Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 280 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafrecht BES, het Wetboek van Strafvordering en het Wetboek van Strafvordering BES in verband met de uitbreiding van de strafbaarheid voor schadetoebrengende gedragingen ten behoeve van een buitenlandse mogendheid (uitbreiding strafbaarheid spionageactiviteiten)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 23 mei 2023

I. ALGEMEEN

Ik heb met veel belangstelling kennisgenomen van het verslag van de vaste commissie voor Justitie en Veiligheid. Het verheugt mij dat meerdere fracties met belangstelling en interesse hebben kennisgenomen van het wetsvoorstel. Ik dank de leden van de verschillende fracties voor de door hen gestelde vragen, die mij in de gelegenheid stellen een aantal begrippen in de voorgestelde strafbaarstelling te verhelderen en het wetsvoorstel op onderdelen van een nadere onderbouwing te voorzien. Met de beantwoording van de vragen hoop ik ook de bedenkingen van de leden van de fracties die nog niet op alle punten van het wetsvoorstel zijn overtuigd, alsnog te kunnen wegnemen. Bij de beantwoording is de indeling van het verslag zoveel mogelijk gevolgd.

De leden van de VVD-fractie hebben met veel belangstelling kennisgenomen van het wetsvoorstel en verwelkomen de zelfstandige strafbaarstelling van spionageactiviteiten. Zij brengen in herinnering dat het wetsvoorstel voortvloeit uit het coalitieakkoord. Deze leden wijzen erop dat in deze tijden van hybride dreigingen en met de komst van de digitalisering de mogelijkheden voor het ontplooien van spionageactiviteiten zijn toegenomen. Verder geven deze leden aan dat spionage vele verschillende verschijningsvormen kent en dat het daarom belangrijk is dat strafbaarstellingen toekomstbestendig en techniekneutraal worden geformuleerd.

De leden van de D66-fractie hebben met interesse kennisgenomen van het wetsvoorstel. Deze leden erkennen met de regering de noodzaak om cruciale belangen, zoals de nationale veiligheid en het functioneren van de democratische en internationale rechtsorde te beschermen tegen spionageactiviteiten, met inachtneming van de maatschappelijke ontwikkelingen en de toenemende geopolitieke spanningen. De leden van deze fractie onderschrijven dan ook de intentie die ten grondslag ligt aan de strafbaarheid van spionageactiviteiten.

kst-36280-6
ISSN 0921 - 7371
's-Gravenhage 2023

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden zien het belang van effectieve en adequate strafbaarstelling van verschillende vormen van spionage. Zij geven aan de uitbreiding van de strafbaarheid een stap in de goede richting te vinden om dergelijke strafbare handelingen beter aan te kunnen pakken.

De leden van de SP-fractie hebben het wetsvoorstel gelezen. Zij geven aan te begrijpen dat spionage door en voor buitenlandse mogendheden een risico is en dat dit aangepakt dient te worden, zeker nu via de digitale weg de informatie die verzameld kan worden makkelijker toegankelijk en belangrijker is. Deze leden benadrukken echter dat dit omgekeerd ook het geval is en dat voorkomen moet worden dat onnodig te veel informatie over eigen inwoners wordt verzameld en bewaard. Ik hoop met de beantwoording van de vragen van deze leden de zorgen die bij hen op dit punt nog leven weg te kunnen nemen en hen ervan te overtuigen dat in dit wetsvoorstel een juiste balans is gevonden tussen de verschillende te beschermen belangen. In de richting van deze leden wil ik op deze plaats graag alvast verduidelijken dat het niet de bedoeling van dit wetsvoorstel is om het mogelijk te maken onnodig informatie over inwoners te verzamelen en te bewaren. Dit wetsvoorstel biedt daarvoor ook geen grondslag. In de strafbaarstelling is gezocht naar een zodanige afbakening dat alleen personen die – ten behoeve van een buitenlandse mogendheid – opzettelijk gevaar in het leven roepen voor een aantal, specifiek aangeduide, zwaarwegende Nederlandse belangen, daarvoor strafrechtelijk ter verantwoording kunnen worden geroepen. Er worden geen nieuwe bevoegdheden geïntroduceerd waarmee gegevens kunnen worden verzameld.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het voorstel. Volgens deze leden schiet de bestaande strafbaarstelling wellicht te kort om de huidige vormen van spionage tegen te kunnen gaan. Met de beantwoording van de vragen van deze leden hoop ik tegemoet te komen aan de behoefte die deze leden nog hebben aan een nadere duiding van een aantal begrippen.

1. Maatschappelijke ontwikkelingen

De leden van de VVD-fractie onderschrijven de constatering dat digitalisering en globalisering in toenemende mate bijdragen aan nieuwe kwetsbaarheden, in het bijzonder op het gebied van spionageactiviteiten met behulp van technische en digitale middelen. Deze leden verwijzen naar het Cybersecuritybeeld Nederland 2022 (hierna: CSBN 2022) en het Dreigingsbeeld Statelijke Actoren 2 (hierna: DBSA 2) en geven aan dat zij zich zorgen maken om risico's voor zowel de nationale als de economische veiligheid. Daarom vragen deze leden aandacht voor preventieve maatregelen om technologie beter te beschermen. Zij vragen in het bijzonder aandacht voor het belang van snelle en volwaardige uitwisseling van dreigingsinformatie tussen overheidsinstellingen en (vitale) bedrijven en vragen wat de inzet van de regering op dit punt is. Graag beantwoord ik de vragen die deze leden hierover stellen als volgt.
Omdat digitale systemen het «zenuwstelsel» van onze maatschappij vormen, maakt het kabinet zich hard voor de versterking van onze digitale weerbaarheid via de verschillende ambities die omschreven staan in de Nederlandse Cybersecurity Strategie, waaronder het nog sneller en efficiënter delen van cybersecurity informatie met private partners door verschillende beleidsacties (Kamerstukken II 2022/2023 26 643, nr. 925). Een concreet voorbeeld hiervan is de ontwikkeling van een publiek-privaat samenwerkingsplatform onder het Programma Cyclotron dat tevens als actie is opgenomen in het actieplan van de NLCS. Via dit platform zijn

publieke en private partners in staat om informatie rondom (dreigende) cyberincidenten sneller en gerichter via een vertrouwde digitale omgeving onderling te delen.
In het huidige cybersecuritystelsel is de primaire taak van het Nationaal Cybersecurity Centrum (NCSC) op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) het verlenen van bijstand aan vitale aanbieders en rijksoverheidsorganisaties (doelgroeporganisaties) bij digitale dreigingen en incidenten. Dit om het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen bij de doelgroeporganisaties te voorkomen of te beperken. Het uitvallen van die systemen bij deze organisaties kan immers maatschappelijke gevolgen hebben. Zo zullen de maatschappelijke gevolgen groot zijn als de dienstverlening van een drinkwaterbedrijf uitvalt. Het NCSC deelt daarom zo snel en volledig mogelijk de dreigings- en incidentinformatie direct met de doelgroeporganisaties. Daarnaast deelt het NCSC informatie met schakelorganisaties, zoals het Digital Trust Center (DTC), waarmee ook bedrijven buiten vitale sectoren worden voorzien van informatie. Al deze schakelorganisaties vormen samen het landelijk dekkend stelsel (LDS) waarbinnen dreigings- en incidentinformatie gedeeld kan worden met organisaties en bedrijven.
Per 1 december 2022 is de Wbni gewijzigd om belangrijke wettelijke beperkingen voor het delen van informatie weg te nemen (Stb. 2022, 441). Door deze wijziging kan het NCSC dreigings- en incidentinformatie in uitzonderlijke gevallen ook rechtstreeks verstrekken aan organisaties die niet binnen de doelgroep van het NCSC vallen of waarvoor geen schakelorganisaties zijn. Voorbeelden van dergelijke organisaties zijn politieke partijen en veiligheidsregio's. Deze wetswijziging regelt ook dat meer dreigings- en incidentinformatie kan worden gedeeld met zogeheten OKTT's (schakelorganisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten). Daarnaast is Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS2-richtlijn) in werking getreden. Op dit moment wordt implementatiewetgeving voorbereid. Daarnaast ligt momenteel het wetsvoorstel bevordering digitale weerbaarheid bedrijven voor behandeling in de Tweede Kamer. Dit wetsvoorstel legt de taken en bevoegdheden van de Minister van Economische Zaken vast op het terrein van digitale weerbaarheid van het niet-vitale bedrijfsleven, zoals het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties.
Op het bredere thema van economische veiligheid wordt op dit moment bovendien een ondernemersloket economische veiligheid ingericht bij de Rijksdienst voor Ondernemend Nederland (RVO). Dit loket wordt op 31 mei 2023 geopend en zal voorzien in informatie en advies op het gebied van economische veiligheid. Het loket zal zich met name richten op bedrijven met een verhoogd risico zoals het kennisintensieve midden- en kleinbedrijf in de hightech maakindustrie.

De leden van de CDA-fractie constateren dat spionage niet alleen voorkomt bij overheden, maar steeds vaker ook bij (grote) bedrijven, onderwijsinstellingen en particuliere instellingen. Daarnaast wijzen deze leden op gevallen waarin buitenlandse overheden burgers afkomstig uit dat land in Nederland lastigvallen, intimideren en bedreigen. De leden van deze fractie vragen op welke manier deze personen, bedrijven en instellingen worden beschermd met dit wetsvoorstel.
Het antwoord hierop luidt dat met de voorgestelde strafbaarstelling het verrichten van schadetoebrengende handelingen, wetende dat daarvan

gevaar is te duchten voor een aantal in de bepaling opgesomde zwaarwegende belangen, strafbaar wordt gesteld. Voor die belangen kan ook gevaar ontstaan wanneer spionageactiviteiten zich richten tegen bedrijven of kennisinstellingen, bijvoorbeeld als het gaat om bedrijven of instellingen die betrokken zijn bij de vitale infrastructuur of die hoogwaardige technologieën gebruiken of ontwikkelen. Ook de veiligheid van een of meer personen is als belang opgenomen. Dit betekent dat als schadetoebrengende handelingen – waaronder intimidatie – zich richten tegen bepaalde personen dit in voorkomende gevallen valt onder de nieuwe strafbaarstelling. Dit is ook strafbaar op grond van de voorgestelde bepaling als niet de persoon die wordt lastiggevallen in gevaar wordt gebracht, maar een derde. Gedacht kan worden aan de situatie waarin iemand wordt geïntimideerd om informatie over een derde te verstrekken.

De leden van de CDA-fractie vragen op welke manier spionageactiviteiten kunnen worden herkend en bewezen die zich richten op informatie die niet staats- of bedrijfsgeheim is. Zij noemen als voorbeeld informatie waarmee kan worden ingespeeld op maatschappelijke ontwikkelingen of waarmee besluitvorming kan worden beïnvloed. Deze leden vragen welke voorwaarden worden gesteld aan de strafbaarheid van deze gedraging. Op grond van het eerste lid, onder 2°, van de voorgestelde strafbepaling is strafbaar het (onmiddellijk of middellijk) verstrekken van inlichtingen, voorwerpen of gegevens aan een buitenlandse mogendheid, wetende dat daarvan gevaar is te duchten voor een of meerdere van de in de bepaling opgesomde zwaarwegende belangen. Of de gedraging strafbaar is, is dus mede afhankelijk van de aard van de informatie die aan de buitenlandse mogendheid wordt verstrekt. Verderop in deze nota naar aanleiding van het verslag – in paragraaf 3 – zal ik, naar aanleiding van een vraag van de leden van de PvdA-fractie, enkele voorbeelden geven van informatie waarover het kan gaan. De informatie hoeft niet rechtstreeks aan de buitenlandse mogendheid te worden overgedragen. Doordat ook het «middellijk» verstrekken van informatie strafbaar is gesteld, kan ook het doorgeven van informatie via tussenpersonen strafbaar zijn. Het verstrekken van de informatie die een gevaar in het leven roept voor de in de aanhef van de bepaling opgesomde belangen levert op zichzelf een schadetoebrengende gedraging op; er hoeft dus niet daarnaast of daaraan voorafgaand een andere schadetoebrengende gedraging te hebben plaatsgevonden. Wel moet bewezen zijn dat de betrokkene er opzet op had het gevaar in het leven te roepen en opzet had op de verstrekking – al dan niet via tussenpersonen – aan de buitenlandse mogendheid. Op dit opzetvereiste wordt nader ingegaan in paragraaf 5.1 van deze nota naar aanleiding van het verslag in reactie op vragen van de leden van de VVD-fractie. Graag verwijs ik deze leden kortheidshalve naar dat antwoord.

De leden van de CDA-fractie wijzen erop dat spionageactiviteiten heimelijk plaatsvinden en soms lastig te ontdekken zijn. Zij stellen in het licht daarvan enkele vragen over hoe in de strafrechtspraktijk wordt omgegaan met de bewijsbaarheid van spionageactiviteiten.
Ik antwoord hierop dat in de praktijk in de regel een ambtsbericht van de AIVD of de MIVD aan de basis zal liggen van een opsporingsonderzoek naar gedragingen die samenhangen met spionage. Het is ook mogelijk dat aangifte wordt gedaan door bijvoorbeeld een getroffen bedrijf of persoon. Daarnaast kunnen politie en openbaar ministerie in een strafrechtelijk onderzoek naar andere feiten op informatie stuiten die duidt op spionageactiviteiten. Ook naar aanleiding van dergelijke signalen kan een opsporingsonderzoek worden gestart. Doordat is gekozen voor een strafmaximum van acht jaar gevangenisstraf, is daarbij een aantal aanvullende opsporingsbevoegdheden beschikbaar, die relevant kunnen zijn bij spionageonderzoeken – in het bijzonder de bevoegdheden opgenomen in

de artikelen 126l, tweede lid, (opnemen vertrouwelijke communicatie in een woning) en 126nba, eerste lid, onderdelen d en e, Sv (onderzoek in een geautomatiseerd werk met het oog op het vastleggen of ontoegankelijk maken van gegevens). Verder is het voorgestelde artikel 98d Sr toegevoegd aan artikel 551 Sv (zie artikel III van het wetsvoorstel) waardoor een aantal verruimde bevoegdheden ter beschikking komt, waaronder de bevoegdheid voor opsporingsambtenaren om zich toegang te verschaffen tot alle plaatsen waar redelijkerwijs vermoed kan worden dat dit strafbare feit wordt begaan. Tegen deze achtergrond is het kabinet van oordeel dat de opsporingsautoriteiten over voldoende middelen kunnen beschikken om spionageactiviteiten bloot te leggen. Uiteraard blijft het mogelijk dat bepaalde spionageactiviteiten – door de heimelijkheid waarmee dergelijke activiteiten gepaard gaan – niet worden ontdekt of dat niet alle betrokkenen kunnen worden opgespoord. Dat neemt niet weg dat door de uitbreiding van de strafbaarheid meer mogelijkheden dan voorheen beschikbaar komen om te reageren op spionageactiviteiten.

De leden van de PvdA-fractie vragen om enkele voorbeelden van niet-staatsgeheime informatie die kan dienen als voorkennis voor staten om bijvoorbeeld in te kunnen spelen op politieke of maatschappelijke ontwikkelingen, om kwetsbaarheden in Nederlandse systemen of processen te identificeren, om besluitvorming te beïnvloeden of om economisch voordeel te behalen.
Graag voldoe ik aan dit verzoek. Hierbij kan bijvoorbeeld worden gedacht aan politieke inlichtingen en informatie over de werkwijze en inrichting van bepaalde (internationale) organisaties, voorgenomen standpunten van lidstaten in internationale overleggen, over gedragingen van (hoge) ambtenaren, ambtsdragers en volksvertegenwoordigers, over (vertrouwelijke) communicatie rondom ambtelijke en politieke besluitvorming en uitvoerende werkzaamheden, over sociaal politieke-verhoudingen, over (strategische) agenda's, over processen en over (economische) kwetsbaarheden, zoals strategische afhankelijkheden. In paragraaf 3 zal ik in reactie op een vraag van deze leden nog enkele concrete voorbeelden van informatie geven die gevaar in het leven kan roepen voor de in de voorgestelde bepaling opgesomde belangen.

De leden van de PvdA-fractie geven aan de mening te delen dat het ongewenst is als landen met een diasporagemeenschap in Nederland leden van die gemeenschap mobiliseren om tegenstanders en critici de mond te snoeren. Deze leden wijzen erop dat dit niet per se tot spionageactiviteiten hoeft te leiden, maar dat dit ook kan dienen om oppositie tegen het regime in dat land de kop in te drukken. Zij vragen in hoeverre dit dan toch strafbaar wordt op grond van dit wetsvoorstel.
Op grond van de voorgestelde strafbaarstelling, zo luidt het antwoord op deze vraag, wordt het strafbaar om «schadetoebrengende handelingen» te verrichten, wetende dat daarvan gevaar is te duchten voor een of meerdere van de in de wet opgesomde belangen, voor zover die gedragingen in heimelijke betrokkenheid met en ten behoeve van een buitenlandse mogendheid zijn verricht. Deze gedragingen worden in de memorie van toelichting aangeduid als «spionageactiviteiten». Het gaat dus om een ruimere categorie van activiteiten dan «klassieke spionage» (het vergaren van (staatsgeheime) informatie). Een van de in de wet genoemde belangen is de veiligheid van personen. Personen die – ten behoeve van een buitenlandse mogendheid – anderen de mond (proberen te) snoeren kunnen in voorkomende gevallen dus strafbaar zijn op grond van de voorgestelde bepaling.
Onder «de veiligheid van de staat», zo beantwoord ik een met het voorgaande samenhangende vraag, zijn de zes nationale veiligheidsbelangen begrepen, waaronder de sociale en politieke stabiliteit. Onder dit

laatste wordt verstaan het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en waarin groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtsstaat en de daarin gedeelde waarden. De verstoring hiervan wordt als een gevaar voor de veiligheid van de staat aangemerkt als de sociale en politieke stabiliteit dermate in het geding is dat sprake is van (potentiële) maatschappelijke ontwrichting. Het gaat dan bijvoorbeeld om situaties waarin bevolkingsgroepen tegen elkaar op worden gezet. Of in de door deze leden genoemde gevallen waarbij sprake is van ontwrichting binnen een bepaalde (diaspora)gemeenschap ook een gevaar voor de sociale en politieke stabiliteit bestaat – en daarmee voor de veiligheid van de staat – zal afhankelijk zijn van de omstandigheden van het geval. Voor «diaspo-raspionage» zal naar verwachting met name het belang «de veiligheid van een of meer personen» gewicht in de schaal leggen. Daarbij wordt aangetekend dat de werking van dit belang niet beperkt blijft tot «diaspo-raspionage». Ook als door schadetoebrengende gedragingen gevaar in het leven wordt geroepen voor bijvoorbeeld individuele politieke dissidenten, kan dit vallen onder het bereik van de nieuwe strafbaar-stelling.

2. Adviezen

De leden van de VVD-fractie onderschrijven tot mijn genoegen het voorstel om het strafmaximum van de nieuwe strafbaarstelling ten opzichte van de consultatieversie van het wetsvoorstel te verhogen van zes naar acht jaar. Zij vragen of ik in contact wil treden met het openbaar ministerie om te bezien of de bevoegdheden opgenomen in de artikelen 126l, tweede lid, (opnemen vertrouwelijke communicatie in een woning) en 126nba, eerste lid, onderdelen d en e, Sv (onderzoek in een geautomatiseerd werk met het oog op het vastleggen of ontoegankelijk maken van gegevens) ook beschikbaar zouden moeten zijn bij concrete verdenkingen van de misdrijven opgenomen in de artikelen 98 en 98c Sr. In antwoord hierop wijs ik deze leden graag op het advies van het openbaar ministerie bij dit wetsvoorstel. Daarin brengt het openbaar ministerie over de gewenste verhoging van het strafmaximum naar acht jaar het volgende naar voren: «Weliswaar wijkt een strafbedreiging van acht jaar af van de rest van de spionage-artikelen, maar bij deze strafbare feiten is de inzet van bovengenoemde opsporingsbevoegdheden minder nodig». Het kabinet leidt daaruit af dat de wens van het openbaar ministerie om voornoemde bevoegdheden te kunnen inzetten specifiek betrekking heeft op de nieuwe strafbepaling. Ten overvloede merk ik daarbij op dat de bevoegdheid opgenomen in artikel 126nba Sv ook in het kader van een opsporingsonderzoek naar overtreding van de artikelen 98 en 98c Sr beschikbaar is. Onderzoek in een geautomatiseerd werk met het oog op de vastlegging en ontoegankelijkmaking van gegevens is op grond van artikel 126nba Sv niet alleen mogelijk bij misdrijven waarop een strafmaximum van acht jaar gevangenisstraf is gesteld, maar ook bij misdrijven die bij algemene maatregel van bestuur zijn aangewezen. In het Besluit onderzoek in een geautomatiseerd werk zijn de artikelen 98, eerste en tweede lid, en 98, eerste lid, Sr als zodanige misdrijven aangewezen.

De leden van de VVD-fractie zijn positief over het feit dat in de memorie van toelichting wordt stilgestaan bij voorlichting. Zij wijzen op het belang van goede voorlichting aan medewerkers binnen bedrijven uit de vitale infrastructuur en topsectoren, specifiek op het gebied van (digitale) spionage en het bredere thema economische veiligheid, om zo meer bewustwording en alertheid te creëren. Zij stellen een aantal vragen over

deze voorlichting, die ik graag in onderlinge samenhang als volgt beantwoord.
Er wordt algemeen voorlichtingsmateriaal over de nieuwe strafbaarstelling ontwikkeld. Hierin wordt aandacht besteed aan de doelgroepen die een grotere kans hebben met spionageactiviteiten in aanraking te komen, zoals personen in dienst van de overheid die werken met gevoelige informatie, personen in dienst van bedrijven of onderwijsinstellingen die zich bezighouden met hoogwaardige technologieën, personen in dienst van bedrijven die zich bezighouden met vitale processen en personen binnen diasporagemeenschappen. Bij de ontwikkeling van het materiaal zullen relevante organisaties betrokken worden. Te denken valt dan onder meer aan het NCSC en het DTC. Zij werken nauw op dit terrein samen en zijn voortdurend, samen met de NCTV, in gesprek over het delen van informatie binnen het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden richting de ontvangers, zoals bedrijven en organisaties, zodat die daar handelingsperspectief aan kunnen verbinden.
Er wordt bovendien zo mogelijk aangesloten op lopende trajecten, zoals bijvoorbeeld de aangekondigde communicatiecampagne in het kader van het beschermen van Nederlandse burgers tegen alle vormen van ongewenste buitenlandse inmenging (Kamerbrief van 6 april 2023, met kenmerk 2023Z06155). Op het gebied van economische veiligheid wordt, zo kwam al eerder in deze nota naar aanleiding van het verslag aan de orde, op dit moment bovendien een ondernemersloket economische veiligheid ingericht bij de RVO. Dit loket zal op hun website voorzien in voorlichtingsmateriaal en andere vormen van informatie op het brede thema van economische veiligheid, waaronder (digitale) spionage.

De leden van de SP-fractie vragen om een nadere toelichting op de wijze waarop een middenweg is gekozen tussen de adviezen over het opzetvereiste.
Een aantal adviesorganen, zo luidt het antwoord op deze vraag, heeft ervoor gepleit het opzetvereiste te laten vervallen (politie en de NVvR) dan wel een culpoze variant toe te voegen aan de strafbaarstelling (openbaar ministerie en de NVvR). Daartegenover staan een advies vanuit het bedrijfsleven waarin het uitgangspunt wordt onderschreven dat sprake moet zijn van (voorwaardelijk) opzet en het advies van de NOvA waarin wordt opgemerkt dat met de keuze voor voorwaardelijk opzet en de daarmee gepaard gaande uitleg in de memorie van toelichting dat dit opzet mede uit objectieve omstandigheden kan worden afgeleid, een «lage lat» wordt gelegd.
Het kabinet meent, deze adviezen afwegende, dat met de keuze voor (voorwaardelijk) opzet een afgewogen begrenzing van de strafrechtelijke aansprakelijkheid tot stand is gebracht. Enerzijds wordt het daarmee mogelijk om ook personen die weliswaar niet erop uit zijn geweest om gevaar in het leven te roepen voor bepaalde zwaarwegende Nederlandse belangen, maar die wel bewust de aanmerkelijke kans daarop hebben aanvaard, strafrechtelijk ter verantwoording te roepen. Anderzijds wordt met het opzetvereiste voorkomen dat de strafrechtelijke aansprakelijkheid te ruim wordt. Voorkomen moet worden – door toevoeging van een culpoze variant – dat een soort onderzoeksplicht wordt geïntroduceerd voor personen werkzaam in spionagegevoelige sectoren en/of internationaal gerichte sectoren. Het is immers geenszins de bedoeling van deze wet om aan gebruikelijk internationaal (handels)verkeer in de weg te staan, en evenmin om op dit punt een «chilling effect» te veroorzaken. Het eerdergenoemde advies vanuit het bedrijfsleven, waarin de keuze voor het opzetvereiste wordt onderschreven, weegt in deze afweging dan ook zwaar.
Of in een concreet geval sprake is van strafbare spionageactiviteiten als bedoeld in de voorgestelde nieuwe bepaling is afhankelijk van de

omstandigheden van het individuele geval. Het overtreden van (digitale) veiligheidsvereisten binnen kritieke sectoren, zoals door deze leden genoemd, kan worden aangemerkt als een «schadetoebrengende handeling» in de zin van de voorgestelde bepaling. Daarmee is echter nog niet gezegd dat ook aan de andere vereisten voor strafbaarheid is voldaan. De omstandigheid dat (digitale) veiligheidsvereisten zijn overtreden kan weliswaar bijdragen aan het bewijs van (voorwaardelijk) opzet, maar is op zichzelf niet zonder meer voldoende om opzet (zowel op het ontstaan van gevaar voor zwaarwegende Nederlandse belangen als op de begunstiging van een buitenlandse mogendheid) aan te nemen. In dit geval kan immers ook (slechts) sprake zijn van onvoorzichtigheid, waarbij bovendien geen sprake hoeft te zijn van (bewustheid bij de overtreder van) betrokkenheid van een buitenlandse mogendheid. De overige omstandigheden van het geval zullen dan ook bepalend zijn. Daarmee is overigens niet gezegd dat tegen de overtreding van belangrijke (digitale) veiligheidsvoorschriften niet opgetreden kan worden, bijvoorbeeld in arbeidsrechtelijke zin.

De leden van de PvdA-fractie verwijzen naar de gemaakte keuze om in de wettekst genoemde begrippen niet van een wettelijke definitie te voorzien. Zij memoreren dat een aantal van deze begrippen al elders in de strafwet zijn opgenomen, zoals het begrip «vitale infrastructuur». De vraag van deze leden of begrippen die op dit moment nog niet in de wet voorkomen alsnog van een wettelijke definitie worden voorzien, beantwoordt het kabinet ontkennend. Van de opgesomde belangen, komt alleen «de integriteit en exclusiviteit van hoogwaardige technologieën» op dit moment nog niet voor in de strafwetgeving. Zoals ook in het DBSA 2 is aangegeven, speelt geopolitiek een steeds dominantere rol in de wereldeconomie. Enerzijds vormen economische en de daarbij horende technologische ontwikkelingen de basis voor politieke en militaire macht. Anderzijds worden economische instrumenten door staten, en de grootmachten in het bijzonder, als machtsmiddel gebruikt om geopolitieke doelen te bereiken. Nederland hoort bij de meest ontwikkelde naties van de wereld op het gebied van economie, wetenschap en techniek en technologische ontwikkelingen staan niet stil. Dit betekent dat nieuwe technologieën kunnen ontstaan. Ook kan het belang van bepaalde technieken voor de maatschappij door maatschappelijke en technologische ontwikkelingen wijzigen. Het is daarom van belang dat juist op dit punt enige ruimte wordt gelaten aan de rechtspraktijk om aan dit begrip invulling te geven en (technologische en maatschappelijke) ontwikkelingen daarin mee te nemen. Het begrip «hoogwaardige technologie» (of «high tech») is een term is die ook in het spraakgebruik voorkomt en heeft in dat opzicht een toegankelijke en voorzienbare invulling. Daarnaast meent het kabinet dat er ook anderszins voldoende handvatten zijn om invulling aan dit begrip te geven. Zo vormt bijvoorbeeld de omstandigheid dat een technologie als «sensitief» is aangemerkt of dat er handelsbeperkingen gelden, een belangrijke aanwijzing dat sprake is van een «hoogwaardige technologie». Bovendien moet er gevaar zijn te duchten voor de «integriteit of exclusiviteit» van deze technologieën. Dat laat zien dat het in de kern gaat om technologieën die «exclusief» zijn (technologieën die niet breed beschikbaar zijn, waarop bijvoorbeeld patenten rusten of die bijvoorbeeld onder geheimhoudingsplichten vallen) of waarbij bij inbreuken op de integriteit (andere) gevaren ontstaan, bijvoorbeeld voor de economische veiligheid, de voedselveiligheid of de veiligheid van personen. In paragraaf 5.1 zal ik in reactie op vragen van deze leden nog nader ingaan op de betekenis van het begrip «hoogwaardige technologieën». Ik hoop daarmee de door deze leden nog gewenste nadere handvatten te kunnen aanreiken.

3. Bestaand beleid en huidig wettelijk kader

De leden van de CDA-fractie wijzen op de bestaande samenwerking tussen overheidsorganisaties en op de aandacht in de Nederlandse Cybersecurity Strategie voor publiek-private informatie-uitwisseling. In antwoord op hun vraag of er op dit moment knelpunten bestaan op het gebied van informatie-uitwisseling en hoe de samenwerking verloopt, verwijs ik deze leden graag naar het antwoord gegeven in paragraaf 1 over informatie-uitwisseling. Zoals daar aangegeven is de Wbni 1 december 2022 gewijzigd om belangrijke wettelijke beperkingen voor het delen van informatie weg te nemen.

De leden van deze fractie stellen verder aan de orde of voor (private) instanties die via een ambtsbericht worden geïnformeerd over spionage-activiteiten voldoende duidelijk is welke maatregelen door hen getroffen kunnen worden. Zij vragen, althans zo begrijp ik hun vraag, of het ambtsbericht zich beperkt tot het informeren van de betrokkene over de vermoedelijke spionage of ook een overzicht bevat van (mogelijk) te nemen maatregelen.
Ik antwoord hierop dat de ontvangers door middel van een ambtsbericht door de inlichtingen- en veiligheidsdiensten worden geïnformeerd over een dreiging voor de nationale veiligheid in relatie tot een persoon of organisatie. Daardoor worden zij in staat gesteld om te handelen. Het is niet aan de diensten om de ontvanger te wijzen op de maatregelen die de ontvanger zou kunnen treffen. Wel wordt, alvorens een ambtsbericht wordt uitgebracht, een inschatting gemaakt van het handelingsperspectief van de ontvanger. De ambtsberichten van de diensten zijn gebaseerd op feiten en omstandigheden uit een bepaalde periode van onderzoek. Daarnaast bevatten ambtsberichten een betrouwbaarheidsaanduiding bij de verstrekte informatie zodat het voor de ontvanger mogelijk is de gegevens te waarderen en in te schatten. Welke conclusies aan de feiten moeten worden verbonden is aan de ontvanger. Dat neemt niet weg dat de diensten de ontvangers in zijn algemeenheid kunnen adviseren of toelichten wat een ambtsbericht betekent. Een ontvanger die niet gewend is met dergelijke berichten om te gaan, weet vaak niet dat het ambtsbericht gebruikt kan worden om maatregelen te treffen. Om die reden wordt een ambtsbericht in voorkomende gevallen overgedragen via persoonlijk contact waarbij een toelichting kan worden gegeven. Los van het al dan niet te verstrekken ambtsbericht en eventuele maatregelen te nemen op de persoon of organisatie waar een ambtsbericht op ziet, kan in voorkomende gevallen een (aanvullend) beveiligingsadvies door de diensten worden verstrekt om een dreiging te mitigeren, dan wel de weerbaarheid te versterken.

De leden van de PvdA-fractie wijzen op de passage in de memorie van toelichting waarin staat dat er situaties denkbaar zijn waarin degene die informatie verstrekt aan een buitenlandse mogendheid daarover rechtmatig beschikt en die informatie niet staats- of bedrijfsgeheim is. Deze leden vragen aan welke situaties daarbij gedacht kan worden en waarom die situaties strafbaar zouden moeten zijn. Zij willen weten hoe door dergelijke informatie de veiligheid in gevaar kan worden gebracht en belangen kunnen worden geschaad. Zij vragen wat «gevoelige (persoons-)informatie» is in dit verband.
Centraal in de nieuwe strafbaarstelling – voor zover deze ziet op het verstrekken van gegevens aan een buitenlandse mogendheid – staat dat het gaat om informatie op grond waarvan gevaar kan ontstaan voor de in de strafbepaling opgenomen zwaarwegende belangen. Dat wil zeggen dat het gaat om informatie die de veiligheid van de staat, van zijn bondgenoten of van een volkenrechtelijke organisatie, de vitale infrastructuur, de integriteit en exclusiviteit van hoogwaardige technologieën of de

veiligheid van een of meer personen in gevaar kan brengen. Met de term «gevoelige informatie» in de memorie van toelichting wordt dus op dergelijke informatie gedoeld.
Gevaar voor voornoemde belangen kan niet alleen ontstaan als gevolg van het delen van (staats- of bedrijfs)geheime informatie met een buitenlandse mogendheid. Informatievergaring via spionage heeft vaak als doel de eigen economie, krijgsmacht en diplomatie te versterken. Buitenlandse inlichtingen- en veiligheidsdiensten zijn om die reden niet alleen geïnteresseerd in het verkrijgen van (separate) staatsgeheimen, maar willen vaak een totaalbeeld van de politieke, militaire, wetenschappelijke, intellectuele en morele kracht van een doelstaat verkrijgen. Hier draagt ook niet-staatsgeheime informatie aan bij. Op die manier kunnen zwakke punten onderkend worden waarop de doelstaat benadeeld kan worden of het eigen land (op internationaal niveau) voordeel kan behalen. Informatie over een bepaalde economische sector, berichten met betrekking tot politieke besluitvorming of inzicht in sociaal-politieke verhoudingen kunnen hierbij bijvoorbeeld van nut zijn, meer dan de «klassieke» staatsgeheime informatie. De verkregen informatie kan ook worden gebruikt om dissidenten en de diaspora in Nederland in de gaten te houden of onder druk te zetten.
Een voorbeeld van niet-staatsgeheime informatie, die wel gevaar kan opleveren voor de veiligheid van de staat, diens bondgenoten of een volkenrechtelijke organisatie – dat in de memorie van toelichting al wordt aangestipt – heeft betrekking op documenten over de werkwijze en inrichting van de inlichtingenstructuur van de NAVO en verslagen van ontmoetingen van de Noord Atlantische Raad. Deze informatie werd in de betreffende casus niet aangemerkt als staatsgeheim, maar geeft wel inzicht in de werkwijze van de organisatie, standpunten van verschillende betrokkenen, de beoordeling door de NAVO van bepaalde situaties en plannen en intenties voor de toekomst. Dergelijke informatie kan worden gebruikt door opponenten, bijvoorbeeld om het besluitvormingsproces te beïnvloeden, om bondgenoten tegen elkaar uit te spelen of om in te spelen op genomen beslissingen of gemaakte plannen. Ook voor informatie over bijvoorbeeld gedragingen van (hoge) ambtenaren, ambtsdragers en volksvertegenwoordigers, communicatie rondom ambtelijke en politieke besluitvorming en uitvoerende werkzaamheden geldt dat deze informatie relevant kan zijn voor buitenlandse mogendheden, bijvoorbeeld om politieke besluitvorming te beïnvloeden, ook zonder dat deze informatie als staatsgeheim gerubriceerd is. Soortgelijke voorbeelden zijn te bedenken bij organisaties die betrokken zijn bij vitale processen of die hoogwaardige technologieën ontwikkelen.
Een voorbeeld op het gebied van economisch en technologisch terrein vormt het op heimelijke wijze verstrekken van unieke niet-staatsgeheime hoogwaardige technologische informatie (tegen betaling) door een medewerker van een hightech bedrijf in Nederland aan een vertegenwoordiger van een buitenlandse inlichtingendienst. Op deze wijze kan bijvoorbeeld waardevolle kennis van dual use goederen in handen komen van een land waar een dreiging vanuit gaat voor onze nationale veiligheid.
Ten aanzien van bedrijfsgeheime informatie wordt daarbij opgemerkt dat, voor zover het gaat om informatie die gevaar in het leven roept voor de hiervoor genoemde belangen en deze informatie aan een buitenlandse mogendheid wordt verstrekt, de hier voorgestelde strafbaarstelling het mogelijk maakt om een hogere straf op te leggen dan wanneer schending van een bedrijfsgeheim ten laste wordt gelegd overeenkomstig artikel 273 Sr. Bovendien richt deze laatste strafbepaling zich primair tot werknemers van bedrijven. Dat betekent dat andere (tussen)personen die deze gevoelige informatie bemachtigen (zonder dat zij daarvoor een misdrijf, zoals computervredebreuk, plegen) en doorgeven aan een buitenlandse mogendheid niet strafbaar zijn op grond van deze bepaling. Als het gaat

om informatie zoals hiervoor beschreven, dan zijn deze personen wel strafbaar wegens spionageactiviteiten op grond van de hier voorgestelde strafbaarstelling.
In het kader van «diasporaspionage» zal veelal geen sprake zijn van staats- of bedrijfsgeheime informatie. Bij informatie die in dit verband gedeeld wordt met buitenlandse mogendheden kan worden gedacht aan informatie over politieke of religieuze voorkeuren van personen, informatie over de identiteit van deelnemers aan demonstraties of van familieleden van bijvoorbeeld activisten.

De leden van PvdA-fractie vragen of een buitenlandse tegenhanger van de NCTV die niet-staatsgeheime informatie over Nederland vergaart om de kracht van ons land in kaart te brengen, strafbaar is op grond van de nieuwe bepaling. Deze vraag beantwoord ik ontkennend. Voor zover deze diensten in openheid en in overeenstemming met internationale rechtsregels informatie vergaren, zal er geen sprake zijn van een schadetoebrengende handeling verricht in heimelijke betrokkenheid met een buitenlandse mogendheid. Voor zover buitenlandse overheidsdiensten in openheid en in overeenstemming met internationale rechtsregels informatie vergaren, zullen zij dan ook niet onder de hier voorgestelde bepaling vallen.

4. Wetgeving in ons omringende landen

Met de leden van de VVD-fractie is het kabinet van mening dat er in een passend strafmaximum voor spionageactiviteiten moet worden voorzien, dat voldoende afschrikwekkend is en voldoende ruimte biedt voor een adequate bestraffing. Het strafmaximum is met het oog daarop ten opzichte van de consultatieversie van dit wetsvoorstel dan ook verhoogd. Voor zover deze leden verwijzen naar strafmaxima die gelden in andere landen, wordt opgemerkt dat het strafmaximum in eerste instantie is afgestemd op de maximumstraffen die in de Nederlandse strafwetgeving zijn gesteld op soortgelijke strafbare feiten. In de gekozen strafmaxima in het Wetboek van Strafrecht komt immers de onderlinge ernst van de verschillende strafbare feiten tot uitdrukking. Daarbij is in het bijzonder gekeken naar de strafmaxima die gelden voor andere misdrijven opgenomen in Titel I van het Tweede Boek van het Wetboek van Strafrecht (misdrijven tegen de veiligheid van de staat). Met het gekozen strafmaximum van acht jaar behoort het nieuwe delict tot de ernstigere misdrijven. Vergelijking van strafmaxima met andere landen vraagt om de nodige terughoudendheid. Voor de beoordeling van de onderlinge zwaarte van straffen zijn immers niet alleen het strafmaximum, maar ook de daadwerkelijk opgelegde straffen, de executiepraktijk, sanctieregimes en bijvoorbeeld mogelijkheden tot vervroegde invrijheidstelling van belang. Daarbij wordt opgemerkt dat het Nederlandse strafmaximum niet uit de pas loopt met bijvoorbeeld het strafmaximum dat in Frankrijk op grond van artikel 411–5 van de Code Pénal (CP) geldt voor het onderhouden van contacten met een buitenlandse mogendheid wanneer het aannemelijk is dat daardoor de fundamentele belangen van de staat worden geschaad. Het strafmaximum dat daarvoor in Frankrijk geldt is tien jaar gevangenisstraf. Evenmin loopt het gekozen strafmaximum van acht jaar uit de pas met het strafmaximum dat op grond van §99 van het Strafgesetzbuch (StGB) in Duitsland geldt voor het uitvoeren van spionageactiviteiten voor een geheime dienst van een buitenlandse mogendheid. Daarvoor geldt in principe een strafmaximum van vijf jaar gevangenisstraf. In bijzonder zware gevallen geldt een strafmaximum van tien jaar gevangenisstraf. Het gaat dan bijvoorbeeld om gevallen waarin geheime overheidsinformatie wordt verstrekt. Op grond van artikel 98a Sr geldt voor dit laatste in Nederland een strafmaximum van vijftien jaar. Al met al meent het kabinet dan ook dat met het gekozen strafmaximum van

acht jaar is voorzien in een doeltreffend en evenredig strafmaximum, dat helpt te voorkomen dat Nederland, ten opzichte van ons omringende landen, een aantrekkelijk doelwit voor spionageactiviteiten is.

De leden van de CDA-fractie verwijzen naar het Duitse StGB waarin ook strafbaar is gesteld het zich tegenover een buitenlandse mogendheid bereid verklaren tot spionageactiviteiten. Deze leden vragen of is overwogen een dergelijke gedraging ook in Nederland strafbaar te stellen of dat dit wellicht op grond van andere bepalingen al strafbaar is in Nederland.
De enkele bereidverklaring om spionageactiviteiten te verrichten wordt met dit wetsvoorstel niet strafbaar. Dat is anders wanneer de betrokkene aan die bereidverklaring handen en voeten geeft, bijvoorbeeld door voorwerpen te verzamelen waarmee hij deze spionageactiviteiten kan verrichten. In dat geval kan sprake zijn van strafbare voorbereiding (artikel 46 Sr). Er is niet gekozen voor strafbaarstelling van de enkele bereidverklaring, omdat het voorstelbaar is – mede gelet op de (subtiele) wijze waarop rekruteringsprocessen door buitenlandse inlichtingendiensten verlopen – dat mensen ondoordacht een dergelijke toezegging doen of een bepaalde druk voelen om dat te doen. Daarmee is niet zonder meer gezegd dat zij een dergelijke toezegging – na gelegenheid te hebben gehad tot zich te laten doordringen wat zij hebben toegezegd en daarop te reflecteren – ook uitvoeren. Het kabinet wil deze – in de kern niet kwaadwillende – mensen de mogelijkheid tot een dergelijke «vrijwillige terugtred» niet ontnemen. Anders kijkt het kabinet aan tegen personen (in dienst van buitenlandse mogendheden) die welbewust anderen proberen aan te zetten tot het verrichten van spionageactiviteiten. Deze uiterst onwenselijke praktijk, waardoor ook goedwillende mensen in het web van een kwaadwillende buitenlandse mogendheid verstrikt kunnen raken, dient van een antwoord te worden voorzien. Om die reden is dan ook in het tweede lid van de nieuwe strafbepaling «het een ander bewegen tot het verrichten van spionageactiviteiten» strafbaar gesteld.

5. Hoofdlijnen van het wetsvoorstel

5.1 Nieuwe strafbaarstelling

De leden van de VVD-fractie vragen aandacht voor het bestanddeel «in heimelijke betrokkenheid met een buitenlandse mogendheid», dat is toegevoegd naar aanleiding van het advies van de Afdeling advisering van de Raad van State. Op de vraag van deze leden of het openbaar ministerie is geconsulteerd over deze toevoeging antwoord ik dat het niet gebruikelijk is om na de consultatiefase adviesorganen opnieuw om advies te vragen. Dat geldt des te meer in de fase na het uitbrengen van een advies door de Afdeling advisering van de Raad van State. Om die reden is dat ook in dit geval niet gebeurd. De zorgen die deze leden hebben geuit over de voorbeelden die zij noemen in het verslag, neem ik graag weg. Dat personen bepaalde uitingen, gericht op het actief beïnvloeden van bepaalde groepen, in het openbaar doen, maakt nog niet dat daarmee geen sprake kan zijn van heimelijke betrokkenheid van de buitenlandse mogendheid bij die activiteit. Van heimelijke betrokkenheid kan ook sprake zijn als de gedraging niet (volledig) heimelijk wordt verricht. Waar het om gaat is dat is gestreefd naar het verheimelijken van de betrokkenheid van de buitenlandse mogendheid bij – in dit geval – de uiting. Die betrokkenheid kan bijvoorbeeld zijn gelegen in het aansturen, financieren of anderszins faciliteren van deze uitingen.
Het onderhouden van contacten met een buitenlandse mogendheid is op zichzelf niet strafbaar. In een open samenleving, met een open economie, die gericht is op internationale samenwerking, zijn dergelijke contacten immers gebruikelijk en onderdeel van het normale internationale verkeer.

Dat wordt anders wanneer ten behoeve van en in heimelijke betrokkenheid met die buitenlandse mogendheid schadetoebrengende gedragingen worden verricht waardoor zwaarwegende Nederlandse belangen in gevaar komen. Naar aanleiding van een ander voorbeeld van deze leden wordt daarbij benadrukt dat het enkele feit dat een persoon openlijke contacten onderhoudt met een buitenlandse mogendheid, niet betekent dat dergelijk handelen buiten de werking van de nieuwe strafbepaling valt. Centraal staat, zoals gezegd, de heimelijke betrokkenheid bij de schadetoebrengende gedraging. Bij personen in dienst van een buitenlandse mogendheid kan worden gedacht aan situaties waarin de gedraging buiten de normale taakuitoefening van de functie van de betrokkene valt, maar wel in opdracht van de buitenlandse mogendheid wordt verricht. Wanneer geen sprake is van heimelijkheid, zou degene aan wie de schade wordt toegebracht ook kunnen optreden tegen de gedraging – bijvoorbeeld door geen toegang tot bepaalde informatie aan iemand te verlenen – om zo te verhinderen dat schade ontstaat. In de heimelijkheid ligt dan ook – naast de schade die wordt toegebracht – de kern van het verwijt dat aan de betrokkene wordt gemaakt bij spionageactiviteiten. Wanneer geen sprake is van heimelijke betrokkenheid, kwalificeren gedragingen daarom niet als spionageactiviteit in de zin van de hier voorgestelde bepaling.

De leden van deze fractie vragen hoe ruim het begrip «buitenlandse mogendheid» moet worden opgevat. Zij stellen enkele vragen over in hoeverre ook buitenlandse bedrijven of organisaties hieronder worden begrepen. Graag beantwoord ik deze vragen in onderlinge samenhang als volgt.
De term «buitenlandse mogendheid» wordt op meerdere plekken in het Wetboek van Strafrecht gebruikt. Met de term wordt gedoeld op elke andere staat dan het Koninkrijk der Nederlanden. Buitenlandse bedrijven en organisaties vallen in principe dus niet onder dit begrip. Voor zover informatie wordt verstrekt of schadetoebrengende gedragingen worden verricht ten behoeve van de private belangen van een buitenlands bedrijf of een buitenlandse organisatie vallen die gedragingen dus niet buiten de reikwijdte van de hier voorgestelde strafbaarstelling. Onder omstandigheden kunnen die gedragingen wel strafbaar zijn op grond van andere bepalingen, bijvoorbeeld omdat sprake is van omkoping of schending van bedrijfsgeheimen. Het voorgaande betekent niet dat het verstrekken van informatie aan of het verrichten van gedragingen in opdracht van een buitenlands bedrijf of buitenlandse organisatie helemaal niet onder het bereik van het voorgestelde artikel 98d Sr kan vallen. Met de woorden «middellijk» en «ten behoeve van» in de bepaling wordt tot uitdrukking gebracht dat ook wanneer indirecte spionageconstructies worden gebruikt, waarbij niet-statelijke dekmantels of facilitators worden ingezet, strafrechtelijke aansprakelijkheid kan worden aangenomen wegens spionageactiviteiten. Waar gedragingen worden gepleegd in opdracht van of voorwerpen of informatie worden verstrekt aan bedrijven of organisaties die (deels) eigendom zijn of op andere wijze onder invloed staan van een buitenlandse mogendheid, is dit in voorkomende gevallen dus strafbaar op grond van de voorgestelde strafbepaling. Wanneer sprake is van «onder invloed staan» van een buitenlandse mogendheid op zodanige wijze dat de gedragingen ook kunnen worden beschouwd als te zijn gepleegd «ten behoeve van» die mogendheid is mede afhankelijk van de precieze omstandigheden van het geval. In het voorbeeld van deze leden, waarbij een buitenlands bedrijf wordt verplicht mee te werken aan een inlichtingenprogramma van een buitenlandse overheid, kan sprake zijn van een situatie waarin inlichtingen «middellijk» worden verstrekt aan die buitenlandse mogendheid. Daarbij wordt aangetekend dat personen die inlichtingen aan dit bedrijf verstrekken daarvoor alleen strafbaar zijn als zij zich ook bewust waren van de aanmerkelijke kans dat deze

inlichtingen zouden worden doorverstrekt aan de buitenlandse mogendheid.

Desgevraagd antwoord ik deze leden dat er geen aanleiding is om een strafverzwaringsgrond op te nemen in de nieuwe bepaling voor gevallen waarin spionageactiviteiten plaatsvinden ten behoeve van een mogendheid die een expliciet vastgestelde dreiging voor de Nederlandse belangen en veiligheid vormt. Spionageactiviteiten op grond van dit wetsvoorstel zijn strafbaar als zij gevaar opleveren voor een aantal in de wet opgesomde zwaarwegende Nederlandse belangen, zoals de veiligheid van de staat. Niet valt in te zien waarom spionageactiviteiten minder ernstig zouden zijn wanneer zij worden gepleegd ten behoeve van een mogendheid ten aanzien waarvan (nog) niet vooraf is vastgesteld dat deze een dreiging voor de Nederlandse belangen vormt, terwijl door die activiteiten wel een gevaar ontstaat voor bijvoorbeeld de nationale veiligheid of de vitale infrastructuur. Een dergelijk onderscheid past ook niet bij het uitgangspunt van een landenneutrale benadering, die de basis vormt voor de bestaande aanpak van statelijke dreigingen (Kamerstukken II 2022/23, 30 821, nr. 175). Bovendien kunnen geopolitieke ontwikkelingen zorgen voor veranderende doelen van buitenlandse mogendheden.

De leden van de VVD-fractie verwijzen naar het advies van het openbaar ministerie om «wetende dat» in de delictsomschrijving te vervangen door «terwijl hij weet of redelijkerwijs moet vermoeden». De VVD-fractie vraagt daarbij specifiek aandacht voor de opmerkingen van het openbaar ministerie over de bewijsbaarheid van het opzet. Voor een nadere toelichting op de keuze voor handhaving van het opzetvereiste verwijs ik deze leden graag naar mijn antwoord in paragraaf 2 van deze nota naar aanleiding van het verslag op een soortgelijke vraag van de leden van de SP-fractie. Het kabinet denkt niet dat met het opzetvereiste een te hoge bewijsdrempel wordt opgeworpen. Het opzetvereiste «wetende dat» omvat blijkens de rechtspraak van de Hoge Raad ook voorwaardelijk opzet. Dat betekent dat een verdachte ook strafbaar is als hij het laten ontstaan van gevaar voor een of meerdere van de in de wet opgesomde belangen weliswaar niet tot doel had, maar de aanmerkelijke kans daarop wel bewust heeft aanvaard (op de koop heeft toegenomen). De aanmerkelijke kans wordt in de rechtspraak objectief ingevuld: het moet gaan om een kans die naar algemene ervaringsregels aanmerkelijk is te achten. Daarmee wordt gedoeld op een in de gegeven omstandigheden reële, niet onwaarschijnlijke mogelijkheid. Zie HR 29 mei 2018, ECLI:NL:HR:2018:718, r.o. 5.3.2. Voor het bewijs dat de verdachte deze aanmerkelijke kans ook bewust heeft aanvaard kan onder omstandigheden worden teruggevallen op de «uiterlijke verschijningsvorm» van de gedraging. Dat betekent dat ook objectieve omstandigheden aan het bewijs van (voorwaardelijk) opzet kunnen bijdragen. Het kabinet heeft dan ook niet de indruk dat met het opzetvereiste een te hoge drempel wordt opgeworpen. Het meent daarentegen dat het vereiste een belangrijke waarborg is om te voorkomen dat de strafrechtelijke aansprakelijkheid te ruim wordt. Zoals in paragraaf 2 aan de orde is gekomen, zou bijvoorbeeld de toevoeging van een culpoze variant leiden tot de introductie van een soort onderzoeksplicht voor personen werkzaam in spionagegevoelige sectoren en/of internationale sectoren. Dit acht het kabinet onwenselijk. Het is immers geenszins de bedoeling van deze wet om aan gebruikelijk internationaal verkeer in de weg te staan, en evenmin om op dit punt een «chilling effect» te veroorzaken. Dat neemt niet weg dat het kabinet, met deze leden en het openbaar ministerie, van mening is dat het belangrijk is om stevige drempels op te werpen tegen onvoorzichtig of nalatig handelen. Daarvoor staan andere dan strafrechtelijke middelen ter beschikking, zoals goede voorlichting, het treffen van voldoende preventieve maatregelen, en – eventueel – arbeidsrechtelijke consequenties voor personen werkzaam

voor de overheid of in vitale sectoren die in strijd met integriteits- en zorgvuldigheidsnormen handelen. Het kabinet zet zich dan ook in om de weerbaarheid te verhogen tegen dreigingen die uitgaan van statelijke actoren (Kamerstukken II 2022–2023, 30 821 nr. 175). De inzet is hierbij onder andere gericht op het voorkomen van ongewenste kennisoverdracht bij overheden, kennisinstellingen en het bedrijfsleven. Verschillende instrumenten worden hiervoor ingezet zoals investeringstoetsing, kennisveiligheid en het verhogen van bewustwording bij relevante partijen op risico's van het weglekken van gevoelige kennis en technologie.
Deze leden verwijzen naar de motie-Valstar c.s. (Kamerstukken II 2022/23, 36 200-X, nr. 25). Op deze motie zal afzonderlijk worden gereageerd door de Minister van Defensie.

De leden van de D66-fractie geven tot mijn genoegen aan zich te kunnen vinden in de – in reactie op het advies van de Afdeling advisering van de Raad van State gegeven – onderbouwing waarom niet is gekozen voor een limitatieve opsomming van schadetoebrengende gedragingen. Zij vragen aan welke schadetoebrengende handelingen kan worden gedacht, die niet al onder strafbaar gestelde gedragingen vallen.
Voor voorbeelden die betrekking hebben op het verstrekken van informatie, verwijs ik deze leden graag naar het antwoord in paragraaf 3 van deze nota op een gelijkluidende vraag van de leden van de PvdA-fractie. Voorbeelden van andere gedragingen zijn het (in strijd met de regels) binnenlaten van personen in een (afgesloten etage van een) overheidsgebouw of bedrijf, het ophalen en rondbrengen van pakketjes met een schadelijke inhoud, het verspreiden van (onware) informatie met als doel bepaalde schade aan te richten of personen of processen te beïnvloeden en het volgen of intimideren van personen. Centraal staat daarbij steeds of door de gedraging gevaar kan ontstaan voor de in de wet opgesomde belangen.

De leden van de D66-fractie vragen om nader toe te lichten waarom is gekozen voor een strafmaximum van acht jaar. Meer in het bijzonder vragen zij waarom aansluiting bij de strafmaxima in de artikelen 98 en 98c Sr niet volstaat.
Zoals deze leden terecht constateren was in de consultatieversie van dit wetsvoorstel, in aansluiting op de artikelen 98 en 98c Sr, gekozen voor een strafmaximum van zes jaar. Naar aanleiding van de uitgebrachte adviezen heeft een heroverweging van dit strafmaximum plaatsgevonden. Bij nader inzien meent het kabinet dat een belangrijk verschil tussen de artikelen 98 en 98c Sr en de hier voorgestelde strafbaarstelling de betrokkenheid van de buitenlandse mogendheid is. Die omstandigheid maakt dat het feit als ernstiger moet worden beschouwd. Door de buitenlandse betrokkenheid draagt het strafbare feit immers ook «een kenmerk van verraad». Vgl. H.J. Smidt, tweede druk bewerkt door J.W. Smidt, *Geschiedenis van het Wetboek van Strafrecht. Deel I*, Haarlem: Tjeenk Willink 1891, blz. 20. Ook voor het verstrekken van staatsgeheimen (artikel 98 Sr) geldt een verhoogd strafmaximum als die staatsgeheimen worden verstrekt aan het buitenland (artikel 98a Sr). Vanuit dat oogpunt meent het kabinet dat met een strafmaximum van acht jaar gevangenisstraf in een evenwichtiger strafmaximum is voorzien.

Ik kan deze leden bevestigen dat de strafbaarheid ten opzichte van de consultatieversie is verruimd doordat, met het strafmaximum van acht jaar, nu ook de voorbereiding van spionageactiviteiten strafbaar is op grond van artikel 46 Sr. Dit staat volgens het kabinet niet op gespannen voet met het lex certa-vereiste. Zoals ook in de memorie van toelichting is uiteengezet, voldoet de voorgestelde strafbaarstelling aan de vereisten van toegankelijkheid en voorzienbaarheid. Dat ook voorbereidingshande-

lingen strafbaar zijn doet daaraan niet af. Op grond van artikel 46 Sr is strafbaar het, kort samengevat, verwerven of voorhanden hebben van voorwerpen om – in dit verband – spionageactiviteiten als bedoeld in artikel 98d Sr te plegen. Hierbij kan gedacht worden aan bijvoorbeeld het verwerven van simkaarten, (lege) gegevensdragers om informatie op te slaan, toegangspassen en het voorhanden hebben van plattegronden, apparatuur waarmee kan worden ingebroken op een locatie of in een geautomatiseerd werk, of het huren van voertuigen. Daarmee is voldoende voorzienbaar in welke gevallen de betrokkene strafbaar handelt.
Voor de inzet van opsporingsbevoegdheden is relevant het wettelijke strafmaximum dat is gesteld op het betreffende grondfeit. De opsporingsbevoegdheden waaraan deze leden refereren kunnen dus ook worden ingezet als de verdenking bestaat dat sprake is van strafbare voorbereiding van spionageactiviteiten, zo kan ik hen bevestigen.

De leden van de D66-fractie informeren naar de betekenis van dit wetsvoorstel voor de aanpak van diasporaspionage. Gevraagd naar voorbeelden uit het recente verleden die wel onder de voorgestelde strafbaarstelling vallen, maar destijds niet tot vervolging konden leiden, antwoord ik dat het helaas niet mogelijk is deze vraag te beantwoorden. De zaken zijn destijds beoordeeld aan de hand van de toen geldende wettelijke kaders. Of bepaalde gedragingen strafbaar zijn (of onder de nieuwe strafbaarstelling zullen zijn) is afhankelijk van de concrete omstandigheden van het individuele geval. Het is aan het openbaar ministerie en – vervolgens – de strafrechter, en niet dit kabinet, om die beoordeling te maken. Wel kan dit kabinet constateren dat tot op heden niet of nauwelijks tot vervolging is overgegaan, mede vanwege het ontbreken van strafrechtelijk handelingsperspectief. Dit wetsvoorstel beoogt de mogelijkheden om tot strafrechtelijke handhaving over te gaan te verruimen. Zoals eerder in deze nota naar aanleiding van het verslag aan de orde is gekomen, biedt de voorgestelde strafbaarstelling (meer) mogelijkheden om personen die bijvoorbeeld anderen de mond proberen te snoeren of te intimideren of die gevoelige informatie over anderen (bijvoorbeeld over politieke of religieuze voorkeuren, over deelnemers aan demonstraties of over familiebanden) verstrekken aan buitenlandse mogendheden strafrechtelijk te vervolgen.
Op de vraag van deze leden in welke mate dit wetsvoorstel eraan kan bijdragen dat personen meer weerstand kunnen bieden aan buitenlandse mogendheden, antwoord ik dat dit niet het primaire doel van dit wetsvoorstel is. Het belangrijkste doel van de voorgestelde strafbaarstelling is personen die zich schuldig maken aan spionageactiviteiten daarvoor strafrechtelijk ter verantwoording te kunnen roepen. Wel denkt het kabinet dat de strafbaarstelling – als neveneffect – kan hebben dat bepaalde personen (iets) meer weerstand kunnen bieden aan bepaalde vormen van drang. Met een beroep op de strafbaarstelling kan worden aangegeven dat het niet mogelijk is te voldoen aan eventuele verzoeken om inlichtingen gedaan door of namens een buitenlandse mogendheid. Het strafrecht is, zo kan ik deze leden bevestigen, niet het enige middel waarop wordt ingezet om dergelijke buitenlandse inmenging tegen te gaan. Bij de aanpak van buitenlandse inmenging wordt ingezet op drie sporen, waarvan het bestuurs- en strafrechtelijke spoor er een is. Daarnaast is er nog het diplomatieke spoor. Binnen dit spoor wordt de dialoog aangegaan met landen die zich schuldig maken aan ongewenste inmenging, worden zij daarop aangesproken en worden, indien nodig, ook diplomatieke stappen ondernomen tegen de betreffende landen. Tot slot is er het weerbaarheidsspoor. Binnen dit spoor wordt ingezet op verhoging van de weerbaarheid van de kwetsbare groepen die mogelijkerwijs vatbaar zijn voor ongewenste buitenlandse inmenging. Zo is onlangs in de Kamerbrief over geïntensiveerde aanpak ongewenste

buitenlandse inmenging (brief van 6 april 2023, met kenmerk 2023Z06155) een communicatiecampagne aangekondigd ter vergroting van de bewustwording en handelingsperspectief.

De leden van de CDA-fractie vragen om voorbeelden van voorwerpen waarvan het verstrekken aan een buitenlandse mogendheid strafbaar wordt op grond van dit wetsvoorstel.
Gedacht kan worden aan gegevensdragers – zoals een USB-stick, een externe harde schijf, een telefoon of een laptop – met waardevolle informatie, aan papieren stukken met (gecodeerde) berichten, foto's van personen, locaties of activiteiten en sleutels of een toegangspas.

De leden van de SP-fractie geven aan te hebben gelezen dat ook het openbaar maken of het verspreiden van schadelijke informatie, bijvoorbeeld over personen, onder de nieuwe strafbaarstelling valt. Daarnaar gevraagd, antwoord ik dat het moeilijk is om een concreet voorbeeld te noemen. Zoals eerder toegelicht hangt de eventuele strafbaarheid van het openbaar maken dan wel verspreiden van schadelijke informatie af van de omstandigheden van het specifieke geval.

De leden van de PvdA-fractie informeren naar buitenlandse wettelijke voorschriften. Zij stellen daarover enkele vragen, die ik graag in onderlinge samenhang als volgt beantwoord.
Als iemand een schadetoebrengende handeling verricht of informatie aan een buitenlandse mogendheid verstrekt, wetende dat daarvan gevaar is te duchten voor de in de strafbepaling opgesomde belangen, dan kan deze persoon zich er niet zonder meer op beroepen dat de gedraging werd verricht ter uitvoering van een buitenlands wettelijk voorschrift. Er kan geen beroep worden gedaan op de strafuitsluitingsgrond opgenomen in artikel 42 Sr. Die bepaling ziet in beginsel immers op Nederlandse wettelijke voorschriften. Dat neemt niet weg dat wanneer de betrokkene door de buitenlandse wettelijke verplichting in een «overmachtssituatie» geraakt, hij wel een beroep kan doen op artikel 40 Sr. Dat wil zeggen dat in situaties waarin de betrokkene als gevolg van een buitenlandse wettelijke bepaling een acute en onontkoombare keuze moet maken tussen naleving van dat wettelijk voorschrift en handelen in strijd met de Nederlandse strafwet, hij zich kan beroepen op overmacht (en om die reden niet strafbaar is) als hij de zwaarstwegende van de twee heeft laten prevaleren. De omstandigheid dat betrokkene in het land waar het wettelijk voorschrift geldt verblijft en daarmee binnen de machtssfeer van die buitenlandse mogendheid verkeert kan, in combinatie met de eventuele gevolgen van overtreding van het buitenlandse voorschrift, bij deze beoordeling worden betrokken. Een andere benadering, waarbij het buitenlandse voorschrift altijd prevaleert, is niet wenselijk. Dat zou immers betekenen dat kwaadwillende buitenlandse mogendheden via wettelijke bepalingen kunnen bereiken dat hun onderdanen onbestraft spionageactiviteiten kunnen uitvoeren tegen Nederland, Nederlandse bedrijven en Nederlandse burgers. In dit verband verwijs ik deze leden ook graag naar de inbreng van de leden van de VVD-fractie in paragraaf 5.1 van het verslag, waarin zij aandacht vragen voor landen die bedrijven verplichten om mee te werken aan inlichtingenprogramma's.

De leden van de PvdA-fractie merken op dat het op prijs is te stellen dat de belangen in de strafbaarstelling zoveel mogelijk worden geduid. Behalve bij de belangen die al elders in het Wetboek van Strafrecht worden beschermd, is ook aangeknoopt bij de zes nationale veiligheidsbelangen zoals beschreven in de Nationale Veiligheidsstrategie, zo constateren zij. Ik antwoord op de vraag van deze leden waarom deze belangen niet in de wet zelf worden verankerd, dat deze veiligheidsbelangen een nadere invulling zijn van het in de bepaling gebruikte begrip «veiligheid

van de staat». Dit laatste begrip komt al op verschillende plaatsen in de (straf)wetgeving voor. Er is dus gekozen voor aansluiting bij bestaande begrippen. Op hun vraag of in de rechtspraak al invulling is gegeven aan deze veiligheidsbelangen, antwoord ik dat ik dergelijke (strafrechtelijke) rechtspraak niet heb gevonden. Er zijn wel andere bronnen waaruit blijkt van de invulling die aan deze veiligheidsbelangen wordt gegeven. Daarbij kan in het bijzonder worden gewezen op de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (Kamerstuk van 3 april 2023 met kenmerk 2023D13646), waarin nader wordt uiteengezet wat onder deze zes veiligheidsbelangen wordt verstaan. Zo geldt ten aanzien van ecologische veiligheid dat deze in het geding is wanneer milieu en natuur langdurig worden aangetast. Een voorbeeld hiervan is vervuiling van het oppervlaktewater. Bij gevaar voor de sociale en politieke stabiliteit kan gedacht worden aan gedragingen die de democratische rechtsstaat aantasten, bijvoorbeeld door handelingen die het functioneren van democratische instituties of processen ondermijnen, of gedragingen gericht op het zodanig tegen elkaar opzetten van bevolkingsgroepen dat sociale structuren hierdoor worden ontwricht. Bij het veiligheidsbelang internationale rechtsorde kan worden gedacht aan de aantasting van vreedzame co-existentie of aantasting van de werking van internationale verdragen. De territoriale integriteit omvat naast de integriteit van het grondgebied en de internationale positie, ook de aantasting van de integriteit van de digitale ruimte. Bij gevaar voor de fysieke veiligheid kan worden gedacht aan levensgevaar, gevaar voor ernstig lichamelijk letsel en gebrek aan primaire levensbehoeften. Ten aanzien van de economische veiligheid wordt opgemerkt dat de verwevenheid van de economie met de nationale veiligheid al geruime tijd wordt onderkend. Zoals ook in het DBSA 2 is aangegeven, speelt geopolitiek een steeds dominantere rol in de wereldeconomie. Enerzijds vormen economische en de daarbij horende technologische ontwikkelingen de basis voor politieke en militaire macht. Anderzijds worden economische instrumenten door staten, en de grootmachten in het bijzonder, als machtsmiddel gebruikt om geopolitieke doelen te bereiken. Van gevaar voor de economische veiligheid is tegen deze achtergrond sprake als gevaar ontstaat voor de vitaliteit van de Nederlandse economie, door gedragingen die erop gericht zijn om de Nederlandse economie of bepaalde economische sectoren ernstige (en blijvende) schade toe te brengen of die erop gericht zijn de eigen economische positie van de buitenlandse mogendheid te versterken.
Deze leden verwijzen in dit verband naar het advies van de NOvA waarin staat dat «een brede en nogal vage definiëring van bepaalde begrippen zich slecht verhoudt met het strafrechtelijk legaliteitsbeginsel». In het advies van de NOvA, zo luidt mijn reactie hierop, wordt in dit verband verwezen naar de termen «vitale infrastructuur» en «de integriteit en hoogwaardige technologieën, niet naar het begrip «veiligheid van de staat». Ten aanzien van de term «vitale infrastructuur» is in reactie op de uitgebrachte adviezen over het wetsvoorstel verduidelijkt in de memorie van toelichting dat dit een al in het Wetboek van Strafrecht voorkomend begrip is en dat er verschillende voorbeelden in de rechtspraak beschikbaar zijn waaruit blijkt dat de rechtspraak met dit begrip uit de voeten kan. Voor een nadere duiding van het begrip «integriteit en exclusiviteit van hoogwaardige technologieën» verwijs ik de leden van de PvdA-fractie allereerst graag naar paragraaf 2 van deze nota naar aanleiding van het verslag, waarin ik in reactie op een vraag van deze leden ook op dit begrip ben ingegaan. Zoals daar aangegeven vallen onder dit begrip in ieder geval «sensitieve technologieën». Voor de invulling van dat begrip kan aansluiting worden gezocht bij de invulling die aan dit begrip wordt gegeven in het kader van de Wet veiligheidstoets investeringen, fusies en overnames. Het begrip «hoogwaardige technologieën» omvat daarnaast ook innovatieve technologieën waarin Nederland een voorsprong heeft en die daardoor van economisch en strategisch

belang zijn. Bij de beoordeling of technologieën als «hoogwaardig» kunnen worden aangemerkt, kan – naast naar sensitieve technologieën en het spraakgebruik – bijvoorbeeld worden gekeken naar of een technologie voorkomt op indexen voor «high tech» technologieën en industrieën, zoals die van de OESO en de EU. Ook kan meewegen of bijvoorbeeld een aangevraagd octrooi of patent aan de orde is. Hoewel deze factoren niet per definitie doorslaggevend zijn, kunnen zij wel een indicatie vormen dat sprake is van «hoogwaardige technologie» waarvan de integriteit en exclusiviteit moet worden beschermd, omdat de technologie van economisch en strategisch belang is. Van een economisch belang kan worden uitgegaan bij een significante bijdrage aan de Nederlandse concurrentiepositie. Er kan sprake zijn van strategisch belang als een technologie bijvoorbeeld bijdraagt aan de strategische autonomie van Nederland (of de EU).

De leden van de PvdA-fractie vragen naar de kwaadaardige toepassing van semi-conductoren. Semi-conductoren of halfgeleiders halfgeleiderchips zijn de essentiële bouwstenen van digitale en gedigitaliseerde producten. Ze vormen het hart van producten die onze economie en maatschappij draaiende houden, zoals toepassingen voor de gezondheidszorg, energie, mobiliteit of communicatie. Daarnaast zijn (geavanceerde) chips onmisbaar voor defensiesystemen en andere militaire toepassingen en voor belangrijke digitale technologieën van de toekomst, zoals kunstmatige intelligentie en 5G (en 6G). Dit maakt de toegang tot halfgeleidertechnologie van groot economisch, maatschappelijk en militair belang.
Hoe geavanceerder halfgeleiders, hoe geavanceerder de elektronische producten waarin ze verwerkt kunnen zijn. Op termijn zal een land dat slechts beperkte toegang heeft tot halfgeleidertechnologie grote problemen kunnen ervaren; nog los van de economische en maatschappelijke toepassingen van halfgeleidertechnologie, is de toegang tot en de betrouwbaarheid van halfgeleidertoepassingen in het militaire en veiligheidsdomein van groot nationaal belang. Gelet op dit belang en de brede toepasbaarheid van semiconductoren is toepassing voor ongewenst eindgebruik voorstelbaar. Niet alleen kan halfgeleidertechnologie door statelijke actoren (andere landen) ingezet worden voor ongewenst eindgebruik, zoals voor militaire toepassingen en daarmee het versterken van de krijgsmacht. Ook kan het weglekken van dergelijke kennis op langere termijn leiden tot afhankelijkheid van derde landen voor deze technologie. Dit zou een risicovolle strategische afhankelijkheid betekenen, omdat het de landen waarvan wij afhankelijk zijn de mogelijkheid geeft hun positie in te zetten als politiek en economisch drukmiddel. Bovendien zet het ons streven naar strategische autonomie en technologisch leiderschap verder onder druk.
Bij de kwaadaardige toepassing van kunstmatige intelligentie kan worden gedacht aan de inzet van gezichtsherkenningstechnologie. In Nederland gelden strikte regels voor het gebruik hiervan, maar er zijn ook buitenlandse overheden die gezichtsherkenningstechnologie inzetten voor doeleinden die in strijd lijken te zijn met rechten en vrijheid van burgers. Het Nederlandse kabinet wil voorkomen dat, door spionageactiviteiten, in Nederland ontwikkelde technieken hiervoor worden ingezet. Hetzelfde geldt voor kwaadaardige toepassing van DNA-techniek.
Agrarische innovaties worden (tot op heden) niet kwaadaardig ingezet door statelijke actoren, maar dragen wel sterk bij aan de wereldwijde voedselzekerheid en zijn van belang voor de Nederlandse concurrentiepositie.
Op de vraag van deze leden waar het belang van een open economie ophoudt en waar het gevaar van spionage begint, antwoord ik dat een kenmerk van spionageactiviteiten is, waarbij in de voorgestelde strafbaarstelling ook wordt aangeknoopt, dat buitenlandse mogendheden heimelijk

betrokken zijn. Spionageactiviteiten, als bedoeld in de hier voorgestelde strafbaarstelling, onderscheiden zich op dit punt van conventionele bedrijfsspionage. Bij gewone bedrijfsspionage kan worden gedacht aan een bedrijf dat zijn eigen positie beoogt te versterken – of de positie van zijn concurrent probeert te verzwakken – door bedrijfsgeheime informatie te gebruiken, bijvoorbeeld voor de ontwikkeling van een product. Bij «spionageactiviteiten» in de hier bedoelde zin gaat het echter om activiteiten verricht in heimelijke betrokkenheid met en ten behoeve van een buitenlandse mogendheid, gericht op de verzwakking van de economie of een economische sector van het andere land en/of versterking van de economie of een economische sector van het eigen land, om zo de eigen internationale (geopolitieke) positie te versterken, of om technologieën te verkrijgen die (ook) kwaadaardig kunnen worden ingezet. De strafbaarstelling van spionageactiviteiten beoogt daarmee een groter belang te beschermen dan alleen de concurrentiepositie van een individueel bedrijf.

5.2 Strafverzwaringsgrond computermisdrijven

De leden van de VVD-fractie hebben met instemming kennisgenomen van de strafverzwaringsgrond die in het wetsvoorstel is opgenomen bij computermisdrijven. Deze leden vragen waarom is gekozen voor een beperking tot bepaalde computermisdrijven en niet, althans zo begrijp ik hun vraag, voor een algemene strafverzwaringsgrond die geldt voor alle misdrijven.
Als uitgangspunt is in het Wetboek van Strafrecht gekozen voor algemene strafbaarstellingen, waarbij in een strafmaximum is voorzien dat ruimte biedt om ook bij de meest ernstige verschijningsvormen van het betreffende feit een passende straf op te leggen. De rechter kan binnen dit strafmaximum alle relevante omstandigheden betrekken bij de bepaling van de op te leggen straf. Met het opnemen van strafverzwaringsgronden dient tegen deze achtergrond spaarzaam te worden omgegaan. Strafverzwaringsgronden worden bovendien over het algemeen slechts opgenomen bij het delict of de delicten waarvoor zij relevant zijn en waarbij de strafverzwarende omstandigheid zich in reële gevallen kan voordoen. Een algemene strafverzwaringsgrond zou tot uitdrukking brengen dat de strafwetgever het bij elk misdrijf goed denkbaar acht dat zo'n feit ten behoeve van een buitenlandse mogendheid wordt gepleegd. Daarvoor bestaat echter geen enkele empirische onderbouwing. Bij computermisdrijven is dit wel aan de orde. Digitale spionage speelt in de praktijk een steeds grotere rol. In dat licht voegt het enkele feit dat de gedraging is gepleegd ten behoeve van een buitenlandse mogendheid een extra mate van verwijtbaarheid en gevaarlijkheid aan de gedraging toe, nu – ook gelet op de aard van computermisdrijven – in dat geval per definitie sprake is van «spionageactiviteiten», die – op termijn – gevaar kunnen opleveren voor Nederlandse belangen of belangen van Nederlandse bondgenoten. Daarbij komt dat bij verschillende computermisdrijven al strafverzwarende omstandigheden zijn opgenomen, maar de omstandigheid dat het feit is gepleegd ten behoeve van een buitenlandse mogendheid nog niet. Dat vindt het kabinet onevenwichtig.

6. Opsporing en vervolging

De leden van de CDA-fractie vragen in hoeverre de opsporing van spionageactiviteiten worden bemoeilijkt door sterk beveiligde systemen waarmee versleutelde berichten kunnen worden verstuurd, zoals PGP-berichten (Pretty Good Privacy).
Ik antwoord hierop dat de opsporing van spionageactiviteiten op verschillende manieren kan plaatsvinden. Evenals bij de opsporing van andere vormen van (zware) criminaliteit dient rekening te worden

gehouden met het gebruik van sterk beveiligde systemen en/of het gebruik van encryptie. Dit kan (langdurige) inzet van opsporingsmiddelen vereisen en de daarbij behorende expertise vergen. Dit betekent dat dergelijke onderzoeken capaciteit vergen en dat bijvoorbeeld de inzet van PGP de opsporing kan bemoeilijken. Het maakt opsporing van deze feiten echter niet onmogelijk. Ook in andere strafzaken hebben we inmiddels gezien dat het mogelijk is toegang te krijgen tot PGP-berichtenverkeer. Opsporing van spionageactiviteiten die worden verricht met behulp van technologie, onderstreept het belang om als opsporingsdiensten te kunnen (blijven) investeren in de benodigde expertise en middelen.

De leden van de PvdA-fractie geven aan te begrijpen dat vanwege immuniteit of onschendbaarheid van bij spionage betrokken personen de nieuwe strafbepaling vermoedelijk maar tot een beperkt aantal zaken zal leiden. Zij vragen om een indicatie van dit aantal. Ook vragen zij om een toelichting waar de uitbreiding van de strafbaarheid bijdraagt aan het tegengaan van spionage.
Gelet op de verschillende omstandigheden waarnaar ook de leden van de PvdA verwijzen, wordt, zo luidt mijn reactie, op basis van overleg met de uitvoeringsorganisaties uitgegaan van twee tot drie spionagezaken per jaar. Ondanks dat het naar verwachting om een beperkt aantal zaken zal gaan, is de nieuwe strafbaarstelling om meerdere redenen van belang. Allereerst gaat van de strafbaarstelling een signaal uit. De open samenleving, open economie, evenals de aanwezigheid van bedrijven en kennisinstellingen die hoogwaardige technologie ontwikkelen en produceren en hoogwaardig wetenschappelijk onderzoek doen, maken Nederland tot een aantrekkelijk en in toenemende mate kwetsbaar doelwit van spionage. Ook feit dat Nederland gastland is voor een groot aantal volkenrechtelijke organisaties en lid is van verschillende bondgenootschappen, zoals de EU en de NAVO, draagt hieraan bij. Een aanvullende strafbaarstelling is daarom van belang om de Nederlandse strafwetgeving op een gelijkwaardig niveau te houden met de wetgeving in andere Europese landen. Daarmee wordt het risico ingeperkt dat Nederland – en daarmee de Nederlandse overheid, Nederlandse bedrijven en Nederlandse burgers – in verhouding tot andere landen een aantrekkelijk richtpunt wordt voor spionageactiviteiten. Daarnaast heeft het kabinet in de brief Aanpak statelijke dreigingen (Kamerstukken II 2022/23, 30 821, nr. 175) uiteengezet hoe de samenhangende en diverse set aan maatregelen en instrumenten eruitziet, die wordt ingezet om statelijke dreigingen tegen te gaan. Hieronder vallen onder meer de Wet veiligheidstoets investeringen fusies en overnames, de rijksbrede aanpak van ongewenste buitenlandse inmenging en maatregelen op het terrein van kennisveiligheid. Het strafrecht is niet het enige instrument dat het kabinet inzet om spionage te voorkomen, maar de nieuw strafbepaling biedt wel extra handelingsperspectief op het moment dat spionageactiviteiten worden onderkend. Ook al is het aantal verwachte zaken per jaar beperkt, het maakt wel dat er, ruimer dan nu het geval is, strafrechtelijk tegen spionage opgetreden kan worden.

7. Verhouding tot hoger recht

De leden van de D66-fractie merken op dat zij met de regering van mening zijn dat het wetsvoorstel niet mag beogen de reguliere functie van diplomatieke en consulaire vertegenwoordigingen in Nederland strafbaar te stellen of af te doen aan de bevoegdheid daartoe. Zij vragen zich af of voldoende inzichtelijk is welke buitenlandse overheidsfunctionarissen en andere personen zich in Nederland begeven ten behoeve van een buitenlandse mogendheid, met welk doel en of die informatie voor eenieder toegankelijk is. Tegen deze achtergrond vragen zij een Neder-

landse variant op de Foreign Agents Registration Act (FARA) op te richten of de beoogde transparantie op een andere wijze te bewerkstelligen. Eerder is in de motie-Brekelmans (Kamerstukken II 2021/2022, 35 925 V, nr. 52) een soortgelijk verzoek gedaan. In die motie wordt verwezen naar de Australische registratie van «agents of foreign influence» en wordt het kabinet verzocht aan te geven of en op welke wijze een openbaar register voor agents of foreign influence zoals in Australië ook in Nederland mogelijk is. In de eerdergenoemde brief Aanpak statelijke dreigingen is gereageerd op deze motie en is aangegeven dat de complexe begripsbepaling van wanneer sprake is van buitenlandse inmenging via deze «agents of foreign influence» maakt dat vaststelling daarvan erg lastig en tijdrovend is. De dreiging die uitgaat van personen die werkzaam zijn ten behoeve van statelijke actoren, wordt in Nederland geadresseerd met een breed palet aan maatregelen dat tevens in bovengenoemde brief wordt benoemd. Een belangrijk element in dit palet is bewustwording.

De leden van de CDA-fractie verwijzen naar de passage in de memorie van toelichting waarin is beschreven dat artikel 10 van het Europees Verdrag voor de Rechten van de Mens (EVRM) onder andere de rechten van journalisten en wetenschappers om informatie te verzamelen, ontvangen en verspreiden beschermt. In de regel vallen journalisten en wetenschappers niet onder het bereik van de nieuwe strafbaarstelling. Deze leden verwijzen naar de passage waarin is aangegeven dat dit anders kan zijn als de hoedanigheid van journalist of wetenschapper wordt misbruikt als dekmantel voor spionageactiviteiten. Zij vragen wanneer dit concreet kan worden aangetoond.
Nederland is een open samenleving, waarbinnen contact met buitenlandse overheden, bedrijven, wetenschappers, journalisten en tussen burgers van groot belang is en moet blijven. Het is om die reden vanzelfsprekend op geen enkele manier de bedoeling om journalistieke, wetenschappelijke, diplomatieke of normale bedrijfsactiviteiten strafbaar te stellen. Journalisten moeten ongestoord hun belangrijke werk kunnen doen. Dit is voor de vrije nieuwsgaring en onze samenleving cruciaal. Voor het behoud van onze sterke wetenschappelijke sector zijn internationale samenwerking en academische vrijheid onontbeerlijk. Tegelijkertijd is voorstelbaar – in uitzonderlijke gevallen – dat ook journalisten en bijvoorbeeld wetenschappers spionageactiviteiten kunnen verrichten voor buitenlandse mogendheden. In geval van een verdenking van spionageactiviteiten via een dekmantel als journalist of wetenschapper, moet op grond van de bepalingen uit de wet degene die de activiteiten verricht het opzet hebben om heimelijk ten behoeve van een buitenlandse mogendheid in de wet opgesomde zwaarwegende Nederlandse belangen in gevaar te brengen, zoals de nationale veiligheid of de veiligheid van personen. Een dekmantel kan bijvoorbeeld maar niet uitsluitend blijken als de betrokkene(n) in dienst zijn van of aangestuurd worden door een buitenlandse mogendheid, zoals een buitenlandse inlichtingendienst. Of dit aantoonbaar het geval is zal afhangen van de omstandigheden van het geval en zal uiteindelijk beoordeeld moeten worden door de strafrechter, waarbij indien nodig ook de verschillende belangen worden meegewogen.

De Minister van Justitie en Veiligheid,
D. Yesilgöz-Zegerius