Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 853

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 17 mei 2022

De vaste commissie voor Buitenlandse Zaken, de vaste commissie voor Digitale Zaken en de vaste commissie voor Justitie en Veiligheid hebben op 13 april 2022 overleg gevoerd met de heer Hoekstra, Minister van Buitenlandse Zaken, over:

- **de brief van de Minister van Buitenlandse Zaken d.d. 29 september 2021 inzake internationaal cyberveiligheidsbeleid – IOB-evaluatie 2015–2021 & kabinetsreactie (Kamerstuk 26 643, nr. 793);**
- **de brief van de Minister van Buitenlandse Zaken d.d. 6 oktober 2021 inzake tegenmaatregelen ransomware-aanvallen (Kamerstukken 26 643 en 33 694, nr. 785);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 11 maart 2022 inzake stand van zaken op het gebied van cyber(security) in relatie tot het conflict in Oekraïne (Kamerstuk 36 045, nr. 40).**

Van dit overleg brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Buitenlandse Zaken,
Kuiken

De voorzitter van de vaste commissie voor Digitale Zaken,
Kamminga

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
Van Meenen

De griffier van de vaste commissie voor Buitenlandse Zaken,
Westerhoff

kst-26643-853
ISSN 0921 - 7371
's-Gravenhage 2022

Voorzitter: Rudmer Heerema
Griffier: Konings

Aanwezig zijn zes leden der Kamer, te weten: Brekelmans, Rudmer Heerema, Koekkoek, Van der Lee, Agnes Mulder en Sjoerdsma,

en de heer Hoekstra, Minister van Buitenlandse Zaken.

Aanvang 15.02 uur.

De **voorzitter**:
Dames en heren, welkom bij dit commissiedebat Internationale cyberveiligheid. Welkom aan de mensen thuis die meekijken en aan de bodes voor de ondersteuning. Op dit moment hebben we drie sprekers vanuit de Kamer. Dank aan de Minister voor de komst naar de Kamer. Het vierde Kamerlid, mevrouw Mulder, komt binnen. Welkom! U bent bijna op tijd; hartstikke goed van u. En nummer vijf komt ook binnen. Het wordt nog druk. Nu moeten we gaan marchanderen met de spreektijden.
Aanwezig zijn vandaag de heer Brekelmans van de VVD, mevrouw Koekkoek van Volt, de heer Sjoerdsma van D66, de heer Van der Lee van GroenLinks en mevrouw Mulder van het CDA. Ik zou willen voorstellen om een spreektijd van zes minuten en in eerste instantie twee interrupties te hanteren. Mocht het nou heel veel drukker worden, dan gaan we even kijken wat verstandig is om te doen. Ik denk dat we dat wel redden.
Ik kondig alvast aan dat we wat langer dan gebruikelijk schorsen vanwege het lopen naar de ambtenarenkamer. Dat verzoek is van de ambtelijke ondersteuning gekomen. Dat willig ik van harte in.
De eerste spreker in de eerste termijn is de heer Brekelmans van de VVD. Gaat uw gang.

De heer **Brekelmans** (VVD):
Dank u, voorzitter. Cyberdreigingen raken direct de veiligheid van alle Nederlanders. Grootmachten als China en Rusland en schurkenstaten als Noord-Korea en Iran voeren dagelijks cyberaanvallen uit. Deze kunnen het dagelijks leven van gewone Nederlanders ontwrichten. We zagen een jaar geleden dat in de Verenigde Staten een olie- en gaspijplijn werd gehackt, waardoor miljoenen mensen niet meer konden tanken en letterlijk stil kwamen te staan. Zoiets kan ook vandaag of morgen in Nederland gebeuren. Daarom is het goed dat IOB een uitgebreide evaluatie heeft gedaan van ons cyberveiligheidsbeleid.
Maar ik begin toch met de actualiteit in Oekraïne, want Rusland heeft diverse cyberaanvallen op Oekraïne uitgevoerd. Het risico bestaat dat na alle sancties ook het Westen nog meer doelwit zal worden. Vorige week heeft de Minister van JenV aan mijn collega mevrouw Rajkowski een toezegging gedaan om met deze Minister te bespreken of ook hackers op de EU-sanctielijst kunnen worden gezet. Ik zou daar nog aan toe willen voegen: kunnen we ook sancties opleggen aan niet alleen individuen, maar ook Russische hackersgroepen? Is de Minister bereid om hiervoor te pleiten binnen de EU?
Daarnaast heeft het EU Cyber Rapid Response Team maanden geleden al hulp aangeboden aan Oekraïne, maar ze hebben nog steeds niet van dit aanbod gebruikgemaakt. Ik vind het persoonlijk onvoorstelbaar. Hoe kan het dat wij onze hulp aanbieden, maar die op de een of andere manier niet matcht met wat Oekraïne nodig heeft? Wat leren wij hiervan? Missen we relevante expertise? Moeten we eerder onze hulp aanbieden en betrokken zijn? Of zijn er andere belemmeringen die we in de toekomst weg moeten nemen? We zien dat Amerikanen wel volop actief zijn, bijvoorbeeld ook cyberexperts uit de private sector. Kortom, wat kunnen we hiervan leren?
Dan ga ik naar China, een meer structurele dreiging. Zij hebben nu verordend dat hackers alle zerodays, ofwel gaten in systemen, moeten

melden bij de Chinese staat. Dat betekent dat China een enorme capaciteit en basis opbouwt om onze systemen te kunnen platleggen. China als cybersuperpower: het vormt een enorme bedreiging voor onze veiligheid. Wat kunnen wij hiertegenover stellen? Ten eerste hardere cyberdiplomatie voeren. De EU Cyber Toolbox is hiervoor een belangrijk middel. Vindt de Minister ook dat China steviger aangesproken moet worden op zijn cyberagressie en dat hier ook meer gedreigd moet worden met specifieke sancties op deze acties? We moeten China duidelijk maken dat we de cyberagressie niet accepteren. Vindt de Minister ook dat hierop meer internationale coördinatie nodig is? Nu voert ieder Europees land vaak nog zijn eigen diplomatie op dit terrein richting China. Soms staat dat zelfs rechtstreeks haaks op elkaar, waardoor we minder krachtig kunnen optreden tegen China.
Ten tweede. Kunnen we nog meer onze krachten bundelen in deze strijd? Is de Minister bereid om bijvoorbeeld in te zetten op een brede interpretatie van collectieve verdediging met gelijkgezinde landen? Dat betekent dat als China één land in de NAVO of de EU aanvalt, we daar dan ook gezamenlijk tegen kunnen optreden, waardoor de drempel voor China om iets richting individuele landen te doen hoger wordt.
Ten derde. In deze doorlopende cyberoorlog moeten we onze diensten de ruimte geven om ook offensief te hacken om op deze manier een cyberaanval te voorkomen. Is het kabinet bereid om deze ruimte te geven? En is het nodig daarvoor een bredere definitie te hanteren van het principe «noodzaak», zoals dat ook in de kabinetsbrief wordt genoemd?
Ten vierde de internationale normen. De Minister beschrijft dat wij daarop enigszins in het defensief zitten, omdat landen zoals China en Rusland andere normen willen hanteren en deze actief internationaal naar voren brengen. Welke stappen kunnen wij zelf zetten om meer dominant te worden in het stellen van internationale normen? Kunnen we bijvoorbeeld aansporen dat het Boedapestverdrag op het gebied van cybercrime op VN-niveau de standaard wordt? Ziet de Minister mogelijkheden om in te zetten op een accountabilityprocedure voor staten die verantwoordelijk zijn voor cyberaanvallen?

De **voorzitter**:
Meneer Brekelmans, u heeft een interruptie van de heer Van der Lee, ik denk op het vorige punt.

De heer **Van der Lee** (GroenLinks):
Ja, het ging even over het offensief hacken of het als Nederland of met bondgenoten op een offensieve manier ontwikkelen van cyberactiviteiten. Ik ben benieuwd hoe de VVD dat precies definieert en ook in hoeverre de VVD vindt dat wij zouden moeten matchen wat sommige statelijke actoren op dit moment doen. China, Noord-Korea, Iran, Rusland; u heeft de voorbeelden zelf genoemd. Moeten wij op dezelfde manier activiteiten gaan ondernemen? Verstaat u dat onder «offensief»? Wat bedoelt u precies?

De **voorzitter**:
Dank voor de vraag. De heer Brekelmans.

De heer **Brekelmans** (VVD):
Ik bedoel dat het nodig kan zijn om zicht te krijgen op wat bijvoorbeeld een land zoals Rusland of China doet en dat je ook in hun systemen kijkt. Dat betekent dat je toch deurtjes open zult moeten zetten, wat gezien kan worden als offensief. Je wacht namelijk niet totdat een aanval heeft plaatsgevonden, maar je probeert die al op voorhand onschadelijk te maken. Dat is een dilemma. Aan de ene kant wil je natuurlijk niet zelf de agressor zijn, maar aan de andere kant wil je niet alleen maar vertrouwen op je eigen verdediging, maar wil je ook meer vooruitkijken. Vergelijk het

met het fysieke domein, waarin je bij wijze van spreken inlichtingenofficieren in die landen actief laat zijn om erachter te komen wat die landen doen. Die analogie kun je ook maken in het digitale domein. Ik zou daar persoonlijk wat meer ruimte voor willen geven, omdat die dreiging ontzettend groot is. Ik ben bereid om wat meer offensieve activiteiten toe te staan om dat soort aanvallen te voorkomen. Ik zeg niet dat we 100% moeten matchen met wat landen zoals Iran en Noord-Korea doen, want wij hebben andere normen wat dat betreft.

De **voorzitter**:
Dank u wel. Aanvullend, de heer Van der Lee.

De heer **Van der Lee** (GroenLinks):
Dank voor het antwoord van de heer Brekelmans. Ik begrijp dat hij met «offensief» vooral bedoelt op een proactieve manier bepaalde op Nederland of bondgenoten gerichte cyberactiviteiten van anderen proberen te voorkomen of tegen te gaan. Maar we zien dat die andere statelijke actoren een veel bredere agenda hebben en echt actief op een destructieve manier proberen samenlevingen te ontregelen. Dat is een veel bredere invulling van «offensief», maar dat is geloof ik niet wat de heer Brekelmans bedoelt.

De heer **Brekelmans** (VVD):
Het is wat moeilijk om hier in de openbaarheid over te spreken, omdat voor ons moeilijk is in te schatten hoe groot die dreiging daadwerkelijk is. Wij zien het risico dat landen zoals Rusland en China al vrij diep in onze vitale infrastructuur zouden zitten of, wat China nu doet rondom zerodays, kwetsbaarheden in onze systemen kennen waardoor zij ons elektriciteitsnet zouden kunnen platleggen, ziekenhuizen of wat dan ook. Als dat daadwerkelijk zo is, dan vind ik wel dat je daar een bepaalde afschrikking tegenover moet stellen. Misschien is die afschrikking wel dat wij – niet wij als Nederland, maar met onze bondgenoten, de Verenigde Staten en andere – tegen Rusland en China kunnen zeggen: als jullie een cyberaanval uitvoeren op onze vitale infrastructuur, dan kunnen wij hetzelfde doen bij jullie. Als je op dat punt moet komen, dan wil je nog wel iets meer toestaan wat dat betreft. Je wil niet alleen een aanval voorkomen, maar ook afschrikking daartegenover kunnen stellen. Ook voor dat tweede zou ik de ruimte willen geven. Als wij zien dat die dreiging dermate groot is dat onze verdediging niet genoeg is maar ook afschrikking nodig is, dan vind ik dat we dat in dat opzicht wel moeten matchen.

De **voorzitter**:
Dank u wel. U mag vervolgen. U heeft nog twee minuten.

De heer **Brekelmans** (VVD):
Ten vijfde. We moeten maximaal inzetten op het inventariseren van onze eigen kwetsbaarheden en het verder opbouwen van onze kennis en capaciteiten. Dat kunnen we onder andere doen door grootschalige cyberaanvallen te simuleren en daarmee oefeningen te doen, waarbij het belangrijk is dat Buitenlandse Zaken daarop aangesloten is. Mijn vraag aan de Minister is: is het mogelijk om het aantal simulaties en oefeningen te intensiveren?
Tot slot het IOB-rapport. Zoals ik al aangaf in mijn introductie is de dreiging groot. Ik heb in mijn vragen al diverse elementen genoemd die in het rapport naar voren komen. Ik wil eindigen met de conclusie die in het rapport getrokken wordt, namelijk dat er geen overkoepelende strategie is, dat er onvoldoende gezamenlijke prioriteiten zijn, dat de centrale aansturing verbeterd moet worden, dat er soms langs elkaar heen gewerkt en dus onvoldoende samengewerkt wordt en dat er meer kennis

en capaciteit opgebouwd moet worden. Om heel eerlijk te zijn: toen ik de dreiging, de omvang daarvan en de potentiële impact naast deze conclusies legde, schrok ik daar best wel van. Mijn vraag aan de Minister is dan ook of hij ook schrok van deze conclusie. Geldt voor hem ook dat hier onmiddellijk actie op moet worden ondernomen? Ik snap dat het niet van de ene op de andere dag kan, maar mijn vraag is wat de Minister in deze kabinetsperiode gaat doen om ervoor te zorgen dat als we over een aantal jaren dit beleid weer gaan evalueren, daar een andere conclusie uit rolt.

De **voorzitter**:
Dank u wel. Ik zie dat niet iedereen van deze aanwezigen bij de pv is geweest. Daarom wil ik graag extra aandacht voor de derde brief op de agenda: de stand van zaken op het gebied van cybersecurity in relatie tot Oekraïne. We hebben daarover in de pv afgesproken dat we hier alleen het internationale gedeelte bespreken, dus niet het nationale aspect van die brief. Dan weet u dat, als u dat in uw bijdrage had verwerkt. Mevrouw Koekkoek van Volt, u bent aan de beurt. Gaat uw gang.

Mevrouw **Koekkoek** (Volt):
Dank u wel. Waar de heer Brekelmans eindigde met het IOB-rapport, wil ik daarmee beginnen. Aan de ene kant ben ik heel blij dat ook de Minister van Buitenlandse Zaken het belang van cyberveiligheid onderkent en dat er een heel aantal aanbevelingen in het IOB-rapport staan waarvan ook Buitenlandse Zaken goed gebruik kan maken. Daarbij valt mij met name op dat de coördinerende Minister van Justitie en Veiligheid een visie heeft, een rijksbrede aanpak van cybersecurity, en daarin heel veel bewindspersonen en departementen noemt. Maar daar zag ik het Ministerie van Buitenlandse Zaken niet tussen staan en ook Digitale Zaken niet. Met name in de laatste commissie zijn er een aantal mooie Europese voorstellen en daar heb ik een aantal vragen over. Welke punten met betrekking tot cyberdiplomatie, internationale cyberdreiging en grensoverschrijdende samenwerking ziet de Minister graag terug in de Nederlandse cybersecuritystrategie, afgekort NLCS? Wordt het Nederlandse internationale cybersecuritybeleid onderdeel van de NLCS? Zo niet, hoe wordt dan afstemming gezocht tussen de verschillende departementen? Zijn er bijvoorbeeld periodieke overleggen? Hoe wordt dat dan vervolgens weer teruggekoppeld naar de Kamer? Hoe ziet de Minister zijn rol in de brede cybersecuritysamenwerking? Wat gaat de Minister doen om de verkokering van het Nederlandse cybersecuritybeleid tegen te gaan?
Dan de nieuwe strategie. Je moet een handelingskader bieden voor asymmetrische cyberaanvallen. Uit de ISIDOOR-oefening blijkt dat het voor veel besluiten van belang is of we aangevallen worden door een statelijke actor of door iemand anders, dus een niet-statelijke actor, maar in de praktijk is helaas niet altijd te achterhalen met wie van de twee we te maken hebben, wie er precies achter een aanval zit. Ik heb een vraag met, denk ik, een uitgebreid antwoord. Hoe wordt deze kwetsbaarheid, dus het niet weten of je met een statelijke of niet-statelijke actor te maken hebt, in de strategie ondervangen?
Sinds 2019 probeert Rusland via de VN een wereldwijd verdrag tot stand te brengen dat geopolitiek tot doel lijkt te hebben om het cybercrimeverdrag van de Raad van Europa te pareren. Rusland wil dit proces versnellen, want de beslissingsruimte van belanghebbenden wordt daarmee onder druk gezet. Hier ligt in mijn optiek een kans voor Europa. In het huidige conflict begint een tweedeling in de wereld zichtbaar te worden, die de internationale cyberveiligheid niet ten goede komt. Om ervoor te zorgen dat swing states, staten die nog twijfelen, niet met Rusland meegaan, moeten we daarom goed naar hun zorgen luisteren en deze swing states meenemen in onze voorstellen. Ik heb daar een aantal vragen over. Is de Minister bereid om deze swing states te consulteren en

hun zorgen en wensen mee te nemen in de voorstellen voor een nieuw internationaal cyberverdrag in plaats van hen te dwingen een keuze te maken tussen de Boedapestconventie en het Russische voorstel? Mijn tweede vraag hierover is hoe de Minister meer zal draagvlak creëren voor de Nederlandse ideeën over internationale cyberveiligheid. Ik was met name nog benieuwd naar hoe, kort samengevat, de mensenrechten daarin een rol spelen, juist omdat swing states... We weten dat daar internationaal gezien weleens anders naar wordt gekeken. Hoe gaan we dan de afweging maken? En welke grenzen en ook kansen zien we daarin?
Ik had ook een vraag over de Joint Cyber Unit, met name over hoe deze unit gaat opereren. Het zijn nu nog de afzonderlijke lidstaten die het mandaat verlenen. Ik wil niet direct zeggen dat we naar een supranationaal mandaat willen, maar ik vraag wel wat de mogelijkheden zijn om snel samen te kunnen werken. Ook hier vraag ik waarin de kansen en de kwetsbaarheden liggen om zo'n Europese Joint Cyber Unit snel te kunnen aansturen, want in de wereld van cyber gaan dingen vaak heel snel.
Tot slot. Volgens Volt is het voor een structurele versteviging van onze cybersecurity, zeker in de internationale context, van belang dat we investeren in kennis en expertise op het gebied van internationale cybersecurity, zodat we structurele en strategische kennis genereren. Het kost tijd om mensen op te leiden en om kennis te vergaren en te delen. Dat kun je dus niet ad hoc oplossen. We zouden dit graag terugzien als extra onderdeel in de gehele strategie. Daarom vraag ik de Minister hoe hij staat tegenover het deels financieren van een cyberleerstoel bij elke universiteit. En hoe staat de Minister tegenover meer langlopende subsidies, dus niet meer op projectbasis, voor organisaties zoals onafhankelijke denktanks?
Helemaal tot slot zou ik me graag willen aansluiten bij de vragen die zijn gesteld door de heer Brekelmans over Oekraïne.

De **voorzitter**:
Dank u wel. De heer Sjoerdsma van D66, u bent aan het woord.

De heer **Sjoerdsma** (D66):
Dank, voorzitter. Voorgaande sprekers hebben al het enorme belang van cyberveiligheid benadrukt. Ik wil daar op drie thema's aan raken: Oekraïne, de Europese samenwerking en het IOB-rapport.
Ik begin met Oekraïne. We hebben allemaal gezien wat Rusland daar heeft geprobeerd. Op een website – ik ben even kwijt welke – is een zeer inzichtelijke tijdlijn bijgehouden van wat Rusland allemaal in Oekraïne heeft geprobeerd aan digitale aanvallen. We hebben ook gezien dat dat ook Nederland raakt, of het nou collateral damage was of bedoeld. Ik noem het effect van een aanval op de havens Hamburg, Antwerpen en Rotterdam, waar negatieve consequenties waren voor olieterminals. Met andere woorden, die digitale aanvallen kunnen heel gericht zijn. Ze kunnen ook grote spillovereffecten hebben. Dat maakt weerbaarheid daartegen van enorm belang. Allereerst over de aanval in Rotterdam. Hebben we kunnen vaststellen dat die inderdaad vanuit Rusland was en hebben wij daar vervolgens diplomatiek en juridisch iets tegen gedaan? Ik zeg het nu meer in algemene zin omdat we er nog over komen te spreken, maar het leek me belangrijk om daarbij stil te staan.
Mijn tweede punt met betrekking tot Oekraïne sluit aan bij de vragen van collega Brekelmans. Het gaat over het Europese defensieteam waar zes of zeven lidstaten aan deelnemen. Dat is wel geactiveerd, maar nog niet ingezet. Is dat inmiddels veranderd? De laatste informatie die ik ken, was van 11 maart. Is er inmiddels iets gebeurd en is dat team aan de slag, ook omdat de aanvallen op Oekraïne overduidelijk doorgaan de afgelopen tijd?
Misschien in wat algemenere zin en ook Europees: voor het geval dat er aanvallen plaatsvinden, zijn er nu ook in VN-verband een aantal normen

vastgesteld. Norm 13c houdt in dat staten hun grondgebied niet bewust mogen gebruiken voor internationale onrechtmatige daden waarbij ook ICT-communicatietechnologie gebruikt kan worden. Norm 13f zegt: staten moeten geen ICT-activiteiten uitvoeren die kritieke infrastructuur van andere staten intentioneel beschadigen. Iets verder in de brief gaat het ook over de diplomatieke en juridische acties die Nederland kan ondernemen. Ik ben benieuwd naar hoe vaak we al gebruik hebben gemaakt van die normen. Hoe vaak hebben we landen al aangesproken? Hoe vaak hebben we al geprobeerd die normen ook in de echte wereld te laten gelden? Ik heb niet de illusie dat het meteen heel veel effect zal hebben, maar ik denk wel dat het heel belangrijk is dat we dat consequent blijven doen als wij zelf op de hoogte zijn van aanvallen en van misstanden vanuit bepaalde landen.
Dan de Europese samenwerking. Vorige week was er in de commissie Digitale Zaken ook een debat, meer over de nationale kant. Mijn collega Lisa van Ginneken heeft daar het een en ander gezegd over de nationale versnippering. We zullen het er hier nu niet over hebben, maar ik moet eerlijk zeggen dat ik ook enige zorgen heb over de Europese versnippering. Laat ik een paar dingetjes noemen. Sommige zijn hartstikke goed: Cyber Diplomacy Toolbox, Cyber Defence Policy, Cyber Resilience Act. Heel goed. Vervolgens heb je een Joint Cyber Unit, EU PESCO Cyber Rapid Response Team, European Cybersecurity Competence Centre en nog een paar afkortingen, die ik hier omwille van de tijd niet allemaal zal herhalen. Iets zegt mij, en volgens mij zegt de IOB dat ook: werk nou niet langs elkaar heen, zorg er nou voor dat het elkaar versterkt. Mijn vraag aan deze Minister is hoe deze cyberdiensten zich tot elkaar verhouden. Wat mogen we van hen verlangen?
Tot slot. De IOB zegt dat er departementoverstijgende aansturing nodig is voor het vaststellen van mandaten en taken omtrent cyberveiligheid en nieuwe strategie. Daarbinnen moet er dan een nieuwe strategie vanuit Buitenlandse Zaken komen. Ik vraag de Minister hoe hij dit gaat vormgeven met zijn collega's, hoe hij ervoor zorgt dat het geen lappendeken van verschillende strategieën wordt, maar een eenduidig document namens het hele kabinet en wanneer we dat mogen verwachten.
Voorzitter. Daar wilde ik het bij laten.

De **voorzitter**:
Dank u wel. U hebt geen interrupties. We gaan naar de heer Van der Lee voor zijn eerste termijn. Gaat uw gang.

De heer **Van der Lee** (GroenLinks):
Dank u wel, voorzitter. Ik sluit me graag aan bij de vele terechte vragen die de collega's al hebben gesteld. Ik zal proberen daar nog wat nieuwe vragen aan toe te voegen. Dat is geen uitdaging, want die heb ik genoeg. Ik begin bij Oekraïne. Ik ben benieuwd, zonder heel specifiek te worden, of de Minister iets kan vertellen over de rol die cyberaanvallen vanuit Rusland in deze oorlog hebben gespeeld en over de kwaliteit en de coördinatie daarvan, vergeleken met wat er militair op de grond is gebeurd. De analisten zijn daar natuurlijk volop mee bezig. Die coördinatie liet te wensen over, lijkt het, als het gaat om de fysieke oorlog on the ground, maar hoe zat het met de digitale kwaliteit in Oekraïne? En in hoeverre strekte dat zich ook uit naar andere landen die Oekraïne hebben gesteund? Ik vraag dat, omdat ik ook wel benieuwd ben in hoeverre de NAVO al vooruitkijkt naar hoe je heel grootschalige cyberaanvallen in de toekomst moet duiden. Kun je op een gegeven moment als land artikel 5 inroepen omdat er een dermate grote cyberaanval op jouw land wordt uitgevoerd dat bijna alle vitale infrastructuur wordt platgelegd en er heel veel onrust, schade, dodelijke ongelukken en wat dan ook plaatsvinden? Kan dan artikel 5 in werking treden? Hoe wordt daarnaar gekeken? Is er al een ladder in de ernst van cyberaanvallen ontwikkeld? Hoe staat het met

het denken daarover binnen de NAVO en misschien ook wel binnen de EU? Maar het lijkt me toch prioritair aan de NAVO om daarover te denken. Ik weet daar eerlijk gezegd heel weinig van en volgens mij de Kamer ook. Het wordt met het jaar relevanter om daar goed over na te denken. Daaraan gekoppeld zie je een zorgpunt dat niet nieuw is. Ik kan ook refereren aan het WRR-rapport, volgens mij uit 2019. Als het gaat om de voorbereiding op een grootschalige digitale ontwrichting, heeft Nederland nog heel veel te doen. Is dat sinds 2019 structureel verbeterd? Ik kan me uit de vorige kabinetsperiode herinneren dat toen ik woordvoerder EZK was, we heel veel debatten hebben gehad over het gebrek aan coördinatie op het digitale domein. Er is inmiddels een Kamercommissie ingesteld, maar wij hebben destijds al gepleit voor een ministeriële onderraad op het terrein van digitalisering en een Minister voor Digitale Zaken om die coördinatie veel sterker te maken. Dat is in de praktijk maar beperkt ingevuld, zo is onze waarneming. Maar misschien kan de Minister aangeven dat het nu juist fantastisch is georganiseerd, dat de coördinatie perfect is, dat we ons heel goed voorbereid hebben op de risico's die we vanuit het buitenland op ons af zien komen en dat we ons er al heel goed tegen gewapend hebben. Ik heb die indruk nog niet, maar misschien kan de Minister ons daarvan overtuigen.
De IOB-evaluatie is daar echt heel kritisch over. Die ziet ook geen overstijgende cyberstrategie. Gaat die er komen? Wanneer dan? En wie is daar de eerstverantwoordelijke voor? Wat is precies de afbakening in verantwoordelijkheden tussen de Minister van Buitenlandse Zaken en andere bewindslieden, bijvoorbeeld op het terrein van de kwantumtechnologie? Ook daar gaat de IOB-evaluatie over. Die zegt: om te zorgen dat je je in de toekomst veilig kunt wanen, is het belangrijk dat je een van de koplopers bent op het terrein van de kwantumtechnologie. Investeren we daar genoeg in? Zorgen we er ook uit het oogpunt van veiligheid voor dat het op orde is? Dat is uiteindelijk misschien meer een taak van de Minister van EZK, maar in hoeverre is het Ministerie van Buitenlandse Zaken betrokken bij het ontwikkelen van een integrale strategie om dat soort kwetsbaarheden in de toekomst te voorkomen?
Dat raakt ook wel aan andere discussies. Dat speelt misschien... Je kunt zeggen dat dat een binnenlands issue is, maar dat is het niet. Ik kijk bijvoorbeeld naar technologie die door Israël is ontwikkeld. Pegasus is een digitale tool waarmee je heel erg veel data naar je toe kunt trekken. Er is een Wob-procedure ingesteld om te achterhalen of de Nederlandse politie al dan niet Pegasus heeft ingekocht. Is het aanschaffen van digitale cybertools waar mondiaal al de nodige discussie over is nou een kwestie waar Buitenlandse Zaken helemaal niks mee te maken heeft? Gaat dat helemaal langs Buitenlandse Zaken heen? Of is dat ook een terrein waar op een integrale manier naar wordt gekeken? Welke tools vinden we wel of niet passen bij onze waarden en normen? En leggen we onszelf als overheid bij bepaalde overheidsdiensten ook grenzen op als we bepaalde tools gebruiken waarvan we eigenlijk vinden dat die überhaupt niet toegelaten zouden moeten worden? Ik hoor graag hoe de Minister zijn rol ziet als het gaat om dit soort zaken.
Encryptie is ook een belangrijk onderdeel. In het verleden heeft het kabinet aangegeven dat het geen maatregelen zal nemen om encryptie te verzwakken. Tegelijkertijd zitten daar ook weer allerlei veiligheidsrisico's aan vast. Dat betekent dat mensen die met encryptie werken daar allerlei oneigenlijke of gevaarlijke dingen mee doen. Hoe staat het kabinet op dit moment in die hele encryptiediscussie? Is het standpunt nog steeds dat Nederland geen maatregelen zal nemen om encryptie te verzwakken? Of is dat alweer ... Sorry?

De **voorzitter**:
Graag via de microfoon, heren.

De heer **Van der Lee** (GroenLinks):
De heer Sjoerdsma hoopt van wel, zegt hij. Ik ben benieuwd wat de actuele positie is, want die kunnen wij op dit moment niet herleiden uit de stukken die we kennen.
Tot slot nog één vraag over het privacy shield framework. Von der Leyen en Biden hebben een akkoord bereikt over het doorsturen van informatie vanuit Europa naar de VS. Daar is in het verleden veel om te doen geweest. Zijn de waarborgen op dit moment echt adequaat? Is het verantwoord dat deze afspraak wordt uitgevoerd? Of zitten hier toch nog strijdigheden in met vigerende Europese privacyregels? Kan de Minister aangeven op welke manier hij erop toe zal zien dat de privacy van Europese burgers in dit opzicht gewaarborgd blijft?
Dat was 'm.

De **voorzitter**:
Dank u wel voor uw bijdrage. Mevrouw Mulder van het CDA, de laatste in de eerste termijn. Gaat uw gang.

Mevrouw **Agnes Mulder** (CDA):
Voorzitter, dank. Laat ik beginnen met het amendement over cyber dat ik met een heel aantal collega's heb ingediend bij de begroting. Dank voor de brief met de update over de amendementen. Daar staat in dat de nadere uitwerking van een nieuwe internationale cyberstrategie rond de zomer wordt afgerond, en dat we daarna zo spoedig mogelijk worden geïnformeerd. Maar is daar nu al wat meer over te zeggen?
Samen met collega Brekelmans had ik ook een motie ingediend. Daarover staat ook een brief op de agenda. Een van de zaken die daar in het internationaal kader uit naar voren komt, is dat alle VN-lidstaten in 2001, waaronder Nederland, hebben bevestigd dat internationaal recht van toepassing is in het cyberdomein. Collega Sjoerdsma ging eigenlijk ook al in op de vraag wat dat betekent en wat we daar dan mee doen. Er is ondertussen een oorlog aan de gang in Oekraïne. Wat heeft die dan voor extra effecten? We hebben natuurlijk al allemaal sancties richting Belarus en Rusland opgetuigd, maar zijn er op basis van wat er misschien al gebeurd is ook stappen genomen richting andere landen die ons mogelijk hebben aangevallen? En als dat niet zo is omdat het private partijen zijn, wat doen we daar dan tegen? Ook onze «eigen private partijen», de anonymous hackers, kiezen nu toevallig de kant van Oekraïne, maar dat kan ook net zo goed anders zijn. Wij spreken Rusland aan op het gedrag van hun private partijen, maar dan moeten we natuurlijk niet dezelfde fout maken. Wij opereren hier vanuit bepaalde waarden: veiligheid, stabiliteit en de rechtsorde. Hoe verdedigen we die dan internationaal? Ik vind ons als Nederlandse samenleving nog niet iedere dag even weerbaar. Ik weet dat ik hier niet op de Nederlandse tak mag ingaan, maar die is wel relevant voor hoe wij met onze democratie omgaan en hoe we die verdedigen naar buiten toe. Daarom wil ik het even kort aanstippen. Ik ben benieuwd hoe de Minister daar nou mee omgaat.
Kijk naar de effecten in Oekraïne, waarover natuurlijk meerdere artikelen zijn verschenen. Het wil niet zeggen dat het allemaal waar is wat daar staat – ik moet het ook uit die openbare bronnen halen – maar op de dag van de invasie, toen de raketten op de luchthavens vielen, tanks de grens overstaken en paramilitairen onderweg waren naar Kiev, viel de verbinding van duizenden modems van de Oekraïense overheid weg. Als gevolg van deze hack hebben ze aan het begin van de oorlog toch een enorm communicatieverlies geleden. Tegelijkertijd werden op diezelfde dag Oekraïense burgers en bedrijven getroffen door een internetstoring. Als er geen destructieve malware was ontdekt aan het spoorsysteem, hadden al die mensen niet eens kunnen vluchten. Daar hebben we het over in de praktijk. Dit is wat er gebeurt met cyberwarfare. Dat krijgt direct een gezicht. Dan heeft het ook nog relatief goed uitgepakt. Dan vraag ik

mij wel het volgende af. Als we nog nooit eerder hebben gezien dat een digitale invasie van een land plaatsvindt samen met een daadwerkelijke invasie met tanks die de grens overgaan, hoe is dan het zicht van de NAVO op Rusland wat betreft cyber? Hoe worden die lessons learned geïmplementeerd in het nationale beleid hier, maar ook in het internationale beleid dat we met elkaar voeren? Daar sluit de vraag van de heer Van der Lee van GroenLinks eigenlijk ook op aan. Ik vond dat hij daar een hele terechte opmerking over maakte.
Wat betreft de IOB-aanbevelingen sluit ik mij gemakshalve maar even aan bij de vragen van de voorgangers, met name die van de heer Sjoerdsma op dit punt, maar ook die van mevrouw Koekkoek en anderen.
Dan laat ik het hierbij. Wij hebben iets te verdedigen hier. Rusland is bang voor democratie. Laten we met elkaar ook hier weerbaar zijn. Laten wij onze democratie verdedigen, iedere dag, met hand en tand, op een positieve manier. Laten we zorgen voor onze inwoners. Die moeten niet te veel last hebben van dit soort regimes, die dat op een heel foute manier aanpakken.
Misschien helemaal tot slot, voorzitter. We hadden net een gesprek over een soort digitale warfare tegen inwoners van landen die risico's lopen omdat ze christen, moslim of wat dan ook zijn. Ook dat element van die mensenrechten gaat hier gewoon dwars doorheen. Ik maak mij daar grote zorgen over. Zijn wij als Westen genoeg geprepareerd om onze waarden goed te verdedigen?
Dank u wel, voorzitter.

De **voorzitter**:
Dank voor uw inbreng in eerste termijn. Ik zie geen verdere interrupties. Dan kijk ik naar de Minister, om te zien welke schorsingsduur hij wenst te hebben. De Minister stelt voor om om 15.45 uur verder te gaan. Dat betekent dat wij twaalf minuten schorsen. Dan gaan wij om 15.45 uur verder.

De vergadering wordt van 15.35 uur tot 15.57 uur geschorst.

De **voorzitter**:
De Minister is terug en heeft zich kunnen voorbereiden op de eerste termijn namens het kabinet. Ik geef hem graag het woord voor de beantwoording in eerste termijn.

Minister **Hoekstra**:
Voorzitter, dank. Dat waren een lange tien minuten. Ik moet eerlijk zeggen dat ik het grootste gedeelte van die ruime periode heb besteed aan rondwandelen en wachten. Dat had een beetje met de logistiek te maken, waarvoor excuus in de richting van de leden van uw Kamer. Ik ga vanzelfsprekend de vele zeer terechte vragen en opmerkingen van een antwoord proberen te voorzien. Ik wilde beginnen met het zeggen van een aantal algemene dingen in de richting van de leden van uw Kamer. Dan wil ik specifiek ingaan op vragen die vanzelfsprekend over Oekraïne en de actualiteit gaan. Daarna ga ik het nog hebben over de EU en statelijke actoren. En vervolgens over de vragen van onder anderen de heer Van der Lee over de cyberstrategie en hoe je daar naar de toekomst toe naar moet kijken. Een deel van de onderwerpen loopt nadrukkelijk in elkaar over, dus ik zou in goed Nederlands bijna willen zeggen: bear with me.

De **voorzitter**:
U heeft één blok.

Minister **Hoekstra**:
Ik heb één blok, absoluut.

Voorzitter. Ik wil nog eens beginnen met datgene te benadrukken wat ook doorklonk bij de heer Brekelmans, de heer Sjoerdsma en anderen: dit is een nieuw oorlogsterrein dat niet meer weggaat en waarvan het belang en de importantie alleen maar gaan toenemen. Zeker omdat het in veel opzichten terra incognita is, zie je dat statelijke actoren en ook niet-statelijke actoren gewoon aan het kijken zijn hoever ze daarin kunnen gaan. Zij vinden over het algemeen dat ze daar behoorlijk ver in kunnen gaan. De mate van uitdagen en geopolitiek belletje trekken die we hebben waargenomen, vind ik eerlijk gezegd enorm. Je ziet ook hoe relatief makkelijk statelijke actoren, maar ook niet-statelijke actoren of degenen die zich in een tussenwereld bevinden, zich daar schuldig aan maken. Vervolgens zie je hoe lastig het is om die van attributie te voorzien. Dat is een enorm probleem, waarvoor we nog heel veel werk hebben te verrichten. Om het te relateren aan mijn eigen portefeuille: cyberdiplomatie is daarmee absoluut een prioriteit, zoals ik eerder aan de Kamer heb geschreven. Dit is een domein dat gaat over de eenentwintigste eeuw en dat is voorzien van kansen en mogelijkheden, ook als het gaat over economische groei en interactie tussen mensen uit alle hoeken en gaten van de planeet, maar dus wel met heel veel dreiging richting onze eigen mensen, onze burgers, richting onze bedrijven maar ook richting onze overheid. Het is belangrijk om dat nog eens te benadrukken.
Ik zou ook nog eens willen benadrukken, ook omdat de heer Van der Lee daar terecht naar vroeg, dat cyber alle grenzen en domeinen overstijgt. Een hele reeks van bewindspersonen is hier terecht bij betrokken. We gaan overigens komen met een geïntegreerde cyberstrategie, waarin we niet alleen nog eens zullen articuleren hoe er binnenlands wordt samengewerkt, maar waarin we dat heel bewust ook verbinden met het buitenland, zodat er straks niet een binnenlandse en een buitenlandse strategie zijn maar dat die zijn geïntegreerd. Vanzelfsprekend neemt BZ de lead daar waar het gaat om het entameren en coördineren van overleg over het internationale normatieve kader, zoals dat zo mooi heet. Wat mogen landen überhaupt doen op het gebied van cyber? Wat mogen ze niet? Wat moeten ze beslist nalaten? Hoe pak je kwaadwillend gedrag aan? Daarmee zullen we naar de Kamer komen. Een van de vragen van de heer Van der Lee was wanneer dat gaat gebeuren. Mijn inschatting is dat dat kort na de zomer zal zijn.
Overigens wordt er wel degelijk al zeer intensief samengewerkt. In de pauze hadden we het er al even over dat er dagelijks contact is tussen de diverse departementen en ook tussen mijn departement en bijvoorbeeld de NCTV, omdat we hier ook dagelijks mee te maken hebben. De Minister van JenV is vervolgens de coördinerend Minister voor cybersecurity en is natuurlijk ook verantwoordelijk voor het aanpakken van cybercrime, zoals al in het woord besloten ligt. Verder zijn BZK, EZK, Defensie en de diensten natuurlijk allemaal met hun eigen stukje bezig. Ik hoor de heer Van der Lee al bijna vragen of dat dan tot verkokering leidt. Je ziet natuurlijk dat dit een probleem en ook een mogelijkheid is die alle aspecten van onze samenleving raakt. Juist daarom zijn alle departementen er heel nauw bij betrokken. Ja, er ligt dan vanzelfsprekend ook altijd een coördinatievraagstuk. Tegelijkertijd vind ik het logisch dat je niet alleen maar één departement voor cyberaangelegenheden zou hebben, want dat zou vervolgens naar elk van de departementen terug moeten met een uitvraag en zou dan met Defensie, Justitie en Buitenlandse Zaken in gesprek moeten. Ik denk dus wel dat het moet kunnen, met een hele stevige rol voor het buitenland voor ons, een stevige rol voor JenV en een stevige rol voor BZK en ook voor OCW en EZK. Nogmaals, het kabinet komt met de geïntegreerde strategie. Dan zal de Kamer daar ongetwijfeld ook het een en ander van vinden.

De **voorzitter**:
Daar heeft de heer Van der Lee een vraag over.

De heer **Van der Lee** (GroenLinks):
Ik begrijp natuurlijk dat er interdepartementaal veel contact is en dat er wordt samengewerkt. Mijn vraag betreft de besluitvorming in het kabinet. Is dit dermate overstijgend dat de besluitvorming in de gehele ministerraad plaatsvindt of is het toch een onderraad waar de meest betrokken bewindslieden samen nadenken over de strategie, op basis van ambtelijke voorbereiding, en de besluitvorming in de ministerraad voorbereiden? Zit daar wel of niet nog een stap tussen?

Minister **Hoekstra**:
Waar nodig zit daar zeker ook een stap tussen. Waar het raakt aan de veiligheid, is de RVI daar natuurlijk het meest geëigende gremium voor. Daar wordt alles overigens ook ambtelijk voorbereid. Ik kan natuurlijk niet over de details praten, maar ik weet uit eigen ervaring bijvoorbeeld dat daar door de diensten ook wordt gerapporteerd over wat men waarneemt. Soms gaat dat over algemene dreigingsbeelden, soms is het specifieke casuïstiek. Dat gebeurt dus absoluut. Uit mijn vorige hoedanigheid weet ik dat er ook altijd contact is en er ook gecoördineerd wordt wanneer zaken niet strikt aan de veiligheid raken, maar bijvoorbeeld aan wat bedrijven of banken overkomt. Tegelijkertijd gaat dit thema niet meer weg en zal het alleen maar groter worden. Ik ben het eens met veel wat daarover is gezegd in de Kamer, ook door de heer Brekelmans en de heer Sjoerdsma. Mijn voorspelling is echt de volgende. Professionele oorlog zal niet verdwijnen, maar reken maar dat deze doos van Pandora nog veel verder opengaat in de jaren die komen gaan. Het goede nieuws is dan – zie ook wat de IOB daarover zegt – dat Nederland echt aan de voorkant zit van activiteit, van assertiviteit, van ingrijpen en ook proberen om anderen daarmee te helpen. Een deel van onze diensten staat ook bekend om de expertise die ze hebben. Maar reken jezelf niet rijk: van alle kanten kijkt men richting het Westen en zeker ook richting Nederland om te zien welke gaten er in de dijk zitten.
Voorzitter. Ik heb de heer Van der Lee gebruikt om meteen een aantal andere vragen te beantwoorden. Dat vindt hij – zo ken ik hem – niet erg. Ik zou een aantal dingen willen zeggen over Oekraïne. Zeer begrijpelijk was dat top of mind bij een aantal leden van uw Kamer. Het is een bijna natuurlijke haak om veel van deze discussies te voeren. Laat ik beginnen met iets wat ik als een veel positievere ontwikkeling beschouw dan ik wellicht had verwacht. Er waren best een aantal experts die ervan uitgingen dat in de allereerste fase van de oorlog Oekraïne direct het onderspit zou delven op het gebied van cyber. Ik heb mensen gesproken, ook nog op de Münchner Sicherheitskonferenz toen we echt aan de vooravond van de oorlog bleken te staan, die ervan uitgingen dat alle informatie meteen gecompromitteerd zou zijn. Ik ben daar samen met collega's ook actief voor gewaarschuwd: de communicatie is vermoedelijk gecompromitteerd. Alle informatievoorziening zou worden overgenomen en zou bijna worden vervangen door desinformatie. Oekraïne zelf zou niet meer in staat zijn om te communiceren met ons, maar ook met de eigen burgers. Eigenlijk zie je, toch een beetje spiegelbeeldig aan wat we op het echte slagveld hebben gezien, dat Oekraïne zich daar veel beter tegen teweer heeft weten te stellen dan in ieder geval mijn verwachting was. Mijn verwachting was gebaseerd op wat ik van experts had gehoord in de dagen en weken daarvoor.
De volgende vraag is natuurlijk: waar komt dat dan door? Dat was ook een vraag van mevrouw Koekkoek en van anderen. Wat zien we nou en waar komt dat door? Het is bijna de klassieke vraag: komt dat nou doordat Oekraïne het zo goed heeft gedaan of doordat Rusland het zo slecht heeft gedaan? Over dat eerste moet je in ieder geval constateren dat Oekraïne sinds 2014 ook op dit gebied een heleboel heeft bijgeleerd. De heer Sjoerdsma vroeg waarom er geen gebruik is gemaakt van de expertise die wij hebben. Voor een deel is dat – ik kan dat ook publiekelijk zeggen –

omdat men in Oekraïne veel gebruik heeft gemaakt van Amerikaanse cyberexpertise. Voor een deel komt het ook doordat hun eigen capabilities toch opgewassen bleken en blijken te zijn tegen de aanvallen van Rusland. Wij zijn echt niet te zuinig geweest met het in de aanbieding doen van cyberhulp die wij zouden kunnen bieden. Wij zijn een land dat, ik denk terecht, bekendstaat om de kwaliteit die we op dit terrein kunnen leveren. Het is dus niet zo dat men heeft gedacht «thanks, but no thanks» over de kwaliteit die Nederland kan leveren. Anders dan bijvoorbeeld bij onze wapens en anders dan bij de expertise die we inbrengen en de voortrekkende rol die we spelen op het gebied van sancties, heeft men, tegen mijn verwachting van zes, zeven weken geleden in, gezegd: «Veel dank voor het aanbod, maar het is nog niet nodig. We kunnen het af met wat we zelf hebben en met wat we krijgen van de Amerikanen.» Dat is overigens geen statisch gegeven. Het is niet gezegd dat dat zo blijft in dit specifieke conflict, om maar helemaal niet te spreken van conflicten die nog gaan komen.

De **voorzitter**:
Heeft u het onderdeel met betrekking tot Oekraïne afgerond of komen er nog een aantal andere onderdelen?

Minister **Hoekstra**:
Er komt nog meer, maar ik luister graag naar de vragen.

De **voorzitter**:
Dan geef ik gewoon het woord aan de heer Brekelmans om een vraag te stellen.

De heer **Brekelmans** (VVD):
We kunnen natuurlijk zeggen: we lopen voorop. In zekere mate is dat ook zo, maar het is toch opvallend dat nu duidelijk is dat de Amerikanen degenen zijn die de hulp aan Oekraïne bieden. Naar mijn observatie als buitenstaander heeft dat met twee dingen te maken. Ten eerste zijn de Amerikanen al veel langer betrokken, dus zij kennen de systemen van Oekraïne en de Russische systemen beter. Op het moment dat de aanval plaatsvindt of dreigt plaats te vinden, is het al te laat. Ten tweede is ook de private sector erbij betrokken, dus niet alleen de Amerikaanse inlichtingendiensten maar ook een team van Microsoft, waar vaak nog veel meer kennis zit dan bij de overheid. Zijn dat ook twee lessen die de Minister hieruit trekt? Dat betekent ook dat als wij zien dat in de toekomst een specifiek land een doelwit zou kunnen zijn, wij daar eerder bij betrokken moeten zijn en ook moeten kijken of wij als overheid alles kunnen leveren of dat de private sector erbij moet worden betrokken.

De **voorzitter**:
De Minister. Straks heeft de heer Van der Lee ook nog een vraag.

Minister **Hoekstra**:
Ik denk dat dat twee zeer terechte punten zijn. Ja, de Amerikanen waren al heel vroeg betrokken en dat helpt zeker. Ik ben het ook eens met het punt dat je sowieso moet kijken hoe je dit veel meer kunt zwaluwstaarten, ook met de belangen in het bedrijfsleven. In andere commissiedebatten hebben we het gehad over de gedachte van de nationale veiligheidsraad, waar je probeert de meer geopolitieke belangen, de veiligheidsbelangen en de economische belangen gezamenlijk te wegen, juist met de departementen – EZK voorop – die een duidelijke link hebben met het bedrijfsleven. Ik vind allebei de gedachten dus zeer logisch. Ik moet er wel bij zeggen ... Dat viel me ook weer op toen ik vorige week bij de NAVO-vergadering zat. Ik wil onze eigen positie niet kleiner maken dan die is. Sowieso zijn er allerlei dingen die we goed doen op het gebied van

cyber. Maar als je dan het gezelschap rondkijkt, is er natuurlijk één land dat er qua omvang en importantie volstrekt uitspringt en dat zijn de Verenigde Staten van Amerika. Het vermogen om in deze situatie te helpen, militair, strategisch en op het gebied van cyber, is onvergelijkbaar met alle andere. Ik probeer dan altijd de inwonersaantallen op te tellen. Dan heb je Amerika, en dan heb je de rest. Ik snap de ambitie van de heer Brekelmans en die ondersteun ik ook graag, maar Amerika is in a league of its own. Zo reëel moeten we ook zijn.

De **voorzitter**:
Er is geen aanvullende vraag. Meneer Van der Lee, uw vraag.

De heer **Van der Lee** (GroenLinks):
Dank aan de Minister voor de beantwoording. Hij schetst de Oekraïense kant van de medaille. Ik was wel benieuwd naar de Russische kant van de medaille. Als je afgaat op publieke bronnen, zie je dat de cyberactiviteiten door verschillende Russische veiligheidsdiensten worden ondernomen die onderling rivaliteit hebben. Heeft dat een rol gespeeld? Welke lessen worden, voor zover de Minister daar publiekelijk wat over kan zeggen, daaruit getrokken voor de organisatie van onze samenwerking met onze bondgenoten binnen de NAVO en binnen Europa, opdat we veel effectiever optreden?

De **voorzitter**:
Voor zover u daar iets over kunt zeggen, Minister.

Minister **Hoekstra**:
Dat kan ik wel. De heer Van der Lee vraagt eigenlijk twee dingen. Ten eerste vraagt hij mij om ook iets te vertellen over de Russische kant van de medaille, waarom de Russen minder effectief zijn geweest dan gevreesd. Ten tweede vraagt hij welke lessen we moeten trekken op het gebied van samenwerking.
Wat die eerste vraag betreft moet ik gewoon erkennen dat op basis van de informatie die mij ter beschikking stond aan de voorkant de Russen het aanmerkelijk minder goed hebben gedaan dan ik had verwacht. Je kunt in ieder geval niet zeggen dat wij de Russische inbreng hebben onderschat. Nogmaals, het is dan altijd de vraag: hebben de Oekraïners het zo goed gedaan of de Russen het zo slecht? Er zijn natuurlijk allerlei berichten – maar dan heb ik het breder over de oorlog – dat het Kremlin de eigen mogelijkheden heeft overschat. Je moet je echt afvragen of de informatie die naar de top is gebracht voldoende eerlijk is geweest. We kennen allemaal het gezegde «je komt niet met slecht nieuws aan bij de tsaar». Heeft dat ook op het gebied van cyber gespeeld? Mogelijk wel. Tegelijkertijd moet je vooral niet rustig in je leunstoel gaan zitten, want wat je leert in dit type conflicten is dat als een land achteraf vooral teleurgesteld is in wat het zelf heeft bereikt, het mogelijk de aanvechting voelt om er de volgende keer meer in te investeren en er harder op door te slaan. Dus ik zou er vooral een waarschuwing uit willen destilleren: denk maar niet dat dat de volgende keer ook weer geldt, of dat richting de volgende statelijke of niet-statelijke actor ook weer geldt dat we er makkelijk vanaf komen.
Dat brengt mij bij het tweede punt van de heer Van der Lee, een zeer terecht punt. Mijn waarneming is dat er allerlei dingen zijn die goed gaan in de coördinatie, ook in NAVO-verband en in EU-verband, maar dat we echt nog maar aan het begin staan van het coördineren van dit hele nieuwe slagveld, als ik het zo mag kwalificeren. Daar is nog heel veel te doen. Het goede nieuws is – en dan beantwoord ik meteen nog een vraag van de heer Van der Lee – dat we inmiddels wel met elkaar hebben erkend dat bijvoorbeeld artikel 5 zou kunnen worden ingeroepen in het geval van een massale cyberaanval. Dan is het nog behoorlijk ingewikkeld om uit te maken waar je die lat precies legt. Dat vraagt nog nadere uitwerking. Op

het gebied van coördinatie tussen landen is er nog een heleboel te winnen als het gaat om de strikt militaire samenwerking binnen EU en NAVO-lidstaten. Op het gebied van cyber hebben we nog veel meer werk te doen. Het is wel zo dat de diensten elkaar over het algemeen goed weten te vinden, is mijn waarneming. Dat is ook wat ik er in algemene zin over kan zeggen. De heer Van der Lee heeft daar gewoon gelijk in. Ik zal er in ieder geval voor zorgen dat we in de strategie waar we na de zomer mee komen, waarin zowel de nationale component als de internationale component naar voren komen, ten aanzien van de internationale component aangeven hoe wij als Nederland zullen proberen om daar meer tractie op te genereren.
Voorzitter. De heer Brekelmans, die ook vroeg naar Oekraïne, wil ik zeggen dat we in reactie op een urgent verzoek van Oekraïne een financiële bijdrage hebben geleverd aan het verhogen van de cyberweerbaarheid. Ook binnen het EU-netwerk van cyber security incident response wordt heel nauw contact onderhouden tussen de teams die daarin samenwerken en het Nederlandse Cyber Security Centre. Daar wordt heel actief afgetapt welke hulp er potentieel nodig zou zijn. De vraag over de Nederlandse inzet heb ik net beantwoord.
Dan heb ik de belangrijkste zaken die specifiek over Oekraïne gaan benoemd. Er ligt nog wel een vraag van mevrouw Mulder of er ook andere landen zijn geraakt en dan wellicht niet door Rusland, maar wellicht door private partijen. We hebben allemaal kunnen zien dat hackerscollectieven en niet-statelijke actoren ook in openbare bronnen kenbaar hebben gemaakt – overigens vaak aan de Oekraïense kant van de streep – dat ze zich in het conflict mengen. Laten we overigens niet naïef zijn. Een deel van de activiteiten vindt ook wel degelijk richting het westen en richting Oekraïne plaats. Er worden actief aanvallen uitgevoerd. Het is wel zo dat je – ik wil daar open over zijn richting de Kamer – de spillover naar Nederland, naar NAVO-bondgenoten en naar de EU relatief beperkt mag noemen. Ik formuleer het met voorzichtigheid, maar als iemand mij acht weken geleden had voorspeld hoe de oorlog eruit zou komen te zien, had ik het veel ernstiger verwacht.

De **voorzitter**:
Dit is een mooi moment voor twee interrupties. Ten eerste de heer Brekelmans en daarna mevrouw Mulder.

De heer **Brekelmans** (VVD):
Ik had nog een vraag gesteld over sancties voor hackers en hackersgroepen.

Minister **Hoekstra**:
Daar kom ik zo nog even op terug, als het goed is.

De **voorzitter**:
Dat is het voordeel van blokjes. Mevrouw Mulder.

Mevrouw **Agnes Mulder** (CDA):
De Minister gaf net deels in de beantwoording aan dat er tussen statelijke en niet-statelijke actoren nog een heel grijs gebied zit. In het Westen en Nederland staan we voor bepaalde democratische waarden. Hoe ga je daarmee om, ook in dit perspectief? Hoe defensief of offensief ben je dan? Eigenlijk is de vraag: hoe gaat Nederland daarmee om? Het valt nu mee, dus dan hoeven we misschien niks offensiefs in te zetten, maar wanneer zou dat eventueel wel plaatsvinden?

Minister **Hoekstra**:
Dat is een hele goede vraag, waar ik niet een heel specifiek antwoord op kan geven. In mijn hoofd moeten we een aantal stappen relatief snel

proberen te nemen. Ik kom daarmee weer indirect terug op het antwoord dat ik eerder gaf aan de heer Brekelmans, de heer Sjoerdsma en de heer Van der Lee. Je moet zorgen dat je eigen capabilities op orde zijn. Daar heeft Nederland ook nog veel werk in te verrichten. Vervolgens moet je het intern in Nederland goed weten te coördineren, niet alleen in het strikte securitydomein, maar ook breder in de samenleving. Denk aan bedrijven. Daar werd terecht naar gevraagd. Sommige dingen zijn echt alleen aan de Staat, maar soms gaat het juist ook om het bedrijfsleven. Dat is twee. Drie. Je moet ervoor zorgen dat je nog veel beter leert coördineren richting de EU en de NAVO-partners. Daar was ik net ook transparant over richting de heer Van der Lee.
Gebeurt er dan niks? Zeker wel. Er gebeurt een heleboel, ook tussen de diensten. Maar mijn waarneming is dat je nog veel meer informatie kunt uitwisselen, dat je elkaar kunt wijzen op waar zaken vandaan komen en elkaar kunt helpen bij de vragen: wat zien we, hoe doe je de attributie, hoe maak je dingen stuk en hoe zorg je bijvoorbeeld voor vervolging? Daar hebben we nog een wereld in te winnen.
Het stuk dat daar weer op volgt, is de vraag van mevrouw Mulder, namelijk of je ook offensief kunt zijn. Dat kan betekenen dat je terugslaat of dat je zelf dingen eerder doet. Dat is op cybergebied overigens behoorlijk ingewikkeld, maar ik vind dat je daar wel over na moet denken, want anders is het geopolitiek belletje trekken gratis. Dan overkomt het je en dan is het beste wat je kunt doen, tevreden zeggen: dit hebben we ook weer stukgemaakt. Dat heeft natuurlijk iets... Ik ben iemand die een diepgeworteld geloof heeft in wederkerigheid in het leven. Dat zou dus een buitengewoon slechte notie zijn, want dat is een aanmoediging voor de andere partij om het de volgende keer weer te proberen, maar dan slimmer.
Daar zit overigens wel één kanttekening bij. Mijn excuses voor het lange antwoord, voorzitter, maar ik los meteen een aantal vragen op die er nog lagen. Er zit één kanttekening bij: op het moment dat je reageert, laat je ook altijd zien dat je wetenschap hebt van wat er gebeurd is. Soms wil je die wetenschap juist niet delen en wil je het gewoon kunnen volgen, zoals we kennen uit het domein van spionage. Als je voor het eerst een spionageroman leest op de middelbare school, dan denk je: je maakt meteen zo'n zaak stuk en je pakt die spionnen op. Maar de realiteit is natuurlijk dat diensten vaak mensen hun gang laten gaan omdat ze liever willen weten wat er gebeurt. Vandaar dat je niet altijd meteen terug moet slaan, maar ik denk wel dat je je arsenaal zou moeten willen verbreden. Dat was een antwoord op de beide interrupties.

De **voorzitter**:
Nou, u heeft nog een vraag van de heer Brekelmans staan, maar daar komt u straks op terug.

Minister **Hoekstra**:
Ja, sorry. Maar dit waren er twee.

De **voorzitter**:
Gaat uw gang.

Minister **Hoekstra**:
Ik kom op een aantal andere zaken die gaan over het internationale.
De heer Brekelmans vroeg specifiek naar China. Daar wil ik nog een aantal dingen over zeggen. Hij vroeg naar meer internationale coördinatie. Er vindt überhaupt steeds meer internationale coördinatie plaats op het gebied van informatiedeling en respons op cyberdreiging vanuit China. Dat doen we binnen de EU, binnen de NAVO en ook in nieuwe internationale coalities. De heer Brekelmans weet dat we in de afgelopen dagen bij elkaar zijn geweest met de NAVO en een paar van de meest bevriende

landen uit de Indo-Pacific. Aan de vooravond van de aanval op Oekraïne hebben we überhaupt met een breder gezelschap gesproken over de EU en de Indo-Pacific. Dat gebeurt dus. Ik moet er wel bij zeggen dat ook daar nog een wereld te winnen is. Het is überhaupt al een enorm karwei om die landen bij elkaar te krijgen en over conventionele zaken te spreken. Het is dus terecht dat de heer Brekelmans daarnaar vraagt. Mochten daar verdiepende dingen over te melden zijn, dan zal ik dat ook doen in de strategie.
De heer Brekelmans vroeg ook: moet China nou niet steviger worden aangesproken? Ik vind dat je dit soort zaken inderdaad ook echt moet uitspreken en attribueren. Ik zeg er wel bij dat je dan toch heel vaak – dat is ook mijn eigen neiging als ik hoor van zo'n zaak en dat begrijp ik overigens heel goed – van de diensten en van ministeries een antwoord krijgt in de categorie «het is waarschijnlijk of zeer waarschijnlijk dát». Dan krijg je natuurlijk ook vaak een dialoog waarin iemand anders gewoon keihard zegt: nietes. Dan abstraheer ik even van China. Dat is het grote ongemak in dat cyberdomein. De EU heeft in 2020 wel al personen en entiteiten uit China die waren gelieerd aan de dreigingsactor APT10 die er toen was op die EU-sanctielijst gezet. Wij spreken ons hier ook in die bilaterale dialoog en in de Europese dialoog expliciet over uit. Recent hebben ook de EU-Chinataskforce en de Nederlands-Chinese ambtelijke consultatie plaatsgevonden. In beide gevallen is er ook gesproken over cyberaanvallen vanaf Chinees grondgebied.
Dan kom ik nog bij een aantal andere internationale dingen.
Mevrouw Koekkoek en de heer Sjoerdsma vroegen ook nog naar wat je nou kan doen op het gebied van coalitievorming. Mevrouw Koekkoek vroeg, even in mijn eigen woorden: hoe trek je een aantal van die anderen nou in je kamp? Dat is een heel terechte vraag. Mijn waarneming is de volgende, en die geldt breder in de discussie over al die landen. Iemand had het net over swing states; dan denk ik onmiddellijk aan Amerika. Maar wat betreft de in-between countries, de landen die zich afvragen op wie ze zich nou vooral moeten richten, werkt stroop toch vaak beter dan azijn. Een van de dingen die wij doen, is het actief helpen van landen met het opbouwen van cyberexpertise. Dat geeft je namelijk een titel om een dialoog te voeren. Is dat de panacee? Nee, natuurlijk niet, en Nederland kan dat ook absoluut niet in z'n eentje oplossen. Maar dat is een manier om cyberdiplomatie te bewerkstelligen. Daar proberen we ook anderen in Europa, die dat ook overigens al in belangrijke mate doen, voor te enthousiasmeren. Verder gaan wij als BZ natuurlijk verder met het ontwikkelen van het normatief kader. Dat is in beweging. Dat is ook een onderwerp waar we actief de dialoog over zoeken, vanzelfsprekend met de landen in Europa en Noord-Amerika, maar ook in Azië. Juist landen in deze geografieën hebben hier namelijk in sterke mate mee te maken. Ik zeg niet dat het niet ook speelt in Afrika en Zuid-Amerika, maar mijn waarneming is dat landen in deze drie geografieën hier het meest onder te lijden hebben.
Dan was er nog een vraag over capaciteit en het regeerakkoord. Dan kom ik wel een beetje op het gebied van binnenland, maar dat ligt toch ook een beetje op het gebied van buitenland. Zijn we nou voldoende geëquipeerd voor dit slagveld? Ik ben het echt met de heer Brekelmans, en ook met anderen die daar net naar verwezen, eens dat de mate van dreiging fors is en dat we echt een been proberen bij te trekken. Maar ik kan bepaald niet uitsluiten dat de mate van dreiging alleen maar verder zal toenemen. De mate van assertiviteit en inventiviteit zal ook toenemen. Dat zal mogelijk in de toekomst nog weer een extra stap van kabinetszijde vragen. Ik kan dat nu niet duiden in mensen of middelen, maar ik wil dat wel graag meenemen als we komen met de strategie. Ik zal dat ook met de collega's in het kabinet bespreken.
Dan de verdere vragen op internationaal gebied. De vraag van de heer Van der Lee over artikel 5 heb ik beantwoord.

De **voorzitter**:
Maar daar heeft de heer Van der Lee toch een vraag over.

De heer **Van der Lee** (GroenLinks):
Ja. Ik vond het antwoord nog wel heel generiek: ja, het zou kunnen dat een land bij een grootschalige aanval een beroep doet op artikel 5. Maar is daar dan niet al wat meer voor in voorbereiding geweest, ook in overleg met de lidstaten? Is besproken op welke schaal het ongeveer moet zijn, wil je daar een beroep op doen, of is dat nog echt helemaal diffuus? Die cyberwarfare is namelijk echt niet zo nieuw en we weten dat het groeit, dus ik neem toch aan dat hier al vaker over gesproken is?

De **voorzitter**:
Dank u wel voor uw vraag. Minister, wat is uw antwoord?

Minister **Hoekstra**:
Het is ongemakkelijk, maar het antwoord is ja en nee. Sinds 2016 wordt er heel serieus naar cyber gekeken. Er is ook afgesproken dat artikel 5 ingeroepen kan worden op het gebied van cyber. Daarmee – de heer Van der Lee weet dat als geen ander – is het nog geen automatisme dat de NAVO in oorlog is als dat artikel wordt ingeroepen. Zie ook de discussies toen Minister-President Kok na 9/11 werd gevraagd of we nu in oorlog zijn. Sommigen herinneren zich dat nog. Kok gaf, in ieder geval in mijn herinnering, echt een adequaat antwoord, maar je zag hem ook worstelen met de vraag: past het denkraam dat we ten aanzien van de NAVO altijd hadden nou op de situatie van die verschrikkelijke aanslag op 9/11 op de Twin Towers? Datzelfde zie je bij de NAVO. Mijn waarneming is dat we nog zouden kunnen werken aan het verder articuleren van in welk geval een cyberaanval nou evident niet de drempel haalt en wanneer wel. Mevrouw Mulder, of de heer Van der Lee, zei het zelf: wat als je een heel land platlegt? Als alle ziekenhuizen, als alles, alles, alles out of order is, dan kom je toch vrij dicht bij de situatie waarin je dat artikel wel zou mogen inroepen. Ik denk dat we nog kunnen werken – ik zie dat ook als huiswerk voor mezelf en uiteraard voor de collega's van Defensie – aan verdere specificatie daarvan, zodat we het grijze gebied van «wanneer wel en wanneer niet» kleiner maken. Dat gaat namelijk helpen in de besluitvorming, is mijn inschatting.

De **voorzitter**:
Aanvullend, de heer Van der Lee.

De heer **Van der Lee** (GroenLinks):
Dank voor deze verdere toelichting. Is het ook zo dat andere lidstaten dit op een vergelijkbare manier zien en bezig zijn met het denken daarover? Is er ook al een afspraak om daar gezamenlijk stappen in te zetten? Of is het zelfs daar nog te prematuur voor?

Minister **Hoekstra**:
Nee, dat gebeurt. Cyber kwam niet alleen in de vorige NAVO-vergadering langs, maar ook in de NAVO-vergadering daarvoor. Mensen benoemen het en maken zich daar natuurlijk ook zorgen over. In veel opzichten wordt het gesprek dat we hier hebben ook dáár gevoerd. Wat zien we in Oekraïne? Wat zien we in de Indo-Pacific? Voor andere landen zijn cyberaanvallen nog veel meer aan de orde van de dag dan voor Nederland, dus: absoluut. Je moet hier, als het gaat over cyber en artikel 5 van de NAVO, het bestaande instrumentarium toepassen op terra incognita. En ja, daar zijn we mee bezig, en ja, er is ook geen panklaar antwoord. Het is misschien teleurstellend wat ik nu ga zeggen, maar wel eerlijk: ook in een conventionele situatie hebben we deze discussie weleens. Ik kan me de vraag van een paar weken geleden, van een van de

leden van uw commissie of misschien van de media, herinneren: zijn we in oorlog als een afzwaaier op NAVO-grondgebied belandt? Ik denk dat de meeste mensen die vraag met nee zouden beantwoorden. Wat nou als het geen afzwaaier is, maar het wel bij één granaat blijft? Ook die klassieke discussie is potentieel al met ambiguïteit omgeven: sommige gevallen zijn heel clear-cut, andere zijn dat niet. Of je het nou leuk vindt of niet, maar dat heb je nog veel sterker op het gebied van cyber.

De **voorzitter**:
Voordat u verdergaat, een interruptie van de heer Brekelmans.

De heer **Brekelmans** (VVD):
Misschien even naast artikel 5. Je zou binnen de EU natuurlijk met elkaar kunnen afspreken dat je er iets tegenoverstelt op het moment dat China een cyberaanval pleegt op een lidstaat, of meerdere aanvallen die misschien niet meteen de vitale infrastructuur lamleggen. Er is een toolbox, maar dat is iets op papier. Ik heb alleen niet de indruk dat in onze contacten met China ... Ik verwacht echt niet dat de Minister dat bilateraal gaat doen, want ik weet heus wel hoe de machtsverhoudingen liggen. Als de Europese Unie probeert om de relatie met China goed te houden, maar China continu cyberaanvallen pleegt, in onze vitale infrastructuur zit, en een database van zerodays opstelt waarmee het ons op talloze manieren kan aanvallen, moeten we als Europese Unie dan niet met elkaar zeggen dat we dat gewoon niet acceptabel vinden, dat we dat in ieder diplomatiek overleg stevig benoemen, en dat we daadwerkelijk sancties opleggen als China te ver gaat? Want anders testen zij hoever ze kunnen gaan en is de boodschap ieder keer: ja, het wordt wel aangekaart, maar we kunnen toch steeds verder gaan. Ik vind dat daar echt een steviger beleid op nodig is.

Minister **Hoekstra**:
Ook hier ga ik een wat langer antwoord geven. Ik ga proberen om deze vraag en de vorige vraag van de heer Brekelmans en nog een paar andere vragen in één antwoord te vouwen. Dit heeft eigenlijk allemaal te maken met het geopolitiek volwassen laten worden van de Europese Unie. We hebben de discussie gehad over strategische autonomie of strategische onafhankelijkheid, zo u wilt. We hebben ook de discussie gehad over hoe je nou die economische macht inzet die de Europese Unie ontegenzeggelijk heeft op andere terreinen. Hoe ga je om met zaken als spionage? Dit is er evident ook één. Ik ben het graag met de heer Brekelmans eens. Hij is zo aardig om tegen mij te zeggen: ik begrijp best dat het moeilijk is voor de Minister. Laat ik daar dan aan toevoegen dat ik ook echt vind dat daar een taak voor mij ligt om daar wel mee aan de gang te gaan, want dit gaat niet meer weg. Het is al zo, om ook zijn vorige vraag te beantwoorden, dat met het EU-cybersanctieregime sancties kunnen worden opgelegd aan hackersgroepen. Dus ja, het kan en ja, het gebeurt ook, maar de lat ligt hoog als het gaat over attributie en de lat ligt hoog als het gaat om opsporing. Ik heb het nog even met JenV gecheckt. Het is geen sinecure. Als je dan naar de getallen kijkt – dan ga ik de heer Brekelmans teleurstellen – zie je dat op dit moment acht personen en vier entiteiten gelist zijn onder het EU-cybersanctieregime, waaronder personen en entiteiten uit Noord-Korea, China en Rusland. Dat is dus eigenlijk een heel kleine groep als je het afzet tegen de waarneming die wij allemaal, alleen al op basis van krantenberichten, hebben over hoeveel er belletje getrokken wordt. Ik ben het dus met hem eens en ik zou hem eigenlijk willen toezeggen dat ik dit op de agenda houd, maar dat we hier ook nog een passage aan wijden in de brief. Ik ben er zelf in ieder geval op gebrand om in ieder geval een zetje te geven aan die geopolitieke volwassenheid en ik denk dat dit een terrein is waarop dat ook zou moeten.

De **voorzitter**:

Aanvullend, de heer Brekelmans.

De heer **Brekelmans** (VVD):
Het kan natuurlijk niet zo zijn dat er honderden, duizenden cyberaanvallen plaatsvinden en dat het maar lukt om in totaal acht mensen en vier entiteiten op de sanctielijst te krijgen. Dan zit het ergens in het systeem niet goed. De toezegging is: ik ga het internationaal aankaarten. Volgens mij hebben wij gezien door de oorlog en de aanval van Rusland op Oekraïne dat het mogelijk is om heel snel het aantal mensen en entiteiten op die sanctielijst uit te breiden en dat naar alle juridische bezwaren die daartegen zijn – zijn mensen wel direct betrokken? – met creativiteit en slagvaardigheid wordt gekeken. Ik zou dat ook in het cyberdomein willen zien. Als al die inlichtingendiensten zeggen «die Russische hackersgroep is er echt niet om ons te helpen om ons internet beter te laten functioneren, die hebben maar één doel en dat is onze systemen ontwrichten», dan moet je toch op een gegeven moment voldoende materiaal hebben om te kunnen zeggen «die gaat op de sanctielijst, daar mogen bedrijven geen zaken meer mee doen en die krijgen geen bankrekeningen meer, geen reisvisum meer» en noem het allemaal maar op? Ik zou daar echt toch een steviger antwoord van de Minister op willen.

Minister **Hoekstra**:
Laat ik dan een onderscheid maken, ook om een misverstand te voorkomen. Ik ben het namelijk zeer eens met wat de heer Brekelmans zegt ten aanzien van hackers uit Rusland. Je moet het ijzer smeden als het heet is. Laat ik hem daar een toezegging op doen. Ik ben het gewoon totaal met hem eens. Ik zal dat in de volgende RBZ inbrengen, maar ik zal ook zorgen dat we dat voor die tijd met de Commissie en met andere lidstaten delen. Waar mogelijk zal ik dat ook in bilaterale contacten delen. Overigens zeg ik erbij dat het probleem van attributie blijft bestaan. Dat is het zeer begrijpelijke antwoord dat wij ook steeds krijgen als ik het vraag aan de diensten of aan JenV. Ik zou daar echt het ijzer willen smeden, juist omdat het nu heet is. Ik vind ook dat je het richting andere actoren moet proberen. Daar moet ik alleen eerlijkheidshalve bij zeggen dat het ijzer daar natuurlijk veel minder heet is. Daar speelt ook weer dat enorme probleem van attributie, maar daar spelen ook andere belangen die lidstaten meewegen. Tussen inlichtingendiensten speelt altijd welke informatie men wel proactief deelt en welke informatie men niet proactief deelt. Ook daar ben ik het dus zeer eens met de route van de heer Brekelmans en hij overigens niet alleen, want de heer Sjoerdsma zei dat net ook, ook ten aanzien van nieuwe initiatieven. Daar ben ik het zeer mee eens. Ik wil daar zelf ook graag een voortrekkersrol in spelen, maar daar gaat het meer moeite kosten om iedereen op dezelfde pagina te krijgen.

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

Minister **Hoekstra**:
Ja. Ik had de vraag ten aanzien van pakketten, projecten, instituties en versnippering in de EU van de heer Sjoerdsma denk ik half beantwoord. In zijn algemeenheid hebben wij een positieve grondhouding ten aanzien van die initiatieven. Je kan je ook heel goed voorstellen dat de EU een rol speelt als clearinghouse op het gebied van informatie-uitwisseling en coördinatie. Dan heb ik nog een paar dingen op het gebied van normen en recht. Mevrouw Koekkoek vroeg nog hoe en of ik een rol zie voor ISIDOOR. Ik kan haar zeggen dat het klopt dat ook daar attributie moeilijk is, maar dat we daar als Nederland – ik zeg dit met voorzichtigheid – relatief goed in zijn. We doen het overigens in nauwe samenwerking met internationale partners. Misschien kan ik met haar afspreken dat we in de strategie ook nog proberen een onderscheid te maken tussen hoe je

omgaat met statelijke versus niet-statelijke actoren, omdat daar wel onderscheid in te maken is.
De heer Brekelmans vroeg naar simulaties. Ik kan een eindeloos lang antwoord geven over op wat voor manieren er geoefend wordt, wat voor sporen daarbij betrokken worden en hoe dat linkt aan de Nederlandse Cybersecurity Agenda, maar kort samengevat bestaat het hele verhaal uit het organiseren van oefeningen in het kader van het Nationaal Crisisplan Digitaal, zoals de tweejaarlijkse oefening ISIDOOR. Bovendien zou ik hieraan willen toevoegen: laten we ook ten aanzien van de strategie aangeven waar de huidige oefeningen voldoen en waar er wellicht nog meer gedaan moet worden. Dat lijkt mij, eerlijk gezegd, verstandig.
De heer Van der Lee had nog een vraag ten aanzien van privacy. Hij kent het coalitieakkoord natuurlijk als geen ander. Dat heeft misschien ook met het vorige ministerschap te maken. In het coalitieakkoord zijn we er zeer expliciet over dat we de privacy van burgers echt willen verbeteren, dat we fundamentele burgerrechten ook online willen erkennen en dat we willen zorgen voor veilige digitale communicatie. Recent heeft de Minister van JenV ook nog antwoorden gestuurd op dit terrein. Er vindt op dit moment een inventarisatie plaats om te onderzoeken of het mogelijk is om aan de ene kant aan de problematiek van de opsporing tegemoet te komen, terwijl we aan de andere kant de encryptie voldoende sterk houden. Nu weet ik even niet of de heer Van der Lee ook in de commissie van JenV een natuurlijke ingang heeft, maar dit is wat ik er in dit stadium over kan zeggen.

De **voorzitter**:
Daar heeft de heer Van der Lee een vraag over.

De heer **Van der Lee** (GroenLinks):
Ik heb niet per se natuurlijke toegang, maar ik heb collega's. Toch even over die samenhang met privacybescherming. Ik weet dat het coalitieakkoord daar terecht veel waarde aan hecht, net als GroenLinks. Tegelijkertijd is een belangrijke drijver onder de ontwikkeling van kwantumcomputers hun capaciteit om encryptie juist te kunnen doorbreken. Vanuit het veiligheidsperspectief is dat misschien ook een heel terecht en belangrijk motief. Tegelijkertijd ontwikkel je die encryptie ook weer om de privacy zo veel mogelijk te beschermen. In die zin zijn het echt tegenstrijdige belangen. Mij is niet geheel helder – misschien komt dat in die strategie die we na de zomer gaan krijgen – waar de Nederlandse overheid nu precies staat. Hoeveel waarde hechten we aan de privacybescherming en dus de mogelijkheden om encryptie toe te passen versus hoe sterk willen wij onze capaciteiten hebben om een voorsprong te hebben, ook in de ontwikkeling van kwantumcomputers, om encryptie van statelijke actoren die ons niet goed gezind zijn weer te doorbreken? Daar ging mijn vraag eigenlijk over, maar het is makkelijker om die vraag te stellen dan die te beantwoorden. Dat begrijp ik.

Minister **Hoekstra**:
Nee, het is natuurlijk een heerlijke vraag. Die vraag is een proxy voor de filosofische vraag waar uiteindelijk geen antwoord op is: de balans tussen veiligheid en vrijheid die we elke dag opnieuw zoeken. Totale veiligheid betekent een politiestaat en totale vrijheid betekent wetteloosheid. Wat wij in deze samenleving met vallen en opstaan proberen te doen, is elke keer opnieuw zo goed mogelijk dat evenwicht leggen. Ik heb de aanvechting om er nog allerlei filosofische gedachten bij te slepen, maar dan begeef ik me te veel op het terrein van de Minister van JenV. Dus ik zou naar haar antwoorden willen verwijzen op die specifieke vragen over hoe we het doen als het gaat om het tegengaan van cybercrime. Ik zou wel de suggestie van de heer Van der Lee willen meenemen dat wij aan kabinetszijde in deze strategie, waar dat voor de hand ligt, aandacht geven

aan het element van privacy. Terecht speelt dat niet alleen in kabinetskringen, maar ook bij de Kamer een prominente rol.
Voorzitter. Er zijn toch stiekem een heleboel vragen gesteld. Ik denk dat ik de vraag van mevrouw Koekkoek over cybercrime hiermee ook heb beantwoord.
De swing states waren ook een vondst van mevrouw Koekkoek. Die vraag heb ik volgens mij ook beantwoord.
De heer Brekelmans had het over de Boedapest-cybercrimeconventie als standaard. Ik had al in de richting van mevrouw Koekkoek gezegd dat stroop meestal beter werkt dan azijn, maar in zijn richting zou ik willen zeggen dat we er absoluut mee bezig zijn. Dat zou namelijk enorm helpen. Nederland is net als meer dan 60 andere landen al verdragspartij. Er zijn overigens ook veel andere landen die hun eigen nationale wetgeving daarop baseren. We zijn ook nog in VN-verband aan het onderhandelen over een VN-verdrag op het gebied van cybercrime. We zetten als Nederland en EU natuurlijk in op een efficiënt VN-cybercrimeverdrag, met een hoge mensenrechtenstandaard. Dat is dan weer deels gestoeld op de Boedapestconventie. We zijn er alleen ook nog niet mee klaar en we weten hoe ingewikkeld dit is.
Voorzitter. Het is altijd gevaarlijk om te zeggen dat je alles gedaan hebt, want dan krijg je een heleboel vingers, maar volgens mij ben ik wel een heel eind. Kwantum hebben we niet opgelost, maar wel gedaan. De hackers en JenV hebben we gedaan. Offensiever hebben we gedaan. Volgens mij ben ik een heel eind.

De **voorzitter**:
Dan gaan we dat gewoon nog even inventariseren voor de eerste termijn. Ik zag volgens mij alle vingers, klopt dat? Mevrouw Koekkoek ook? Dan geef ik u het eerst het woord, want u moet zo weg. Daarna gaan we verder.

Mevrouw **Koekkoek** (Volt):
Ik heb inderdaad nog één vraag, die deels ook niet bij deze Minister ligt. Ik had de vraag gesteld of het nuttig of mogelijk kan zijn om een cyberleerstoel bij iedere universiteit deels te financieren en/of langere subsidies te stimuleren, dus dat we niet alleen maar op projectbasis investeren in kennis. Bij welke organisatie dan ook; het kan ook naar denktanks gaan of andere organisaties. Omdat ik inderdaad straks weg moet, ga ik hem nu meteen opvolgen. Ik kan me voorstellen dat dit antwoord niet direct gegeven kan worden. Wellicht is het mogelijk dat hierop teruggekomen wordt vanuit de strategie, waar we nog een brief over krijgen, of een tussenbrief. De reden waarom ik de vraag stel – dat geeft meteen de context mee en dan kan ik weg – is dat het heel erg toegaat naar: vanuit de kennis die we hebben, moeten we investeren in de kennis die we nog niet hebben. Ik snap dat dat normaliter bij iets als OCW zit, maar het lijkt me in dit geval verstandig als het juist ook vanuit BZ en vanuit de strategie gaat, vandaar dat ik de vraag hier stel.

Minister **Hoekstra**:
Ook omdat ik het als een bespiegeling had beschouwd in plaats van als een uitnodiging om de Minister van OCW en al die universiteiten nu in dit AO een cyberleerstoel aan hun broek te doen, had ik gedacht: daar moet ik voorzichtig in zijn. Ik zou er nog aan kunnen toevoegen dat we überhaupt al inzetten op verschillende meerjarige initiatieven. Er zijn allerlei programma's waaraan we meewerken en die we financieren. We hebben een heel stevig kennisnetwerk op het gebied van cyber, waar de universiteiten van Leiden en Amsterdam, de Nederlandse Defensie Academie, HCSS, Clingendael en TNO aan meewerken. Het gaat vooral om het doelgericht samenbinden van kennis, het weghalen van hiaten en het zorgen dat je geen dubbelingen hebt. Ik heb ten aanzien van een

leerstoel en een nieuw thema altijd de neiging om te denken «hé, dat is best een aardig idee», maar ik vind dat wel echt aan de Minister van OCW, zeker als ik nu hoor wat er al aan initiatieven is. Met goedvinden van mevrouw Koekkoek zou ik het hierbij willen laten.

De **voorzitter**:
Heel goed. We gaan tot een afronding komen in deze eerste termijn. De heer Sjoerdsma was eerst, daarna mevrouw Mulder, daarna de heer Brekelmans en daarna de heer Van der Lee. De heer Sjoerdsma was eerst. Gaat uw gang.

De heer **Sjoerdsma** (D66):
Dank aan de Minister voor zijn beantwoording. Ik had nog een vraag gesteld over Rotterdam. Daar ben ik toch nog wel benieuwd naar.

De **voorzitter**:
Ja, dat is waar, Rotterdam.

Minister **Hoekstra**:
Het is terecht dat de heer Sjoerdsma daar nog een keer naar vraagt. Het antwoord begint met een wedervraag, zou ik bijna willen zeggen, omdat namelijk niet geheel duidelijk is welke aanval in de vraag wordt bedoeld. Dat moet ik dan echt even zelf hernemen voordat ik daar een goed antwoord op kan geven. Mag ik er anders in tweede termijn even op terugkomen? Want de heer Sjoerdsma heeft inderdaad deze vraag gesteld. Er zijn meerdere zaken aan de hand, dus ik wil zeker weten dat ik de vraag van een goed antwoord voorzie. Mogelijk vraagt het ook nog overleg met andere ministeries.

De **voorzitter**:
Ik kijk vragend naar de heer Sjoerdsma.

De heer **Sjoerdsma** (D66):
Ik wil het best specificeren, maar ik ben nu natuurlijk benieuwd naar alle aanvallen die de Minister zou kunnen noemen. Heel specifiek: het betreft een aanval die gelijktijdig is waargenomen in niet alleen Rotterdam, maar ook in Hamburg en Antwerpen, en die zijn effect had op onder andere olieterminals en het niet meer kunnen ontladen van bepaalde scheepvaart.

Minister **Hoekstra**:
Laat ik het volgende doen, want de heer Sjoerdsma heeft gelijk. Hij heeft ook in eerste termijn overigens al die brede vergelijking getrokken. Ik ga even kijken of ik dat in tweede termijn van een antwoord kan voorzien. Anders ga ik dat op een andere manier oplossen. Het kan zijn dat dit nog overleg vraagt met JenV en IenW.

De **voorzitter**:
Dank u wel. Mevrouw Mulder. Meneer Van der Lee hoeft overigens niet; die is ook ruim aan bod geweest.

Mevrouw **Agnes Mulder** (CDA):
Ik had nog even navraag gedaan naar het amendement. Ik weet dat rond de zomer de officiële reactie zou komen, maar misschien is er op dit moment al iets meer over te zeggen. Ik had ook het volgende gevraagd. In de brief van – laat ik even specifiek zijn – 29 september staat: «Wanneer landen op enigerlei manier in strijd daarmee handelen» – dus met het internationale normatieve kader voor cyberspace – «is een reactie op zijn plaats.» Ik was even benieuwd naar de reacties van Nederland tot nu toe.

Minister **Hoekstra**:
Ik heb eerlijk gezegd een groot gedeelte van de eerste termijn geprobeerd, misschien te impliciet, die vraag te beantwoorden, zowel daar waar het ging over meer capaciteit als over meer middelen. Ik heb volgens mij gezegd dat we daarop echt extra stappen gaan zetten. Maar laat ik ook zo eerlijk zijn om te erkennen dat ik denk dat dit doorgaat en dat het mogelijk op een later moment niet genoeg zal blijken te zijn.
Het tweede deel van de vraag van mevrouw Mulder was: hoe geven we daar uiting aan in de bilaterale contacten? Ik heb het voorbeeld van China gegeven. Dat doen we als Nederland en als Europa op meerdere plekken en op meerdere momenten. Dat is overigens allemaal – maar dat heb ik eerder ook gezegd – in een context waarin attributie wel echt heel erg ingewikkeld is. Dat misschien even tot zover.

De **voorzitter**:
Mevrouw Mulder, voldoende? Niet? Dan kunt u er in tweede termijn op terugkomen.

De heer **Brekelmans** (VVD):
Ik had nog een vraag gesteld over offensief hacken. De Minister zei daarvan dat hij die beantwoord had, maar eigenlijk is mijn vraag in twee zinnen de volgende. We zijn al in een cyberoorlog verwikkeld. Andere landen gebruiken daar methoden voor. Ik zou niet willen dat wij die strijd met één of twee handen op onze rug voeren. De Minister hoeft wat mij betreft niet heel gedetailleerd in te gaan op wat allemaal wel en niet mag, maar ik zou eigenlijk graag een geruststellend antwoord willen, namelijk dat wij voldoende ruimte geven aan onze diensten om die cyberoorlog te voeren.

Minister **Hoekstra**:
Als de heer Brekelmans het zo zegt, dan klinkt het nog offensiever dan hij het misschien bedoelt. Hij zegt: de diensten voldoende mogelijkheden geven om offensief de cyberoorlog te voeren. Dat zou ik niet helemaal op die manier voor mijn rekening durven nemen. Het is wel zo dat het Defensie Cyber Commando indien nodig in staat is om een tegenaanval uit te voeren om een vijandelijke actie af te wenden of om een essentieel belang van de Staat te beschermen. Het is wel belangrijk om hier nog te markeren dat voor zo'n tegenaanval vanuit de krijgsmacht dan wel een internationale rechtsgrond moet zijn. Er moet dus een noodzaak voor zijn en er is ook een regeringsbesluit voor nodig. Het is belangrijk om ons dat te realiseren. Waarom ik het niet helemaal terzijde wil schuiven, is omdat ik het wel met de heer Brekelmans eens ben: je wilt eigenlijk dat er naast het uitsluitend kunnen verdedigen ook sprake is van cyberdeterrence. Dan helpt het als anderen weten dat er potentieel een prijs gaat worden betaald. Voor bredere afschrikking moet je dus kijken naar het ontwikkelen van dat soort opties, naast alle diplomatieke repercussies, naast de sanctielijsten, naast het aanspreken, naast andere dingen. Ik heb net al gezegd dat ik het er zeer meer eens ben dat je daar in Europa naar moet kijken. Ik ben er niet a priori tegen. Het is wel echt heel ingewikkeld. De lat ligt hoog, ook als het gaat om een regeringsbesluit. Daarvan kan je van zeggen: dat kan je toch elke vrijdag nemen? Dat is waar, maar je moet er een rechtsgrond voor hebben en je moet die attributie hebben. Eerlijk is eerlijk, we staan echt nog maar aan het begin van die meer offensieve pilaar.

De **voorzitter**:
Aanvullend, de heer Brekelmans.

De heer **Brekelmans** (VVD):

Dat begrijp ik. Dank voor deze heldere uitleg. Ik zou nog van de Minister willen weten wat zijn inzet is. We spreken vaak, volgens mij op een goede manier, over de nieuwe geopolitieke realiteit. Deze is minder zichtbaar. Het is bij cyber altijd zo dat er geen tanks door de straten rijden en er geen raketten op steden vallen. Maar op het moment dat het zo is dat China en Rusland in onze vitale infrastructuur zitten en dat ook gebruiken als dreiging naar ons, vind ik dat er veel urgentie is om daar iets tegenover te stellen. Ik begrijp dat wij dat met onze rechtsstaat moeilijk vinden, maar ik zou aan de Minister willen vragen dat hij dat als iets urgents ziet. Hoe verhouden wij ons tot die nieuwe geopolitieke realiteit? Gaan wij die cyberdeterrence ook echt invulling geven?

Minister **Hoekstra**:
Nogmaals, ik begrijp echt de reden dat de heer Brekelmans het vraagt. Ik denk dat hij niet zozeer mijn onwil bespeurt, maar dat hij van mij hoort hoe ingewikkeld het is en hoeveel ingewikkelde elementen hieraan zitten. Ik zou het als volgt willen voorstellen aan hem en aan de leden van uw commissie. Want ik denk dat de heer Brekelmans echt beetheeft: dit ding gaat niet meer weg. Als je twintig keer een digitale klap op je neus hebt gekregen, ga je dan alleen maar elke keer tevreden zeggen dat de schade wel meeviel, of ga je daar ook iets anders op bewandelen, zeker als de attributie lastig is, nog los van wat je aan bredere sanctiemaatregelen zou kunnen nemen? Ik zou dat willen meenemen in de strategie. We moeten er als kabinet op puzzelen of dat allemaal tot in het laatste detail in de volle openbaarheid kan of niet. Daar moet ik even een pas op de plaats maken.

De **voorzitter**:
Heel goed. Ik kijk even naar de commissieleden: kunnen we direct overgaan naar de tweede termijn? Ja. Ja. Ja. Ja. Hartstikke goed. Dan wil ik voor de tweede termijn het woord geven aan de heer Brekelmans. Gaat uw gang.

De heer **Brekelmans** (VVD):
Dank aan de Minister voor de beantwoording van de vragen. Ik ben blij met zijn toezegging dat hij binnen de EU wil pleiten voor sancties richting Russische hackers en hackersgroepen, om die ook op de sanctielijst te plaatsen. Ik was ook blij met de toezegging die hij zojuist deed dat hij wil kijken hoe offensief hacken onderdeel van de cyberstrategie kan zijn, ook vanwege de geopolitieke realiteit waar we in zitten en waar het voeren van een cyberoorlog eigenlijk al onderdeel van uitmaakt. Ik begrijp dat de Minister en het kabinet naar een manier moeten zoeken over hoe wij dat gesprek met de Kamer voeren, want het is misschien inderdaad niet iets wat je in alle openbaarheid wil doen, maar we willen wel op principieel niveau de discussie met elkaar daarover kunnen voeren. Ik denk dat daar een koerswijziging op nodig is.
Ten slotte nog één punt over diplomatie en cyberdiplomatie. Het is natuurlijk heel erg de vraag in de contacten met China, als er tien punten op de agenda staan: hoe zwaar maak je deze? Ik begrijp dat we een brede agenda en een brede relatie hebben, maar als ik kijk naar onze grootste veiligheidsdreiging die we hebben ten opzichte van China, dan is dat waarschijnlijk in het cyberdomein. Het is niet heel waarschijnlijk dat zij ooit een conventionele militaire aanval op ons zullen uitvoeren. Ik vind dus dat cyber ook in dat opzicht hoog op de agenda moet staan. Dat betekent dat we het benoemen, maar dat betekent ook dat we daar gezamenlijk als EU in optreden en dat we ook bereid zijn om het bredere pakket, die toolbox zoals het zo ambtelijk klinkt, daadwerkelijk in te zetten op het moment dat we zien dat China nog agressiever en op nog grotere schaal cyberactiviteiten uitvoert. Ik hoop dus en ik spoor de Minister ertoe

aan dat hij daar echt werk van gaat maken en dat hij dit in de bredere agenda ten opzichte van China een hoge prioriteit geeft.

De **voorzitter**:
Dank u wel. De heer Sjoerdsma.

De heer **Sjoerdsma** (D66):
Dank, voorzitter. Dank ook aan de Minister voor zijn beantwoording. Ik deel de zorgen van de VVD – maar die zorgen heb ik ook gehoord bij de Minister – niet alleen over hoe verstrekkend dit soort aanvallen kunnen zijn, maar ook over hoe frequent ze aan het voorkomen zijn, hoe frequenter ze nog gaan worden en ook hoe kwetsbaar je daarvoor kan zijn, zeker in een steeds digitalere samenleving zoals wij die zijn. Daar moet dus iets tegenover staan. Daaruit kwamen ook een aantal vragen voort die ik nog in de eerste termijn had gesteld en die ik misschien toch voor de zekerheid wil herhalen. Ik verwees naar de 13.c.-norm uit het UNGGE-rapport van 2015 en de 13.f.-norm, waarin wordt gezegd dat je je grondgebied niet mag gebruiken voor ICT-activiteiten die – ik zeg het maar even plat – andere landen serieus schaden. Ik ben nog steeds benieuwd hoe vaak we dit diplomatiek of juridisch hebben aangekaart. Ik denk dat dat een belangrijke vraag is, die een beetje aansluit op de inbreng van de heer Brekelmans. Hij focust wat meer op wat wij offensief terugdoen, maar ik denk dat je dit «out in the open» een beetje moet proberen uit te vechten. Dan kan het zijn dat het heel moeilijk is met de attributie. Dat snap ik heel goed en dat is ook heel ingewikkeld, maar zodra inlichtingendiensten zeggen dat er sprake is van een zeer hoge mate van waarschijnlijkheid, zou ik het eigenlijk wel een keer willen proberen.
Dank u wel.

De **voorzitter**:
Dank u wel. De heer Van der Lee, GroenLinks.

De heer **Van der Lee** (GroenLinks):
Dank, voorzitter. Dank aan de Minister voor de beantwoording. De vragen die ik heb gesteld, heeft hij beantwoord, maar vooral door te verwijzen naar de overkoepelende strategie die we na de zomer krijgen. Dat wordt dus een heel belangrijke strategie. Ook het debat dat we daarover zullen hebben, wordt belangrijk. Ik maak me wel wat zorgen over het tempo waarin we ons voorbereiden op die alsmaar grotere cyberwarfareactiviteiten, ook in het kader van artikel 5 van de NAVO, waar ik al het nodige over heb gezegd. Daar zal ik dan ook zeker op terugkomen.
Ik maak me wel een beetje zorgen over de discussie die we nu voeren over «offensief». Ik kan me wel voorstellen dat we, daar waar we nu financiële en economische sancties hanteren, in termen van cyberdeterrence ook op zoek gaan naar digitale sancties. Maar die afschrikking bestaat eruit dat je transparant bent over wanneer je bepaalde digitale sancties inzet. Dat is een andere benadering dan cyberwarfare op een offensieve manier, want dat kan echt beschouwd worden als een oorlogsdaad. Dan zit je naar mijn gevoel toch al in een hele andere categorie. Ik ben dus benieuwd of het mogelijk is om in die strategie ook digitale sancties te benoemen, zodat een land dan weet dat, als het bepaalde dingen doet, het instellen van die sancties de repercussie kan zijn. Dat is toch wat anders dan een veel breder cyberoffensief, zeker als dat niet heel duidelijk politiek is ingekaderd. Gelukkig geeft de Minister aan dat het een politiek besluit moet zijn van de ministerraad en dat er een rechtsgrond moet zijn. Het lijkt me heel belangrijk om daar allemaal aan vast te houden. Vandaar dat ik hoop dat we dit toch iets meer kunnen nuanceren en ook meer in de categorie van sancties zouden kunnen brengen.

De **voorzitter**:
Dank u wel. U krijgt daar een interruptie op van de heer Brekelmans.

De heer **Brekelmans** (VVD):
Ja, ik heb daar toch een snelle vraag over aan de heer Van der Lee. Als we de vergelijking maken met conventionele oorlogsvoering, heeft Rusland – laten we dat even als voorbeeld nemen – een leger klaarstaan waarmee het het Westen zou kunnen aanvallen of bombarderen. Daar stellen wij iets tegenover. Wij zeggen namelijk: op het moment dat jullie dat doen, hebben wij een minstens net zo groot leger klaarstaan dat hetzelfde doet. In de analogie van het digitale termijn zegt Rusland mogelijk: wij hebben ingebroken in jullie systemen en wij zijn daar al jaren mee bezig; wij kunnen jullie elektriciteitsnetten of jullie ziekenhuizen platleggen. Dan zouden wij zeggen: wij niet bij jullie, want wij hebben niet een offensief programma gehad en wij hebben niet in jullie systemen gezeten. Dan is er dus sprake van een disbalans en dan staan landen met een agressief cyberprogramma, zoals Rusland en China, sterker. Vindt GroenLinks dan ook niet dat wij, als wij waarnemen dat zij dat doen, daar ook iets offensiefs tegenover moeten stellen? Anders staan we niet met 1–0 achter, maar met 10–0.

De heer **Van der Lee** (GroenLinks):
Ik denk dat de nuance die ik probeer over te brengen, nog niet helemaal is geland bij de VVD. Voor ons is dit echt een grote prioriteit. Wij hebben veel discussie gehad over investeringen in Defensie. Wij hebben altijd benadrukt dat wij meer geld willen voor cybersecurity. Dat is de oorlog van de toekomst, helaas. Daar moeten we onze capaciteiten dus voor versterken. Dat betekent ook dat je je daarvoor moet wapenen. De vraag is wel wanneer je bepaalde cyberwapens inzet. Ik vind dat er dan echt wel een verschil is tussen het inzetten van specifieke sancties op specifieke acties en een bredere offensieve capaciteit die je ontwikkelt. Daar kan ik me als afschrikking nog wat bij voorstellen, maar het inzetten daarvan moet je niet zomaar doen. Dat moet je ook niet uit handen geven. Hier wordt dat moeilijk, zeker vanuit het perspectief van de Kamer. We weten heel vaak niet de details van specifieke aanvallen en de attributie is een ingewikkeld probleem. Als je dan te snel overgaat tot een grootschalige offensieve cyberreactie, kun je behoorlijk wat losmaken. Daar zit mijn punt van zorg. Ik zou dat toch wat meer willen inkaderen en dus niet een te snelle vrijbrief hiervoor willen geven. Ik deel wel het belang van het versterken van onze capaciteiten op dit punt, maar ik kan me voorstellen dat je specifieke digitale sancties kunt leggen op bepaalde activiteiten die aantoonbaar vanuit een statelijke actor komen.

De **voorzitter**:
Aanvullend, de heer Brekelmans.

De heer **Brekelmans** (VVD):
Dit voert te ver voor deze tweede ronde, maar dan is de vraag natuurlijk wat je onder «sancties» verstaat. Op het moment dat een land in staat is om onze vitale infrastructuur plat te leggen, denk ik dat wat wij typisch onder «sancties» verstaan – namelijk het bevriezen van tegoeden en dat soort dingen – niet in evenwicht is. Maar ik hoor de heer Van der Lee ook zeggen dat het wel ter afschrikking moet kunnen. Het punt van afschrikking op het cyberdomein is echter dat afschrikking pas geloofwaardig is als je in de systemen van een ander land zit. Als een land als Rusland zegt dat het onze vitale infrastructuur lam kan leggen en als wij dat op een geloofwaardige manier wederzijds willen kunnen zeggen, moet je al in dat systeem zitten. Dat is offensief. Dat wil niet zeggen dat je die vitale infrastructuur platlegt, maar om überhaupt een geloofwaardige deterrence te hebben, zul je al offensieve activiteiten moeten onder-

nemen. Ik hoorde de heer Van der Lee zeggen dat hij voor die afschrikking openstaat. Betekent dat ook dat hij openstaat voor dat soort offensieve activiteiten, in beperkte mate, om dat voor elkaar te krijgen?

De **voorzitter**:
Dat is de concrete vraag.

De heer **Van der Lee** (GroenLinks):
Ik denk dat we elkaar in die zin kunnen naderen. Er zijn ook berichten geweest over het feit dat een Nederlands team in staat is geweest om in te breken bij een Russisch team, dat weer een rol heeft gespeeld bij informatie die een rol speelde in de Amerikaanse verkiezingen. Als je een sanctie of een digitale offensieve actie richt op het team dat in een statelijke actor verantwoordelijk is voor het platleggen van infrastructuur hier, kan ik daar ver in meegaan. Maar als antwoord zelf een actie ondernemen om de infrastructuur in die staat lam te leggen, vind ik een escalatie waar ik niet zomaar voor zou willen kiezen. Daar zit misschien toch echt nog een verschil.

De **voorzitter**:
Was u klaar met uw tweede termijn?

De heer **Van der Lee** (GroenLinks):
Ja.

De **voorzitter**:
Dank u wel. De laatste in de tweede termijn is mevrouw Mulder, CDA.

Mevrouw **Agnes Mulder** (CDA):
Voorzitter, dank. U vroeg net: is het antwoord voldoende? Toen zei ik: nou, nee. Maar dat heeft ook wel een beetje te maken met het dilemma dat hier natuurlijk voorligt: je kan hier niet alles zeggen. Dat snap ik ook wel weer, maar dat geeft bij mij wel een onbevredigend gevoel. Ik had gevraagd hoe het precies zit: wanneer neem je die acties, hoe doe je dat en hoe weten wij ook als Kamer wat daar speelt? Daarvan getuigt het hele debat van zojuist tussen de collega's. Dat is natuurlijk precies waar het om draait. Daarom voelt het voor mij ook niet zo dat ik weet waar we exact staan. Ik had daarbij geschreven: «Hoe is dat nu gegaan? Defensief of offensief?» Misschien hebben we ook al wel offensieve dingen gedaan; geen idee. Dat is gewoon de worsteling die ik hiermee heb, maar ik denk dat we het plan dat rond of na de zomer komt, maar even moeten afwachten en dat we dit gesprek dan maar verder gaan voeren. Ik vind dat we best wel wat offensiever mogen zijn op het moment dat het gaat om onze vitale delen en kritische infrastructuur, zoals de energiesector maar ook bruggen, sluizen en alles wat je maar kunt bedenken wat ons in een positie zou brengen die ons heel kwetsbaar maakt. Maar dat wordt ongetwijfeld al meegenomen in dit hele geheel.

De **voorzitter**:
Dank u wel. Ik kijk even naar mijn rechterzijde. Kunt u direct antwoorden?

Minister **Hoekstra**:
Ja, voorzitter, laat ik dat doen.

De **voorzitter**:
Gaat uw gang.

Minister **Hoekstra**:
Voorzitter. Ik zal een paar specifieke vragen beantwoorden, maar volgens mij is er in ieder geval één rode draad door de laatste opmerking van

mevrouw Mulder en ook door wat de heer Sjoerdsma en de heer Brekelmans eerder zeiden. Mijn indruk is dat het nuttig zou zijn, zou de Kamer daar behoefte aan hebben, om rondom de strategie ook een technische briefing te doen. Dat moet dan misschien een technische briefing zijn zonder telefoons, als ik het zo huiselijk mag zeggen. Ik kan me veel bij de Kamer levende vragen immers gewoon heel goed voorstellen. Het is aan de Kamer of men daar behoefte aan heeft. Dan moeten we daar een modus voor verzinnen, maar ik kan me het ongemak voorstellen als je vrij veel dingen in de krant leest en tegelijkertijd niet al die dingen tot in elke mate van detail kunt bediscussiëren. Die suggestie zou ik dus willen doen. Het is verder aan de Kamer of men daarvan gebruik wil maken en of dat dan vooral de leden zijn van deze commissie, van de commissie voor JenV of van de commissie voor BZK. Dat laat ik dan allemaal helemaal aan de Kamer, maar ik wil die suggestie in ieder geval wel doen. Er zijn volgens mij een heleboel dingen die we vandaag echt goed hebben kunnen bespreken, maar er zijn paletstukjes waarover het ongemakkelijk converseren is. Dat wilde ik dus in algemene zin zeggen.
Voorzitter. Ik heb de heer Brekelmans goed verstaan over hoe hoog dit onderwerp op de lijst moet in de diplomatieke en de bilaterale contacten. Dat begrijp ik van zijn kant heel goed. Ik zou daar overigens aan willen toevoegen dat we dat wat mij betreft niet uitsluitend op één land zouden moeten doen. We zouden het juist ook vanuit Europa moeten willen veralgemeniseren. Het klopt dat er nu drie, vier – sommigen zeggen vijf – statelijke actoren zijn die we vrij hoog op het lijstje hebben staan en andere niet. Dat soort dingen, is mijn waarneming, zijn ook nooit statisch. Ook de volgorde verandert nog weleens. Ik ben het dus zeer met de heer Brekelmans eens, maar ik zou het willen veralgemeniseren. Volgens mij is hij daar ook helemaal niet op tegen.
De heer Sjoerdsma maakt nog heel terecht een punt van de bredere kwetsbaarheid. Mevrouw Mulder verwees net ook naar de bruggen. Toen ik jong was, kon je je dat niet voorstellen. Als je in Friesland ging varen, had je het idee dat elke brug openging omdat er een brugwachter aan dat ding zat te draaien. Dan stopte je 50 cent in een potje. Voor een deel van de bruggen was dat ook toen al anders. Tegenwoordig zit er in heel veel van onze infrastructuur een digitale component. Datzelfde geldt voor ziekenhuizen en alles op het veiligheidsdomein. Wie daar toegang toe heeft, heeft echt de sleutel in handen tot het potentieel lamleggen van de Nederlandse samenleving. Ik ben het dus zeer eens met wat de heer Sjoerdsma zei ten aanzien van de kwetsbaarheid. Dat maakt het domein des te belangrijker.
De heer Sjoerdsma vroeg ook hoe we hebben gereageerd op de schendingen van het normatieve kader. Heel eerlijk, daar zijn een paar voorbeelden van, maar dat is ook nog behoorlijk beperkt. We hebben in '21 een belangrijke rol gespeeld om ervoor te zorgen dat de EU, de NAVO en ook individuele landen zich expliciet hebben uitgesproken tegen die cyberaanvallen vanaf Chinees grondgebied. Dat waren die zogenaamde Microsoft Exchange Server-hack en die hele desinformatieoperatie van Ghostwriter. Daar hebben we echt een voortrekkersrol in gespeeld. We hebben daar boven water, als ik het zo mag formuleren, op gereageerd. We hebben eenzelfde type rol gespeeld bij de recente aanvallen in Oekraïne. Daarin hebben de sg van de NAVO en de Hoge Vertegenwoordiger van de EU een rol gespeeld. Tegelijkertijd zou ik me zomaar kunnen voorstellen dat als ik deze twee voorbeelden geef, de Kamer zegt: dat zijn mooie voorbeelden, maar de lijst was toch tientallen of misschien wel honderden gevallen lang; moet daar dus niet meer op gebeuren? Dat zou ik dan eerlijk gezegd ook met de Kamer eens zijn. Ik zal me ook inspannen om daar nog meer te doen.
De heer Sjoerdsma had nog die vraag over Rotterdam. Met zijn goedvinden wil ik daar even krijgsberaad op houden. Daar kom ik

schriftelijk op terug. Dan overleg ik met de collega's in het kabinet daarover.
Richting de heer Van der Lee zou ik de hoop willen uitspreken dat ik toch ook een belangrijk deel van zijn vragen wel gewoon in dit AO heb beantwoord. Hij zat mij natuurlijk ongelofelijk te plagen, maar dat ga ik allemaal verwerken de rest van deze dag. Ik hoop dat ik een deel van zijn vragen toch echt heb beantwoord. En ja, een deel van de vragen heeft ook te maken met de strategie. Die moeten dus ook in die strategie beantwoord worden. Nogmaals, ik denk dat een technische briefing zou kunnen helpen. Dat is een toezegging richting mevrouw Mulder, maar daarmee ook richting de hele Kamer.
Ik heb nog de behoefte om één ding toe te voegen aan daar waar de heer Van der Lee mild kritisch was over de offensieve opmerkingen van de heer Brekelmans. Wat hier altijd een uitgangspunt bij moet zijn, is proportionaliteit. Dat ben ik eens met de heer Van der Lee. Wat ik met de heer Brekelmans eens ben, is dat je onverstandig bezig bent als je niet zorgt voor in ieder geval het vermogen tot equality of arms. Op het moment dat iemand de hele bestekla opentrekt en die in je rug of in je buik probeert te steken, is het wel wat ongemakkelijk als je daar maar heel beperkt op kan reageren. Is dat dan altijd offensief in de betekenis van «we doen exact hetzelfde terug»? Ik denk dat niet per se. Dus daarom snap ik ook wel weer de nuance die de heer Van der Lee maakt, want je kan diplomatiek dingen doen, je kan qua sancties dingen doen. Je kan dus wel degelijk dingen doen, ook op het terrein van sancties of vervolging, die wel degelijk een afschrikwekkende werking hebben. En toch, als je ziet – daarom was ik dat wel echt met de heer Brekelmans eens – hoe lastig dat gaat, als je ziet hoe lastig de attributie plaatsvindt en als je ziet hoe vaak ook niet-statelijke actoren, waarbij je natuurlijk toch vaak het vermoeden hebt dat er wel een statelijke actor indirect achter schuilgaat, erbij betrokken zijn, vind ik gewoon dat wij ons arsenaal beter op orde moeten brengen. Ik denk niet dat we dat af hebben richting de strategie. Dat zeg ik erbij om de verwachtingen te managen. Ik vind wel dat we daarin een richting moeten aangeven. Vervolgens zullen we de onderdelen van de strategie de komende jaren moeten vervolmaken. Het woord «offensief» zullen we dan definiëren, maar dat zal niet alleen maar... Nogmaals, de heer Van der Lee heeft gelijk ten aanzien van de proportionaliteit, maar de heer Brekelmans heeft ook gelijk dat je dat niet alleen maar kan afdoen met sancties.

De **voorzitter**:
De heer Van der Lee, kort.

De heer **Van der Lee** (GroenLinks):
Dank voor dit antwoord. Mijn pleidooi was ook wel om te kijken in hoeverre je digitale middelen als sanctie zou kunnen inzetten. Dat kan ook zijn: een reactie op aanvallen van hackteams van de statelijke actor waar het om gaat. Juist omdat de attributie zo complex is, is mijn zorg wel dat het ook vanuit de disruptieve strategieën van statelijke actoren mogelijk is om een conflict te creëren tussen het westen en een andere statelijke actor dan de daadwerkelijke dader. Daarom zou ik wel nog extra veel waarborgen willen hebben bij het daadwerkelijk offensief inzetten van de capaciteit die wij volgens mij ook moeten ontwikkelen.

Minister **Hoekstra**:
Mijn donkerbruine vermoeden is dat het kabinet en de Kamer het sowieso heel erg eens zijn over de waarborgen. Vervolgens moet je wel met elkaar articuleren welk type reactie op welk type aanval past. Ja, dat moet proportioneel zijn, maar het lijkt me verstandig dat je dat gevecht niet moet voeren met anderhalve hand op de rug.

De **voorzitter**:
Dank u wel. Dit was uw tweede termijn.

Minister **Hoekstra**:
Dank u wel, voorzitter. Ik heb ervan genoten.

De **voorzitter**:
Hartstikke goed. Dan komen we tot een afronding.
– De Minister komt schriftelijk terug op de vraag van de heer Sjoerdsma over de aanval op de haven van Rotterdam en andere havens.

U gaat de krijgsraad daarvoor raadplegen. Ik krijg daar graag een datum bij. O, u heeft het over «krijgsberaad». Wanneer kunnen we de schriftelijke reactie verwachten?

Minister **Hoekstra**:
Deze week en volgende week zijn korte weken, maar ik probeer de reactie eind volgende week bij de Kamer te hebben of ik fiets die in een brief die ik toch nog moet schrijven.

De **voorzitter**:
Hartstikke goed, want ik houd niet van open eindjes. Dan is er nog een toezegging.
– De Kamer ontvangt de geïntegreerde cyberstrategie kort na het zomerreces. Daarin gaat de Minister in ieder geval nader in op sancties, inclusief digitale sancties, oefeningen en simulaties, attributie van aanvallen door statelijke en niet-statelijke actoren, het element van privacy en het al dan niet voeren van een offensiever cyberbeleid.

Daarnaast zag ik instemmend geknik toen u een technische briefing voorstelde. Ik denk dat ik even naar de griffier moet kijken om een voorstel daarover te schrijven voor de procedurevergadering. Dan kunnen we daarover besluiten.
Heb ik iets gemist, collega's? Dat is niet het geval. Dan constateer ik dat er geen tweeminutendebat is aangevraagd en sluit ik deze vergadering.
Dank u wel.

Sluiting 17.17 uur.