ontwikkelen. Maar ik ga daar niet al te veel op in, want dat is toch echt een debat wat uiteindelijk, denk ik, bij Economische Zaken thuishoort en niet bij mij.

Mevrouw **Buitenweg** (GroenLinks):
Dan gaan we niet dat hele debat hier doen, maar ik maak me juist zorgen als dat vooral ook gezien wordt als iets van Economische Zaken, want dat heeft natuurlijk een heel direct effect. Ik heb verschillende voorbeelden toegestuurd gekregen van bedrijven, waaronder een bedrijf dat ik noemde, dat een techniek heeft ontwikkeld om met name de infrastructuur van het internet beter te beveiligen. Als dat hier met heel veel

kennis en kunde is gemaakt en vervolgens, omdat hier toch weinig durfinvesteringen zijn, in Amerika moet worden vermarkt, dan verliezen we kennis en kunde die juist heel cruciaal zijn voor de cyberveiligheid. Mijn verzoek aan de Minister is dan niet om hier een heel betoog te houden over de investeringsagenda, maar wel om het niet alleen over te laten aan zijn collega vanuit het idee dat het over investeringen gaat, maar juist dat heel nadrukkelijk te betrekken bij de vraag wat de gevolgen zijn voor de veiligheid op het moment dat hier wel de kennis en kunde volgens nummertje 6 van de veiligheidsagenda worden ontwikkeld, maar we de producten vervolgens kwijtraken aan Amerika. Kan hij dat echt nadrukkelijk wel blijven volgen met zijn collega en het niet alleen aan Economische Zaken overlaten?

Minister **Grapperhaus**:
Eerst dit. U zegt zelf al dat er veel durfkapitaal is.

Mevrouw **Buitenweg** (GroenLinks):
Niet hier, in Amerika.

Minister **Grapperhaus**:
Misschien kan ik het even afmaken. Er is veel durfkapitaal, ook in Nederland. Er is heel veel private equity. Ik vrees dat het een misverstand is dat het alleen in Amerika is. Dat is een. Twee, het is zeker niet uit te sluiten dat activiteiten die hier zijn opgezet op enig moment een zwaartepunt krijgen in een ander land. We zien dat voortdurend gebeuren in het bedrijfsleven door overnames, fusies en andere vormen van bedrijfsinvesteringen. U kunt daar Amerika voor noemen. Daar ga ik inderdaad niet in treden. Dat is het investeringsbeleid en daar ga ik niet over. Ik moet vanuit het kabinet zorgen dat de cybersecurityontwikkeling in Nederland optimaal is. Mevrouw Buitenweg heeft een terecht punt dat dit betekent dat we als overheid moeten stimuleren dat bedrijven die zich richten op kennis- en productontwikkeling op het gebied van cybersecurity, hier zo veel mogelijk ruimte en gelegenheid krijgen. Vandaar dat we ook in zo'n onderzoeksinstituut willen investeren. Laat dat heel duidelijk zijn. Ik kom daar nog op.
Of die kennis en producten die hier ontwikkeld worden en waarin wij als overheid een stimulerende rol hebben gehad, uiteindelijk in andere vormen ook elders vercommercialiseerd worden, respectievelijk dat het eigendom van de productontwikkeling bij andere partijen terechtkomt, is een economische afweging waarover ik in een vrije economie niet ga. Het allerbelangrijkste is dat wij zorgen dat die kennis en producten ook hier zoveel mogelijk ontwikkeld worden in het belang van onze eigen cybersecurity. We zullen er zelf ook van moeten kunnen profiteren. Dat ben ik geheel met mevrouw Buitenweg eens. Als we dat stimuleren, moeten we er vervolgens ook de vruchten van kunnen plukken.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
De heer Verhoeven had enkele vragen. Over het afwegingskader wil ik het het eerst hebben. De AIVD en de MIVD werken op basis van de Wet op de inlichtingen- en veiligheidsdiensten. Deze discussie is vorige week bij de Wet computercriminaliteit III ook aan de orde geweest. Politie en OM werken op basis van het Wetboek van Strafvordering. Dat is een heel verschillend wettelijk kader, want politie en OM hebben alleen al te maken met een toetsing vooraf door de rechter-commissaris. Zo is de Wet computercriminaliteit III ook heel nadrukkelijk ingericht. Er is een toetsing vooraf door de rechter-commissaris en er is ook nog eens een toetsing voor die rechter-commissaris door de CTC binnen het Openbaar Minis-

terie. Dat is een soort voortoetsing voordat de zaak wordt voorgelegd aan de rechter-commissaris. Dan is er – dat geldt ook weer specifiek in de situatie van politie en Openbaar Ministerie – als het tot een zaak komt, nog een toetsing achteraf door de rechter ter zitting. Dat is een toetsing die heel anders is dan de toetsing die de diensten hebben, want die hebben alleen hun systeemtoetsing achteraf. Vorige week hebben we daarover in de Eerste Kamer goed met elkaar gediscussieerd. Uit het aannemen van het wetsvoorstel concludeer ik dat de meerderheid van de Eerste Kamer onderstreept dat er echt een hele zware toetsing vooraf zit op het werk van politie en OM. Ik ga nu niet in op de toetsingscriteria die worden gehanteerd, maar de conclusie is toch echt dat daar een heel goed en zwaar afwegingskader in zit. Ik denk dat daarmee de waarborgen bestaan waar de heer Verhoeven, terecht overigens, naar vroeg.
Ik ben er bijna, voorzitter, ik heb alleen nog een paar vragen van de heer Verhoeven, te beginnen met een vraag over de ethische hackers. Ik wil vooropstellen dat ik de samenwerking met de community van ethische hackers een van de grote verworvenheden vind van ons Nederlandse model. Ik blijf ze dus nauw betrekken bij het beleid, net als de andere stakeholders. Concreet is het NCSC, het Nationaal Cyber Security Centrum, in nauw gesprek met de ethische hackers om ervaringen op het gebied van responsible disclosure op te halen, zodat we gezamenlijk kunnen leren van de ervaringen van de afgelopen jaren. Dit stelt ons in staat om ook de leidraad die daar het fundament van vormt, nog dit jaar te actualiseren. Die wordt overigens ook ieder jaar gepubliceerd op de website van het NCSC.
Hoe willen we ervoor zorgen dat die ethische hackers en onderzoekers van het NCSC ook in de toekomst blijven vertrouwen als het NCSC soms gemelde zero-days doorspeelt? De heer Verhoeven zegt terecht dat het belangrijk is dat het NCSC een organisatie is die het vertrouwen geniet van onderzoekers en ethische hackers. Juist van die groep, want ik heb al gezegd dat het NCSC sterk aan de samenwerking hecht. De bijdrage van ethische hackers aan het digitaal veilig maken van Nederland is significant. De inlichtingen- en veiligheidsdiensten zijn een van de partijen waarmee binnen de wettelijke kaders, die strikt zijn, informatie gedeeld kan worden. Ik benadruk «kan worden», omdat het altijd aan het NCSC is om eerst nut en noodzaak daarvan af te wegen. Bij samenwerking met ethische hackers zal het NCSC dat altijd in goed overleg met die melder doen. Er kunnen situaties zijn – we hebben het dan over het belang van de nationale veiligheid – waarin het verstrekken van gegevens nodig kan zijn om die diensten, waarover we het hebben gehad, hun wettelijke taken te laten uitvoeren. Ik wil hier nog eens duidelijk zeggen dat mijn lijn voor het NCSC, het Nationaal Cyber Security Centrum, is dat er altijd in goed overleg met de melder gehandeld moet worden. Daarmee kan het NCSC ook echt die rol van vertrouwenspartner waarmaken.
De heer Verhoeven heeft ook nog een vraag gesteld over het cybersecurityinstituut. Ik zeg het heel voorzichtig, maar volgens mij sluit die aan bij waarmee mevrouw Buitenweg eerder kwam. Ik moet dat natuurlijk wel even zeker weten. Vanuit het kabinet zijn we gestart met een verkenning naar de mogelijkheden voor versterking van de kennis- en innovatieketen voor cybersecurity met onder andere de opzet van de kennis- en innovatieagenda. We bekijken hoe we die goed met publieke en private partijen voor de lange termijn kunnen opzetten. Dat is echt van belang, dat we voor de lange termijn innoveren op dit punt. In dat kader is er de wenselijkheid van een gespecialiseerd cybersecurityinstituut. Die verkenner gaat onderzoeken waarnaar ik in de brief van 26 juni verwijs. Hij gaat alle relevante actoren bevragen, financieringsstructuren in kaart brengen en kijken hoe we de verbetering van technologieoverdracht kunnen verwezenlijken. Ik zeg u toe dat die rapportage er zal zijn voor de begrotingsbehandeling van OCW, én EZK moet ik er dan even met nadruk

bij zeggen. U zult vanuit de verantwoordelijkheid van OCW en EZK hierover worden geïnformeerd.
Dan heb ik als laatste nog twee dingen. De heer Verhoeven vroeg ik of bereid ben om samen te werken met partijen als HackerOne om bug bountyprogramma's voor ministeries en overheidsinstanties op te zetten. Ik ben daar zeker toe bereid, maar hecht eraan dat dit een commercieel verdienmodel is, dus het afnemen van die diensten moet altijd binnen de kaders gebeuren die gelden voor overheidsinkopen. Ik denk dat dat helder is. Ik wil in ieder geval zeggen dat die bereidheid er altijd is.
Als allerlaatste vroeg de heer Verhoeven of het NCSC het aanspreekpunt wordt voor alle CERT's en dat is het zeker. Het NCSC staat in het kader van het nationale responsenetwerk andere CERT's bij en kan ze ook helpen. Volgens mij heb ik alles beantwoord, voorzitter.

De **voorzitter**:
Interruptie van de heer Verhoeven.

De heer **Verhoeven** (D66):
Over die zero days en de politie. Heb ik het goed begrepen dat de Minister zegt: voor de diensten verloopt het uiteraard via de Wet op de inlichtingen- en veiligheidsdiensten, plus het door de Minister van Binnenlandse Zaken daartoe ontwikkelde kader? Daar heb je dus eigenlijk twee zaken waarbinnen je als dienst moet blijven bij het gebruik. En voor de opsporingsdiensten geldt dat het via CC3 afdoende geregeld is en daarom acht de Minister het niet nodig om voor de politie eenzelfde kader te hebben als er is voor de diensten. Is dat in feite het antwoord van de Minister op mijn vraag?

Minister **Grapperhaus**:
Ja, waarbij ik nog niet heb genoemd dat er voor de politie en het OM ook nog een systeemtoetsing achteraf bestaat via de Inspectie Justitie en Veiligheid. Dat staat me zo helder voor de geest omdat we daar vorige week dinsdag uitvoerig over hebben gesproken in de Eerste Kamer. Ik wil dat even voor iedereen rustig herhalen. Dat betekent dus in de eerste plaats dat als de politie aan de slag wil, zo noem ik het maar even eenvoudigweg, met hacksoftware, men dan eerst langs het Openbaar Ministerie moet, dat daartoe een gespecialiseerde commissie heeft die dat eerst moet toetsen. Als het OM daar aanleiding voor ziet, moet men het voorleggen aan de rechter-commissaris. Dat is de toetsing vooraf. We hebben het er ook bij het wetsvoorstel Computercriminaliteit III uitvoerig over gehad dat dat een rechter-commissaris is die ook gespecialiseerde kennis heeft, die hem voldoende in staat stelt om die beoordeling te maken. Vervolgens is er, als er een strafzaak komt, ook nog een keer de toetsing door de rechter op de zitting of er terecht van dat instrument gebruik is gemaakt en of de toetsing destijds door de rechter-commissaris wel goed is geweest. Hoger beroep en cassatie noem ik even, maar ik ga daar nu verder niet uitvoerig op in. Daar zit een heel grondige, rechterlijke, onafhankelijke toetsing in. En ten slotte is er afgezien daarvan nog de mogelijkheid dat de Inspectie Justitie en Veiligheid in het kader van het systeemtoezicht zaken onder de loep neemt. Dat kunnen ook zaken zijn die helemaal niet voor de rechter zijn gekomen. De inspectie doet er dan verslag van of daarbij alles is gegaan zoals het had moeten gaan.

De heer **Verhoeven** (D66):
Volgens mij moet ik toch proberen om twee dingen uit elkaar te halen om mijn punt te maken. Je hebt natuurlijk de inzet van een bevoegdheid. Die moet je heel goed regelen bij wet, met toezicht, met systeemtoetsen of met een toets vooraf, toezicht achteraf. Dat is allemaal in de wetten geregeld. Dat moet dan ook conform de gedachtegang van de heer Van Dam: blijf nou niet doorzeuren over iets wat aangenomen is, we moeten

het daar nu mee doen. Prima. Het Ministerie van Binnenlandse Zaken heeft wel een kader gemaakt, en dat gaat niet zozeer over de bevoegdheid, maar veel meer over het gebruik van die onbekende kwetsbaarheden zelf. Hoe worden ze gebruikt, hoe worden ze bewaard, hoe worden ze gedeeld? Dat is nu echt iets heel anders en er is ook niet een inspectie op toegerust om daar goed op te controleren, zeker niet als er geen kader is. Daarom de volgende vraag. Waarom is er niet voor alle overheidsonderdelen eenzelfde kader voor de inzet en het gebruik van die zero-daysopsporing? Even los van de bevoegdheid, want die wordt al getoetst via wetgeving. Dat is mijn punt. Dus mijn vraag is eigenlijk: als er toch al een kader is voor de diensten, waarom datzelfde kader voor die zero days en het gebruik ervan – niet de inzet van de bevoegdheid – niet ook gebruiken voor de opsporing?

Minister **Grapperhaus**:
Dat heb ik al eerder aangegeven. Er zit hoe dan ook voor politie en Openbaar Ministerie een ander afwegingskader, omdat zij toetsen in het kader van het Wetboek van Strafvordering. Ik zie u meteen nee schudden, maar dat is al direct een strenge invulling van het afwegingskader dat ze hebben. Daaraan ziet u al dat er geen volledige parallel te trekken is met het afwegingskader voor de diensten. In de brief van 8 november 2016 is ook heel duidelijk uiteengezet hoe de rijksoverheid omgaat met die onbekende kwetsbaarheden. Bij de behandeling van de Wet computercriminaliteit III heeft uw Kamer met een amendement voorzien in een wettelijk verankerde procedure voor het uitstellen van de melding via de rechter-commissaris. Door Staatssecretaris Dijkhoff is gezegd: daarmee is ook heel duidelijk het afwegingskader ingevuld en is voldoende helder op basis waarvan die besluiten worden genomen. Het is niet aan mij, maar ik denk dat dit echt heel duidelijk in de procedures is verankerd. Vandaar ook dat het goed is geweest dat we dat vorige week nog een keer hebben doorgenomen in de Eerste Kamer.

De **voorzitter**:
Daarmee komt er een einde aan de interruptie van de heer Verhoeven, maar nog niet aan de eerste termijn van de Minister, want de heer Van Dam heeft hier ook nog een vraag over.

De heer **Van Dam** (CDA):
Ik heb niet een vraag hierover, maar ik constateer dat een aantal vragen van mij nog niet beantwoord zijn, onder andere een vraag over de verhouding van de brief van 20 april met als titel Naar een veiliger samenleving tot de Nederlandse Cybersecurity Agenda van 20 april. Een ander punt is de coördinerende rol van de Minister in relatie tot de abstractie van alle beleidsdoelstellingen. Hoe gaan wij als Kamer op een gegeven moment controleren hoe die 93 miljoen besteed is aan al die afzonderlijke maatregelen?

Minister **Grapperhaus**:
Wat het laatste betreft heb ik aangegeven dat ik periodiek bij uw Kamer verantwoording zal afleggen over de voortgang, ook over hoe er uiteindelijk met die 95 miljoen wordt omgegaan. Verder zijn we over de volle maatschappelijke breedte bezig met private en publieke partijen om maatregelen te nemen die passen in de ambities die we in de Cybersecurity Agenda hebben geformuleerd. Ik moet als coördinerend bewindspersoon dat monitoren en ik moet ook monitoren wat de voortgang van dat geheel is. Over die voortgang ga ik de Kamer periodiek berichten. Verder over de cybersecurity en cybercrime: die twee stukken waar u het over heeft, versterken elkaar. Dat geldt in het bijzonder voor de aanpak van cybercriminaliteit tegen de vitale sector, maar ook voor het treffen van

preventieve maatregelen zoals alleen al het versterken van cybersecurity awareness.

De heer **Van Dam** (CDA):
Ik wil alleen maar uitstralen dat ik echt heel graag wil dat wij tot concrete maatregelen komen. Daarin wil ik de Minister in zijn ongelofelijk lastige rol als coördinerend Minister een steun in de rug geven. Er ligt een enorme ambitie en het is verdeeld over meerdere ministeries. Ik zal ook op een later moment in deze commissie zijn coördinerende rol over dat hele terrein controleren. Ik vind het heel moeilijk om in beeld te krijgen waar die extra 97 miljoen die eraan komt, aan besteed wordt, maar ik vind dat wel heel belangrijk. Anders zie ik zo'n beetje hetzelfde gebeuren als wat er op het terrein van het onderwijs gebeurt, namelijk dat er geld ingaat, maar dat we met z'n allen achteraf helemaal niet kunnen reconstrueren wat ons dat dan heeft opgeleverd. Dat vind ik gewoon te veel geld en te veel belang. Dat is mijn punt.

Minister **Grapperhaus**:
Even geen misverstand. Ik zei net al dat ik natuurlijk verder verslag ga doen van hoe we dat geld, die 95 miljoen, zullen gaan uitgeven. Dat zal ook bij de departementale begroting aan de orde komen, laat dat duidelijk zijn. Dat wil ik hier echt benadrukt hebben. Een ander punt: misschien is het ten aanzien van die coördinerende rol goed om nog even te zeggen dat ik heel bewust erop heb aangestuurd, in overleg met de collega's, de Staatssecretarissen van EZK en van BZK... De Staatssecretaris van Economische Zaken is de trekker van de digitale economie en de Staatssecretaris van Binnenlandse Zaken is de trekker van het project Digitale Overheid. We hebben met elkaar afgesproken dat het van belang was om eerst de Cybersecurity Agenda neer te zetten, omdat die als het ware het fundament moet worden waar die twee andere projecten steeds weer goed op kunnen steunen. Mijn coördinerende rol betekent dat ik inderdaad ook betrokken blijf bij het zodanig uitwerken van die andere producten dat cybersecurity daar nog steeds als een wezenlijk element deel van uitmaakt. Daarover zal ik periodiek met uw Kamer opnieuw in algemene overleggen, of anderszins, in gesprek treden.

De **voorzitter**:
Dank u wel. Daarmee komt er een einde aan de eerste termijn van de zijde van de Minister. Ik zie dat de leden behoefte hebben aan een korte tweede termijn. Ik wijs erop dat er om 16.30 uur stemmingen zijn, dus ik zou u willen verzoeken om het kort te houden; meneer Verhoeven in het bijzonder. Als eerste geef ik het woord aan de heer Rutte van de VVD.

De heer **Arno Rutte** (VVD):
Voorzitter, dank u wel. Veel dank aan de Minister. Het onderwerp cybersecurity kan alle kanten uit vliegen, zoals de heer Van Dam ook zei, maar ik heb het idee dat wij als overheid samen met private partijen een agenda hebben gemaakt waar wij aan werken. Je ziet dat we elkaar in de Kamer op heel veel thema's vinden. Dat vind ik heel goed, net als de Minister, bijvoorbeeld bij die productaansprakelijkheid. We zijn er nog niet, want we weten nog niet hoe we het precies gaan doen, maar we zullen met elkaar dat pad af moeten lopen. De heer Alkaya is er niet meer, maar hij zei daarover dingen die mij ook uit het hart gegrepen zijn; dat een product gewoon aan zijn normale economische levensduur moet voldoen en dat daar ook een fatsoenlijke veiligheid bij hoort. Dat is heel goed. Mijn opmerking dat ook bij services en diensten op het gebied van onlineveiligheid wordt gekeken wat productaansprakelijkheid kan doen, sluit daarbij aan.
Ik vind het ook heel goed dat we uitgebreid van gedachten hebben gewisseld over Kaspersky en de criteria van de Minister gehoord hebben.

Alle begrip dat hij niet kan gaan tot de bodem van de details bij dit soort afwegingen, maar het is wel goed dat wij als Kamer snappen hoe dit soort afwegingen gaan. In de toekomst zullen we hiermee waarschijnlijk vaker te maken krijgen. Dan kunnen we dat een plek geven, en dat is goed. Organisaties kunnen daar dan ook op anticiperen.
Tot slot, de cybervrijwilligers bij de politie. Ik benadruk nogmaals dat er organisaties zijn die zitten te wachten met hun mensen en die zeggen: kom bij ons. Het gaat om cybervrijwilligers en financiële deskundigen. Ik zou zeggen: maak daar zo snel mogelijk gebruik van. Daar zal ik het bij laten.

De **voorzitter**:
Dank u wel. Meneer Van Dam, CDA.

De heer **Van Dam** (CDA):
Voorzitter. Ik wil vooropstellen dat ik onder de indruk ben van de documenten. Er zijn veel voornemens. Op pagina 2 van de brief van 20 april staat een alinea, waarvan ik de Minister vraag om die nog eens te lezen: «Het beleidsterrein cybersecurity richt zich op het voorkomen van schade door verstoring, uitval en misbruik van ICT. Hieraan zijn verschillende beleidsthema's verwant die onder verantwoordelijkheid van andere bewindspersonen worden vormgegeven.» En dan komt er: de Minister en Staatssecretaris van Binnenlandse Zaken, de Minister en Staatssecretaris van Economische Zaken en Klimaat, Buitenlandse Zaken, Defensie, de luchtmacht en de krijgsmacht. In deze context is er nog een nauwe samenhang met de Digitaliseringsstrategie, de Brede Agenda Digitale Overheid, de Defensienota, de geïntegreerde Buitenland- en Veiligheidsstrategie, de internationale Cyberstrategie, de integrale aanpak van cybercrime en de Defensie Cyber Strategie. Ik wens u echt heel veel sterkte – of klinkt dat te cynisch? – om die coördinerende rol in te vullen. Het is echt heel belangrijk dat dit gebeurt. U mag van ons verwachten dat we dat ook volgen. Daar zit wel een beetje zorg hoe je al die kruiwagens bij elkaar houdt. Dat is mijn diepe zorg, met nog steeds respect voor alles wat er op papier staat.

De **voorzitter**:
Dank u wel. Ten slotte de heer Verhoeven van D66.

De heer **Verhoeven** (D66):
Dank, voorzitter. Fijn dat de heer Van Dam inderdaad ook geen cynisme wil bij de ingewikkeldheid van dit dossier. Als we hier cynisch over gaan doen, over de complexiteit en dat we niks kunnen bereiken, dan doen we de Minister en het kabinet tekort. Ik wil de Minister danken voor de beantwoording. In zekere mate begint de discussie over cybersecurity nu concreet te worden. Er tekent zich nu wel een richting af op bepaalde onderdelen van het beleid en het begint dus substantieel te worden. Ik vind dat echt een compliment waard, want dat was een aantal jaren niet het geval. Toen was het een buzzwoord zonder inhoud en nu is het beleid met steeds meer concrete richting. Ik vind dat echt winst. Dank daarvoor. De mooie toezegging over de ethische hackers en over het instituut kunnen we verder bespreken bij de begroting.
Tot slot de punten die samen te vatten zijn in het woord «kader». Ik ben blij met de discussie over Kaspersky en ik ben benieuwd of die drie criteria de aanzet zijn tot een goed onderbouwd beleid hoe om te gaan met buitenlandse spelers op de markt. De discussie over Nederland dan wel Europa en over de beveiliging van IoT-apparaten is ook een kwestie van een goed kader hebben. Over zero-day blijf ik zeggen dat ik de beantwoording van de Minister snap, want ik weet hoe de discussie in de Eerste en de Tweede Kamer is verlopen over de Wet Computercriminaliteit III en de wetgeving over zero-day bij de politie. Ik zal me dus rustig

houden, want ik hoef geen concrete brief en ik zal ook geen motie indienen. Ik geef de Minister in overweging om erover na te denken of het zinnig is om het kader dat er al is bij Binnenlandse Zaken voor de diensten te gebruiken of te benutten voor de onder hem ressorterende opsporingsdiensten. Waarom niet?

De **voorzitter**:
Hartelijk dank. Daarmee komt er een einde aan de tweede termijn van de zijde van de Kamer. De Minister kan direct antwoorden.

Minister **Grapperhaus**:
Voorzitter. Ik zal heel kort antwoorden. Laat ik vooropstellen dat juist het feit dat Kamerleden als de heer Verhoeven zich niet rustig houden, ertoe leidt dat we in deze discussie ook echt verderkomen, en dat is niet gratuit, maar ik ben zeer erkentelijk voor het feit dat we dit lastige, ingewikkelde onderwerp, ook voor de mensen thuis, zorgvuldig met elkaar kunnen bespreken. In dat verband zeg ik toe dat ik nog eens naar het punt van de heer Verhoeven zal kijken en dat zal overwegen. Ik onderstreep de punten die de heer Rutte naar voren bracht over de oproep om vrijwilligers en het bedrijfsleven erbij te betrekken. Laat ik heel duidelijk zeggen dat het laatste uitvoerig wordt betrokken bij de publiek-private consultaties die onder andere plaatsvinden in het kader van de roadmap veilige hard- en software die ik net noemde.
Ten slotte wil ik afsluiten met wat de heer Van Dam zegt. De heer Van Dam heeft erop gewezen dat het onderwerp cybersecurity veel ministeries en dus ook veel delen van de samenleving raakt, en zo is het precies. Cybersecurity is echt een heel wezenlijk onderwerp voor onze huidige, maar ook onze toekomstige samenleving, want we zijn voor allerlei maatschappelijke processen en voor het goed functioneren daarvan in belangrijke mate afhankelijk van digitale technologieën, op allerlei manieren, die ik hier verder niet ga uitwerken.
Juist daarom is het van belang om cybersecurity als een fundament te leggen onder al onze digitale ambities, of ze nou maatschappelijk zijn, voor het nog beter laten functioneren van zorginstellingen en ziekenhuizen, of economisch, om ervoor te zorgen dat ons bedrijfsleven een nog grotere internationale concurrentiekracht krijgt. We moeten daar echt goede cybersecurity onder leggen.
Die coördinerende rol is een zware rol, dat ben ik met de heer Van Dam eens. Juist daarom stel ik goede periodieke overleggen met uw Kamer zeer op prijs, dat wil ik hier uitdrukkelijk gezegd hebben, want het is goed om dat mee te krijgen. Op een aantal punten heb ik toezeggingen gedaan, zoals u heeft gehoord. Ik heb gezegd dat ik bepaalde punten in overweging neem of meeneem naar mijn collega's. Het is echt goed dat we over dit onderwerp, dat wezenlijk is voor de komende tijd, met elkaar in dialoog blijven.
Dank u wel, voorzitter.

De **voorzitter**:
Ik dank u zeer. Ik herhaal nog even de toezeggingen en ik leg uit dat dit toezeggingen zijn die zich vertalen in een schriftelijk bericht aan de Kamer. Dat laatste was geen toezegging in de zin van deze lijst.
– De Minister zegt toe de Kamer voor de begrotingsbehandeling van Justitie en Veiligheid, Onderwijs, Cultuur en Wetenschap en Economische Zaken en Klimaat te informeren over de resultaten van de verkenning Cybersecuritykennisontwikkeling;
– De Minister zegt toe de Kamer jaarlijks te informeren over de hard- en software-roadmap uit de Nederlandse Cybersecurity Agenda en neemt daarbij mee het thema softwareaansprakelijkheid. Deze brief wordt opgesteld in samenwerking met de Staatssecretaris van Economische Zaken en Klimaat.

Er is geen VAO aangevraagd. Ik dank de Minister, zijn ambtenaren, de leden, de griffie, de verslagdienst, de ondersteuning en u allen op de publieke tribune en elders. Ik wens u allemaal nog een hele mooie dag toe.

Sluiting 16.19 uur.