Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafrecht BES in verband met de uitbreiding van de strafbaarheid voor spionage

MEMORIE VAN TOELICHTING

I. Algemeen

Dit wetsvoorstel strekt tot uitbreiding van de strafbaarheid voor spionage. Daartoe wordt een aanvullende bepaling in het Wetboek van Strafrecht en het Wetboek van Strafrecht BES geïntroduceerd. Die bepaling voorziet in een zelfstandige strafbaarstelling van het verrichten van handelingen ten behoeve van en het verstrekken van informatie en voorwerpen aan buitenlandse mogendheden, indien degene die de gedragingen verrichtte (voorwaardelijk) opzet had op het ontstaan van gevaar voor een aantal zwaarwegende belangen, zoals de nationale veiligheid en de veiligheid van in Nederland verblijvende personen. Daarnaast wordt de strafmaat van een aantal computerdelicten die een belangrijke rol kunnen spelen bij spionageactiviteiten verhoogd indien deze zijn gepleegd ten behoeve van een buitenlandse mogendheid. Het wetsvoorstel vloeit voort uit het Coalitieakkoord 2021-2025 *Omzien naar elkaar, vooruitkijken naar de toekomst* (p. 38) en is toegezegd bij brief van 10 december 2020 (Kamerstukken II 2020/21, 30977, nr. 157).

Over het algemeen wordt bij «spionage» gedacht aan het heimelijk of onrechtmatig vergaren van (gevoelige) informatie of objecten door, of in opdracht van een buitenlandse mogendheid. Er zijn echter ook andere gedragingen die in verband kunnen worden gebracht met spionage (hierna: spionageactiviteiten), zoals sabotage, het interveniëren in (besluitvormings)processen of beïnvloeding van personen. Spionageactiviteiten kunnen zich zowel richten op overheden en volkenrechtelijke organisaties als op bijvoorbeeld bedrijven en universiteiten. Steeds vaker worden daarbij ook digitale en andere technische middelen ingezet. Een andere verschijningsvorm van spionage betreft de zogenoemde «diasporaspionage», waarmee wordt gedoeld op landen met een diaspora in Nederland die hier – openlijk en heimelijk – (persoons)gegevens verzamelen en burgers uit deze gemeenschap proberen te beïnvloeden vanuit een (vermeend) eigen intern veiligheidsbelang. Spionageactiviteiten omvatten aldus een veelheid aan gedragingen, die met elkaar gemeen hebben dat zij worden verricht door of ten behoeve van een buitenlandse mogendheid en schade toebrengen aan zwaarwegende belangen, zoals de nationale veiligheid en de veiligheid van personen.

Spionageactiviteiten tasten de soevereiniteit van Nederland aan. Zij brengen schade toe aan het handelingsvermogen van de Nederlandse overheid, het functioneren van de democratische en internationale rechtsorde en de daarin gedeelde waarden, de nationale veiligheid, het verdien- en concurrentievermogen van Nederland en kunnen bijdragen aan maatschappelijke ontwrichting. Om die reden is het van belang dat voldoende middelen beschikbaar zijn om spionage tegen te gaan. De hierna beschreven ontwikkelingen hebben aanleiding gegeven om opnieuw te kijken naar het beschikbare instrumentarium om spionageactiviteiten tegen te gaan. Dit heeft tot de conclusie geleid dat een aanvullende strafbaarstelling aangewezen is. Het strafrecht biedt op dit moment namelijk nog onvoldoende mogelijkheden om op te treden tegen spionageactiviteiten waarbij geen sprake is van een schending van (staats-, ambts- of bedrijfs-) geheimen, maar die wel de Nederlandse belangen ernstig schaden, of waarbij andere schadelijke handelingen worden verricht dan het verstrekken van informatie. Een aanvullende strafbaarstelling is ook van belang de Nederlandse strafwetgeving op een gelijkwaardig niveau te houden met de wetgeving in andere Europese landen en daarmee te voorkomen dat het risico ontstaat dat Nederland – en daarmee de Nederlandse overheid, Nederlandse bedrijven en Nederlandse burgers – in verhouding tot andere landen een aantrekkelijk doelwit wordt voor spionageactiviteiten. Dat geldt des te meer omdat Nederland een gastland is voor een groot aantal volkenrechtelijke organisaties en onderdeel uitmaakt van verschillende bondgenootschappen, waardoor Nederland ook jegens hen een verantwoordelijkheid heeft om maatregelen te nemen tegen spionage.

In het hiernavolgende wordt eerst een beschrijving gegeven van de maatschappelijke ontwikkelingen die aanleiding zijn geweest om opnieuw naar het (strafrechtelijk) instrumentarium om spionage te adresseren te kijken (paragraaf 1). Daarna volgen een beschrijving van de bestaande beleids- en wettelijke kaders voor het optreden tegen spionage (paragraaf 2) en van de wettelijke kaders in ons omringende landen (paragraaf 3). Vervolgens worden de hoofdlijnen van het wetsvoorstel uiteengezet (paragraaf 4). Daarna volgen paragrafen over de opsporing en vervolging (paragraaf 5), de verhouding tot hoger recht (paragraaf 6) en de uitvoerings- en financiële consequenties (paragraaf 7). Deze memorie eindigt met een artikelsgewijze toelichting.

1. Maatschappelijke ontwikkelingen

Maatschappelijke ontwikkelingen waaronder globalisering en digitalisering hebben geleid tot veranderingen van zowel de wijze waarop en de mate waarin spionage plaatsvindt als de verschijningsvormen van spionage. De wereld verandert in hoog tempo. Nieuwe spelers hebben het wereldtoneel betreden en traditionele bondgenootschappen verdwijnen of veranderen van samenstelling. Staten proberen op een offensieve wijze hun eigen belangen te behartigen waardoor bestaande verhoudingen veranderen. Daarbij hanteren zij in toenemende mate andere regels, normen en waarden dan die in Nederland en de internationale (westerse) gemeenschap worden gehuldigd.

Nederland hoort bij de meest ontwikkelde naties van de wereld op het gebied van economie, wetenschap en techniek. Een open economie en vrijhandel liggen sinds jaar en dag aan de basis van het Nederlandse verdienvermogen. Dit brengt ons de noodzakelijke financiering, schaalvoordelen, uitwisseling van talen en kennis en essentiële concurrentieprikkels. Dit is een grote kracht en heeft van Nederland als relatief klein land een wereldspeler gemaakt waar het gaat om kennis, innovatie, handel en investeringen. De open samenleving, open economie, evenals de aanwezigheid van bedrijven en universiteiten die hoogwaardige technologie ontwikkelen en produceren en hoogwaardig wetenschappelijk onderzoek doen, maken Nederland echter ook tot een aantrekkelijk en in toenemende mate kwetsbaar doelwit van spionage. Het feit dat Nederland gastland is voor een groot aantal volkenrechtelijke organisaties en lid is van verschillende bondgenootschappen, zoals de EU en de NAVO, draagt er eveneens aan bij dat Nederland een interessant doelwit is voor spionage. Openbaar geworden incidenten, zoals rondom de OPCW en de casus beschreven in de brief van 10 december 2020 (Kamerstukken II 2020/21, 30977, nr. 157) vormen hiervan een illustratie. Uit het jaarverslag over 2020 van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) blijkt dat de Nederlandse overheid en in Nederland gevestigde internationale organisaties doelwit zijn van spionageactiviteiten. Buitenlandse mogendheden proberen onder andere binnen te komen bij ministeries, opsporings- en veiligheidsdiensten, politieke partijen en cultureel-maatschappelijke organisaties.

Digitalisering en globalisering zorgen daarbij voor nieuwe kwetsbaarheden, omdat landsgrenzen steeds minder een drempel opwerpen. De digitalisering van de samenleving heeft tot gevolg dat spionageactiviteiten in toenemende mate met behulp van technische en digitale middelen worden verricht. Het Cybersecuritybeeld Nederland 2020 (CSBN 2020) laat zien dat spionage en (voorbereidingen tot) sabotage van statelijke actoren het grootste digitale risico vormen voor de nationale veiligheid. Uit onderzoek van de AIVD en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) (hierna ook: de inlichtingen- en veiligheidsdiensten) blijkt dat meerdere Nederlandse topsectoren doelwit zijn (geweest) van (digitale) spionage.[1]

Spionage richt zich steeds meer niet alleen op het verkrijgen van staats- of bedrijfsgeheime informatie. Ook andere (ongerubriceerde) informatie 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 en de concurrentiepositie te versterken.

Verder zijn er meerdere gemeenschappen aanwezig in Nederland uit landen die vanuit een (vermeend) intern veiligheidsbelang op indringende en ontwrichtende wijze invloed proberen uit te oefenen binnen die gemeenschappen. Landen met een dergelijke diasporagemeenschap in Nederland worden – zoals ook hierboven geschetst – steeds assertiever en schrikken er daarbij niet voor terug leden van de diasporagemeenschap te mobiliseren om tegenstanders en critici binnen de gemeenschappen de mond te snoeren of onder druk te zetten om anderszins mee te werken. Familie- of vriendschapsbanden kunnen hierbij door een buitenlandse mogendheid als drukmiddel worden ingezet om handelingen ten behoeve van deze mogendheid te verrichten.

Voorgaande ontwikkelingen hebben aanleiding gegeven om opnieuw te kijken naar het beschikbare instrumentarium om spionageactiviteiten tegen te gaan.

2. Bestaand beleid en huidig wettelijk kader

Met de introductie van de aanpak statelijke dreigingen in 2019 (Kamerstukken II 2018/19, 30821, nr. 72) is een werkwijze ontstaan waarbij alle relevante partijen op een blijvende en continue basis bijdragen aan de weerbaarheid tegen statelijke actoren. De landenneutrale aanpak richt zich op de gehele maatschappij en werkt volgens een vaste systematiek van belangen-dreiging-weerbaarheid: welke veiligheidsbelangen moeten worden beschermd, wat is de dreiging vanuit statelijke actoren en hoe kan de weerbaarheid vergroot worden. Voor de dreiging van spionage door statelijke actoren is tot op heden vooral ingezet op het verhogen van de weerbaarheid.

Zoals ook in de inleiding werd geduid volgt uit het Cybersecuritybeeld Nederland 2020 dat spionage en (voorbereidingen tot) sabotage van statelijke actoren het grootste digitale risico vormen voor de nationale veiligheid.[1] Het kabinet werkt via de Nederlandse Cybersecurity Agenda (NCSA) met een brede aanpak aan het verhogen van de digitale weerbaarheid van Nederland, ook ten opzichte van de dreiging van statelijke actoren.[2] In dit kader heeft de AIVD in juni 2019 "Offensief cyberprogramma, een ideaal businessmodel voor staten" gepubliceerd.[3] De AIVD en de MIVD zetten zich in voor de bewustwording van de risico's van statelijke dreigingen zoals spionage en leggen waar mogelijk uit aan bedrijven, overheden en kennisinstellingen hoe ze dit nu en in de toekomst kunnen voorkomen dan wel er mee om kunnen gaan.

De Nederlandse inlichtingen- en veiligheidsdiensten trachten met onderzoeken onder andere zicht te krijgen op de spionageactiviteiten van andere landen. Met tegenmaatregelen proberen zij de Nederlandse veiligheidsbelangen te beschermen. Zo is bijvoorbeeld het dreigingsbeeld statelijke actoren (DBSA) opgesteld om de weerbaarheid van de samenleving in de vorm van bewustwording te vergroten. Een andere maatregel voor het tegengaan van spionageactiviteiten is om bestuursorganen, personen of instanties, zoals onderwijsinstellingen, kenniscentra of werkgevers, via voorlichting of in een concrete casus een ambtsbericht (op basis van de artikelen 62 en 67 Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv2017) te informeren over spionageactiviteiten die de Nederlandse inlichtingen- en veiligheidsdiensten hebben waargenomen. Daarmee worden de ontvangers in staat gesteld (rechts)maatregelen te treffen.

In aanvulling hierop is het van belang ook binnen het strafrecht voldoende mogelijkheden te bieden voor de aanpak van (ernstige vormen van) spionage. Versterking van de strafrechtelijke aanpak is een element van het bredere Nederlandse beleid zoals uiteengezet in de Kamerbrief over het tegengaan van statelijke dreigingen (Kamerstukken II 2018/19, 30821, nr. 72) en de beleidsreactie op het DBSA en de voortgang van de aanpak statelijke dreigingen (Kamerstukken II 2020/21, 30821 nr. 125).

Het Wetboek van Strafrecht bevat verschillende bepalingen die kunnen worden ingezet om ook strafrechtelijk op te treden tegen gedragingen die samenhangen met spionage. In het bijzonder

[1] Kamerstukken II 2019/20, 26 643, nr. 695.
[2] Kamerstukken II 2019/20, 26 643, nr. 695.
[3] AIVD-publicatie, "Offensief cyberprogramma, een ideaal businessmodel voor staten", zie: https://www.aivd.nl/documenten/publicaties/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten.

kan daarbij worden gedacht aan de strafbaarstellingen rondom het schenden van (staats-, beroeps-, ambts- en bedrijfs-) geheimen. Zie de artikelen 98 e.v. en 272 e.v. Sr. Deze bepalingen vergen echter dat sprake is van informatie waarvan geheimhouding geboden is. In gevallen waarin informatie niet geheim is, maar wel onrechtmatig is verkregen, bijvoorbeeld door het inbreken in computers of door diefstal en verduistering, kan daartegen in voorkomende gevallen eveneens strafrechtelijk worden opgetreden. Er zijn echter ook situaties denkbaar waarin degene die de informatie aan de buitenlandse mogendheid verstrekt daarover rechtmatig beschikt, terwijl die informatie niet (staats- of bedrijfs-)geheim is. Het delen van dergelijke informatie met een buitenlandse mogendheid is op dit moment niet strafbaar, terwijl ook in dergelijke gevallen zwaarwegende belangen van Nederland, Nederlandse bondgenoten, volkenrechtelijke organisaties gevestigd in Nederland of Nederlandse burgers ernstig geschaad kunnen worden. Op basis van ervaringen van de inlichtingen- en veiligheidsdiensten kan geconstateerd worden dat statelijke actoren ook belangstelling hebben voor het verkrijgen van dergelijke informatie. Zoals in paragraaf 1 al aan de orde kwam, kan ook ongerubriceerde informatie 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 of personen te beïnvloeden of om economisch voordeel te behalen en de eigen concurrentiepositie te versterken. Een voorbeeld is het geval waarin buitenlandse mogendheden op heimelijke wijze een contact met een Nederlandse ambtenaar (in Nederland of in het buitenland) opbouwen en onderhouden met het doel via dit ambtelijke contact informatie te verkrijgen over (vooralsnog) ongerubriceerde, maar wel cruciale of kwetsbare (politiek gevoelige) overheidsinformatie. Op deze plaats kan verder nog worden gewezen op diasporaspionage, waarbij vaak sprake is van het delen van niet geheime, maar wel gevoelige (persoons)informatie met een buitenlandse mogendheid, zoals gegevens over politieke voorkeur of religieuze achtergrond.

Bovendien geldt dat, zoals in paragraaf 1 beschreven, spionageactiviteiten niet alleen het delen van informatie of objecten met buitenlandse mogendheden omvatten. Het kan ook gaan om het ondersteunen of faciliteren van een buitenlandse mogendheid met bijvoorbeeld het ophalen en bezorgen van pakketjes, het volgen van personen, het plegen van sabotage en het verspreiden van informatie. Hoewel voor bijvoorbeeld de sabotage van vitale processen geldt dat dergelijke handelingen (onder omstandigheden) op grond van (Boek 2, Titel VII van) het Wetboek van Strafrecht kunnen worden geadresseerd, geldt dat niet voor een aantal van de andere genoemde voorbeelden.

3. Wetgeving in ons omringende landen

Een aantal ons omringende landen heeft specifieke bepalingen in hun strafwetgeving opgenomen om spionage tegen te gaan. Net als in Nederland gaat het daarbij bijvoorbeeld om strafbaarstelling van het delen van (staat)geheime informatie. Maar het gaat ook om bepalingen die betrekking hebben op het delen van niet (staats-, beroeps-, ambts-, of bedrijfs-) geheime informatie en het verrichten van andere activiteiten dan het verzamelen en delen van informatie. Een belangrijk kenmerk van verschillende buitenlandse strafbaarstellingen vormt het ontstaan van gevaar voor bepaalde belangen.
In Duitsland is, naast het delen van staatsgeheimen, op grond van §99 van het Strafgesetzbuch (StGB), strafbaar het uitvoeren van een spionageactiviteit («geheimdienstliche Tätigkeit») voor de geheime dienst van een buitenlandse mogendheid, gericht op het verstrekken van voorwerpen of inlichtingen (§99(1)(2) StGB). Ook het zich bereid verklaren tot dergelijke activiteiten tegenover (een tussenpersoon van) een buitenlandse geheime dienst is strafbaar (§99(1)(2) StGB). Het strafmaximum wordt verhoogd in «besonders schweren Fällen». Hiervan is in de regel sprake in gevallen waarin het gaat om geheime (overheids)informatie («Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten werden»), waarbij de betrokkene zijn vertrouwenspositie heeft misbruikt of wanneer er door de daad gevaar ontstaat voor een «schweren Nachteils für die Bundesrepublik Deutschland» (§99(2) StGB).

In Frankrijk zijn in de Code Pénal (CP) verschillende gedragingen die samenhangen met spionage afzonderlijk strafbaar gesteld. Strafbaar is het onderhouden van contacten met een buitenlandse mogendheid, buitenlands bedrijf, buitenlandse organisatie, een door een buitenlandse mogendheid gecontroleerd bedrijf of organisatie of diens agenten (hierna: buitenlandse actor) met het oogmerk om vijandelijkheden of daden van agressie tegen Frankrijk uit te lokken (artikel 411-4 CP) dan wel wanneer het aannemelijk is dat de fundamentele belangen van de staat daardoor worden geschaad («il est de nature à atteinte aux intérêts fondamentaux de la nation») (artikel 411-5 CP). Onder de fundamentele belangen van de staat worden verstaan de onafhankelijkheid, de integriteit van het grondgebied, de republieke vorm van bestuur, de middelen om zich te verdedigen en diplomatie te bedrijven, de bescherming van de bevolking, het milieu, de essentiële elementen van het wetenschappelijke en economische potentieel en het culturele erfgoed (artikel 410-1 CP). Eveneens strafbaar is het verstrekken, beschikbaar stellen en verzamelen van voorwerpen en inlichtingen aan een buitenlandse actor indien het aannemelijk is dat daardoor de fundamentele belangen van de staat worden geschaad (artikelen 411-6, 411-7 en 411-8 CP). Daarnaast bevat het Franse wetboek strafbaarstellingen van het vernielen, onbruikbaar maken of misbruiken van voorwerpen en installaties (artikel 411-9) en het verstrekken van valse informatie aan de Franse civiele en militaire autoriteiten (artikel 411-10) indien het aannemelijk is dat daardoor de fundamentele belangen van de staat worden geschaad.
Op grond van §107 van het Deense Wetboek van Strafrecht, het Straffeloven, is in Denemarken strafbaar hij die, ten behoeve van een buitenlandse mogendheid of organisaties inlichtingen vergaart of verstrekt die, in het belang van de Deense staat of maatschappij, geheim moeten worden gehouden, ongeacht of de inlichtingen juist zijn of niet.
In een aantal ons omringende landen, waaronder het Verenigd Koninkrijk, wordt verkend of aanvullende wetgeving nodig is om spionageactiviteiten van buitenlandse mogendheden beter te kunnen adresseren. Aanleiding hiervoor in het Verenigd Koninkrijk is de ontwikkeling die heeft plaatsgevonden ten aanzien van spionageactiviteiten, mede naar aanleiding van technologische en maatschappelijke ontwikkelingen. Daarbij worden nieuwe strafbaarstellingen overwogen, zoals de zelfstandige strafbaarstelling van sabotage, economische spionage en buitenlandse inmenging. In de consultatiefase ligt daarbij nog de vraag voor in welke mate er gedragingen zijn die onder deze noemers vallen, maar die niet met behulp van bestaande strafbaarstellingen kunnen worden geadresseerd. Blijkens de officiële website van de Britse overheid worden op dit moment de reacties op het discussiestuk dat ter consultatie op internet is geplaatst verwerkt. Zie: https://www.gov.uk/government/consultations/legislation-to-counter-state-threats.

4. Hoofdlijnen van het wetsvoorstel

Uit het voorgaande blijkt dat maatschappelijke ontwikkelingen hebben geleid tot nieuwe verschijningsvormen van spionage, waaronder digitale spionage en diasporaspionage. De digitalisering en globalisering bieden bovendien niet alleen Nederlandse burgers en bedrijven meer mogelijkheden, maar zorgen ook voor nieuwe dreigingen, waaronder kwetsbaarheid voor spionage. De open samenleving, open economie, evenals de aanwezigheid van bedrijven en universiteiten die hoogwaardige technologie ontwikkelen en produceren en hoogwaardig wetenschappelijk onderzoek doen, een groot aantal volkenrechtelijke organisaties en verschillende gemeenschappen uit landen die vanuit een (vermeend) intern veiligheidsbelang invloed proberen uit te oefenen, maken Nederland daarbij tot een aantrekkelijk doelwit van spionage. Zoals in paragraaf 2 uiteengezet wordt beleidsmatig sterk ingezet op het tegengaan van spionage. Ook het strafrecht speelt bij deze aanpak een rol. Het strafrecht biedt op dit moment echter nog onvoldoende mogelijkheden om op te treden tegen schadelijke spionageactiviteiten waarbij geen sprake is van een schending van (staats-, ambts- of bedrijfs-) geheimen of waarbij andere handelingen worden verricht dan het verstrekken van informatie. Mede om te voorkomen dat de Nederlandse wetgeving op dit punt achterblijft bij wetgeving in ons omringende landen, waardoor Nederland het risico loopt in verhouding tot die landen een aantrekkelijker doelwit te worden voor spionage, wordt voorgesteld een afzonderlijke strafbaarstelling in het Wetboek van Strafrecht op te nemen. Tegen de achtergrond van de digitalisering en de mogelijkheden die dat biedt voor spionageactiviteiten wordt daarnaast voorgesteld om de strafmaat te verhogen voor een aantal computerdelicten die in dat

verband een belangrijke rol kunnen spelen indien die worden gepleegd ten behoeve van een buitenlandse mogendheid.

4.1 Nieuwe strafbaarstelling

Met het wetsvoorstel wordt een nieuwe bepaling in het Wetboek van Strafrecht en het Wetboek van Strafrecht BES geïntroduceerd (98d Sr, 104d WvSr BES), waarin strafbaar wordt gesteld het verrichten van handelingen ten behoeve van een buitenlandse mogendheid, wetende dat daarvan gevaar is te duchten voor een of meerdere van de opgesomde belangen. Omdat spionageactiviteiten in de praktijk een veelheid aan gedragingen kunnen betreffen, is in de voorgestelde strafbaarstelling gekozen om het verrichten van «handelingen» onder de hiervoor genoemde omstandigheden strafbaar te stellen. Bij «handelingen» kan onder meer gedacht worden aan het verzamelen van inlichtingen en het plegen van sabotage, maar ook bijvoorbeeld aan het afleveren van pakketjes, het in de gaten houden, volgen of intimideren van in Nederland verblijvende personen en de openbaarmaking of verspreiding van informatie. In de nieuwe strafbaarstelling wordt afzonderlijk genoemd het verstrekken aan een buitenlandse mogendheid van inlichtingen, voorwerpen of gegevens (hierna: informatie of voorwerpen). Deze gedraging – die een klassieke spionageactiviteit betreft – is afzonderlijk opgenomen, om zeker te stellen dat ook het verstrekken van informatie of voorwerpen die de betrokkene rechtmatig onder zich heeft strafbaar is, indien de betrokkene die informatie of voorwerpen opzettelijk heeft verstrekt aan een buitenlandse mogendheid wetende dat daarvan gevaar is te duchten voor de in de aanhef van de voorgestelde bepaling opgenomen belangen. Anders dan op grond van bestaande bepalingen in het Wetboek van Strafrecht (zie paragraaf 2) hoeft het geen (staats-, beroeps-, ambts- of bedrijfs-) geheime informatie te betreffen. Indien wel sprake is van dergelijke geheime informatie, kan de officier van justitie afhankelijk van de omstandigheden van het geval kiezen voor een vervolging op grond van de bestaande bepalingen of deze nieuwe bepaling. Bij die afweging zal de mate waarin de delictsbestanddelen van de verschillende bepalingen zijn vervuld een rol spelen. Als de gedraging bijvoorbeeld niet is gepleegd ten behoeve van buitenlandse mogendheid, zal in de regel alleen vervolging op grond van de al bestaande strafbaarstellingen die dit vereiste niet kennen, mogelijk zijn. Daarnaast kan het gaan om bijvoorbeeld overwegingen ten aanzien van de strafmaat en de (maatschappelijke) kwalificatie van de gedraging.
Blijkens de bepaling is zowel het onmiddellijk als middellijk verstrekken van informatie en voorwerpen strafbaar. Daarmee is ook het verstrekken van informatie en voorwerpen via bijvoorbeeld tussenpersonen strafbaar, mits aan het opzetvereiste is voldaan (zie hierna). Ook voor de andere gedragingen geldt dat het vereiste dat zij «ten behoeve» van een buitenlandse mogendheid zijn verricht, niet betekent dat de betrokkene zelf rechtstreeks in contact stond met een buitenlandse mogendheid ten behoeve van wie de handelingen zijn verricht; tussenpersonen kunnen een rol spelen. Ook wanneer de 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, kan sprake zijn van het verrichten van de handelingen ten behoeve van respectievelijk het middellijk of onmiddellijk verstrekken van informatie of voorwerpen aan een buitenlandse mogendheid.

Opzetvereiste

Degene die de in de voorgestelde bepaling opgenomen gedragingen verricht, is daarvoor alleen strafbaar indien hij de gedragingen heeft gepleegd «wetende dat» er gevaar is te duchten voor de in het eerste lid van de voorgestelde bepalingen genoemde zwaarwegende belangen. Hiermee wordt tot uitdrukking gebracht dat de verdachte zich bewust moet zijn geweest – in de zin van opzet – van deze gevaarzetting en die tot drijfveer moet hebben gehad of op de koop toe hebben genomen. De verdachte moet er daarnaast opzet op hebben gehad de handelingen te verrichten ten behoeve van een buitenlandse mogendheid. In dit opzetvereiste schuilt een belangrijke beperking van de strafbaarheid. Personen die bijvoorbeeld niet konden weten dat zij handelingen verrichtten voor een buitenlandse mogendheid, zijn niet strafbaar. Het opzetvereiste «wetende dat» omvat blijkens de jurisprudentie van de Hoge Raad ook voorwaardelijk opzet (zie HR 30 mei

2008, ECLI:NL:HR:2008:BC8673, *NJ* 2008/318). Dat betekent dat een persoon ook strafbaar is als hij bewust de aanmerkelijke kans heeft aanvaard (op de koop heeft toegenomen) dat gevaar zou komen te duchten voor de genoemde belangen en dat zijn handelingen werden verricht ten behoeve van een buitenlandse mogendheid. Bij het bewijs van (voorwaardelijk) opzet kunnen objectieve omstandigheden een rol spelen. Dit betekent dat bijvoorbeeld ook het karakter van de handelingen en de aard van de betreffende informatie betrokken kunnen worden bij de vaststelling van het opzet. Hierbij kan worden gedacht aan omstandigheden zoals de heimelijkheid van het contact of de handelingen, het handelen in strijd met integriteitscodes, het gebruikmaken van versleutelde communicatie of codetaal en de gevoeligheid van de betrokken informatie.

Er kunnen zich situaties voordoen waarin een persoon handelingen verricht ten behoeve van een buitenlandse mogendheid bijvoorbeeld omdat hij daartoe onder druk gezet of gedwongen wordt. Hoewel dat ook bij andere vormen van spionage voorkomt, speelt dit in het bijzonder bij de diasporaspionage. De nieuwe strafbaarstelling kan er in voorkomende gevallen aan bijdragen dat personen meer weerstand kunnen bieden aan vormen van drang. Onder verwijzing naar de strafbaarstelling kunnen zij aangeven dat het niet mogelijk is te voldoen aan eventuele verzoeken gedaan door of namens een buitenlandse mogendheid. Er zijn echter ook gevallen voorstelbaar waarin personen dusdanig onder druk worden gezet dat van hen niet gevergd kan worden dat zij weerstand bieden aan die druk – en in zekere zin zelf ook «slachtoffer» zijn van de buitenlandse mogendheid. Voorkomen moet worden dat personen in dergelijke gevallen strafbaar zijn. Daartoe kan worden teruggevallen op de strafuitsluitingsgronden. In het bijzonder kan worden gewezen op artikel 40 Sr. Op basis van die bepaling is niet strafbaar «hij die een feit begaat waartoe hij door overmacht is gedrongen». Hieronder vallen naast situaties van absolute overmacht ook gevallen waarin sprake is van «psychische overmacht» (de verdachte heeft gehandeld onder van buiten komende drang waaraan de verdachte redelijkerwijs geen weerstand kon en ook niet behoefde te bieden (vgl. HR 9 oktober 2012, *NJ* 2012/594)) en «overmacht als noodtoestand» (de verdachte werd geconfronteerd met een conflict van belangen, waarin het maken van een keuze tussen twee onderling strijdige belangen acuut en onontkoombaar is, waarbij de verdachte de zwaarstwegende heeft laten prevaleren (vgl. HR 18 mei 2010, *NJ* 2010/289)). De mate waarin de verdachte zichzelf in een overmachtssituatie heeft gebracht waarin het strafbare feit voorzienbaar was («culpa in causa») kan een rol spelen bij de beoordeling van een beroep op deze strafuitsluitingsgrond.

Belangen

Zoals hiervoor aan de orde kwam zijn opzettelijke handelingen verricht ten behoeve van een buitenlandse mogendheid alleen strafbaar indien degene die de handeling verricht kon weten of de aanmerkelijke kans op de koop toenam dat daarvan gevaar te duchten is voor een of meerdere van de in het eerste lid opgesomde belangen. Dat het gaat om «gevaar» dat van de handelingen is «te duchten» betekent, net als bij andere delictsomschrijvingen waarin deze term wordt gebezigd, dat het gevaar zich (nog) niet hoeft te hebben verwezenlijkt. Het belang hoeft (nog) niet te zijn geschaad. Het gaat er om dat sprake is van een reële (voorzienbare) mogelijkheid van schade voor het desbetreffende belang.

In de strafbaarstelling wordt aangeknoopt bij een aantal te beschermen belangen die door de handelingen kunnen worden geschaad. Hoewel er enige overlap tussen de verschillende belangen kan bestaan, worden zij afzonderlijk genoemd. Er is dus niet gekozen voor een overkoepelende term zoals «fundamentele belangen van de staat» of «gewichtige belangen van de staat». Omdat het zich bewust zijn van de gevaarzetting – in de vorm van (voorwaardelijk) opzet – een belangrijke voorwaarde voor (en daarmee ook beperking van) de strafbaarheid vormt, wordt het van belang geacht op dit punt zoveel mogelijk duiding te geven ten aanzien van de belangen waar het om gaat.

Het eerste belang dat genoemd wordt is de «veiligheid van de staat, van zijn bondgenoten of van een volkenrechtelijke organisatie». Hieronder kunnen worden begrepen de zes nationale veiligheidsbelangen, zoals beschreven in de Nationale Veiligheidsstrategie 2019, te weten

territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en het functioneren van de internationale rechtsorde. Met «volkenrechtelijke organisatie» wordt – net als elders in het Wetboek van Strafrecht – gedoeld op een samenwerkingsvorm tussen staten die zijn grondslag vindt in het volkenrecht, met gemeenschappelijke doelstellingen en met ten minste een orgaan om die doelstelling te vervullen. Zie Kamerstukken II 1998/99, 26469, nr. 3, p. 13. De volkenrechtelijke organisatie is opgenomen, ten eerste vanwege het belang van dergelijke organisaties voor de internationale en Nederlandse rechtsorde en veiligheid. De belangen van deze organisaties zijn onlosmakelijk verbonden met de belangen van de Nederlandse nationale veiligheid. De internationale rechtsorde is, zoals uit het voorgaande blijkt, dan ook benoemd als een van de zes nationale veiligheidsbelangen in de nationale veiligheidsstrategie. Ten tweede omdat Nederland verschillende volkenrechtelijke organisaties huisvest. Nederland is een belangrijk gastland van internationale organisaties. Den Haag, als stad van Vrede en Recht, behoort met Brussel, Genève en Wenen tot de internationale top van vestigingsplaatsen. In artikel 1 van de Regeling aanwijzing volkenrechtelijke organisaties in Nederland 2015 wordt een opsomming gegeven van als volkenrechtelijke organisatie aangewezen organisaties in Nederland. Het gastlandschap voor internationale organisaties is een pijler van de invulling van artikel 90 van de Nederlandse Grondwet, die stelt dat de regering de ontwikkeling van de internationale rechtsorde bevordert. Het draagt bij aan de reputatie van Nederland in het buitenland en aan het Nederlandse internationale netwerk. De aanwezigheid van internationale organisaties levert een positieve bijdrage aan de Nederlandse economie, zowel door directe uitgaven van deze organisaties in Nederland als via bedrijven die in het kielzog van internationale organisaties naar Nederland komen. Nu Nederland een groot aantal volkenrechtelijke organisaties huisvest, betekent dat ook dat Nederland een verantwoordelijkheid heeft om deze organisaties te beschermen tegen spionage.

Het tweede belang dat is opgenomen in de voorgestelde wettekst is de «vitale infrastructuur». De vitale infrastructuur wordt gevormd door het samenstel van de vitale processen. Het gaat daarbij om voorzieningen, systemen of delen daarvan die van essentieel belang zijn voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn (vgl. Kamerstukken II 2014/15, 34034, nr. 3, p. 9). Elektriciteitsvoorziening, toegang tot internet, drinkwatervoorziening en betalingsverkeer zijn voorbeelden van vitale processen. Verwezen wordt ook naar het overzicht van processen die op dit moment in Nederland zijn geïdentificeerd als vitaal.[4] Door de continuïteit, weerbaarheid, vertrouwelijkheid of integriteit van vitale processen te verstoren kan een kwaadwillende buitenlandse mogendheid de stabiliteit van de Nederlandse samenleving verminderen dan wel maatschappelijke ontwrichting veroorzaken. In het jaarverslag over 2019 van de AIVD en in het DBSA werd benoemd dat er richting (diverse onderdelen van) de Nederlandse vitale infrastructuur een reële dreiging vanuit buitenlandse mogendheden uit gaat, die er op gericht is om systemen in deze sectoren (op een nader door deze buitenlandse mogendheden gewenst moment) te verstoren of zelfs te saboteren. Door de vaak noodzakelijke interactie en communicatie tussen de systemen van verschillende entiteiten (veelal via internet) kan een succesvolle digitale aanval op één entiteit gevolgen hebben voor een veel groter gedeelte van de vitale infrastructuur (het zogenaamde cascade effect).

Het derde belang dat wordt genoemd is de «integriteit en exclusiviteit van hoogwaardige technologieën». De ontwikkeling van hoogwaardige technologieën is van groot belang. Zij dragen bij aan maatschappelijke kwesties, zoals de energietransitie, de productie van gezond en duurzaam voedsel en de bestrijding levensbedreigende ziektes. Zowel vanuit Nederland als vanuit de EU wordt innovatie dan ook gestimuleerd. Technologische ontwikkelingen brengen echter ook risico's met zich mee, zeker als ze in kwaadwillende handen vallen en tegen Nederland of andere landen worden ingezet. Het gaat daarbij niet alleen om risico's voor de nationale veiligheid, voor vitale processen en de veiligheid van personen, maar ook voor de economische en strategische positie van Nederland. Veel technologie en kennis heeft grote innovatieve waarde en levert daarmee een belangrijke bijdrage aan de Nederlandse welvaart. Ongewenste kennisoverdracht schaadt de

[4] Zie: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

concurrentiepositie van Nederland en kan ontwrichtende gevolgen hebben voor de economie en de samenleving. Om die reden zijn de integriteit en exclusiviteit van hoogwaardige technologieën als afzonderlijk belang opgenomen in de voorgestelde bepaling.
Onder «hoogwaardige technologieën» wordt verstaan militaire technologieën, technologieën die een «dual use» toepassing hebben[5]; (andere) technologieën die van essentieel belang zijn voor het functioneren van defensie, opsporings-, inlichtingen- en veiligheidsdiensten bij de uitoefening van hun taken; technologieën die essentieel zijn om onaanvaardbare risico's voor de verkrijgbaarheid van bepaalde essentiële producten of voorzieningen te voorkomen; en technologieën die worden gekenmerkt door een breed toepassingsbereik binnen verschillende vitale processen of processen die raken aan de nationale veiligheid. Verder kan worden gedacht aan vernieuwende technologieën die (ook) gebruikt kunnen worden voor sabotage of spionage of die anderszins kwaadaardig kunnen worden toegepast tegen Nederland of andere landen. Tot slot worden onder «hoogwaardige technologieën» begrepen innovatieve technologieën die van groot belang zijn voor de economische en strategische positie van Nederland, zoals quantum-computing, kunstmatige intelligentie, hoogwaardige micro-elektronica (waaronder semi-conductoren), DNA-technieken en agrarische innovatie als zaadveredeling, precisielandbouw en kassentechnologie.

Als vierde en laatste beschermingswaardig belang wordt genoemd «de veiligheid van een of meer personen». Dit belang is opgenomen, mede met het oog op de zogenoemde «diasporaspionage». Bij deze vorm van spionage – waarbij een buitenlandse mogendheid zich, zoals ook in paragraaf 1 is omschreven, richt op het aan zich binden en controleren van diasporagemeenschappen – worden methoden als intimidatie en chantage niet geschuwd. Een gevolg van deze vorm van spionage kan zijn, zoals eerder al aan de orde kwam, dat de veiligheid van personen hierdoor in gevaar komt. Dit geldt niet alleen voor de personen die onder druk worden gezet, maar ook voor personen over wie bijvoorbeeld persoonsgegevens (adres, politieke voorkeur, religieuze achtergrond, familiebanden, etc.) aan buitenlandse mogendheden worden verstrekt. Uiteraard heeft dit belang ook betekenis voor gevallen waarin de veiligheid van individuen die niet behoren tot een diasporagemeenschap, bijvoorbeeld (individuele) politieke dissidenten die in Nederland verblijven, in het geding is.

Een ander bewegen tot spionageactiviteiten

Voorgesteld wordt om niet alleen degene die de hiervoor beschreven gedragingen ten behoeve van de buitenlandse mogendheid verricht, maar ook degene die de ander beweegt om dergelijke gedragingen te verrichten strafbaar te stellen. Ook personen werkzaam voor buitenlandse inlichtingendiensten, evenals (andere) eventuele tussenpersonen vallen aldus binnen het bereik van deze strafbaarstelling. Uitlokking is als zodanig in algemene zin strafbaar gesteld in artikel 47 Sr. Uitlokking is op grond van die bepaling echter alleen strafbaar indien een of meerdere van de opgesomde uitlokkingsmiddelen zijn ingezet. In het kader van spionageactiviteiten is het echter van belang dat tussenpersonen niet alleen strafbaar zijn als zij bijvoorbeeld personen giften in het vooruitzicht stellen, bedreigen of misleiden, maar ook als zij personen «slechts» overtuigen of aansporen om spionagehandelingen te verrichten, en die personen daartoe vervolgens over gaan. Om dat te verzekeren wordt voorzien in een aparte strafbaarstelling in het voorgestelde artikel 98d, tweede lid, Sr en artikel 104d, tweede lid, WvSr BES. Deze strafbaarstelling omvat ook gevallen waarin degene die de spionagehandelingen verricht niet strafbaar is, bijvoorbeeld omdat hij een beroep op een strafuitsluitingsgrond kon doen. Deze strafbaarstelling omvat daarmee ook vormen van «doen plegen».

4.2 Strafverzwaringsgrond computermisdrijven

Zoals hiervoor beschreven, biedt de digitalisering aanvullende mogelijkheden voor spionageactiviteiten. Deze activiteiten omvatten bijvoorbeeld het inbreken in computersystemen, het plaatsen van kwaadaardige software of het overnemen van gegevens. Op deze wijze kunnen (vitale) processen en het werk van overheden en bedrijven verstoord of stilgelegd worden of kan

[5] Technologieën die doorgaans een normale, civiele toepassing hebben, maar die ook kunnen worden gebruikt voor militaire doeleinden.

bijvoorbeeld gevoelige informatie worden verkregen die buitenlandse mogendheden kunnen aanwenden om besluitvormingsprocessen te beïnvloeden of economische schade aan te richten. Dergelijke handelingen gepleegd ten behoeve van buitenlandse mogendheden kunnen derhalve grote gevolgen hebben, niet alleen voor de individuele burger, (overheids)organisatie of het bedrijf dat direct door de activiteit wordt geraakt, maar ook voor de Nederlandse samenleving als geheel. De ernst van deze feiten komt echter tot op heden nog onvoldoende tot uitdrukking in de strafmaat die geldt voor de verschillende computermisdrijven. In verschillende computermisdrijven zijn wel strafverzwarende omstandigheden opgenomen, zoals de omstandigheid dat het strafbare feit is gepleegd met het oogmerk om zichzelf of een ander wederrechtelijk te bevoordelen. De omstandigheid dat het feit is gepleegd ten behoeve van een buitenlandse mogendheid geldt echter nog niet als strafverzwarend. Voorgesteld wordt die strafverzwaringsgrond alsnog op te nemen bij computermisdrijven die een belangrijke rol kunnen spelen bij spionage. Het strafmaximum wordt daardoor met een derde verhoogd indien die feiten zijn gepleegd ten behoeve van een buitenlandse mogendheid.

Op zichzelf vallen de in de computermisdrijven opgenomen gedragingen ook onder de reikwijdte van het begrip «handelingen» in de voorgestelde artikelen 98d Sr en 140d WvSr BES. De computermisdrijven kunnen desalniettemin een meerwaarde hebben ten opzichte van die bepalingen in gevallen waarin niet bewezen kan worden dat de betrokkene wist of op de koop toenam dat daarvan gevaar te duchten is voor de in de voorgestelde strafbaarstelling genoemde belangen. In dergelijke gevallen kan worden teruggevallen op de computerdelicten. Indien in dat geval wel duidelijk is dat de gedragingen zijn gepleegd ten behoeve van een buitenlandse mogendheid, kan dat gegeven als strafverzwarende omstandigheid ten laste worden gelegd.

5. Opsporing en vervolging

Op basis van een inschatting van de betrokken uitvoeringsorganisaties zal dit wetsvoorstel jaarlijks tot een beperkt aantal zaken leiden. In de praktijk zal in de regel een ambtsbericht van de AIVD of de MIVD aan de basis liggen van een opsporingsonderzoek naar gedragingen die samenhangen met spionage. Het is ook mogelijk dat aangifte wordt gedaan door bijvoorbeeld een getroffen bedrijf of een persoon uit een diaspora. Daarnaast kunnen politie en OM over eigen informatie beschikken uit strafrechtelijke onderzoeken. Dit laatste zal met name voorkomen bij onderzoeken naar (hightech) cybercrime. De toenemende vermenging tussen criminele- en statelijke actoren in het cyberdomein is daarvan een oorzaak. Deze vermenging is ook in het CSBN 2021 geconstateerd. Op basis van deze eigen informatie – en de onduidelijkheid over de aard van de actor – kan het OM besluiten een nieuw strafrechtelijk onderzoek te openen. Als een van de inlichtingen- en veiligheidsdiensten beschikt over voor de opsporing of vervolging relevante informatie, is er de mogelijkheid om via een ambtsbericht de Landelijke Officier van Justitie te informeren op basis van artikel 66 van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: WIV 2017). De inlichtingen- en veiligheidsdiensten hebben op grond van artikel 17 WIV 2017 zelf geen bevoegdheid tot het opsporen van strafbare feiten. Niet in alle gevallen waarin spionageactiviteiten plaatsvinden die mogelijk in aanmerking komen voor een strafrechtelijke vervolging, zal een ambtsbericht worden afgegeven. De inlichtingen- en veiligheidsdiensten dienen immers binnen het eigen stelsel een afweging te maken tussen enerzijds de wettelijke plicht tot het beschermen van eigen bronnen en het voortzetten van inlichtingenonderzoek ten faveure van bijvoorbeeld de kennis van modus operandi van de betrokken buitenlandse mogendheid en anderzijds de noodzaak de dreiging op korte termijn te mitigeren zoals via het uitbrengen van een ambtsbericht met inachtneming van eventuele diplomatieke gevolgen. Voorafgaand aan het eventueel uitbrengen van een ambtsbericht zullen de inlichtingen- en veiligheidsdiensten het handelingsperspectief toetsen bij Landelijke Officier van Justitie Terrorismebestrijding op basis van artikel 66 WIV 2017 en waar nodig ook overige belanghebbenden binnen de rijksoverheid betrekken.

Bovendien zal het niet in alle gevallen mogelijk zijn (alle) betrokkenen bij spionageactiviteiten te vervolgen en te berechten. In voorkomende gevallen kan sprake zijn van immuniteit en/of onschendbaarheid onder internationaal recht. Te denken valt hierbij aan leden van diplomatieke en

consulaire zendingen en officiële missies. In dergelijke gevallen zijn aanhouding en vervolging niet aan de orde, tenzij de zendstaat van de buitenlandse overheidsfunctionaris hiermee instemt. Met de zendstaat wordt hier bedoeld de staat in wiens opdracht de buitenlandse overheidsfunctionaris handelt. Het is ook mogelijk (bij digitale activiteiten) dat betrokkenen bijvoorbeeld vanuit het buitenland opereren en hun identiteit niet achterhaald kan worden of uitlevering niet mogelijk is. De nieuwe strafbaarstelling biedt echter – door de uitbreiding van de strafbaarheid – in meer gevallen dan nu mogelijkheden om een vervolging in te stellen, evenals om in meer gevallen een verzoek aan het buitenland om rechtshulp te doen. Aan de basis van een dergelijk verzoek om rechtshulp in het strafrechtelijke domein dient immers een strafbaar feit te liggen.

6. Verhouding tot hoger recht

De voorgestelde strafbaarstelling kan tot gevolg hebben dat verschillende rechten worden beperkt. In het bijzonder kan worden gedacht aan het recht op vrijheid van meningsuiting. Dit recht wordt onder andere beschermd door artikel 10 van het Europees Verdrag voor de Rechten van de Mens (EVRM). Het recht op vrijheid van meningsuiting omvat zowel het recht om een mening te koesteren, als om informatie of denkbeelden te verstrekken en te ontvangen. In het recht op vrijheid van meningsuiting ligt het recht op informatiegaring besloten. Beperkingen die worden gesteld aan de vrijheid om informatie te vergaren of verspreiden gelden als een beperking van de vrijheid van meningsuiting. Beperkingen van dit recht zijn op grond van artikel 10, tweede lid, EVRM toegestaan mits zij bij wet zijn voorzien, een legitiem doel dienen, en noodzakelijk zijn in een democratische samenleving.

Bij wet voorzien
Een beperking op het recht op vrijheid van meningsuiting en informatiegaring vergt een wettelijke grondslag. Deze wettelijke grondslag moet voldoen aan de vereisten van toegankelijkheid («accessibility») en voorzienbaarheid («foreseeability»). De wettelijke grondslag moet dus kwalitatief in orde zijn en voldoende waarborgen bieden tegen willekeurig optreden. Volgens het Europees Hof voor de Rechten van de Mens (EHRM) is echter een logisch gevolg van het feit dat wetgeving algemene normen stelt dat wetgeving tot op zekere hoogte open (vage) normen omvat («are inevitably couched in terms which, to a greater or lesser extent, are vague»). De wet mag enige ruimte laten om veranderende omstandigheden mee te kunnen nemen («keep pace with changing circumstances») en nadere invulling van normen via rechterlijke interpretatie is toegestaan. Zie o.a. EHRM 25 mei 1993, appl.no. 14307/88 (*Kokkinakis*), §40; EHRM 11 november 1996, appl.no. 17862/91 (*Cantoni*), §31, EHRM 23 september 1998, appl.no. 72/1997/856/1065 (*McLeod*), §41; EHRM 12 februari 2009, appl.no. 21906/04 (*Kafkaris*) §140-141.
Met de voorgestelde regeling wordt in de benodigde wettelijke grondslag voorzien. De strafbaarstelling is voldoende nauwkeurig en specifiek. Zoals in paragraaf 4.1 aan de orde is gekomen, is er bewust voor gekozen om de verschillende belangen afzonderlijk te benoemen om zo meer handvatten te geven voor de beoordeling welke gedragingen onder de strafbaarstelling vallen. Daarnaast kan worden gewezen op het opzetvereiste, dat als wezenlijke voorwaarde voor verwijtbaarheid en strafbaarheid een drempel opwerpt, evenals de strafuitsluitingsgronden, die strafbaarheid voorkomen in gevallen waarin de gedraging de betrokkene niet kan worden verweten of daarvoor een rechtvaardiging bestond. Naar aanleiding van de doenvermogentoets zal voorlichtingsmateriaal worden ontwikkeld over spionage en dit wetsvoorstel.

Legitiem doel
Het tweede lid van artikel 10 EVRM somt verschillende legitieme doelen op. Hier kan in het bijzonder worden gewezen op het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid, de bescherming van de rechten van anderen en het voorkomen van de verspreiding van vertrouwelijke mededelingen. De in het voorgestelde artikel 98d Sr en 104d WvSr BES opgesomde belangen (de veiligheid van de staat, van zijn bondgenoten of van een volkenrechtelijke organisatie, de vitale infrastructuur, de integriteit en exclusiviteit van hoogwaardige technologieën, de veiligheid van een of meer in Nederland verblijvende personen) kunnen onder deze doelen worden geschaard.

Noodzakelijk in een democratische samenleving
Bij dit vereiste is relevant of er een dringende maatschappelijke behoefte («pressing social need») bestaat tot overheidsingrijpen. Lidstaten hebben hierbij een zekere «margin of appreciation», een afwegingsruimte.
Zoals hiervoor in deze memorie van toelichting is beschreven zijn er verschillende maatschappelijke ontwikkelingen die nopen tot een aanvullende strafbaarstelling. Spionageactiviteiten hebben zich ontwikkeld en hebben nieuwe verschijningsvormen. Staten proberen op steeds assertievere wijze hun eigen belangen na te streven en daarbij hanteren zij in toenemende mate andere regels, normen en waarden dan die in Nederland en de internationale (westerse) gemeenschap worden gehuldigd. Spionageactiviteiten die in dat kader worden uitgeoefend zijn schadelijk voor de soevereiniteit en het handelingsvermogen van de Nederlandse overheid, het functioneren van de democratische en internationale rechtsorde en de daarin gedeelde waarden, het verdien- en concurrentievermogen van Nederland alsmede voor de veiligheid van burgers en gemeenschappen. Daarbij is van belang dat – naast het in kaart brengen van spionageactiviteiten en het in een concreet geval nemen van tegenmaatregelen om de (voortzetting van de) activiteiten te verhinderen – kan worden opgetreden tegen personen die deze activiteiten ontplooien. De huidige strafrechtelijke bepalingen bieden op dit moment op onderdelen echter onvoldoende (krachtige) handvatten om tegen schadelijke gedragingen op te treden, zoals eerder in deze memorie is beschreven. Om de risico's van spionageactiviteiten te verminderen en genoemde schade te vermijden is het dan ook van belang om de strafbaarstelling van spionage te verruimen. Zoals eerder in deze memorie aan de orde gekomen, is daarbij gezocht naar een zorgvuldige afbakening van de gedraging, onder andere via het opzetvereiste en de opsomming van belangen. Bovendien is aangeknoopt bij zeer zwaarwegende en beschermingswaardige belangen. Het strafmaximum van zes jaar gevangenisstraf doet recht aan de ernst van het feit en sluit aan bij de strafmaat die geldt voor soortgelijke delicten.

Journalisten en wetenschappers
Artikel 10 EVRM beschermt ook de rechten van journalisten en wetenschappers om informatie te verzamelen, te ontvangen en te verspreiden. Het is geenszins de bedoeling van de voorgestelde bepaling om journalistieke en wetenschappelijke activiteiten te verhinderen of bemoeilijken. In de regel zullen activiteiten van journalisten en wetenschappers niet onder het bereik van de bepaling vallen. Zij zullen in de regel immers geen opzet hebben op het laten ontstaan van gevaar voor de in de nieuwe bepaling opgesomde zwaarwegende belangen. Bij de beoordeling van het opzet spelen bovendien het recht op vrije nieuwsgaring en de academische vrijheid een rol. Wanneer sprake is van journalistieke of wetenschappelijke activiteiten kan tot uitgangspunt worden genomen dat aan het opzetvereiste niet is voldaan. Dat is uiteraard anders indien de hoedanigheid van journalist of wetenschapper wordt misbruikt als dekmantel voor spionageactiviteiten.

Artikel 7 van de Grondwet
De vrijheid van meningsuiting wordt ook beschermd door artikel 7 van de Grondwet. Het derde lid van dit artikel bepaalt dat niemand voorafgaand verlof nodig heeft voor het openbaren van gedachten en gevoelens door andere middelen dan de drukpers en omroep, behoudens ieders verantwoordelijkheid volgens de wet. Dit recht impliceert het recht een mening te uiten, waarbij alleen de wet in formele zin beperkingen kan stellen. Zoals hiervoor aan de orde kwam, biedt de hier voorgestelde strafbaarstelling deze grondslag in een wet in formele zin. Van voorafgaan verlof is bij het strafrecht naar zijn aard geen sprake. Strafrechtelijk optreden strekt ter handhaving achteraf van een overschrijding van een wettelijke norm, in casu de voorgestelde strafbaarstelling van spionagehandelingen. Voor de overige overwegingen ten aanzien van de verhouding van de nieuwe strafbaarstelling tot de vrijheid van meningsuiting wordt verwezen naar de voorgaande passage over artikel 10 EVRM.

Diplomaten
Het verzamelen van informatie over een gastland is een reguliere functie van diplomatieke en consulaire vertegenwoordigingen in Nederland. Deze functie is vastgelegd in, onder andere, het

Verdrag van Wenen inzake diplomatiek verkeer (*Trb.* 1962, nr. 101). Het wetsvoorstel beoogt niet deze reguliere functie van diplomatieke en consulaire vertegenwoordigingen in Nederland strafbaar te stellen of afbreuk te doen aan de bevoegdheid daartoe. Afgezien van dat in dergelijke gevallen veelal niet zal zijn voldaan aan het vereiste opzet op het in gevaar brengen van in de voorgestelde bepaling opgenomen zwaarwegende Nederlandse belangen, ontneemt de omstandigheid dat de activiteiten zijn verricht overeenkomstig de daarvoor geldende de verdragen de strafbaarheid aan het handelen. Overigens zal veelal ook sprake zijn van diplomatieke onschendbaarheid of immuniteit.

Gelet op voorgaande meent het kabinet dat de voorgestelde regeling noodzakelijk is en met voldoende waarborgen is omkleed.

7. Uitvoerings- en financiële consequenties

Als gevolg van de uitbreiding van de strafbaarheid van spionage zullen naar verwachting meer zaken opgespoord, vervolgd en voor de rechter gebracht worden. Naar verwachting betreft dit een beperkt aantal zaken per jaar, zo kwam in paragraaf 5 al aan de orde. De kosten die met dit wetsvoorstel gemoeid zijn, bestaan uit personeelskosten, kosten voor opleiding en voor de tenuitvoerlegging van vrijheidsstraffen. Deze uitvoeringskosten zijn beperkt en worden gedekt uit de begroting JenV.
De strafprocedure wijzigt door de voorgestelde wetswijziging niet. Naar verwachting zijn de gevolgen voor (werkprocessen en automatisering bij) de verschillende bij de strafrechtspleging betrokken organisaties en voor de rechtsbijstand dan ook beperkt.
Wel zullen de politie en het OM meer structureel in overleg treden met de inlichtingen- en veiligheidsdiensten ten behoeve van informatie-uitwisseling over en coördinatie van de uitvoering en handhaving van de in dit wetsvoorstel voorgestelde strafbare gedragingen. Voor informatie-uitwisseling tussen de uitvoeringsorganisaties lijken vooralsnog geen nieuwe of aanvullende afspraken benodigd; de bestaande afspraken in het kader van het afstemmingsoverleg waarin onder andere terrorisme en cyber gerelateerde zaken worden besproken, lijken hiervoor te volstaan. Omdat geen nieuwe informatie wordt uitgewisseld naar aanleiding van dit wetsvoorstel wordt beoordeeld dat een gegevensbeschermingseffectbeoordeling niet hoeft te worden uitgevoerd.
In aanvulling op intensievere afstemming naar aanleiding van dit wetsvoorstel zullen de politie en het OM hun opleidingen en beleidsregels opnieuw moeten bezien in het licht van de voorgestelde uitbreiding van de strafbaarheid van spionage. Als hierboven beschreven brengt het wetsvoorstel, vanwege de specialistische kennis die is vereist voor de betreffende casuïstiek, personeelskosten met zich en zijn kosten begroot voor de tenuitvoerlegging van veroordelingen voor overtreding van de in dit wetsvoorstel voorgestelde normen.

II. Artikelsgewijze toelichting

Artikel I, onderdeel A en Artikel II, onderdeel A

Met deze artikelonderdelen wordt voorzien in rechtsmacht in gevallen waarin de spionageactiviteiten in het buitenland worden gepleegd. Daarbij zal het in beginsel gaan om spionageactiviteiten vanuit het buitenland gericht tegen de nationale veiligheid van Nederland, de Nederlandse vitale infrastructuur, door Nederlandse bedrijven en wetenschappelijke instellingen ontwikkelde hoogwaardige technologieën, de veiligheid van Nederlandse ingezetenen (ongeacht waar zij zich bevinden) en de veiligheid van personen die (tijdelijk) feitelijk in Nederland verblijven (zoals toeristen, zakenlieden of vluchtelingen). Zowel de nieuwe strafbaarstelling als het gewijzigde onderdeel a van de rechtsmachtbepalingen richten zich immers in eerste instantie op de bescherming van gewichtige nationale rechtsbelangen (vgl. Kamerstukken II 2012/13, 33572, nr. 3, p. 4). Deze gewichtige belangen kunnen onder omstandigheden echter ook in het geding zijn bij in het buitenland door buitenlanders gepleegde gedragingen die de veiligheid van onze bondgenoten en volkenrechtelijke organisaties raken, zoals (instellingen van) de VN, de NAVO, of de EU (uitgebreid beschermingsbeginsel). Ook voor dergelijke situaties wordt met de voorgestelde

aanvulling van artikel 4 Sr en artikel 4 WvSr BES voorzien in rechtsmacht. Het is aan het openbaar ministerie om, in het kader van de opportuniteitsafweging, te beoordelen of voornoemde belangen in het geding zijn en of vervolging is aangewezen.

Artikel I, onderdeel B en artikel II, onderdeel B

Deze artikelonderdelen voorzien in de invoeging in het Wetboek van Strafrecht en het Wetboek van Strafrecht BES, in de titel over misdrijven tegen de veiligheid van de staat, van een nieuwe bepaling waarin handelingen die samenhangen met spionage afzonderlijk strafbaar worden gesteld. Deze strafbaarstelling is toegelicht in paragraaf 4.1 van het algemeen deel van deze memorie van toelichting.

Artikel I, onderdelen C, D en E en artikel II, onderdelen C, D en E

Deze onderdelen voegen zowel in het Wetboek van Strafrecht dat geldt voor Europees Nederland als in het Wetboek van Strafrecht BES aan een aantal computerdelicten die een belangrijke rol kunnen spelen bij spionage, een strafverzwaringsgrond toe. Het strafmaximum wordt met een derde verhoogd indien het feit is gepleegd ten behoeve van een buitenlandse mogendheid. Voor een toelichting wordt verwezen naar paragraaf 4.2 van het algemeen deel van deze memorie.

De Minister van Justitie en Veiligheid,