33
Spionage door Rusland

Aan de orde is het **debat** over **spionage door Rusland**.

De **voorzitter**:
Aan de orde is het debat over spionage door Rusland. Ik heet de minister van Buitenlandse Zaken en de minister van Defensie van harte welkom en geef de heer Verhoeven namens D66 het woord.

De heer **Verhoeven** (D66):
Voorzitter, dank u wel. Begin oktober, want dit debat is inderdaad een tijd geleden aangevraagd, bleek dat onze inlichtingendienst, de MIVD, een Russische cyberoperatie had verstoord. Dat is een wereldprestatie, dat mag ook wel gezegd worden. De MIVD voorkwam dat de Russische militaire inlichtingendienst kon inbreken bij de OPCW. Dat was een agressieve en schaamteloze aanval van spionage. Bovendien bleek dat dezelfde spionnen ook actief waren in de MH17-zaak, bij de antidopingautoriteit en bij de Amerikaanse verkiezingen.

Het is niet meer te ontkennen dat Rusland actief probeert verkiezingen, internationale onderzoeken en de publieke opinie te beïnvloeden en te ondermijnen. Eerder waren mensen, ook hier, in deze Kamer, nog geneigd om deze dreiging wat te bagatelliseren; dat zou allemaal wel meevallen en er waren geen bewijzen van. Laat die naïviteit nu voor iedereen voorbij zijn; dit is gewoon een reële, actuele en ook continue dreiging.

Daarom ben ik blij dat de minister van Binnenlandse Zaken een overheidscampagne tegen nepnieuws begint. Zo kunnen we die beïnvloeding in de gaten houden en beperken in het komende verkiezingsjaar. Eerder heeft de Kamer al gesproken over dit onderwerp en over de gevolgen voor de relatie met Rusland. Ook cyberaanvallen worden nu een aanleiding om sancties in te stellen. Deze hackers worden ook op de EU-sanctielijst geplaatst, dus dat is al geregeld. Daarmee zorgen we ervoor dat dit soort cyberaanvallen ook niet onbestraft blijven. Hoe wordt dit sanctieregime nu ingezet, vraag ik de minister van Buitenlandse Zaken. Welke stappen gaat hij zetten? Graag een reactie.

Deze cyberaanval staat niet op zich. De OPCW-hackers zijn ook aangeklaagd in verband met een nucleair elektriciteitsbedrijf. In 2015 legden Russische hackers het elektriciteitsnet van Oekraïne plat en in 2017 was er een aanval van Russische malware, NotPetya, die een terminal in de Rotterdamse haven platlegde.

De minister van Defensie zei zelfs dat er sprake is van een cyberoorlog, en dat was geen verstandige uitspraak. Dat is ook een uitspraak die vragen oproept. Is er inderdaad sprake van een cyberoorlog? Wat is de definitie? Als het figuurlijk bedoeld was, wat werd er dan precies wel bedoeld, vraag ik haar.

Bovendien zei een cybergeneraal van het ministerie van Defensie bij Nieuwsuur dat ze graag auto's wil hacken. Dat is helemaal geen goed plan, want als ik met mijn kinderen in de auto naar Frankrijk zit, wil ik niet dat de auto onveilig is of door Defensie onveilig gehouden wordt. Criminelen kunnen dan immers ook die auto hacken en een ongeluk veroorzaken?

Daarom komt D66 vandaag met een initiatiefwet om regels te stellen voor het gebruik van cyberwapens door de overheid, want het moet een bredere afweging zijn dan alleen maar de smalle benadering van de nationale veiligheid en de mogelijkheid om verdachten te kunnen volgen of targets te kunnen uitschakelen. Ook veiligheidsbelangen in bredere zin in de economie, privacy en de vitale infrastructuur van ons land moeten worden meegewogen.

Tot slot. Ook ik zal het op deze laatste dag van het parlementaire jaar kort houden, een rode draad voor ons allen wat mij betreft. Ja, voorzitter, dat is ook mijn voornemen voor 2019, hoewel dat nu al een beetje afbrokkelt doordat ik er langer over praat, maar dat is dan een restje van het verleden.

Voorzitter. De dreiging is duidelijk. Cyberaanvallen komen steeds vaker voor, met als gevolg een soort digitaal Wilde Westen. Daarom roep ik de minister van Buitenlandse Zaken op om zich in te zetten voor een internationaal verdrag om regels en principes vast te leggen over cyberoorlog, net als de Geneefse Conventie, maar dan voor digitale oorlogvoering, om cyberaanvallen op kritieke civiele infrastructuur zoals elektriciteitsnetwerken, waterzuivering of ziekenhuizen te voorkomen. Ik weet dat dat niet makkelijk is. Attributie blijft altijd lastig bij cyberaanvallen, maar het is nu tijd om het te doen. Steunt de minister deze oproep? Hoe gaat hij zich hiervoor internationaal inzetten? Is hij bereid om met een groep gelijkgezinde landen op zoek te gaan naar een gezamenlijk voorstel binnen de Verenigde Naties?

Dank u wel.

De **voorzitter**:
Dank u wel, meneer Verhoeven. Dan geef ik nu het woord aan mevrouw Bruins Slot, namens het CDA.

Mevrouw **Bruins Slot** (CDA):
Voorzitter. Hier zijn complimenten voor de MIVD op zijn plaats. De inlichtingendienst heeft een cyberaanval van de Russen verijdeld. Laat iedereen nu ook de naïviteit voorbij zijn; ik heb het vaker gezegd. De Russen zijn in onze straten en in onze eigen achtertuin van de Tweede Kamer aan het spioneren. Daarom is het ook goed dat dit kabinet fors investeert in de MIVD, maar ook fors investeert in cyber.

Niet alleen Rusland, maar ook andere landen zoals China en hackersgroepen zijn actief in en tegen Nederland. Nederland is ook een interessant doelwit. Het doel is spionage, beïnvloeding, verstoring, maar het uiteindelijke doel kan ook vernietiging van vitale systemen zijn. Er is eigenlijk maar weinig meer over van ons vredesdividend. Dat noodzaakt tot scherpe, krachtige en effectieve maatregelen om digitale aanvallen af te kunnen slaan en op een passende wijze ook te kunnen vergelden. Deze ministers hebben al een keer eerder geschreven dat zij een breed strategisch kader ontwikkelen, zoals publieke attributie — dat heeft de minister nu gedaan — afschrikking, inzet van offensieve capaciteiten en een brede respons in het cyber-

domein. Het zijn eigenlijk onderdelen van de cyberdiplomatie waar de AIV in 2012 al op aandrong. Inmiddels zijn al zes jaar verstreken. Hoe staat het nou met de uitwerking van die verschillende individuele maatregelen? Deze minister zet zich er ook voor in om vanuit de Europese Unie tot cybersancties over te gaan. Hoe staat het daarmee?

De hackpoging van Rusland op de OPCW betrof spionage op een internationale organisatie. Dat roept wel de vraag op wanneer een cyberaanval een inbreuk is op de internationale rechtsorde of bijvoorbeeld een schending is van artikel 5. In navolging van D66 vindt het CDA dat door staten snel bindende juridische afspraken moeten worden gemaakt over en een praktische uitwerking moet worden gegeven aan de vertaling van het oorlogsrecht naar het digitale domein. Ooit is natuurlijk de Tallinn-manual opgesteld. Dat is gedaan door juristen, maar dat is een niet-bindend juridisch kader. Staten moeten natuurlijk met elkaar op politieke niveau overeenstemming bereiken over hoe je dat precies gaat uitvoeren. Nu bestaat het risico dat iedere staat daar zijn eigen draai aan geeft. Graag hoor ik een reactie van de bewindspersonen hierop.

Er zit echt een ander element aan vast. Dat betekent dat ook in Nederland duidelijk moet zijn wanneer een digitaal optreden van een staat ook daadwerkelijk een militaire aanval is, een oorlogsdaad. Wanneer is bijvoorbeeld een ontwrichtende cyberaanval op een ziekenhuis waardoor patiënten overlijden ook een officiële oorlogsdaad? Dat betekent dat je als land, dat Nederland, ook de vraag moet gaan beantwoorden wie wanneer welke partij aanspreekt op welke grondslag. En dat integrale beeld ontbreekt in ieder geval voor het CDA op dit moment. Het CDA vraagt de minister dus om ook voor Nederland een vertaalslag van het oorlogsrecht naar het digitale domein te maken en de Kamer dit te laten weten. Graag een reactie.

Ook is het van belang dat we internationaal weerbaar zijn en ons kunnen verdedigen. Dat vraagt om een NAVO die offensief cybersoldaten kan inzetten. De vraag is wel onder welke voorwaarden en wanneer die inzet is toegestaan. Graag een reactie van de minister van Defensie hierop.

Ik heb nog wel een vraag over de actie van de MIVD. De vier spionnen zijn nu naar de grens begeleid. Waarom is niet overwogen om de spionnen te arresteren, te vervolgen of uit te leveren aan de Verenigde Staten?
Door het antwoord van de directeur van de MIVD op de persconferentie lijkt het erop dat de diensten alleen op deze manier effectief kunnen opereren. Betekent dit dat onze diensten bepaalde bevoegdheden missen die ze wel nodig hebben of zouden moeten hebben om op dit punt nog effectiever te kunnen zijn? Graag een reactie van de minister.

Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Bruins Slot.

Dan geef ik nu het woord aan mevrouw Karabulut namens de SP.

Mevrouw **Karabulut** (SP):
Voorzitter. In eerdere debatten heb ik al gesteld dat inbreken op een wifinetwerk van een belangrijke internationale organisatie, in dit geval de Organisatie voor het Verbod op Chemische Wapens, de OPCW, onacceptabel is. En dat doe ik nu weer. Het is goed dat op tijd is opgetreden tegen deze Russische cyberoperatie. De uitzonderlijke openheid over dit incident en het handelen van de inlichtingendiensten heb ik toegejuicht. Dat verdient navolging.

Toen door de minister de openheid werd gezocht over dit Russische optreden, is nadrukkelijk gewezen op een oorlog met Rusland, een cyberoorlog waarin we verwikkeld zouden zijn. Daaraan werd de oproep gekoppeld "niet naïef" te zijn. Naïef is natuurlijk helemaal niemand hier in de Kamer. Wel ben ik van mening dat het onverantwoord is om een term als "oorlog" te gebruiken. Dat impliceert nogal wat. Je zou dergelijk woordgebruik "naïef" kunnen noemen, al is dat misschien nog iets te vriendelijk. Een vraag hierover. Kan de minister voorbeelden noemen van oorlogshandelingen tegen vitale infrastructuur op het gebied van cyber tegen Nederland of een van onze bondgenoten, waarbij onomstotelijk is vastgesteld dat Rusland, de Russische Staat, erachter zit?

Want hier raken we volgens mij een kernprobleem. Hoe kun je zeker weten wie er achter een aanval zit? "Attributie" heet dat met een moeilijk woord. In het geval van de OPCW is het duidelijk, maar in veel andere gevallen niet. Veel experts stellen dat het bijna niet mogelijk of zelfs onmogelijk is om de dader aan te wijzen. Dit omdat digitale sporen gewist kunnen worden. Het zou zelfs mogelijk zijn bij cyberaanvallen sporen achter te laten die een onschuldige als dader aanwijzen. Kan de minister hierop ingegaan? Hoe wordt met dit probleem omgegaan? Is attributie soms onmogelijk?

"Terecht is de Russische cyberoperatie bij de OPCW veroordeeld, maar dit soort veroordelingen treft alleen doel als zelf niet aan dit soort afkeurenswaardige praktijken wordt deelgenomen, als zelf geen cyberoorlog wordt gevoerd", zo citeer ik de minister. Ik herinner me wel een interessant stuk over een Nederlandse hack in Rusland, waar eerder dit jaar nieuws over was. De Verenigde Staten zouden hiermee geholpen zijn in het onderzoek naar Russische inmenging bij de verkiezingen van 2016. Maar wat is er nog meer gebeurd? Wat heeft Nederland daar allemaal gedaan? Waarom was deze hack nodig? Kan dit allemaal? Waarom is dit wel acceptabel?

Dan offensieve cyberinzet. Gevraagd naar de begrenzingen hiervan, stelde de minister niet uit te sluiten ook zonder de zogenaamde "artikel 100-procedure" offensief op te treden, dus buiten militaire missies waarin Nederland actief is. Kan de minister dit toelichten? Ik vind het uitermate zorgelijk. Kan ook gezegd worden of Nederland in het verleden al eens offensieve cyberaanvallen heeft gepleegd? En neemt de minister afstand van de levensgevaarlijke suggestie van oud-MIVD-chef Pieter Cobelens, gisteren in de krant, om "heel Moskou zonder spanning te zetten"?

Los van het eigen optreden is het handelen van bondgenoten hierbij ook relevant. Denk aan de onthullingen van Edward Snowden. Hij legde bloot hoe de Verenigde Staten zo'n beetje de hele wereld, vijanden maar ook vrienden,

bespioneerden, inclusief internationale organisaties zoals de Verenigde Naties en het Internationaal Atoomenergieagentschap. Zelfs de EU en Europese politici, tot en met Merkel, werden door de Amerikanen afgeluisterd. Een ouder voorbeeld betreft de zogenaamde "Stuxnetaanval" op Iran, die bijzonder schadelijk was en volgens tal van experts uit de Verenigde Staten kwam met Israëlische medewerking. Graag een reactie hierop.

Voorzitter. We kunnen het ons niet permitteren om hierover naïef te zijn, zou ik willen zeggen. Daarom de volgende vragen. Kan de minister zeggen hoe deze spionage zich verhoudt tot de spionage waar Rusland de laatste jaren van beschuldigd wordt? Is er in het digitale tijdperk sprake van radicalisering op het gebied van spionage door grootmachten? Is ondermijning van de internationale rechtsorde schering en inslag geworden? Hoe komen we tot de-escalatie? En op welke wijze kunnen we belangrijke infrastructuur beschermen tegen dergelijke aanvallen? Dat lijkt mij de uitdaging van dit moment.

De **voorzitter**:
Dank u wel, mevrouw Karabulut. Dan geef ik nu het woord aan de heer Koopmans namens de VVD.

De heer **Koopmans** (VVD):
Voorzitter, dank u wel. Nederlanders voelen zich bedreigd door Rusland. En terecht, want Rusland voert een zeer agressieve politiek van spionage en andere infiltratie. Moskou probeert door middel van hybride oorlogsvoering, angstzaaien en desinformatie andere landen en ook internationale organisaties te verzwakken, hun politiek te beïnvloeden en hun bevolking te verwarren. Dat tast ook het veiligheidsgevoel van Nederlanders aan.

In april van dit jaar onderschepte de MIVD vier Russische spionnen die wilden inbreken op het wifinetwerk van de in Den Haag gevestigde OPCW. Dit is een internationale organisatie die onderzoek doet naar de dodelijke vergiftigingen onlangs in Salsbury in Engeland, en naar het gebruik van chemische wapens in Syrië, waar honderden of misschien wel duizenden mensen door zijn vermoord. Uit de buitgemaakte laptops van de spionnen bleek ook nog dat die Russen hadden geprobeerd om in te breken op het MH17-onderzoek. Kortom, de Russische spionage is niet alleen gericht tegen Nederland en tegen in Nederland gevestigde internationale organisaties, waar Nederland gastheer van is en een taak voor heeft, maar ook tegen de internationale rechtsorde en daarmee dus tegen de hele wereld.

Voor de VVD leidt dit tot drie conclusies. Allereerst moeten wij de MIVD en andere geheime diensten die met de MIVD hebben samengewerkt, heel erg bedanken en lof toezwaaien. Het toont maar weer eens aan hoe belangrijk ze zijn voor onze veiligheid en het toont ook aan hoe belangrijk het is samen te werken met onze bondgenoten. Eerder hebben we van de minister begrepen — daar ben ik blij mee — dat ook de brexit geen gevolgen heeft voor de veiligheidssamenwerking. Ik zie de minister knikken, dus ik zal daar verder niet naar vragen.

Ten tweede: we moeten niet naïef zijn over de dreiging uit Moskou. Die vereist actie. We moeten verder investeren in onze veiligheid, zoals het kabinet nu ook doet. Ook moeten we zorgen dat er krachtige bevoegdheden zijn voor die diensten, dus ook voor ons cyberleger, met alle waarborgen, ook voor de privacy van mensen, opdat ze ons veilig kunnen houden. Verder moeten we doorgaan met de samenwerking met onze bondgenoten. Even los van de verontwaardiging die af en toe klinkt als president Trump iets geks zegt of als onze Britse vrienden zich weer eens in de voet schieten met hun brexit: die samenwerking en bondgenootschappen zijn essentieel voor onze veiligheid. Die moeten we dus vooropstellen.

Het derde punt: die Russische spionage is ook een wake-upcall. Er zijn ook in Nederland mensen die ik "Poetinfluisteraars" zou willen noemen, mensen die zich, toen deze hack naar buiten kwam, in allerlei bochten probeerden te wringen of probeerden goed te praten wat hier gebeurde door president Poetin. Wij mogen niet naïef zijn, wij moeten niet in die propaganda trappen, wij moeten niet meegaan in dat verhaal. Wij moeten ons daartegen weren. Dat zeg ik dus hardop via u, voorzitter, tegen de Poetinfluisteraars, die misschien luisteren.

Voorzitter, tot slot. We moeten Nederland veilig houden en beschermen tegen die Russische agressie. Gelukkig helpen onze geheime diensten daarbij en werkt ook ons leger hier hard aan. Maar we moeten niet alleen investeren in onze defensie, maar ook in onze bondgenootschappen. Die zijn, zoals ik al zei, belangrijker dan de dagelijkse politiek en het opgeheven vingertje. We moeten vooral waakzaam zijn als het gaat om die Poetinfluisteraars.

Zelfs tegen die Poetinfluisteraars, maar vooral tegen iedereen hier en iedereen die elders luistert, wil ik zeggen: vredig kerstfeest.

Dank u wel.

De **voorzitter**:
Dank u wel, meneer Koopmans. Mevrouw Karabulut wil iets aardigs terugzeggen.

De heer **Koopmans** (VVD):
Ik dacht dat ik al een kerstwapenstilstand met mevrouw Karabulut had.

Mevrouw **Karabulut** (SP):
Ja, ik ben niet zo oorlogszuchtig. Een oorlog met meneer Koopmans zit er niet in, voorlopig.

Terecht veroordeelt de heer Koopmans de Russische cyberaanval op de OPCW. In mijn verhaal heb ik aandacht gevraagd voor dezelfde soort spionage van bondgenoten, zoals de VS, die ook internationale organisaties en zelfs bevriende staatshoofden hebben bespioneerd. Kan dat op dezelfde afkeuring van de VVD rekenen?

De heer **Koopmans** (VVD):
Ik denk dat we niet kunnen praten over iets wat vergelijkbaar is. We hebben het hier over Russische hacks in een organisatie die ons allemaal probeert te beschermen tijdens aanvallen met chemische wapens. Chemische wapens zijn wereldwijd verboden. Chemische wapens worden toch

gebruikt in Syrië en hebben daar 1.000 of meer slachtoffers gemaakt. Ze worden zelfs door de Russische geheime dienst gebruikt in Groot-Brittannië, ons buurland. Daarnaast is gebleken dat die Russische spionnen ook proberen het MH17-onderzoek te infiltreren. Dat MH17-onderzoek is toch echt van een andere orde. Ik wil dat dus niet vergelijken. Ik zou het zorgwekkend vinden als mevrouw Karabulut zegt: dat is wel erg, maar wat de Amerikanen of die anderen doen, is ook niet zo leuk; dus ja, kunnen we het niet een beetje tegen elkaar wegstrepen? Nee. Het is afschuwelijk. Laten we vooropstellen dat we de Russische spionage hier veroordelen.

De **voorzitter**:
Tot slot, mevrouw Karabulut.

Mevrouw **Karabulut** (SP):
Ik heb toch de indruk dat de heer Koopmans een soort van oorlog wil beginnen, terwijl ik bevestig dat wat de Russen doen, onacceptabel is. Ook de VS hebben in het verleden chemische wapens ingezet in oorlogen. Dat is ook niet goed. Maar ook de Verenigde Staten hebben gespioneerd in de VN, de EU en zelfs bij Merkel. Dan is het toch niet zo raar dat ook deze vorm van spionage afgekeurd zou moeten worden, dat we ons ook daartegen dienen te beschermen? Of vindt de heer Koopmans het ene wel afkeurenswaardig en het andere niet?

De heer **Koopmans** (VVD):
We hebben nu niet een debat over spionage in het algemeen. Ik denk ook dat mevrouw Karabulut nu niet een soort filosofisch-historisch debat over spionage wil gaan openen. We hebben het over de afschuwelijke spionage die hier vlakbij door de Russen heeft plaatsgevonden. Die ging over chemische wapens, over honderden of duizenden mensen die vermoord zijn. En het ging ook over het MH17-onderzoek. Dan vind ik het ongepast om andere handelingen erbij te slepen en te zeggen: ja, maar die doet ook aan deze spionage. Nee, het gaat hier over afschuwelijke Russische spionage, over chemische wapens, over MH17. Ik vind niet dat we dat gelijk moeten stellen met wat voor dingen dan ook.

Mevrouw **Karabulut** (SP):
Ik vind dat verontrustend, omdat de heer Koopmans pretendeert bij dit alles altijd vanuit onze veiligheid te redeneren. Maar wanneer het een bondgenoot of een ander land betreft dat even niet in het rijtje past, kijkt de VVD blijkbaar weg.

Laat ik een vervolgvraag stellen. Wat vindt u van de inmenging van zowel Rusland als de Verenigde Staten in buitenlandse verkiezingen? Het is bekend dat de Verenigde Staten in tal van landen hebben geprobeerd om de verkiezingen te beïnvloeden en dat ze daar ook miljarden voor hebben uitgetrokken. Dus Rusland, zeker niet goed. Maar dat is toch vanuit geen enkel land goed? Of mogen wij het wel doen en de Russen niet? Is dat de rechtsorde die u voorstaat?

De heer **Koopmans** (VVD):
Mevrouw Karabulut zegt hier twee dingen. Ze zegt ten eerste dat wij wegkijken. Nee, we hebben het hier over afschuwelijke spionage door Rusland. Daar kijken we nu heel gericht naar. En dan zeggen we allemaal: dat is onaanvaardbaar, dat heeft hier geen enkele plaats. Gelukkig hoor ik mevrouw Karabulut dat ook nog ergens zeggen.

Mevrouw Karabulut zegt ten tweede dat spionage in het algemeen een slechte zaak is en vraagt of we dat niet altijd moeten veroordelen. We kunnen hier natuurlijk een debat hebben over spionage in het algemeen, maar dat hebben we niet.

De **voorzitter**:
Dank u wel.

De heer **Koopmans** (VVD):
Ik wil mijn verhaal toch even afmaken. Maar als we het hebben over misdaden, dan veroordelen we die. Als we het hier hebben over een specifieke misdaad, dan hebben we het over die specifieke misdaad. Wat voorop moet staan, is de veiligheid van Nederland, de veiligheid van Nederlanders. Die werd hier heel concreet door die Russen aangetast. Dan ben ik blij — in de geest van het kerstfeest; laat ik het maar zeggen — dat ook mevrouw Karabulut het met mij eens is dat dat onaanvaardbaar is.

De heer **Kuzu** (DENK):
Ik wil daar toch even op doorgaan. Als we het hebben over Russen die bij ons spioneren, dan spreken we daar schande van. Dat ben ik ook met de heer Koopmans eens. Dat zal ik straks ook laten blijken in mijn bijdrage. Ik wil toch even doorgaan op wat mevrouw Karabulut terecht aanhaalde. Meneer Koopmans, wat vindt u er dan van dat andere landen zich schuldig maken aan precies dezelfde praktijken? Veroordeelt u dat in zijn algemeenheid of zegt u: nee, het gaat om de Russen; die moeten we wat steviger aanpakken, want die gaan verder dan andere landen?

De heer **Koopmans** (VVD):
Ik krijg nu toch nog wat extra bewondering voor mevrouw Karabulut. Want de heer Kuzu heeft het hier over andere landen die zich schuldig maken aan precies hetzelfde. Dat zei mevrouw Karabulut tenminste niet. Ik heb het gezegd en ga het nog een keer herhalen; ik vind het erg jammer dat ik dat nu moet doen. Wat die Russen hebben gedaan is niet iets wat alle andere landen zomaar hebben gedaan. Nee, de Russische spionage ging over chemische wapens. Afschuwelijke wapens. U heeft de beelden gezien. Afschuwelijke wapens. Daar zijn honderden, duizenden mensen in de afgelopen jaren mee vermoord. In ons buurland Engeland zijn daar mensen door doodgegaan. Het gaat om chemische wapens, die daar in Engeland, zo wijzen de onderzoeken uit, werden gebruikt door de Russen. Die Russen zijn hier opgepakt. Hier om de hoek, meneer Kuzu, zeg ik via u, voorzitter. Die Russen hebben ook geprobeerd in te breken in het onderzoek naar de MH17. Dat is toch echt iets anders. Spionage, of het nou van Rusland is, van de Verenigde Staten, van Turkije of van wie dan ook, is slecht als het slecht is. Dan benoemen we het en zeggen we: dat is slecht. Maar als het gaat om chemische wapens

en honderden, duizenden doden en om het onderzoek naar MH17, dan zeg ik: dat is niet vergelijkbaar. Ik vind het heel zorgwekkend dat de heer Kuzu nu zegt: ja, dat is allemaal hetzelfde.

De heer **Kuzu** (DENK):
De heer Koopmans moet zich in de kerstgedachte niet zo druk maken. Hij hoeft zich ook geen zorgen te maken over het standpunt van DENK hierover. In alle punten die de heer Koopmans aanhaalt, ga ik in een heel ver stadium met hem mee. Wat Rusland heeft gedaan met betrekking tot de MH17 en met deze activiteiten is afschuwelijk. Mijn vraag was in het algemeen: veroordeelt u andere spionageactiviteiten, zoals van de Verenigde Staten, van Israël en van andere landen ook? Het antwoord daarop klinkt bevestigend, dus u hoeft zich niet zo zorgen te maken. Fijn kerstfeest.

De **voorzitter**:
Dank u wel, meneer Koopmans.

De heer **Koopmans** (VVD):
Ik wilde nog wel even zeggen dat de heer Kuzu terecht zegt dat wat slecht is, als slecht benoemd moet worden. Maar wat heel erg slecht is, moeten we ook heel erg slecht durven noemen.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan geeft ik nu het woord aan de heer Van Ojik namens GroenLinks.

De heer **Van Ojik** (GroenLinks):
Zo komt er in ieder geval toch nog een beetje debat, voorzitter.

De MIVD heeft, samen met de Britten en onze eigen AIVD goed werk geleverd. Dat gebeurt vaker, althans dat neem ik aan. Maar meestal weten we dat niet. Dan wordt er bewust voor gekozen om de operaties geheim te houden. Nu is dat niet gebeurd. Bewust werd voor openbaarheid gekozen, zodat het, althans zo stond het in de brief, de Russische inlichtingenofficieren moeilijker wordt gemaakt om in de toekomst nog internationaal te opereren.

Als dat nu geldt, zou dat misschien vaker kunnen gelden. Is er sprake van een nieuwe aanpak? Zo vraag ik het kabinet. Krijgen we nu vaker te horen van geslaagde of misschien soms ook minder geslaagde operaties? Welk effect is met de openheid precies beoogd en welk effect is ermee bereikt?

De operatie heeft bij mijn fractie nog een andere vraag opgeroepen, namelijk over de taakverdeling tussen onze diensten. Is het vanzelfsprekend, zo zou ik de bewindslieden willen vragen, dat de MIVD bij dit soort operaties het voortouw heeft? Is de taakverdeling tussen MIVD en AIVD — met name AIVD — altijd helder? Hoe ziet die taakverdeling er dan uit? Graag een reactie.

In de Europese Unie is aangedrongen — ik geloof dat de heer Verhoeven er ook over sprak — op snelle voortgang met dat cybersanctieregime. Hoe staat het daar nu mee, zou ik aan de minister van Buitenlandse Zaken willen vragen. Is er sprake van snelle voortgang? Wanneer kunnen we de inwerkingstelling van dat cybersanctieregime verwachten?

Ten slotte mijn laatste vraag op dit punt. De brief, van 4 oktober zeg ik uit mijn hoofd, kondigt aan dat Nederland het ondermijnende gedrag van de Russische militaire inlichtingendiensten in de Europese Unie en de NAVO aan de orde gaat stellen. Is dat inmiddels gebeurd? Zo ja, wat heeft dat opgeleverd? Is het ook aan de orde geweest in de OVSE Ministeriële Raad van begin december? Cybersecurity is daar een prioriteit. De Russen zitten er aan tafel. Is dat een voordeel en een kans om er met de Russen over te praten of is het juist een reden om dit forum met dit onderwerp enigszins te mijden? Graag de appreciatie van de minister op dit punt.

Voorzitter. Cyber is dé dreiging van de toekomst. Dat blijkt maar weer uit wat er onlangs is gebeurd, inderdaad op een steenworp afstand van waar wij nu staan. En daarom wil het kabinet meer investeren in cyber. Maar het Defensie Cyber Commando dat ruim vier jaar geleden werd opgericht, komt wat moeizaam van de grond. Van de beoogde 200 medewerkers zijn er pas 80 tot 100 in dienst, zo meldde NRC Handelsblad gisteren nog. Het commando zou het militaire optreden in het cyberdomein moeten verankeren, zo zei de toenmalige minister bij de oprichting. Maar van optreden lijkt nog weinig sprake. Het beeld dat oprijst, is meer dat van een soort van helpdesk die andere met IT-kennis bijstaat. Nuttig, maar misschien niet helemaal wat werd beoogd.

De baas van het commando erkent in hetzelfde stuk in NRC Handelsblad van gisteren dat de kritiek in elk geval deels terecht is. We hebben geduld en tijd nodig, en die moeten ons gegund worden, zegt ze. Maar het probleem is natuurlijk dat mogelijke aanvallers die tijd helemaal en op geen enkele manier gunnen. Hoe gaan we versnellen en wat is er nodig? Zou uitbreiding van onze cybersecuritycapaciteit niet veel meer prioriteit moeten hebben dan bijvoorbeeld de aanschaf van nieuwe onderzeeërs, extra JSF-vliegtuigen of de herinvoering van de tank?

Dank u wel.

De **voorzitter**:
Dank u wel, meneer Van Ojik. Dan geef ik nu het woord aan mevrouw Ploumen namens de PvdA.

Mevrouw **Ploumen** (PvdA):
Voorzitter, dank u wel. Ik las net, twee minuten geleden, het bericht in de Guardian dat de VS en het Verenigd Koninkrijk China beschuldigen van een jarenlange hackingcampagne. Hackers gelinkt aan de Chinese overheid — ik citeer de Guardian — zouden een campagne hebben opgezet om intellectueel eigendom en gevoelige commerciële en bedrijfsmatige data te hacken. De VS en het VK zouden dit de afgelopen twee jaar al op het hoogste niveau met China besproken hebben. Dit laat zien dat het debat dat we vandaag hebben, over veel meer moet gaan dan de

treurige Russische poging om het eerbiedwaardige instituut OPCW te hacken.

Voorzitter. Het is goed dat onze diensten zo alert waren en goed ook dat er openheid is betracht. Ik zou aan het kabinet een aantal vragen willen stellen. Eerst nog even naar Rusland. De minister heeft geschreven dat de dialoog met Rusland ondanks deze mislukte cyberoperatie gaande moet blijven. Hoe ziet die dialoog er eigenlijk uit sinds die dag dat ambassadeurs over en weer op het matje werden geroepen? Heeft de zetel in de Veiligheidsraad bijgedragen aan een dialoog met Rusland? Wat is de inzet van die dialoog en wat wil de regering bereiken? Natuurlijk wil zij gerechtigheid voor de nabestaanden en de slachtoffers van MH17, maar wat wil de regering nog meer bereiken? Wordt er gesproken over dit soort pogingen om cyberoperaties op Nederlands grondgebied uit te voeren?

Voorzitter. Wat doet Nederland om de digitale weerbaarheid te vergroten? Het gaat om Rusland. Ik heb net de kwestie van de Chinese hackpoging aangehaald. Volgens het Verenigd Koninkrijk zou dat ook bij bondgenoten across Europe aan de orde zijn. Weet het kabinet van deze pogingen en wat doet ze om onze digitale weerbaarheid te vergroten, zowel defensief als offensief? Met welke voorwaarden en waarborgen is offensieve inzet omkleed? En hoe zit het, zeg ik de heer Ojik na, met de capaciteit en welke afwegingen liggen er eigenlijk ten grondslag aan de keuzes die gemaakt moeten worden voor de inzet van mensen en materieel?

Voorzitter. In de brief die we in oktober kregen van minister Blok is hij heel expliciet over de rol van de VS. Ik citeer: "Het is in het bijzonder in ons belang om de VS als onmisbare bondgenoot voor de Europese veiligheid betrokken te houden binnen de NAVO". Ik zou aan de minister willen vragen hoe het kabinet zich dat voorstelt met zo'n onvoorspelbare bondgenoot die alle waarden van de vrije wereld verkwanselt. Waarom is dat nog een bondgenoot? Graag een toelichting van het kabinet.

Tot slot. In diezelfde brief wordt de NAVO-norm aangehaald. Er is nog een andere norm wereldwijd afgesproken. 0,7% van het bruto nationaal inkomen zou moeten gaan naar uitgaven voor ontwikkelingssamenwerking, in dienst van de stabiliteit. Dat is uiteindelijk ook waar de bestedingen volgens de NAVO-norm aan bij zouden moeten dragen. Ik hoor daar eigenlijk niks over van deze ministers. Ik zou aan hen willen vragen waarom het kabinet in zijn brieven eigenlijk nooit over die 0,7%-norm spreekt, in een tijd met een zonnige economische context, een tijd waarin het belang groeit van wereldwijde stabiliteit, evenwichtige ontwikkeling en het terugdringen van mondiale ongelijkheid. Die 0,7%-norm is net zo goed als de NAVO-norm een norm die we met elkaar overeengekomen zijn.

Dank u wel, voorzitter.

Mevrouw **Bruins Slot** (CDA):
Ik heb alleen een korte vraag ter verduidelijking. Mevrouw Ploumen begon terecht haar betoog met China. Begreep ik nou dat ze gevraagd heeft aan de beide bewindspersonen of Nederland ook getroffen is door deze hack? De staatssecretaris van Buitenlandse Zaken zegt immers heel duidelijk dat niet alleen de UK is getroffen, maar ook de allies, de bondgenoten. Dat zijn natuurlijk niet alleen de Verenigde Staten. Dat kunnen wij ook zijn.

Mevrouw **Ploumen** (PvdA):
Ik heb aan het kabinet gevraagd of zij op de hoogte waren van het feit dat het VK dit al twee jaar wist en in gesprek was. En daar ligt natuurlijk de vraag onder wat dat betekent voor Nederland.

Mevrouw **Bruins Slot** (CDA):
En ook de vraag of wij ook een van de landen zijn ...

Mevrouw **Ploumen** (PvdA):
Zeker.

Mevrouw **Bruins Slot** (CDA):
... die de negatieve effecten van die campagne ondervonden.

Mevrouw **Ploumen** (PvdA):
Zo is het, ja.

De **voorzitter**:
Dank u wel. Dan geef ik nu het woord aan de heer Stoffer namens de SGP.

De heer **Stoffer** (SGP):
Voorzitter. Het internet is een nieuw, maar steeds belangrijker domein van oorlogvoering. Dat bleek onder andere ook toen ons land na het neerschieten van de MH17 geconfronteerd werd met Russische desinformatie en cyberaanvallen gericht tegen de Onderzoeksraad voor Veiligheid. Hoe reëel die strijd is, bleek opnieuw tijdens de persconferentie op 4 oktober jongstleden waar de minister van Defensie, het hoofd van de MIVD en de Britse ambassadeur de wereld inzicht gaven in de geslaagde verstoring van een Russische cyberoperatie bij de OPCW in Den Haag.

Complimenten voor het knappe werk van onze mensen bij de MIVD en hun Britse collega's, zoals ik ze eerder ook al hoorde van collega's in de Kamer. Wij sluiten ons daar graag bij aan. Hiermee gaven Nederland en het Verenigd Koninkrijk een helder en terecht signaal richting Rusland en de Russische militaire inlichtingendienst af: wij doorzien jullie en stop daar gewoon mee.

Intussen heeft mijn fractie nog wel een aantal vragen. De eerste vraag is: hoe versterken we onze cyberveiligheid voor de langere termijn? Dat Nederland op dit moment al extra in cyberveiligheid investeert, is cruciaal. Heel goed dat de regering daar nog een schep bovenop gaat doen. Kan de minister van Defensie een tipje van de sluier oplichten over met hoeveel geld en hoe onze cybercapaciteit verder versterkt wordt? Komen er bijvoorbeeld meer operationele cybereenheden? Kan de minister garanderen dat hierbij nauw wordt afgestemd met de NAVO? Moeten we, zoals generaal-majoor buiten dienst Cobelens recent in NRC bepleitte, niet inderdaad en veel harder lik-op-stukbeleid voeren via een veel assertievere houding?

Het is van belang dat er heldere juridische kaders bestaan voor defensieve en offensieve cyberoperaties, zonder dat

onze cybersoldaten aan handen en voeten gebonden zijn. Hoe zorgen we ervoor dat Defensie niet wederrechtelijk, maar wel effectief kan optreden? Bieden de huidige juridische kaders genoeg ruimte voor echte slagkracht?

Voorzitter. Wat de SGP betreft roepen de confrontaties met Rusland om een gerichte Ruslandstrategie met aandacht voor militaire verhoudingen en cyberoorlogvoering, maar ook voor de bredere economische, politieke en diplomatieke betrekkingen met Rusland. Mijn vraag is dan ook of het kabinet de noodzaak ziet van zo'n strategie en overweegt die op stellen. Graag een reactie van beide ministers. De brutale spionageactie van Rusland, maar ook vergelijkbare acties van andere landen mogen natuurlijk niet zonder gevolgen blijven. Blijft de regering binnen de EU actief zoeken naar draagvlak voor zwaardere sancties?

Ik dank u wel.

De **voorzitter**:
Dank u wel, meneer Stoffer. Dan geef ik nu het woord aan de heer Voordewind namens de ChristenUnie.

De heer **Voordewind** (ChristenUnie):
Dank u wel, voorzitter. Het leek wel alsof we getuige waren van een slechte versie van een James Bondserie toen we zagen hoe de vier mensen probeerden om het wifinetwerk van de OPCW te hacken. Dat zou je bijna denken, ware het niet dat het gaat om een grove schending van de integriteit van een belangrijk internationaal orgaan: de OPCW, de organisatie die chemische wapens en de inzet daarvan moet controleren. Ik vraag aan de ministers of er inmiddels Russische repercussies zijn geweest nadat de vier mensen zijn uitgezet door Nederland. We weten van eerdere acties dat dat weer kan leiden tot tegenacties. Kan de minister daar wat over zeggen?

Is het openbaar maken van dergelijke spionageacties een tactiek die we vanaf nu vaker gaan inzetten? Het gebeurde nu voor het eerst, en terecht. Ik steun het kabinet in die actie, want dit ging echt alle perken te buiten. Was dit nu eenmalig of zegt de minister dat we dit nog weleens vaker kunnen gaan gebruiken om de Russen af te schrikken? Kan de minister overigens ook iets zeggen over in hoeverre andere landen proberen in te breken op systemen in Nederland, bijvoorbeeld China of Iran? Overweegt de minister dergelijke acties ook openbaar te maken?

Klopt het dat er al voor de verijdelde cyberinbraakpoging op de parkeerplaats in Den Haag vanuit Rusland geprobeerd is om in te breken in de systemen van de OPCW? Zijn er sindsdien misschien nog andere hackpogingen gedaan? Klopt het dat de vijfde persoon op de foto die op Schiphol werd gemaakt een medewerker was van de Russische ambassade hier in Den Haag? Wat is er sinds de hackpoging veranderd in de relatie met Rusland en specifiek in de omgang met de Russische ambassade?

Verklaart de minister deze Russische cyberactie ook als een soort verkapte erkenning van de Russische betrokkenheid bij het gebruik van chemische wapens in Syrië? Ziet hij daar een link? Waarom zouden de Russen dat anders hebben gedaan? Een zelfde vraag kan gesteld worden met betrekking tot het onderzoek naar de aanslag op de vlucht MH17. We weten nu dat Russische spionnen zowel in Nederland als in Maleisië geprobeerd hebben om informatie te bemachtigen. Waarom zouden ze dat op deze manier doen als volgens hen er totaal geen Russische betrokkenheid zou zijn bij het neerhalen van de MH17? Is de minister het met mij eens dat dit de Russische rol hierin alleen maar onderstreept?

Voorzitter. Dan de belangrijkste vraag: wat moet nou onze reactie verder zijn? De Europese Raad heeft inmiddels de economische en financiële sancties tegen Rusland verlengd tot en met juli 2019. Dat is een goede zaak. Wij zien daar ook alle aanleiding toe, maar wat gebeurt er nu naar aanleiding van deze cyberacties? Gaat dat cybersanctieregime nu ook echt van start? Ziet de minister van Buitenlandse Zaken daar genoeg steun voor in de Europese Unie? Wanneer verwacht hij een besluit op dat punt?

Dan citeer ik ten slotte nog graag uit de brief van de minister van Defensie van 19 oktober, die naar aanleiding van deze kwestie is gestuurd: "De nieuwe veiligheidscontext vereist een herijking waarbij Europa en het westen zichzelf beter equiperen om de internationale rechtsorde te kunnen beschermen met (...) machts- en drukmiddelen. Onze veiligheid staat voorop (...)"

Voorzitter. Ik ben het helemaal eens met de minister van Defensie, maar hoe denkt de minister van Buitenlandse Zaken hierover in het kader van het commerciële project North Stream 2? Is de minister het met mij eens dat de aanleg van deze gaspijplijn niet helpt om Europa beter te equiperen om de internationale rechtsorde te beschermen tegen economische machts- en drukmiddelen? Verwacht de minister nog een succesvolle uitkomst van het overleg tussen Rusland, Oekraïne en de EU over het behoud van de gasdoorvoer door Oekraïne?

Voorzitter, tot slot. We moeten Rusland ondanks alles duidelijk maken, in woord en in daad, dat het Westen geen vijand is en wil zijn van Rusland. Maar zolang Rusland zich zo roekeloos en agressief blijft opstellen, zo lang Rusland het Westen wél als vijand behandelt, past geen andere opstelling van onze kant dan samen met onze bondgenoten ons inderdaad beter te equiperen om de internationale rechtsorde te kunnen beschermen.

Ondanks dat wens ik iedereen alvast een gezegende kerst.

De **voorzitter**:
Dank u wel, meneer Voordewind. Dan geef ik nu het woord aan de heer Kuzu namens DENK.

De heer **Kuzu** (DENK):
Voorzitter, dank u wel. Zo vlak voor het kerstreces houden wij dit debat naar aanleiding van een persconferentie waarin onthullingen werden gedaan. De zondag daarna zat de minister van Defensie bij WNL Op Zondag. Daar zei zij: "We zijn in oorlog met de Russen." Dat is stevige taal. Later nuanceerde zij deze boodschap door te zeggen: "Onze inlichtingen- en veiligheidsdiensten moeten ons beschermen tegen cyberattacks van buitenlandse mogendheden."

Voorzitter. DENK is het daar wel mee eens. We kennen de wereld van de spionage vooral van films, geheime intriges,

pijprokende mannen achter kranten, dubbelspionages en spectaculaire ontmaskeringen. Maar technologie wordt elke dag geavanceerder en wordt ook steeds vaker tegen de burgerbevolking ingezet. DENK is het ermee eens dat we ons daartegen moeten bewapenen. DENK keurt ook de schaamteloze pogingen van Rusland af om het internationale recht en de daarbij behorende instellingen te ondermijnen. Prima dat onze inlichtingendiensten met een tip van de Britten wisten te voorkomen dat de OPCW, de VN-waakhond op het gebied van chemische wapens, werd gehackt.

De werkwijze van de Russen deed ons echter meer denken aan de klunzige Johnny English dan aan James Bond. Toch waren minister Bijleveld en meneer Eichelsheim van de MIVD trots. Dat lieten zij ook maar al te graag merken aan Moskou. Wij vroegen ons af: waarom eigenlijk? Alle details van de operatie werden aan de pers getoond. Dat wordt normaal gesproken niet gedaan. Waarom gaf de MIVD zo veel openheid en is het niet buiten de publiciteit om afgehandeld? Heeft het misschien te maken met de zaak-Skripal, waardoor de Russen een vete hebben met de Britten? Worden wij door de Britse inlichtingendienst en door de Britten niet misschien misbruikt in dit geval? Dat vraag ik de minister van Defensie. En wat betekent dit voor de escalatie van de verhoudingen van het Westen met Rusland?

Voorzitter. Spioneren is zo oud als de weg naar Rome. Westerse overheden beschuldigen vooral Rusland en China — terecht, zeg ik erbij — van het uitvoeren van hackaanvallen. Maar westerse landen hebben zelf ook niet altijd schone handen. Zo braken Amerikaanse, Israëlische, Britse en Nederlandse overheidshackers ook geregeld in op het grondgebied van andere landen. En waarom spreken wij dan van trots als wij informatie verzamelen over andere landen, maar spreken wij van schande als diezelfde landen dat bij ons doen? Wassen wij onze handen niet in onschuld terwijl wij net zo fout kunnen zitten?

Voorzitter. Ik rond af. Wij zijn niet gecharmeerd van de Russische arrogantie, niet alleen bij de verijdelde hackaanval op de OPCW in Den Haag, maar ook bij andere internationaal gevoelige kwesties zoals de annexatie van de Krim, het MH17-dossier, het Olympische dopingschandaal, de aanwezigheid van Russische troepen in de Donbass en de aanval op een VN-hulpkonvooi in Syrië. Dat lijstje kan nog veel langer gemaakt worden. En hoewel het gepresenteerde bewijsmateriaal overweldigend is, noemde de minister van Buitenlandse Zaken Lavrov het uitzetten van de vier Russische spionnen in april "een misverstand tijdens een routinereis". Nederland werd onder andere "megafoondiplomatie" en "georganiseerde propaganda" verweten. Nogmaals, DENK veroordeelt het Russische handelen en de Russische werkwijze. Mijn fractie heeft eigenlijk maar één oproep en één vraag aan de minister. Ik zou tegen haar willen zeggen: wijs niet alleen met de vinger naar Rusland, want andere landen doen het net zo goed. Het voorbeeld China werd al aangehaald, maar ook westerse landen zoals de Verenigde Staten, Israël et cetera doen het. De vraag aan de minister is om dat dan ook te veroordelen en dat ook in de openbaarheid te brengen wanneer het nodig is.

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel. Dan geef ik tot slot het woord aan de heer De Roon namens de PVV.

De heer **De Roon** (PVV):
Voorzitter. Dankzij onze veiligheidsdienst werd een hondsbrutale Russische hackoperatie gestopt. Er is doelgericht en effectief opgetreden om een digitale inbraak bij de OPCW te verhinderen en de inbrekers het land uit te gooien, waarvoor de complimenten van de PVV. De feiten en de achtergronden die in oktober aan het publiek werden gepresenteerd, waren overtuigend maar bovendien ook zeer gedetailleerd. Zo zagen we foto's van bewakingscamera's, hackapparatuur en mobiele telefoons. We weten nu ook dat de Russische spionnen op de hotelkamer hebben genoten van blikjes Heinekenbier, dat blijkbaar lekkerder smaakte dan Russische wodka.

De hackoperatie komt op veel mensen nogal amateuristisch over. Het taxibonnetje wordt vaak aangehaald en ook de laptop die niet was schoongemaakt na eerdere operaties is als voorbeeld daarvan genoemd. Nou is de vraag — een beetje een retorisch vraag hoor, maar ik stel hem toch — of dat amateurisme of gemakzucht was. Was het misschien gemakzucht omdat eerdere hackoperaties niet werden verstoord? We weten toch allemaal, zo vraag ik aan de bewindslieden, dat hackoperaties wereldwijd aan de orde van de dag zijn?

In ieder geval lijkt het erop dat met de gedetailleerde presentatie naar buiten toe door onze regering van wat men allemaal heeft geconstateerd en bevonden, de Russen ook weer op scherp zijn gezet. Heeft u ze niet wijzer gemaakt dan ze zouden moeten zijn? Ik had me ook kunnen voorstellen dat u ze gewoon aanhoudt, de apparatuur in beslag neemt, voor mijn part een foto daarvan en van de koppen van die Russische spionnen wereldwijd bekendmaakt en zegt: ze zijn gepakt en het land uitgezet. Dan heeft u namelijk hetzelfde effect bereikt, zonder al die poespas; het was bijna een tv-show. De wijze van optreden naar buiten toe over deze inlichtingenoperatie roept gewoon vragen op. Waarom zo uitgebreid met toeters en bellen? Gaan we dit nou ook vaker zien in de toekomst?

De regering geeft als voornaamste reden op dat er bewust is gekozen om zo naar buiten op te treden om het internationaal opereren van inlichtingenofficieren moeilijker te maken, maar dan hoef je niet allerlei details openbaar te maken die nu wel naar buiten zijn gebracht, dacht ik. Tijdens de persconferentie stelde de minister van Defensie het nog scherper, want ze zei: "Door het in de openbaarheid brengen, denken wij dat dit soort acties in de toekomst een halt kunnen toe worden geroepen." Maar als dat nou de voornaamste drijfveer is, zo vraag ik aan de bewindslieden, waarom treden de regering en de diensten dan niet vaker naar buiten met dit soort bevindingen? Concreet kan je ook de vraag stellen, en dan kom ik toch weer op een punt dat ook door anderen is aangehaald, waarom bijvoorbeeld Chinese hackoperaties niet tentoon worden gesteld. Die operaties en aanvallen zijn vaak economisch en militair-strategisch van aard. Laten we wel wezen: meer dan 50% van alle hackoperaties wereldwijd draagt een Chinese signatuur. Toch horen we de regering daar niet over, terwijl

we wel zien dat de regering de Chinese bewindslieden onlangs nog met veel geknuffel binnenhaalde.

Laat er geen misverstand zijn: de PVV vindt dat er geen enkel onderscheid hoort te zijn. Alle hackoperaties op Nederlandse bodem of schadelijk voor Nederlandse belangen moeten natuurlijk aangepakt worden. Maar de vraag is: deelt de regering die mening nou ook? Of is een hack op een internationale organisatie een zwaarder delict dan een hack op onze industrie of krijgsmacht? Wordt een Russische hack anders beoordeeld dan een Chinese of een Iraanse hack? En treden we alleen naar buiten als hackers zich lijfelijk in Nederland bevinden of ook in andere situaties? Veel vragen dus, maar één ding staat vast: het Nederlandse beleid is veranderd door het actief naar buiten treden van de regering in deze spionagezaak. Maar hoe en wat dat voor de toekomst betekent, blijft de vraag. Daar zouden wij graag wat meer inzicht in krijgen.

Dan nog over de gegevens die op een van de laptops zijn aangetroffen. Er zouden pogingen gedaan zijn om in Maleisië informatie over het onderzoek rond vlucht MH17 buit te maken. Mijn vraag is: was dat nou inderdaad alleen maar een poging of is er daadwerkelijk informatie buitgemaakt door de Russen?

Tot zover, voorzitter. Dank u wel.

De **voorzitter**:
Dank u wel, meneer De Roon. Dan zijn we hiermee aan het eind gekomen van de eerste termijn van de kant van de Kamer. Ik kijk of de ministers kunnen antwoorden. Ja? Een minuut of twee minuten schorsen? Oké, dan schorsen we voor twee minuten.

De vergadering wordt van 17.22 uur tot 17.30 uur geschorst.

De **voorzitter**:
Ik geef de minister van Defensie het woord.

Minister **Bijleveld**:
Dank u wel, voorzitter. Zou het spreekgestoelte misschien nog ietsje lager mogen?

De **voorzitter**:
U kunt het zelf.

Minister **Bijleveld**:
O, kan ik het ook zelf doen?

De **voorzitter**:
Maar ik doe het graag.

Minister **Bijleveld**:
Doet u het maar even, voorzitter.

De **voorzitter**:
Ja, is goed.

Minister **Bijleveld**:
Ja, dank u wel!

Op vrijdag 13 april heeft de MIVD — daar is eigenlijk door iedereen aandacht aan besteed — een cyberoperatie van de Russische militaire inlichtingendienst in Den Haag verstoord. Ik sluit mij aan bij de complimenten die hier in de Kamer ten aanzien van de MIVD en de collega-diensten, die er ook bij betrokken waren, zijn gegeven. Dit soort operaties van de GROe — want het was een statelijke actor — moet een halt worden toegeroepen, zeker op Nederlands grondgebied. Door die ondermijnende activiteiten zo in detail bloot te leggen en de GROe ook als verantwoordelijke aan te wijzen, heeft het kabinet een heldere en duidelijke boodschap afgegeven. Wij willen dit niet tolereren. Door het publiek maken van dergelijke operaties — daar heeft een aantal leden van uw Kamer ook terecht over gesproken — werken we er stap voor stap naartoe dat Nederland een steeds minder aantrekkelijk doelwit voor cyberaanvallen wordt. Dat is een van de redenen waarom wij dat zo nadrukkelijk hebben gedaan.

Voorzitter. Ik heb er al een aantal keren met leden van de Kamer over gesproken, ook bijvoorbeeld naar aanleiding van het jaarverslag van de MIVD: de machtsverhoudingen in de wereld veranderen en de gebeurtenissen die op 13 april plaatsvonden staan helaas niet op zichzelf. Ze zijn een concrete illustratie van de manier waarop Rusland systematisch de internationale veiligheidssituatie en rechtsorde ondermijnt en een dreiging vormt voor Nederlandse bondgenootschappelijke en Europese belangen. De leden van de Kamer zijn in de technische briefing op 12 december uitgebreid geïnformeerd over het Russische politieke en veiligheidsbeleid. In tegenstelling tot het Westen, waar wordt gedacht in termen van zelfbeschikking van landen, denkt Rusland in termen van invloedssferen. Dat vormt een serieuze bedreiging voor de internationale stabiliteit in het algemeen en het NAVO-bondgenootschap in het bijzonder. Aan de oostflank van het NAVO-verdragsgebied is sprake van een opbouw van Russische strijdkrachten, en ook houdt Rusland met enige regelmaat grootschalige militaire oefeningen waarvan het gebrek aan transparantie op gespannen voet staat met de internationale afspraken. Rusland is de afgelopen jaren ook bereid gebleken militaire middelen in te zetten in bijvoorbeeld Georgië, Oekraïne en Syrië. De illegale annexatie van de Krim vormt een schending van het internationale recht en een bedreiging voor de Europese en internationale veiligheidsarchitectuur. Dat het geen incidenten zijn hebben we onlangs ook nog gezien met het Russische optreden in de Zee van Azov.

Voorzitter. Wij moeten ons dus rekenschap geven van de veranderingen in de internationale veiligheidssituatie na een periode van relatieve stabiliteit en voorspelbaarheid in Europa. We kunnen het ons niet veroorloven naïef te zijn over de veranderende context. Daar speelt cyber een belangrijke rol bij. Dan is het van belang, zoals terecht door de heer Koopmans is gezegd, om onze veiligheid voorop te stellen. Maar het vraagt ook daadwerkelijk dat we anders naar de situatie in de wereld kijken. Een sterke en verenigde NAVO, waarin alle bondgenoten schouder aan schouder staan, biedt garanties voor onze veiligheid wat ons betreft. Daarover is aan mij ook een vraag gesteld. Het is in ons belang om binnen de NAVO de VS als bondgenoot bij de Europese veiligheidscontext betrokken te houden. Dat

betekent dat wij een volwaardige partner moeten zijn in het bondgenootschap, ook op het terrein van cyber.

Voorzitter. Als het gaat om de vraag wat er is gebeurd, is het belangrijk dat wij dit ook hebben laten zien. Bij een van de laatste NAVO-vergaderingen hebben wij ook nadrukkelijk onze cybersoldaten aangeboden. Ik zal daar zo op terugkomen. Dan is het belangrijk dat wij dit soort dingen attribueren als ze op Nederlands grondgebied plaatsvinden, juist omdat wij eraan gehouden zijn om zo'n internationaal bondgenootschap dat hier zit, te beschermen. Dat is onze taak. Het is een operatie onder de Wiv geweest — ik zal daar zo op terugkomen — waarbij we duidelijk hebben voorkomen dat er uiteindelijk een hack is gezet bij de OPCW. In die tijd werd er onderzoek gedaan naar de chemische aanvallen in Syrië en stond ook de zaak Skripal centraal. Door het zo naar buiten te brengen, hebben wij laten zien dat wij dit hier niet tolereren.

Voorzitter. Ik ga naar de vragen van de Kamerleden. Ik loop ze gewoon op volgorde af. Ik zal met name de vragen op inlichtingengebied beantwoorden en collega Blok de vragen op het terrein van het buitenlandbeleid.

Ik begin met de vragen van de heer Verhoeven. In het debat over het jaarverslag van de MIVD hebben we al nadrukkelijk over het gebruik van de term "cyberoorlog" gesproken. Maar ik denk dat het goed is om hier in de Kamer nog eens te zeggen dat het door het hybride karakter van veel conflicten niet altijd meer duidelijk is op welk moment er precies sprake is van een conflict of oorlog in de traditionele zin van het woord. Conflictvoering verandert en het digitale domein speelt daarbij een hele belangrijke rol. Ook in het digitale domein is niet eenduidig vast te stellen wanneer artikel 5 precies in werking treedt. Dit is dus altijd een onderwerp van politieke besluitvorming en het wordt van geval tot geval beoordeeld.

Naar aanleiding van de Russische hackpoging op ons grondgebied kwam er een discussie op gang over het veranderende karakter van de conflictvoering. Dat was inderdaad in de tv-uitzending waar ik was. Dat is ook wat ik heb gezegd, waarop ik heb geduid en waarvan we ons wat mij betreft allemaal bewust moeten zijn. Daarop werd mij gevraagd of de acties van Rusland in het digitale domein als "cyberoorlog" bestempeld kunnen worden. Die vraag heb ik bevestigend beantwoord. Ik heb daar overigens niks van teruggenomen. Ik weet dat u niet aan het debat over het jaarverslag van de MIVD hebt meegedaan, maar dat punt is daarin nadrukkelijk naar voren gekomen. Ik heb de vraag inderdaad bevestigend beantwoord, want je zou het wel degelijk zo kunnen noemen. Het staat immers vast dat het digitale domein een steeds belangrijkere plaats inneemt tijdens conflicten. Bovendien is het door het hele hybride karakter van veel conflicten ook niet altijd meer duidelijk op welk moment er precies sprake is van een conflict of oorlog in de traditionele zin van het woord. We hebben daar al uitgebreid met elkaar over gesproken. Ik wil hier ook nog wel een keer herhalen dat dit niet wegneemt dat er op dit moment uiteraard geen sprake is van oorlog in de klassieke betekenis van het woord, maar ik heb hiermee wel willen bereiken waar we nu mee bezig zijn, namelijk een discussie over en bewustwording van het feit dat conflictvoering verandert en dat het digitale domein daarbij een belangrijke rol speelt. Daarover moeten we wat mij betreft nog steeds niet naïef zijn.

Voorzitter. De heer Verhoeven verwees daarbij ook naar zijn aangekondigde initiatief. Ik zie dat initiatief met belangstelling tegemoet. Ik weet natuurlijk niet precies welke punten daarin staan. Hij heeft daar net iets over gezegd. Het kabinet wacht het voorstel met belangstelling af. We zullen dat dan natuurlijk langs de gebruikelijke weg met de Kamer bespreken. Maar omdat ik nu de mogelijkheid heb, wil ik hier in de Kamer toch iets zeggen over het staand kabinetsbeleid ten aanzien van de omgang door inlichtingen- en veiligheidsdiensten met onbekende kwetsbaarheden, want daar gaat het volgens mij voor een deel over. Bij iedere onbekende kwetsbaarheid wordt een afweging gemaakt van het belang van het niet-melden van de kwetsbaarheid in het kader van de nationale veiligheid en het belang dat door melden kan worden behartigd. Die afweging wordt gemaakt door de Commissie Melden Kwetsbaarheden, die onder leiding staat van de directeur-generaal van de AIVD en de directeur van de MIVD. De dg AIVD en de directeur MIVD informeren de betrokken minister over hun besluit. Dus ook wij zullen daar dan altijd naar kijken. Er zijn dus wel degelijk mogelijkheden. Ik wil dat hier in de Kamer nog wel nadrukkelijk gemeld hebben namens het kabinet.

De heer **Verhoeven** (D66):
Dank voor deze opmerkingen van de minister namens het kabinet. Mijn voorstel gaat verder dan de diensten. Ik hoef daar nu verder niet diep op in te gaan, maar omdat de minister er nu ook over begint, wil ik dat toch zeggen. Wat de minister zegt over de diensten, weet ik, maar het gaat over Defensie en politie. We hebben ruim een jaar geleden in de Kamer een uitgebreide discussie gevoerd over de wet die het voor de politie mogelijk maakt om op dit gebied actief te zijn. Daar heeft D66 bedenkingen bij, maar die hoeven nu ook niet besproken te worden. Wat wel een aardige vraag zou kunnen zijn, is de vraag aan de minister van Defensie hoe Defensie omgaat met onbekende kwetsbaarheden, want daar is eigenlijk het minst over duidelijk en daar ben ik ook wel benieuwd naar.

Minister **Bijleveld**:
Die kwetsbaarheden worden keurig besproken en gemeld, zoals ik net zei. Als ik kijk en zie wat er aangekondigd wordt, want het gaat dan om de dienst waar ik over spreek ...

De heer **Verhoeven** (D66):
Ter aanvulling op het antwoord van de minister, het gaat wat mij betreft niet alleen over de dienst of de MIVD, maar ik heb het in mijn voorstel ook nadrukkelijk over Defensie zelf. Daar is vrij weinig over duidelijk. Als door Defensie gezegd wordt: "we willen auto's hacken", dan neem ik aan dat er bij Defensie al nagedacht wordt over de mogelijkheden om op basis van onbekende kwetsbaarheden bepaalde apparaten of vehikels te onderscheppen, op basis van het belang van de nationale veiligheid.

Minister **Bijleveld**:
Over alles wat we in het belang van de nationale veiligheid doen, zeggen we niets in de openbaarheid, dat weet u. Overigens, zo'n uitspraak "wij willen auto's hacken" komt mij geenszins bekend voor. In de uitzending op tv die ik gezien heb, is door de directeur van het Defensie Cyber

Commando gezegd: we zijn zo afhankelijk geworden van techniek dat het mogelijk is dat auto's gehackt kunnen worden. Dat is wat zij heeft gezegd en dat is iets anders dan dat er gezegd wordt dat Defensie auto's gaat hacken. Dat is echt totaal iets anders. Dat is ook helemaal niet aan de orde van de dag.

Ik zal zo op de gestelde vragen ingaan. Volgens mij haalt u nu een uitspraak van de commodore Boekholt verkeerd aan. Ik zal uw wet met belangstelling afwachten en wij zullen daarnaar kijken. Het kabinet zal in de volle breedte kijken naar de politie en Defensie, eigenlijk naar alles wat daarin staat, en er dan op reageren, zoals dat hoort bij een initiatief.

De **voorzitter**:
Tot slot.

De heer **Verhoeven** (D66):
Dat lijkt me voor nu prima en ook meer dan genoeg. Dat komt dan vanzelf de kant op van het kabinet, zeg ik tegen de minister. Als we het over dit soort zaken hebben, zowel de uitspraken van de minister in een televisieprogramma over cyberoorlog als de uitspraken van een generaal over het in de toekomst tot de mogelijkheden behoren van het hacken van een auto, vind ik het wel van belang dat er goed nagedacht wordt over uitingen. Juist op dit soort gebieden is zorgvuldige communicatie cruciaal. De minister zegt dat zij er niets van heeft teruggenomen, maar ik heb wel degelijk nuancerende opmerkingen gezien en die vond ik heel verstandig.

Minister **Bijleveld**:
We hebben hier al een heel debat aan besteed, waar de heer Verhoeven niet bij was, maar ik heb er zelf niets van teruggenomen. Dat heb ik ook zo in dat debat gezegd. Ik zie dat een aantal mensen die daar wel bij waren, bevestigend knikken. Dat waren de vragen die de heer Verhoeven aan mij had gesteld.

Dan ga ik naar de vragen van mevrouw Bruins Slot, en dat sluit mooi aan, want zij zei dat wij de naïviteit voorbij moeten zijn, zoals ik al naar voren heb gebracht. We moeten ons in Nederland meer bewust zijn van de gevaren die er op dit terrein zijn. Dat was volgens mij ook een van de voorbeelden van commodore Boekholt.

Mevrouw Bruins Slot zei dat er wordt gespioneerd in onze achtertuin en dat we fors moeten investeren in de MIVD en in cyber. Zij vroeg hoe het staat met de uitwerking van een aantal maatregelen in het AIV-rapport over digitale oorlogvoering uit 2011. Het toenmalige kabinet heeft in 2012 met de Defensie Cyber Strategie de eerste stappen gezet voor de implementatie van dat AIV-advies, waarover mevrouw Bruins Slot zelf ook wat heeft gezegd. Er zijn toen stappen gezet voor digitale oorlogvoering, zoals oprichting van het Defensie Cyber Commando en versterking van de diensten. Wij zetten als kabinet die lijn voort met de nieuwe Defensie Cyber Strategie die, zoals afgesproken, net voor de begroting is aangeboden aan uw Kamer. We investeren fors in de capaciteiten van Defensie om effectief op te treden in het hele digitale domein. We versterken het DCC, de MIVD en de verdediging van onze eigen netwerken en systemen, dus defensief en offensief. De versterking van onze digitale slagkracht en een actiever attributiebeleid — daar had u het ook over — zijn hierbij wat ons betreft inderdaad speerpunten. Dus in beide — in de Nationale Cyber Security Strategie, die daar ook nog als koepel overheen komt, en in de GBVS — is hier nadrukkelijk aandacht voor.

Voorzitter. Mevrouw Bruins Slot vroeg wanneer digitaal optreden van een staat een oorlogsdaad is. Geldt het oorlogsrecht ook in het digitale domein? Het kabinet is hierover klip-en-klaar. We hebben het volgens mij ook al in andere debatten besproken, maar ik zeg het hier nog maar een keer. Het geldende internationale recht, ook het humanitair oorlogsrecht, geldt onverkort ook voor het digitale domein. Nederland zet zich juist internationaal in om de toepassing van het internationaal recht in het digitale domein te bestendigen. Wanneer een daad gekwalificeerd kan worden als een gewapende aanval of een oorlogshandeling is en blijft altijd een politieke afweging die per geval gemaakt moet worden.

Dan vroeg u vervolgens of artikel 5 van toepassing kan zijn bij een cyberaanval. Artikel 5 kan inderdaad van toepassing zijn bij een cyberaanval, maar dan moet de besluitvorming over een collectieve NAVO-reactie, zoals altijd, op basis van artikel 5 plaatsvinden. En dat is te allen tijde voorbehouden aan het hoogste orgaan van het bondgenootschap, de Noord-Atlantische Raad, zoals u weet. Ook in het digitale domein is dus niet altijd eenduidig vast te stellen wanneer artikel 5 in werking treedt. Dus dat blijft altijd een onderwerp van politieke besluitvorming en wordt van geval tot geval beoordeeld. Dat geldt ook als artikel 5 van het NAVO-verdrag niet aan de orde is omdat er niet sprake is van een aanval op een NAVO-lidstaat. Elke lidstaat van de VN heeft trouwens ook het recht om zichzelf te verdedigen tegen een oorlogsdaad onder artikel 51 van het VN-Handvest. Ik denk dat het goed is om dat ook hier te benoemen.

Mevrouw Bruins Slot zegt zelf dat het onaanvaardbaar is dat de GROe iets dergelijks doet en de internationale rechtsorde ondermijnt. Zij vraagt waarom de vier Russische inlichtingenofficieren alleen het land uit zijn begeleid en niet zijn gearresteerd. Wie heeft dat besloten? Dit was nadrukkelijk geen opsporingsonderzoek. Dat hebben de generaal van de MIVD en ikzelf ook naar voren gebracht, ook bij het openbaar maken. Het was een contra-inlichtingenoperatie, uitgevoerd op basis van de Wiv 2002. Op basis van de toen — het gaat dan over april — bij ons beschikbare informatie hebben we ervoor gekozen dat de snelheid van handelen bovenaan moest staan. Het kon namelijk niet worden uitgesloten dat het handelen van de inlichtingenofficieren van de GROe, statelijke actoren, zeer schadelijke gevolgen zou hebben voor de OPCW. Een aantal van u heeft daar ook over gesproken. Verstoring was de snelste en meest effectieve manier om de Russische inlichtingenoperatie een halt toe te roepen en deze belangen te beschermen. Verstoren maakt ook onderdeel uit van de bestaande modus operandi van inlichtingendiensten. Het is dus een inlichtingenoperatie. Het besluit om de Russische inlichtingenoperatie te verstoren is genomen door de directeur van de MIVD. Het onderzoek dat we daarop hebben gevolgd, heeft uiteindelijk ook in samenwerking met de Amerikanen geleid tot een strafrechtelijke procedure van de Verenigde Staten. Dus zo is ervoor gekozen, want voor ons stond "zorgen dat er niet gehackt kon worden" bovenaan.

Heeft de MIVD dan behoefte aan meer bevoegdheden om betrapte spionnen wel vast te houden of anderszins? Dat was uw vervolgvraag. Wat mij betreft zijn die niet nodig, want de MIVD is in die zin geen opsporingsdienst en de AIVD in die zin ook niet. Zij hebben dus ook geen bevoegdheid tot het vasthouden van mensen. En dat moet wat ons betreft ook zo blijven. Naar mijn idee geeft de wet de MIVD op dit moment voldoende bevoegdheden voor het uitvoeren van zijn taken. Ik denk dat uitbreiding vooralsnog ook niet nodig is. Het is ook niet zo dat gebrek aan bevoegdheden de reden was om niet tot aanhouding over te gaan. We hebben er echt voor gekozen om te verstoren vanwege de snelheid, en naar buiten te begeleiden. De spullen zijn achtergebleven, en die konden daardoor door ons bekeken worden, zoals u heeft gehoord. Daarop is waardevolle informatie gevonden, waarvan we ook een deel openbaar hebben gemaakt.

Dan vroeg u volgens mij ten slotte: hoe staat de NAVO in relatie tot het offensieve cyberterrein? Dat zijn tenminste de vragen die ik genoteerd heb, voorzitter. De NATO heeft in 2016 het cyberdomein erkend als domein van militair optreden. Er wordt nu heel hard gewerkt aan de operationalisering van dat cyberdomein. Zo is er recent een mechanisme ontworpen waarmee bondgenoten cybercapaciteiten kunnen inzetten voor NAVO-missies en operaties. En Nederland heeft zich tijdens de NAVO-top in 2018, waarbij collega Blok en ik beiden aanwezig waren, bereid verklaard waar nodig en als dat mogelijk is met cybercapaciteiten bij te dragen aan NAVO-missies en operaties.

Voorzitter. Dan ga ik naar de vragen van mevrouw Karabulut.

De **voorzitter**:
Eerst mevrouw Bruins Slot.

Mevrouw **Bruins Slot** (CDA):
Ik heb nog een praktische vraag. Een van de belangrijkste zaken in dat AIV-advies was dat er een praktische uitwerking moest worden gegeven van de toepassing van het internationaal recht in het digitale domein. De minister heeft zonet feitelijk alleen gezegd dat die regels van toepassing zijn. Maar het gaat natuurlijk om het feit dat staten met elkaar overeenkomen ...

Voorzitter, ik zie non-verbaal dat de minister van Buitenlandse Zaken hierop terug gaat komen, dus ik beëindig mijn interruptie.

De **voorzitter**:
Is goed!

Minister **Bijleveld**:
Inderdaad. Dat is non-verbaal goed gezien door mevrouw Bruins Slot: daar zal de minister van Buitenlandse Zaken op ingaan.

Ik was bij mevrouw Karabulut aanbeland, voorzitter. Een van haar vragen was, en dat sluit eigenlijk wel aan op waar ik was gebleven: zijn er door Nederland al offensieve cyberoperaties uitgevoerd? Nee. Dat heeft u goed gezien: tot dusverre heeft het DCC geen offensieve operaties uitgevoerd. DCC heeft echter in de jaren dat het nu bestaat wel een hele belangrijke rol gespeeld bij de vergroting van de digitale weerbaarheid en alertheid van de krijgsmacht, bijvoorbeeld ook bij de Nederlandse eenheden — ik denk dat het goed is om dat hier ook te zeggen — die de enhanced Forward Presence in Litouwen vormen.

Dan vroeg mevrouw Karabulut of er ook offensief optreden buiten artikel 100 mogelijk is. Nou, u weet dat de krijgsmacht in z'n totaliteit, en dus ook het DCC, want het Defensie Cyber Commando valt daaronder, kan worden ingezet voor de bescherming van de belangen van het Koninkrijk, voor de bescherming van het eigen en bondgenootschappelijk grondgebied, en voor de handhaving of bevordering van de internationale rechtsorde. En voor inzet van het Defensie Cyber Commando — ik heb het net in de richting van mevrouw Bruins Slot ook min of meer gezegd — zijn dezelfde regels van toepassing als bij de inzet van de krijgsmacht. Dus in geen geval kan de krijgsmacht offensieve cybercapaciteiten inzetten buiten de bestaande juridische kaders. Als het optreden plaatsvindt tijdens een gewapend conflict, zoals de uitvoering van de verdedigingstaak, of bij inzet op verzoek van een ander land om dat land te helpen verdedigen, dan valt dat optreden binnen het humanitair oorlogsrecht. En in internationale missies en operaties is de internationaalrechtelijke grondslag bepalend voor de bevoegdheden tot optreden. De bevoegdheden voor de uitvoering van de operaties worden in het missiemandaat bepaald, en die worden dan weer verder uitgewerkt in de Rules of Engagement.

Mevrouw Karabulut vroeg ook of attributie überhaupt mogelijk is. Zij zei eigenlijk: het lijkt wel onmogelijk, als ik zelf naar de stukken kijk. Attributie is niet onmogelijk. Het is wel technisch zeer complex. Daar heeft mevrouw Karabulut zeker gelijk in. Maar de diensten investeren hier in gezamenlijkheid fors in, zodat het ook echt mogelijk is om te attribueren.

Mevrouw Karabulut had eerder al gezegd dat zij blij was met de openheid waarvoor was gekozen, mede omdat het de OPCW betreft. Zij vroeg: kan de minister andere voorbeelden noemen van oorlogshandelingen tegen een vitale sector, of in Nederland of bij bondgenoten? Niet alles kan altijd, zoals mevrouw Karabulut weet, maar er zijn zeker voorbeelden te noemen van cyberaanvallen op bondgenoten waarbij de autoriteiten van die landen op z'n minst een sterke verdenking van Russisch handelen hebben uitgesproken. Ik kan er een aantal noemen. Estland heeft dat gedaan in 2007. Duitsland heeft dat gedaan bij een aanval op de Bondsdag in 2015. In de Verenigde Staten — dat is vandaag ook genoemd — waren er in 2016 aanvallen op de Democratische Partij. In Noorwegen is dat in 2017 gebeurd. In Tsjechië heeft de minister van BZ dat ook in 2017 gedaan. Het is dus wel degelijk zo dat er vaker wordt gezegd dat de Russen betrokken zijn bij dit type activiteit.

Mevrouw Karabulut vroeg wat ik vond van het artikel in de Volkskrant waarin oud-MIVD-baas Pieter Cobelens werd aangehaald. Hij zei dat we na een hackpoging van de Russen gewoon een kwartier het licht uit moeten doen in Rusland, in de badkamer van Poetin en in heel Moskou. De vraag was wat ik daarvan vind. Ik ben het daar niet mee eens. Dat wil ik hier wel klip-en-klaar zeggen. Voor Nederland is het juist een internationaal speerpunt om wereldwijd

erkenning te bewerkstellingen van het feit dat het geldend internationaal recht net zo goed van toepassing is op het cyberdomein. Ik heb er net een hele tijd over gesproken. Een volkenrechtelijk mandaat en een proportionele inzet van de krijgsmacht zijn hier kernelementen in.

Dan vroeg mevrouw Karabulut ook nog naar een Nederlandse hack in Rusland. Zij vroeg wat wij daar gedaan hebben. Daar zal ik toch het antwoord op moeten geven dat ik u vaker moet geven, namelijk dat wij over lopende operaties van de AIVD, of de MIVD in dit geval, in het openbaar geen uitspraken doen. U kunt er wel van op aan dat onze diensten binnen de kaders van de Wet op de inlichtingen- en veiligheidsdiensten werken en dat wat wij doen dus is toegestaan.

Voorzitter. Ik ben al bij de heer Van Ojik, die volgens mij een of twee vragen aan mij heeft gesteld. Er komen ...

Mevrouw **Karabulut** (SP):
Ik zal proberen het te vatten in één vraag. De minister stelt dat zij geen afstand neemt van haar eerdere uitspraken dat we in cyberoorlog zijn met Rusland, maar heeft tegelijkertijd gezegd dat wij niet in oorlog zijn met Rusland. Kan de minister dat nogmaals bevestigen? Want als de minister eraan zou vasthouden dat wij in cyberoorlog zijn met Rusland, vraag ik mij af op welke wijze wij daar dan over zijn geïnformeerd. Dat zijn we namelijk niet.

Mijn tweede vraag heeft hiermee te maken. De minister zei eerder dat buiten de artikel 100-operaties ook cyberoperaties uitgevoerd kunnen worden, maar uit haar beantwoording van zo-even begreep ik dat dat niet het geval is. Kan zij daar ook duidelijkheid over scheppen?

Minister **Bijleveld**:
Ik begin met de eerste vraag. Ik heb inderdaad geen afstand genomen van wat ik heb gezegd. Mevrouw Karabulut was wel degelijk aanwezig bij het debat over het jaarverslag van de MIVD, dus zij herkent dit. Ik heb net, helemaal aan het begin van mijn verhaal, ook gezegd: dat neemt niet weg dat er op dit moment geen sprake is van oorlog in de klassieke betekenis van het woord. Ik heb willen bereiken dat we weggaan van de naïviteit. U heeft daar natuurlijk uw opmerkingen bij, maar de bewustwording moet groter worden. Het is belangrijk dat we allemaal zien dat de aard van conflictvoering in de wereld verandert. Die combinatie heb ik gemaakt, zoals ik net in mijn antwoord al heb gezegd.

Zoals ik al in het antwoord op een vraag van mevrouw Bruins Slot heb aangegeven, kunnen offensieve cybercapaciteiten in militaire operaties worden ingezet, al dan niet ter ondersteuning van de conventionele militaire capaciteiten. Die inzet valt dan helemaal onder het betreffende missiemandaat. Daar kan het dus in staan. Voorts noem ik de geldende geweldsinstructies, de rules of engagement. Dat heb ik net ook al aangegeven. De juridische kaders zijn niet anders dan die voor de inzet van conventionele middelen. De bestaande volkenrechtelijke regels gelden. Die zullen ook door ons worden toegelicht. Er zal in zo'n geval ook altijd sprake zijn van een afweging.

Volgens mij is dat wat er nu over te zeggen is. Aan wat ik net heb uitgelegd, heb ik nu in tweede instantie in die zin ook niets toe te voegen. En dat zal dan ook altijd onder het mandaat van de CDS gebeuren. Daar zult u over worden ingelicht, et cetera.

Mevrouw **Karabulut** (SP):
Begrijp ik dan goed dat de minister zegt dat aan nieuwe of ruimere regels geen behoefte is en dat wij, conform artikel 100 en het geldend internationaalrechtelijk kader, zullen worden geïnformeerd als offensieve acties worden of zullen worden toegepast?

Minister **Bijleveld**:
Ik zeg inderdaad dat we het huidige internationaalrechtelijk kader hanteren. De minister van Buitenlandse Zaken zal ingaan op de vragen over de ruimere regelgeving, waar mevrouw Bruins Slot net op duidde. Ik heb uitgelegd hoe wij zouden opereren als wij ingezet worden. Dat valt onder de kaders die u bekend zijn. Die hanteren wij niet anders dan bij een conventionele inzet. Dat valt dus allemaal onder de aansturing van de CDS. Daar wordt u over geïnformeerd, zoals u daar ook in conventionele zin over geïnformeerd wordt.

Mevrouw **Karabulut** (SP):
Voorzitter, staat u mij nog een vraag toe?

De **voorzitter**:
Ja.

Mevrouw **Karabulut** (SP):
Dat vind ik echt heel aardig, voorzitter. Dank u wel.

De **voorzitter**:
Dat ben ik ook.

Mevrouw **Karabulut** (SP):
Ik ben blij dat de minister afstand heeft genomen van de uitspraken van die ex-MIVD'er die heel Moskou wil platleggen. Stel je voor dat we in zo'n wereld terecht zouden komen! Dat willen we niet, dat willen we juist voorkomen. Ik heb gevraagd naar de in de krant geopenbaarde betrokkenheid van Nederlandse hacks in Rusland om de Amerikanen te helpen. Er zijn eerdere voorbeelden dat informatie door de MIVD wordt verzameld, dat die met bijvoorbeeld de Amerikanen wordt gedeeld en dat die vervolgens voor andere doelen worden gebruikt, bijvoorbeeld voor target killings. Op welke wijze worden wij hierover dan wel geïnformeerd? Echt applaus dat wanneer we de Russen betrappen, we dat openbaren. Maar ik wil ook wel weten wanneer de informatie die door ons wordt verzameld voor bepaalde doeleinden, met de Amerikanen wordt gedeeld, zeker wanneer zij die voor andere doeleinden gebruiken.

Minister **Bijleveld**:
Zoals u weet, werken onze diensten geheel en al onder de Wiv en hebben wij procedures afgesproken over het informeren van de Kamer. Dat loopt via de CIVD. Dat is wat ik erover kan zeggen. Ik kan het niet mooier maken. U zult niet

in het openbaar worden geïnformeerd over lopende operaties van de AIVD en MIVD. U kunt ervan op aan dat we onder de Wiv werken. Daar zijn regels voor en daar is een toezichtregime op. U weet dat allemaal. Wij praten daarover verder en leggen verantwoording af aan de Kamer in de CIVD.

Mevrouw **Karabulut** (SP):
Dat is natuurlijk voor mij als volksvertegenwoordiger uitermate problematisch, zeker wanneer ik via goede journalistiek en onderzoekswerk verneem dat er informatie wordt gedeeld met bondgenoten, die door die bondgenoten vervolgens wordt ingezet voor target killings waarbij burgerslachtoffers vallen. Hier komen we hopelijk nader over te spreken. Ik zou willen vragen of de minister haar oordeel kan vellen over cyberoperaties zoals inmenging in verkiezingen maar ook over cyberoperaties van bijvoorbeeld bondgenoten, de Amerikanen, zoals onthuld door Edward Snowden. Keurt de minister die ook af, net als de Russische operaties?

Minister **Bijleveld**:
Ik kan het gewoon niet mooier maken voor mevrouw Karabulut. Over operaties van de diensten zeggen we in de openbaarheid niets. Beïnvloeding van verkiezingsprocessen mag niet gebeuren, door wie dan ook. Dat is totaal helder. Daar zijn wij als regering volgens mij altijd klip-en-klaar over. geweest.

Ik ben bijna aan het eind van de vragen die aan mij gesteld zijn. De heer van Ojik vroeg, in aansluiting op mevrouw Bruins Slot, of het DCC in staat is zijn taken uit te voeren. Wat kunnen ze? Defensie heeft het Defensie Cyber Commando niet voor niets opgericht. Het bestaat inderdaad sinds september 2014. Dat heb ik net gezegd in antwoord op een vraag van mevrouw Bruins Slot. Het kabinet verwacht dat het hele cyberaspect een steeds prominenter onderdeel zal zijn van een toekomstig conflict. Niet voor niks hebben we uiteindelijk ook met het openbaar maken van wat hier gebeurde hopelijk de bewustwording in zijn totaliteit onder de Nederlandse bevolking vergroot. Het is van belang om te werken aan een volwaardig inzetbaar DCC. Daar wordt nu stap voor stap naartoe gewerkt. Wij investeren vanaf 2019 extra in digitale veiligheid, waarvan een deel voor het DCC is bestemd. Het DCC zet in op personele uitbreiding om de inzetbaarheid te vergroten. Ik hoorde een aantal leden van de Kamer zeggen dat dit niet zo was, maar in het NAVO-plan is er wel degelijk aandacht voor cyber opgenomen, juist omdat het karakter van oorlogvoering verandert. Om in het digitale domein helemaal succesvol te zijn is diepgaande kennis onontbeerlijk. Je hebt te maken met schaarse specialisten op de arbeidsmarkt. Het is niet vanzelfsprekend dat die zomaar allemaal bij Defensie komen werken. Maar generaal Boekholt doet er heel erg haar best voor om dat wel te bereiken. In de Defensie Cyber Strategie heb ik duidelijk aangegeven hoe wij die cybercapaciteiten in de toekomst willen versterken.

De heer Van Ojik vroeg naar de taakverdeling tussen de diensten. De taakverdeling tussen de beide diensten staat in de Wiv aangegeven. Bij deze operatie was er sprake van een optreden van een militaire Russische inlichtingendienst. Dus lag optreden door de MIVD in dit geval voor de hand. Zo zijn de taken verdeeld. Die diensten stemmen hun optreden altijd op elkaar af. Daar kunt u van op aan. Er wordt zeker ook op het cyberdomein gewoon eendrachtig samengewerkt.

Mevrouw Ploumen vroeg, in aanvulling op de heer Van Ojik, of er voldoende wordt geïnvesteerd in digitale weerbaarheid. Ik heb net al aan de heer Van Ojik uitgelegd dat wij daar extra in investeren. We investeren 95 miljoen euro structureel in digitale veiligheid. 20 miljoen daarvan is bestemd voor Defensie. Wij hebben een Nederlandse cybersecurityagenda gemaakt en een Defensie Cyber Strategie. Bij mijn weten hebben we daar op 16 januari een debat over.

Dan de vragen van de heer Voordewind ...

De heer **Van Ojik** (GroenLinks):
Misschien toch nog even over dat cybercommando. Er werd net al even over dat artikel gesproken. Ik geloof dat het in NRC Handelsblad stond, maar goed, dat doet er nou verder niet zo veel toe. Hoewel, voor NRC vast wel. De strekking van dat stuk was eigenlijk: we hadden er veel meer van verwacht. Toen het in 2014 door de voorganger van deze minister werd gelanceerd, was het idee dat het zelfstandig zou interveniëren en dat het echt een slagkracht zou hebben op cyberterrein. Er zouden 200 mensen werken, met een flink budget. Maar dat is er allemaal nog niet zo van gekomen. Dat is eigenlijk de strekking, als je dat stuk leest. Is dat iets wat de minister herkent of zegt ze "dat is helemaal niet waar, we zitten goed op schema"?

Minister **Bijleveld**:
Ik zeg maar eerlijk dat ik niet precies weet met welk startschema er is begonnen. Dat kan ik zo even niet duiden, maar ik heb wel gekeken hoe het vanaf 2014 is gegaan. Ik heb er voor de Defensie Cyber Strategie naar gekeken en daar gaan we ook nog met elkaar over spreken. Ik denk dat er de afgelopen tijd grote stappen zijn gezet, ook omdat dit kabinet wel degelijk veel extra investeert in de cyberkant. Wij doen dat juist ook omdat wij zien dat de oorlogsvoering veel meer hybride wordt. Je ziet ook dat er in de NAVO meer aandacht voor is. Je ziet dat bijvoorbeeld een van de PESCO-projecten bedoeld is om te kijken hoe je op het terrein van cyber beter samen kunt werken. Daar is Estland in de lead. Ik vind wel degelijk dat er grote stappen worden gezet.

Voor het maken van de Defensie Cyber Strategie heb ik een hele groep mensen bij elkaar gezet en heb ik hun gevraagd: wat verwacht u eigenlijk van het optreden van Defensie? Daar was ook de commandant van het Defensie Cyber Commando nadrukkelijk bij aanwezig. Sterker nog, we hebben het daar georganiseerd. Dan zie je dat er grote stappen zijn gezet. Ik denk dat er nu zo'n 80 tot 100 mensen aan het werk zijn. Het hadden er misschien meer kunnen zijn, maar we zoeken heel nadrukkelijk naar nieuwe mensen. We proberen samenwerkingsafspraken met bedrijven te maken. Je ziet dat Nederlandse bedrijven, maar ook andere overheidsinstanties, een heel nadrukkelijk verwachtingspatroon hebben ten aanzien van Defensie, want zij willen dat Defensie een aantal dingen doet, zowel defensief als offensief.

Ik ben eigenlijk wel gematigd positief over de stappen die er zijn gezet. Dat er nog meer moet gebeuren, is helder. Niet voor niks praten we vandaag hierover. Niet voor niks heeft het kabinet ook in het NAVO-plan nadrukkelijk gekozen voor extra investeringen op het terrein van cyber. Dus ik ben ietsje positiever dan de heer Van Ojik. Misschien wel omdat we bijna bij kerst zijn, voorzitter! Ik heb daar ook veel Kamerleden over gehoord.

De **voorzitter**:
Dat wordt door iedereen gezegd, maar ondertussen wordt er op de gewone, normale manier met elkaar gedebatteerd.

Mevrouw Bruins Slot.

Mevrouw **Bruins Slot** (CDA):
Is een van de problemen bij dit punt, dat de heer Van Ojik terecht aandraagt, niet dat het veel interessanter is om te werken als cybersoldaat bij de Militaire Inlichtingen- en Veiligheidsdienst, omdat je dan in de praktijk mag werken? Bij het Defensie Cyber Commando zit je eigenlijk alleen maar in oefenscenario's.

Minister **Bijleveld**:
Dat is misschien wel één van de punten. Er wordt natuurlijk wel heel nadrukkelijk samengewerkt door de MIVD en het DCC, maar het zou misschien best wel één van de punten kunnen zijn. Ik weet niet of het echt het grootste punt is, want het is natuurlijk sowieso moeilijk om dit type specialisten te vinden. Bij de MIVD, en overigens ook bij de AIVD, slagen we er overigens redelijk in om die mensen te vinden. We kunnen dus nog eens kijken wat daarachter zit.

Mevrouw **Bruins Slot** (CDA):
Om een vergelijking te maken met de conventionele militairen ...

Minister **Bijleveld**:
Conventionele of confessionele?

Mevrouw **Bruins Slot** (CDA):
De minister twijfelt tussen confessioneel of conventioneel, maar dat zijn echt twee verschillende begrippen.

Laten we gewoon een normale infanterist nemen. Die mag gewoon schieten. Die mag gewoon offensief optreden. Tot nu toe hebben de cybersoldaten van het DCC alleen maar mogen incasseren. Ik kan me dan ontzettend goed indenken dat ze wel bij de Militaire Inlichtingen- en Veiligheidsdienst aan de slag gaan, omdat ze daar daadwerkelijk actief iets aan onze veiligheid kunnen doen, in plaats van bezig te zijn met het uitvoeren van serious gaming en oefenscenario's. Hoe kan de minister daar in de toekomst verandering in brengen?

Minister **Bijleveld**:
Ik denk dat we over dit punt bij de Defensie Cyber Strategie misschien wat langer met elkaar kunnen praten, want ik weet niet of dit debat zich daar het beste voor leent. Zij zijn wel degelijk ook bezig geweest om over de hele breedte van de krijgsmacht de weerbaarheid te vergroten. Dus het is meer dan dat u aanhaalt. Maar dat we daar in de toekomst anders naar zullen moeten kijken, is mij ook wel helder. Het lijkt mij typisch een onderwerp dat we bij het debat over de cyberstrategie verder kunnen bespreken.

Voorzitter. Ik ben aangeland bij de heer Voordewind, die de vraag stelde of er andere landen zijn die inbreken op Nederlandse systemen. De heer Voordewind zal niet verbaasd zijn, maar ik kan daar in het openbaar niets over zeggen, net zomin als over de Russische repercussies op de OPCW-hackpoging. Wel is het zo dat in het Cybersecuritybeeld Nederland, dat u van mijn ambtsgenoot van JenV hebt ontvangen, en in de jaarverslagen van de diensten natuurlijk wel melding wordt gemaakt van de groeiende dreiging door statelijke actoren. Zowel Rusland als China worden overigens genoemd in het digitale domein. Dat zijn ook de twee actoren die de grootste dreiging vormen.

Voorzitter. Dan had de heer Stoffer volgens mij eenzelfde type vraag als al was gesteld over de juridische kaders die er zijn. Het is helder. De krijgsmacht, waaronder het DCC, kan worden ingezet precies zoals we het anders doen, onder de geldende regels die er zijn. Volgens mij hoef ik daar niet verdergaand iets over te zeggen dan ik net heb gedaan. Helaas kan ik de vraag van de heer Van Roon ook niet in de openbaarheid beantwoorden. Over het MH17-onderzoek kunnen wij in de openbaarheid niets meer zeggen dan wij al hebben gedaan.

Voorzitter. Dan ben ik aan het eind van mijn termijn. Ik wil afrondend zeggen dat ik graag de complimenten die door de Kamer zijn uitgesproken, wil overbrengen aan alle mensen van de verschillende diensten, die eendrachtig hebben gewerkt aan deze verstoringsoperatie bij de OPCW, en dat het ontzettend van belang is geweest dat dit zo goed gedaan is.

De **voorzitter**:
Dank u wel. Dan geef ik nu het woord aan de minister van Buitenlandse Zaken.

Minister **Blok**:
Dank u wel, voorzitter. Zoals de minister van Buitenlandse Zaken net heeft aangegeven ...

De **voorzitter**:
Van Defensie.

Minister **Blok**:
... van Defensie net heeft aangegeven — ik heb ook wel dingen net aangegeven, maar dat was in vorige debatten — staat de cyberoperatie van Rusland die de aanleiding vormt voor dit debat niet op zich. We hebben te maken met een verslechterende veiligheidssituatie en een zeer assertief optreden van Rusland en overigens ook een aantal andere landen. Dat heeft directe consequenties voor de Nederlandse veiligheid. De allereerste implicatie is dat Nederland zich samen met onze bondgenoten zowel in Europees verband als in NAVO-verband moet aanpassen en zorgen voor

eigen weerbaarheid. Tegen die achtergrond heeft het kabinet ook de nodige maatregelen aangekondigd. Verderop zal ik ingaan op de daarover gestelde vragen.

Ik zal mijn antwoorden verder indelen langs de volgende lijn. Vragen die gesteld zijn over cyberdiplomatie en cybersancties; de relaties met Rusland en een aantal losse onderwerpen. Maar eerst de vragen die gesteld zijn over cyberdiplomatie en cybersancties. De heer Verhoeven en mevrouw Bruins Slot vroegen in welke staat het cybersanctieregime zich op dit moment bevindt. Nederland zet zich binnen de Europese Unie met een aantal andere landen in voor een sanctieregime en de Europese Raad heeft opdracht gegeven aan de Commissie om dat verder uit te werken. Het gaat om een regime dat niet op voorhand op specifieke landen gericht is; het kan ook betrekking hebben op individuen. Op dit moment vindt die uitwerking plaats in Brussel. Nederland speelt daar ook een actieve rol in. Wij hopen dat in de eerste helft van 2019 dat sanctieregime van kracht zal worden. Daar is wel unanimiteit voor nodig. Als het eenmaal van kracht is, kunnen daaronder ook individuen of landen op een lijst worden gezet.

Het waren ook de heer Verhoeven en mevrouw Bruins Slot die vroegen of het geen tijd wordt om een aanvullend internationaal verdragsraamwerk voor cybersecurity en cyberaanvallen in het leven te roepen. Die vraag is op verschillende plaatsen aan de orde gesteld. Er is op dit moment al internationale regelgeving over het fatsoenlijk verkeer tussen verschillende landen. De suggestie dat er geen regelgeving zou zijn, is op zich onjuist en ook onwenselijk. Die suggestie wordt namelijk ook graag gewekt door landen die zich schuldig maken aan ongewenste praktijken. Het is dus van groot belang dat wij allereerst met elkaar erkennen dat gewoon het bestaande recht, het staande internationaal recht, van toepassing is in cyberspace zoals het ook elders van toepassing is en dat er geen legitimatie gevonden kan worden voor het doen van cyberoperaties door te suggereren dat er geen recht zou zijn.

De vraag om te onderhandelen over verdere invulling, kan ook een vraag zijn ingegeven door de wens om te suggereren dat er geen recht zou zijn. Daarmee suggereer ik niet dat dat de vraag van de heer Verhoeven of mevrouw Bruins Slot zou zijn, maar we moeten wel goed in de gaten houden dat de Nederlandse stelling niet voor niets is dat er internationaal recht is, dat dat ook van kracht is in cyberspace en dat daar geen aanvullend onderhandelingstraject voor nodig is.

Ik ben het wel met de beide vragenstellers eens dat het van groot belang is dat de rechtsregels die er al zijn, geëerbiedigd worden en dat we er met elkaar voor moeten zorgen — mevrouw Bruins Slot wees ook naar het Tallinn Manual — dat er praktische handvatten zijn voor hoe je nu in een concrete situatie welke rechtsregel het beste toepast. Tegen deze achtergrond, waar het gaat om implementatie, ziet Nederland inderdaad een belangrijke rol voor zichzelf. Die spelen we ook. Ik heb zelf nog niet zo lang geleden een congres over de Tallinn Manual toegesproken hier in Den Haag. Maar we moeten niet meegaan in een suggestie dat er überhaupt geen recht van toepassing zou zijn.

Mevrouw Bruins Slot vroeg hoe het staat met de cyberdiplomatie. Dat is een van de speerpunten die het kabinet in de Geïntegreerde Buitenland- en Veiligheidsstrategie heeft aangegeven, omdat we ook op dat moment — dat speelde nog voor deze OPCW-hack — zagen dat er sprake is van een toenemende dreiging. Dat betekent dat we zorgen dat überhaupt de kennis bij onze diplomaten op het gebied van cybersecurity wordt vergroot. We zorgen ervoor dat uiteindelijk op iedere post iemand aanwezig is die goed op de hoogte is van zowel cyberdreiging als het internationaalrechtelijke raamwerk waarbinnen gewerkt kan worden. Daarnaast zullen we de komende jaren zorgen dat er specifieke cyberexpertise aanwezig zal zijn op de posten in Génève, Moskou, Peking, Washington, Brussel en Singapore.

Wat doen die dan, was de vervolgvraag van mevrouw Bruins Slot. Dat is een combinatie van het operationaliseren van de acties die mogelijk zijn, diplomatieke acties, maar ook juridische acties. Dat is in lijn met die Tallinn Manual. Het is van groot belang dat we dat gezamenlijk doen met landen die er hetzelfde over denken en dat we proberen om landen waarvoor dat nog niet geldt ook aan onze kant te krijgen. Wij zetten de mensen natuurlijk ook in bij het implementeren van het internationaal recht en het beperken van de dreiging die uit kan gaan van zowel statelijke actoren als criminele actoren. Daarvoor organiseren wij ook internationale bijeenkomsten, zoals het Global Forum on Cyber Expertise.

De heer Van Ojik vroeg of het attribueren ...

De **voorzitter**:
Voordat u verdergaat, wil mevrouw Bruins Slot een vraag stellen.

Mevrouw **Bruins Slot** (CDA):
Ik wil de minister nog bedanken voor zijn uitgebreide verhandeling over de toepasbaarheid van het internationale recht in het digitale domein. Het gaat inderdaad om de praktische uitwerking. Dat komt ook overeen met het betoog dat het CDA heeft gehouden. De vraag die ik daarbij heb gesteld is: hebben we dat nou in Nederland ook voldoende voor onszelf opgeschreven? Hoe zien wij die interpretatie? Zijn wij het bijvoorbeeld helemaal en voor honderd procent eens met alle punten van de Tallinn Manual?

Minister **Blok**:
Wij hebben dat zeker voor ogen. Moet ik de vraag van mevrouw Bruins zo begrijpen dat zij vraagt: wilt u dat ook met de Kamer delen? Voor dit onderdeel, de toepassing van het bestaande recht op cyberaanvallen, heb ik daar natuurlijk geen enkel bezwaar tegen. Als mevrouw Bruins dat wil, zullen wij dat verschaffen.

Mevrouw **Bruins Slot** (CDA):
De minister zegt: "de toepassing van het bestaande recht". Als ik smal interpreteer wat de minister tegen mij zegt, zou het feitelijk het beschrijven zijn welke rechtsregels van toepassing zijn. Maar het gaat natuurlijk om de praktische uitwerking. Welke grenzen stelt Nederland zelf? Wanneer vinden wij een digitale aanval ontwrichtend? Wanneer zeggen we dat een digitale aanval ook een oorlogsdaad is? Welk afwegingskader hebben we? Hoe doen we dan precies de attributie? Ik vraag dit duidelijk omdat het mij lijkt dat

wat de minister zegt, een smalle interpretatie is. En ik vraag nadrukkelijk om een brede interpretatie.

Minister **Blok**:
Ik wil nou niet in een discussie over smal en breed vervallen. Ik geef aan dat ik graag bereid ben met u te delen hoe Nederland daarmee omgaat. Dat doe ik mede namens collega Bijleveld. Daarbij gaat het inderdaad om het type vraag dat mevrouw Bruins Slot noemt.

Mevrouw **Bruins Slot** (CDA):
Dank voor die toezegging. Op welke termijn zou dat kunnen?

Minister **Blok**:
Dit is geen kwestie van "even in een weekje". Ik wil dit echt zorgvuldig doen. Ik wil toezeggen om dit in het eerste halfjaar van 2019 naar de Kamer te sturen.

De heer Van Ojik vroeg of we vaker openlijk zullen attribueren. In de jaarverslagen van de inlichtingendiensten is natuurlijk al eerder aangegeven dat de diensten constateren dat er sprake is van ongewenste cyberactiviteit, onder meer door de Russische Federatie, China en Noord-Korea. Of we een actie van een van deze landen, of van een ander land, specifiek zullen attribueren, zullen wij natuurlijk van geval tot geval afwegen. Het bekendmaken van wat je weet en wat je niet weet, is natuurlijk voor de staat die die acties onderneemt ook niet zonder belang. Nu konden we een flinke tik op de vingers geven door deze operatie bekend te maken. Het kan zijn dat in een ander geval juist het belang van het beter kunnen bestrijden van dit soort van operaties met zich meebrengt dat je niet de specifieke operatie bekendmaakt, maar je je weer moet beperken tot het in het jaarverslag bekendmaken dat er activiteiten zijn. Dit is dus echt een kwestie van maatwerk, vanuit het doel om deze activiteit effectief te kunnen bestrijden.

Ik kom bij de vragen die gesteld zijn over de relaties met Rusland. De heer Van Ojik vroeg of wij deze hack ook aan de orde hebben gesteld bij de OVSE en in andere internationale fora. Dat is inderdaad het geval. Zowel in de OVSE als ook in de VN-Veiligheidsraad en natuurlijk in de OPCW, omdat die laatste het doelwit was van deze acties.

Mevrouw Ploumen vroeg ...

De heer **Van Ojik** (GroenLinks):
Ik ben nog wel geïnteresseerd in de OVSE. Daar is cybersecurity een prioriteit, als ik het goed begrijp. Daar zit je met de Russen aan tafel. Dat kan een voordeel zijn, maar dat kan ook een nadeel zijn. Ik heb in de stukken gezien dat er soms sprake is van vertrouwenwekkende maatregelen die we zouden moeten gaan nemen op dit terrein. Daar ben ik voor. Maar het is ook ingewikkeld, want je deelt misschien informatie ... Nou ja, volgens mij begrijpt de minister waar ik naartoe wil. Is dit nou een goed forum om het aan de orde te stellen? Of zegt de minister: ik ben liever heel voorzichtig bij de OVSE, want de Russen zitten daarbij? Ik vraag me af hoe dat gaat.

De **voorzitter**:
De minister kan zelf antwoorden; u gaat het invullen voor de minister.

Minister **Blok**:
Mijn antwoord is volmondig: dit is een goed forum. Ik ben het met de heer Van Ojik eens dat het een grote waarde op zich heeft dat we, naast de VN, een overlegforum hebben waar Rusland aan tafel zit. Maar zo'n overlegforum zou niet kunnen functioneren als je daar niet ook zaken aan de orde stelt die niet door de beugel kunnen. Dat moet natuurlijk niet je enige agenda zijn. Ik zal zo meteen ingaan op de vraag van mevrouw Ploumen hoe die bredere dialoog eruit ziet. Je zoekt dus ook bewust in de OVSE naar punten waar we overeenstemming over kunnen bereiken. De OVSE is ook actief op terreinen als economische samenwerking en zelfs milieusamenwerking — ook niet altijd makkelijk! We zoeken daar nadrukkelijk naar een brede agenda, maar benoemen ook helder wat fout is.

Dat is dan meteen ook het bruggetje naar de vraag van mevrouw Ploumen hoe wij nou invulling geven, ook na deze Russische acties, aan de combinatie van druk en dialoog. Onze lijn blijft om dingen waar we elkaar kunnen vinden, zoals economische relaties, culturele relaties en uitwisselingen van studenten of wetenschappers, plaats te laten vinden, net zoals onze diplomatieke kanalen open zijn. Ikzelf spreek zo nu en dan bij internationale bijeenkomsten mijn collega Lavrov weer aan. Natuurlijk zorg je dat die lijnen open zijn en dat dat niet alleen uit woorden bestaat maar ook een bredere band met zich meebrengt. Maar daar hoort ook bij dat bij zaken zoals deze, en in de relatie met Rusland zijn er helaas nog veel meer, zoals het optreden in Oekraïne of Syrië, helder moet zijn wat wij onacceptabel vinden. We hebben niet voor niets recent helaas bekend moeten maken dat ook Nederland constateert dat Rusland het INF-verdrag schendt. Heel zorgelijk, maar dan moeten we daar ook heel helder over zijn. Maar, nogmaals, dat betekent niet dat we zeggen: en nou kan er geen handel meer gedreven worden of geen normaal diplomatiek verkeer plaatsvinden.

Inderdaad draagt het lidmaatschap van de VN-VR daaraan bij. Aan de ene kant omdat we bij de successen die we gelukkig hebben kunnen boeken — de resoluties die zijn aangenomen, de sancties tegen mensenhandelaren — natuurlijk met alle leden van de Veiligheidsraad, dus ook Rusland, van tevoren contact zoeken om te zorgen dat we successen kunnen boeken. Tegelijkertijd hebben we helaas nog steeds belangrijke onderwerpen, met name Syrië maar ook op andere terreinen, waar we van tevoren wel die contacten zoeken maar helaas moeten constateren dat dat in de Veiligheidsraad niet leidt tot conclusies en resoluties die ook echt een stap vooruit zijn. Ook hier geldt dat het feit dat je lid bent van de Veiligheidsraad betekent dat je elkaar vaker en op andere plekken tegenkomt dan wanneer je geen lid bent. Mevrouw Ploumen weet natuurlijk ook uit eigen ervaring dat dat mij, collega Kaag en de premier de gelegenheid biedt om op andere plaatsen de Russische Federatie, en overigens ook andere landen, aan te schieten over zaken die wij van belang vinden. Dat hebben we dus ook nadrukkelijk gedaan. Voor een deel was dat in de openbaarheid. Na de aansprakelijkheidsstelling van Rusland vanwege de inzet van de Buk bij de aanslag op de MH17 ben ik ook direct naar de VN gevlogen om gebruik te maken

van het lidmaatschap, om het ook daar aan de orde te kunnen stellen.

De heer Voordewind vroeg of er Russische tegenreacties zijn geweest na het openbaar maken van de mislukte operatie in Den Haag. De tegenreactie was het ontbieden van onze ambassadeur. Er zijn geen andere tegenreacties geweest.

De heer Voordewind vroeg ook of er een verband is tussen spionage met betrekking tot de MH17 en de operatie hier. Het was voor Nederland al eerder duidelijk dat er Russische betrokkenheid is bij het neerschieten van de MH17, want we hadden Rusland al aansprakelijk gesteld voordat de OPCW-hack plaatsvond en we dus ook de aanvullende informatie hadden rond de pogingen om MH17-informatie te krijgen. Dit heeft ons beeld dus niet veranderd.

Voorzitter. Dan stap ik over van de relatie met Rusland naar een aantal andere vragen. De heer Koopmans vroeg of de brexit gevolgen heeft voor de veiligheidssamenwerking. In het terugtrekkingsakkoord dat voorligt, zijn daarover de goede afspraken gemaakt. Er zijn een heleboel redenen om van harte te hopen dat het Verenigd Koninkrijk met het terugtrekkingsakkoord zal instemmen, maar veiligheidssamenwerking is zeker niet de minst belangrijke. Ik kan niet speculeren over wat er gebeurt als we toch met een harde brexit te maken hebben. We gaan elkaar na het reces nog uitgebreid spreken over de scenario's daarvoor.

Mevrouw Ploumen vroeg naar aanleiding van de berichtgeving die vanmiddag naar buiten kwam, hoe Nederland reageert op het nieuws vanuit de VS en het Verenigd Koninkrijk dat China de afgelopen jaren betrokken is geweest bij een hack. Wij spreken politieke steun uit voor de informatie en het oordeel dat beide landen naar buiten hebben gebracht. Het is niet zo dat ik informatie met de Kamer kan delen over deze specifieke activiteiten in Nederland. Ook hiervoor geldt dat het vertellen van wat je wel en niet weet, ook van waarde is voor andere landen. Ik kan hierover dus niet meer informatie verstrekken dan dat ik politieke steun uitspreek voor de informatie die naar buiten is gekomen.

De **voorzitter**:
Laatste vraag, mevrouw Bruins Slot.

Mevrouw **Bruins Slot** (CDA):
De Amerikanen wel. Op de site van de BBC staat — als die informatie klopt — dat Nederland ook door dit collectief van hackers is aangevallen.

Minister **Blok**:
Maar dat verandert niets aan wat ik u net meegeef: het verstrekken van informatie over wat wij wel of niet weten over andere diensten is ontzettend interessant voor die andere diensten.

De **voorzitter**:
Mevrouw Bruins Slot, ik zie u twijfelen. Maar het schijnt dat wij het kerstgevoel hebben, dus u mag nog een keer.

Mevrouw **Bruins Slot** (CDA):
En vanwege het kerstgevoel moet ik het heel kort houden.

De **voorzitter**:
Goed zo.

Mevrouw **Bruins Slot** (CDA):
Klopt de bewering van de VS dat Nederland hierdoor ook aangevallen is?

Minister **Blok**:
De Chinezen zullen nu met grote interesse willen weten wat ik daarop ga antwoorden. Het antwoord is dat ik daar geen informatie over ga geven. Maar ik neem aan dat mevrouw Bruins Slot ook heel goed weet waarom ik het antwoord geef dat ik geef.

De **voorzitter**:
Gaat u verder. U kijkt naar mevrouw Karabulut of ze nog een vraag voor u heeft. Nee? Ik trek het weer in, mevrouw Karabulut.

Minister **Blok**:
Dan vroeg mevrouw Ploumen met enige scherpte of de VS nog een bondgenoot is. Het is zeker zo, dat hebben wij ook vaker in de Kamer bediscussieerd, dat Nederland een aantal beslissingen van de kant van de huidige Amerikaanse regering betreurt: het opzeggen van het klimaatakkoord, het verplaatsen van de ambassade naar Jeruzalem, het opzeggen van het nucleair akkoord met Iran, de handelsconflicten die oplaaiden. Maar dat leidt niet tot de conclusie dat de VS geen bondgenoot is. De VS zijn om zeer actuele maar ook om historische redenen een van onze belangrijkste bondgenoten. Zij zijn een van de belangrijkste, grootste democratische rechtsstaten in de wereld en een grote partner als het gaat om onze collectieve verdediging. Nederland, de NAVO zou zonder de rol van de Verenigde Staten niet in staat zijn om zichzelf goed te verdedigen. Hoewel wij conflicten of in ieder geval een discussie hebben over vrijhandel, geloven wij absoluut in de grote waarde van een vrijemarkteconomie. Hoewel we het niet altijd eens zijn over de rol die de Verenigde Naties of andere multilaterale organisaties moeten spelen, staan we wel aan de kant van de landen die zeggen dat internationaal recht boven particuliere belangen van landen gaat. Internationale samenwerking is van groot belang. Er is dus nog steeds veel meer dat ons bindt dan dat ons scheidt.

Mevrouw Ploumen vroeg naar aanleiding van de brief over de defensie-uitgaven, die we volgens mij nog uitgebreid gaan bespreken, waarom het kabinet geen uitspraken doet over de OS-norm. We hebben in het regeerakkoord een enorme extra investering in OS gedaan. Er is wel degelijk sprake van dat dat budget fors oploopt. Het is niet zo dat we dat in ieder debat of in iedere brief herhalen, maar dat doet niets af aan het feit dat dat gebeurt.

Dan heeft de heer Voordewind nog twee vragen gesteld over Nord Stream. Ik meen dat de Kamer ook daarover een apart debat wil voeren. Ik heb de Kamer daar de afgelopen week ook een brief over gestuurd. Ik wil dat debat dus graag

voeren, maar indachtig de vraag om het nu kort te houden stel ik voor dat we dat voeren op het moment dat de Kamer dat plant in januari.

Dan hoop ik hiermee de vragen in de eerste termijn beantwoord te hebben.

De **voorzitter**:
Mevrouw Karabulut.

Mevrouw **Karabulut** (SP):
Ik heb echt gewacht maar ...

De **voorzitter**:
Ja, dat zag ik.

Mevrouw **Karabulut** (SP):
... ik wilde nog één oordeel van de minister. We spreken hier terecht schande van Russische en Chinese spionage, maar de grootste hackers, spionnen in dezen zijn misschien wel de Amerikanen. Door de onthullingen van Edward Snowden weten we dat op grote schaal is gespioneerd in de VN, bij het Energie Atoomschap, in de EU, en dat zelfs bondskanselier Merkel is afgeluisterd. Is de minister van mening dat deze spionagepraktijken net zo goed schandelijk zijn?

Minister **Blok**:
Als Nederland geconfronteerd wordt met spionageactiviteiten van een bevriend land of een bondgenoot op ons grondgebied, dan geven wij in niet mis te verstane bewoordingen weer dat wij het daar niet mee eens zijn.

Mevrouw **Karabulut** (SP):
De voorbeelden die ik net noemde, zijn zeer ernstig en zeer vergaand. Vindt de minister dat net zo goed schandelijk, net als de Russische, Chinese of whatever spionage? Hij mag zijn eigen bewoordingen kiezen. Ziet de minister dat dit type spionage toeneemt? En welke de-escalatiemogelijkheden ziet de minister?

Minister **Blok**:
Dat is weer een andere vraag. Om antwoord te geven op de eerste vraag: als er op ons grondgebied spionageactiviteiten zijn, door wie dan ook, dan zullen we de betrokkenen daarop aanspreken. Mevrouw Karabulut wees bijvoorbeeld op Duitsland. Volgens mij is daar toen ook van Duitse zijde helder op gereageerd. Zij reageren net zo als wij zouden reageren als dat bij ons aan de orde is. Is er sprake van een toename? Dit is nou bij uitstek een terrein waarover geen openbare statistieken bekend zijn. Zoals de minister van Defensie terecht zei, heeft Nederland gewoon de Wet op de inlichtingen- en veiligheidsdiensten, die bepaalt hoe wij in het belang van onze eigen veiligheid — want ik ben nou eenmaal minister van dit land — omgaan met het inwinnen van informatie. Dat is op zich niet verboden. Dat doen wij hier onder keurig toezicht van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten en de commissie voor de Inlichtingen- en Veiligheidsdiensten, waar een deel van uw Kamer lid van is. Dat kan allemaal geen verrassing zijn. Als het spiegelbeeldig op ons terrein plaatsvindt, dan reageren wij daar helder op.

Mevrouw **Karabulut** (SP):
Maar dat het niet verboden is, maakt het niet ook wenselijk. Wij bespreken hier de Russische spionagezaak, omdat het schandelijk is en omdat het niet mag. Wij willen dus dat Rusland, China en andere landen dat niet doen. Dan snap ik niet dat wij datzelfde zouden doen. De minister wil daar niet over spreken, maar we hebben een aantal voorbeelden uit het verleden, zoals de betrokkenheid bij de Amerikaanse operatie richting de Russen, waarbij Nederland ook heeft gehackt. De minister erkent gelukkig dat het niet alleen die landen zijn waar wij graag over spreken, maar dat het ook bondgenoten zijn. Dan zou mijn vervolgvraag zijn: als de minister inderdaad wil dat we dit in de toekomst gaan voorkomen, net als escalatie, welke stappen denkt hij dan in internationaal verband bij al die betrokkenen te kunnen nemen?

Minister **Blok**:
Nederland heeft een Wet op de inlichtingen- en veiligheidsdiensten. Die heeft deze Kamer aangenomen en daarmee heeft ze terecht aangegeven dat zij het van belang vindt dat Nederland ter verdediging van onze eigen veiligheid informatie vergaart. Andere landen doen dat ook. Ik laat aan hun parlementen over hoe zij dat inkaderen. Ik vind overigens dat er een nadrukkelijk verschil is tussen democratische rechtsstaten en landen die dat niet zijn, en de Russische Federatie valt onder die categorie. Dat onderscheid wil ik in zijn algemeenheid maken. Hoe andere landen hun wetten invullen, als dat democratische rechtsstaten zijn, is verder aan hen. Als er op ons grondgebied activiteiten plaatsvinden, ook als dat is van een andere democratische rechtsstaat, dan geven wij in niet mis te verstane woorden weer dat wij dat niet acceptabel vinden.

De **voorzitter**:
Dank u wel. Dan gaan we nu naar de tweede termijn van de kant van de Kamer. Ik geef de heer Verhoeven namens D66 het woord.

De heer **Verhoeven** (D66):
Voorzitter, dank. Ik zal eerst mijn motie indienen.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat er sprake is van een wereldwijde toename in cyberaanvallen door statelijke actoren, zoals de WannaCry- en NotPetya-aanvallen;

overwegende dat dergelijke aanvallen kritieke civiele infrastructuur kunnen raken, de democratische rechtsorde kunnen schaden of gebruikt kunnen worden door cybercriminelen voor cybercriminaliteit;

overwegende dat de Talinn Manual ziet op digitale oorlogsvoering, maar dat dit een niet-bindend juridisch onderzoek is over de werking van internationaal recht op cyberconflicten en cyberoorlogsvoering;

verzoekt de regering het initiatief te nemen om internationale overeenstemming te bereiken over de praktische toepassing van het bestaande internationale recht op het digitale domein en de Kamer hierover te informeren,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 35 (33694).

De heer **Verhoeven** (D66):
Dan wil ik dankzeggen voor de beantwoording. Ik ben overigens even nagegaan hoe het zat met die specifieke uitspraak van een medewerker van Defensie. Ik citeer: "Een gewoon voorbeeld zou zijn dat we de snelheidsmeter van een voertuig manipuleren." Dan heb je dus inderdaad niet gezegd dat je auto's wil hacken, maar dan laat je ook heel duidelijk merken dat je echt iets wil gaan doen op dat gebied. Laten we zorgvuldig communiceren, dat zal ik voortaan ook doen, en wel even opletten, want dit is niet niks. Het gaat gewoon allemaal gebeuren. Over een paar jaar is het echt aan de orde van de dag dat dit gebeurt en ik wil daar wat grip op. Daar kom ik op terug met mijn nota.

Tot slot, de kerstgedachte. In zo'n jaar gaan er altijd een aantal dingen mis en dan moet je soms weleens wat rechtzetten.

De **voorzitter**:
Ik zit er helemaal klaar voor.

De heer **Verhoeven** (D66):
Een van de dingen die ik graag recht zou willen zetten, is het volgende. Er was ooit een initiatiefnota van de heer Koopmans, die ik hier vandaag trof, en daar heeft D66 per abuis tegengestemd, terwijl daar toch goede elementen in zitten. Ik wil toch nog eens benadrukken dat dat volgend jaar anders zal gaan en dat we beter zullen opletten bij het stemmen.

De **voorzitter**:
Dat klinkt goed. Dat staat ook in de Handelingen, meneer Koopmans, dus hij kan er niet meer op terugkomen.

De heer **Verhoeven** (D66):
Hiermee eindig ik mijn bijdrage en die van mijn partij aan het parlementaire jaar 2018, voorzitter.

De **voorzitter**:
Dank u wel, meneer Verhoeven. Dan ga ik naar mevrouw Bruins Slot, namens het CDA.

Mevrouw **Bruins Slot** (CDA):
Voorzitter. Allereerst wil ik namens het CDA waardering uitspreken voor het werk van de medewerkers van de beide inlichtingendiensten. Zij houden onze samenleving veilig en we zien het resultaat van hun werk eigenlijk nooit, behalve op 4 oktober, toen we de presentatie hadden. Het is wel goed om dat te benadrukken.

Ik ben tevreden met de antwoorden van de beide bewindspersonen. Op een aantal terreinen is echt actie ingezet, ook als het gaat om de cybersancties. Inmiddels heeft de minister van Defensie ook een Defensie Cyber Strategie gemaakt. Daarvoor geldt, maar daar zullen we in een ander debat op terugkomen: hoe zorgen we ervoor dat we onze cybersoldaten ook binnen de juiste kaders offensief kunnen gaan inzetten? Want ik ken geen ander wapensysteem waarbij je alleen maar defensief bezig bent. Als je niet ook het offensief goed onder de knie krijgt, dan loop je op een gegeven moment achter.

Voorzitter. Ik kijk uit naar de analyse die de minister gaat sturen over de Nederlandse vertaling van de Tallinn Manual, over hoe die in de praktijk toepassing krijgt en wat dat bijvoorbeeld betekent voor bepaalde afwegingen.

Het laatste, voorzitter. Ik zal verder niet ingaan op de vragen die mevrouw Ploumen stelde over China. De minister is, denk ik, met reden cryptisch. Ik ga de berichtgeving nauwlettend volgen.

Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Bruins Slot.

Dan geef ik nu het woord aan de heer Koopmans namens de VVD.

De heer **Koopmans** (VVD):
Voorzitter. U kijkt zo naar mij, maar ik wilde eigenlijk alleen maar u bedanken en de ministers bedanken voor de beantwoording en iedereen nogmaals een mooi kerstfeest toewensen.

De **voorzitter**:
Dat is heel fijn en heel aardig, meneer Koopmans. Dank u wel. Ik dacht dat mevrouw Karabulut u ging interrumperen, maar dat is niet het geval.

De heer Stoffer namens de SGP.

De heer **Stoffer** (SGP):
Tja, voorzitter, ook zo'n beetje tegen het einde van het jaar ... Ik heb dit jaar prachtige moties ingediend met de heer Verhoeven. Dus ik dacht: laten we dit jaar ook afsluiten met een gezamenlijke motie. En die luidt als volgt.

Ik zie de minister een beetje kijken, zo van "wat wordt dit nu ", maar dat wordt duidelijk in het dictum.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat Nederland, de EU en Rusland gebaat zijn bij goede economische en politieke betrekkingen maar dat deze betrekkingen momenteel onder druk staan;

overwegende dat helderheid over de wijze waarop Nederland en de EU inspelen op de veranderende betrekkingen met Rusland van groot belang is;

overwegende dat dit een actuele, geïntegreerde en toekomstbestendige strategie vereist;

verzoekt de regering een Ruslandstrategie op te stellen en deze in het voorjaar van 2019 aan de Kamer voor te leggen,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 36 (33694).

De heer **Stoffer** (SGP):
En, voorzitter, dan rest mij ook iedereen een gezegend kerstfeest te wensen en een goede jaarwisseling.

De **voorzitter**:
Dank u wel, meneer Stoffer.

Dan ga ik nu naar de heer Voordewind. Nee? Dan kijk ik naar de heer Kuzu. Ook niet. De heer De Roon? Ook niet. Dan kijk ik of de ministers kunnen reageren. Er zijn twee moties ingediend. Eentje wordt nog overhandigd, van de heer Stoffer. Ik weet niet waarom het zo snel gaat. Iets met de kerst, begrijp ik.

Dan geef ik eerst het woord aan de minister van Defensie.

Minister **Bijleveld**:
Voorzitter. Ik heb met mijn collega van Buitenlandse Zaken nu afgestemd, zodat wij allebei "zalig kerstfeest" kunnen zeggen in deze Kamer en allebei één motie voor onze rekening nemen. Omdat die over Rusland nog zal worden overhandigd, zal de heer Blok die voor zijn rekening nemen.

Inderdaad, het is altijd mooi als je naar een rustperiode kan toewerken. Dat wou ik hier nog wel een keer zeggen: voor onze mannen en vrouwen die overal in de wereld opereren is het niet altijd vanzelfsprekend dat ze dat met het thuisfront kunnen doen. Maar ook hier wil ik nog wel een keer zeggen dat ik vanaf deze plek ook aan hen denk en hun ook een zalig kerstfeest en een goed nieuw jaar wens.

Het oordeel over de motie op stuk nr. 35 laat het kabinet aan de Kamer.

De **voorzitter**:
Dank u wel. Dan geef ik nu het woord aan de minister van Buitenlandse Zaken.

Minister **Blok**:
Dank u wel, voorzitter. Ik zal ingaan op de motie op stuk nr. 36, die vraagt om een Ruslandstrategie op te stellen. Daarin wordt gevraagd om zo'n strategie in het voorjaar van 2019 aan de Kamer voor te leggen. Ik zou de Kamer willen vragen om "in het voorjaar" weg te laten. Want ik begrijp de wens, maar als we zo'n strategie zorgvuldig uitwerken ... Er wordt ook gewerkt aan een Chinastrategie. Die komt in het voorjaar van 2019. Daar zouden we dan aanzienlijk meer tijd voor kunnen hebben. Als het gewijzigd kan worden in "in 2019" dan kan ik haar aan het oordeel van de Kamer overlaten.

De heer **Stoffer** (SGP):
Dat kan zeker, want dat "voorjaar" was een toevoeging van de heer Verhoeven!

(Hilariteit)

De heer **Stoffer** (SGP):
Maar binnen het jaar, daar kunnen wij samen mee leven, denk ik.

De **voorzitter**:
De motie-Stoffer/Verhoeven (33694, nr. 36) is in die zin gewijzigd dat zij thans luidt:

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat Nederland, de EU en Rusland gebaat zijn bij goede economische en politieke betrekkingen maar dat deze betrekkingen momenteel onder druk staan;

overwegende dat helderheid over de wijze waarop Nederland en de EU inspelen op de veranderende betrekkingen met Rusland van groot belang is;

overwegende dat dit een actuele, geïntegreerde en toekomstbestendige strategie vereist;

verzoekt de regering een Ruslandstrategie op te stellen en deze in 2019 aan de Kamer voor te leggen,

en gaat over tot de orde van de dag.

Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 37, was nr. 36 (33694).

Het gaat goed!

Minister **Blok**:
Deze invulling van de kerstgedachte kan ook! Ik wil van mijn kant toch niet aan de feestvreugde afdoen door ook iedereen een heel goede kerst en vooral een rustig 2019 te wensen.

De **voorzitter**:
Dank u wel.

De beraadslaging wordt gesloten.

De **voorzitter**:
Daarmee zijn we aan het eind gekomen van dit debat. Over de ingediende moties zullen we rond kwart voor acht stemmen.

De vergadering wordt van 18.51 uur tot 19.49 uur geschorst.