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)

MEMORIE VAN TOELICHTING

I. Algemeen

Dit wetsvoorstel strekt tot uitbreiding van de strafbaarheid voor spionageactiviteiten. 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 schadetoebrengende 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 personen. Ook wordt bepaald dat de verruimde mogelijkheden tot opsporing die beschikbaar zijn bij misdrijven tegen de veiligheid van de staat, bij de opsporing van dit misdrijf kunnen worden ingezet, en wordt voorzien in rechtsmacht indien het feit buiten Nederland is gepleegd. 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 (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 te adresseren. 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 om de Nederlandse strafwetgeving op een gelijkwaardig niveau te houden met de wetgeving in andere Europese landen. Daarmee wordt het risico voorkomen 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). Na een bespreking van de adviezen (paragraaf 2) beschrijven de daaropvolgende paragrafen de bestaande beleids- en wettelijke kaders voor het optreden tegen spionage (paragraaf 3) en de wettelijke kaders in ons omringende landen (paragraaf 4). Vervolgens worden de hoofdlijnen van het wetsvoorstel uiteengezet (paragraaf 5). Daarna volgen paragrafen over de opsporing en vervolging (paragraaf 6), de verhouding tot hoger recht (paragraaf 7) en de uitvoerings- en financiële consequenties (paragraaf 8). 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 2021 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 2022 (CSBN 2022) 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 of I&V-diensten) blijkt dat meerdere Nederlandse topsectoren doelwit zijn (geweest) van (digitale) spionage. Dit is mede beschreven in de jaarverslagen van de AIVD van 2021 (Kamerstukken II 2021/22, 30977, nr. 162) en van de MIVD (Kamerstukken II 2021/22, 29924, nr. 228).

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 eigen 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. Adviezen

Over dit wetsvoorstel zijn adviezen ontvangen van de politie, de Nederlandse Orde van Advocaten (NOvA), de Raad voor de rechtspraak (Rvdr), het College van procureurs-generaal (OM), de Nederlandse Vereniging voor Rechtspraak (NVvR) en de I&V-diensten. Via internetconsultatie.nl zijn daarnaast enkele individuele reacties ontvangen, evenals twee adviezen vanuit het bedrijfsleven. Een concept van dit wetsvoorstel is voorgelegd aan de openbare lichamen Bonaire, Sint Eustatius en Saba, evenals – in verband met het concordantiebeginsel – aan Curaçao, Aruba en Sint Maarten. Zij hebben geen gebruikgemaakt van de geboden gelegenheid om een advies uit te brengen.
Over het algemeen lijkt bij de adviesorganen steun te bestaan voor het wetsvoorstel. Het OM onderschrijft de conclusie dat een aanvullende strafbaarstelling aangewezen is. Het strafrecht biedt volgens het advies op dit moment nog onvoldoende mogelijkheden om op te treden tegen spionageactiviteiten waarbij geen sprake is van schending van (staats-, ambts- of bedrijfs-) geheimen. De Rvdr geeft aan het belang van het wetsvoorstel te onderkennen. De NvVR merkt onder verwijzing naar een aantal bronnen, waaronder het Dreigingsbeeld statelijke actoren en het CSBN 2020, op dat daarmee de noodzaak is gegeven om te komen tot een samenstel van effectieve strafbaarstellingen van gedragingen die neerkomen op (voor fundamentele belangen) schadelijke interventies van statelijke actoren in de Nederlandse democratische rechtsstaat en samenleving als geheel. Volgens de NVvR resulteren de voorgestelde uitbreidingen in een «modernere draagwijdte van het misdrijf spionage». De I&V-diensten steunen het wetsvoorstel, mede tegen de achtergrond van de zich ontwikkelende spionagedreiging en de al langer toenemende geopolitieke spanningen. De strafbepaling biedt volgens het advies van de I&V-diensten meer mogelijkheden tot handelen wanneer spionage wordt vastgesteld, terwijl van de aangescherpte wetgeving ook een normerende en afschrikkende werking uit kan gaan in de richting van personen die spionageactiviteiten voor buitenlandse mogendheden (zouden) overwegen. In de adviezen vanuit het bedrijfsleven wordt steun uitgesproken voor het wetsvoorstel. Voor zowel de vitale infrastructuur als voor bedrijven in onder meer de topsectoren en kennisinstellingen is de dreiging door statelijke actoren zeer reëel, aldus deze adviezen, en de schade van spionage is voor het verdienmodel (potentieel) hoog. De adviserende organisaties vanuit het bedrijfsleven wijzen op het belang dat naast de verhoging van weerbaarheid ook repressief kan worden opgetreden en dringen erop aan de voorgestelde wijzigingen snel door te voeren. Verschillende adviesorganen die steun uitspreken voor het wetsvoorstel, vragen wel nog om aanvullingen en verduidelijkingen van het wetsvoorstel en de memorie van toelichting, in het bijzonder op het punt van het opzetvereiste (politie, OM, NVvR), de strafmaat (politie, OM, NVvR, advies vanuit bedrijfsleven), de mogelijkheden om bepaalde opsporingsbevoegdheden in te kunnen

zetten (politie, OM, NVvR) en de afbakening van een aantal in het wetsvoorstel gebruikte begrippen, te weten het begrip «buitenlandse mogendheid» (OM, NVvR), de «veiligheid van de staat» (Rvdr, NVvR) en «vitale infrastructuur» (Rvdr).
De NOvA meent dat het wetsvoorstel niet goed is onderbouwd en noemt daarbij concreet een aantal punten die dit zouden illustreren. Genoemd worden de afbakening van de in het wetsvoorstel opgenomen belangen (met name «vitale infrastructuur», «de integriteit en exclusiviteit van hoogwaardige technologieën» en «buitenlandse mogendheid»), de keuze voor universele jurisdictie, hoe moet worden omgegaan met conflicterende (wettelijke) plichten, de verhouding tot internationaal publiekrecht (functionele immuniteiten), waarom het huidige strafrechtelijke instrumentarium niet volstaat en de invulling van het voorwaardelijk opzet.
In de individuele reacties wordt aandacht gevraagd voor de reikwijdte van een aantal begrippen, waaronder het begrip «spionage» en het begrip «buitenlandse mogendheid», evenals voor de bewijsbaarheid van spionage, nu dergelijke handelingen vaak onopvallend worden verricht.

Naar aanleiding van de adviezen is het strafmaximum van de voorgestelde strafbepaling verhoogd van zes jaar gevangenisstraf in het aanvankelijke voorstel naar acht jaar in het nu voorliggende wetsvoorstel. De politie, het OM en de NVvR hebben tot deze verhoging geadviseerd, zodat een aantal aanvullende bevoegdheden die relevant kunnen zijn in spionageonderzoeken – in het bijzonder de bevoegdheden opgenomen in de artikelen 126l, tweede lid (opnemen vertrouwelijke communicatie in een woning) en 126nba Sv (onderzoek in een geautomatiseerd werk) – daarmee beschikbaar komen. In een van de adviezen vanuit het bedrijfsleven is eveneens gepleit voor een strafmaatverhoging ten behoeve van een hoger afschrikkend effect. Hoewel het kunnen toepassen van bepaalde opsporingsbevoegdheden op zichzelf geen dragende onderbouwing vormt bij het bepalen van een strafmaximum, hebben voornoemde adviezen wel aanleiding gegeven om opnieuw naar de strafmaat te kijken. Met het aanvankelijk opgenomen strafmaximum van zes jaar gevangenisstraf werd aangesloten bij het strafmaximum van de artikelen 98 en 98c Sr (schending staatsgeheimen). Er kan evenwel worden gesteld dat de omstandigheid dat activiteiten in het kader van de nieuwe bepaling worden verricht ten behoeve van een buitenlandse mogendheid maakt dat het feit als ernstiger moet worden beschouwd. In dat geval 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. Nu voor de nieuwe strafbepaling geldt dat daarbij steeds sprake is van betrokkenheid van een buitenlandse mogendheid, ligt het voor de hand in een hoger strafmaximum te voorzien dan in de artikelen 98 en 98c Sr, waarbij dit niet geldt. Met een strafmaximum van acht jaar gevangenisstraf wordt uitdrukking gegeven aan de ernst van dit feit, mede gelet op de maatschappelijke ontwikkelingen waarbij buitenlandse actoren op steeds assertievere wijze hun eigen belangen nastreven en daarbij in toenemende mate andere regels, normen en waarden hanteren dan die in Nederland en de internationale (westerse) gemeenschap worden gehuldigd. Met dit strafmaximum is ook verzekerd dat voorbereidingshandelingen strafbaar zijn (artikel 46 Sr). Anders dan in een van de adviezen vanuit het bedrijfsleven geadviseerd, wordt de geldboetecategorie niet aangepast. In de consultatieversie van het wetsvoorstel was al voorzien in een geldboete van de vijfde categorie, de hoogste geldboetecategorie voor natuurlijke personen. Voor rechtspersonen geldt dat bij deze strafbedreiging een geldboete van de zesde categorie of – indien die geldboetecategorie geen passende bestraffing toelaat – een geldboete van ten hoogste tien procent van de jaaromzet kan worden opgelegd (artikel 23, zevende lid, Sr). Doordat naar de wettelijke omschrijving een geldboete van de vijfde categorie op het feit is gesteld, is het eveneens mogelijk de maatregel van ontneming van wederrechtelijk verkregen voordeel op te leggen (artikel 36e Sr).
Een rechtspersoon die slachtoffer is geworden van spionage kan zich verder, net als een natuurlijk persoon, in het strafproces voegen als benadeelde partij, voor zover de rechtspersoon zelf rechtstreeks schade heeft geleden (artikel 51f, eerste lid, Sv); zie HR 11 april 2006, ECLI:NL:HR:2006, *NJ* 2006/263, zo wordt nog opgemerkt naar aanleiding van het eerdergenoemde advies. Daarmee wordt voorzien in voldoende middelen om plegers van deze feiten – naast een eventuele gevangenisstraf – ook financieel te raken.
Verder is overeenkomstig het advies van de NVvR het voorgestelde artikel 98d Sr toegevoegd aan artikel 551 Sv en het voorgestelde artikel 104d WvSr BES aan artikel 123 van het WvSv BES. Dat

betekent dat – net als bij een aantal andere misdrijven tegen de staat – een aantal verruimde bevoegdheden voor de opsporing van dit feit beschikbaar komen. Zie hierover de artikelsgewijze toelichting op de artikelen III en IV.
Het advies van de NVvR om de behandeling van deze strafbare feiten te concentreren bij één rechtbank wordt niet overgenomen. In concentratie wordt alleen in bijzondere gevallen voorzien. In «spionagezaken» zal weliswaar in voorkomende gevallen gebruik worden gemaakt van bijvoorbeeld rapporten van de I&V-diensten, maar dat kan ook aan de orde zijn in andere zaken, zoals wanneer andere misdrijven tegen de staat zijn gepleegd of bij een verdenking van een terroristisch misdrijf. Dit lijkt op zichzelf dus een onvoldoende rechtvaardiging voor wettelijke concentratie. Andere adviesorganen hebben hiertoe niet geadviseerd.

Verder is deze memorie van toelichting overeenkomstig de uitgebrachte adviezen op verschillende punten aangevuld. In het bijzonder gaat het om de toelichting op de verschillende in de wettekst gebruikte begrippen waarvoor in de adviezen aandacht is gevraagd. Deze zijn van een nadere duiding voorzien. Anders dan geadviseerd door de NOvA zijn voor deze begrippen geen wettelijke definities opgenomen. Zoals in paragraaf 7 nog nader uiteen wordt gezet, is het niet in strijd met het legaliteitsbeginsel dat een wet tot op zekere hoogte open normen bevat. De wet mag enige ruimte laten om veranderende omstandigheden mee te kunnen nemen. Nadere invulling van normen via rechterlijke interpretatie is toegestaan. Bij de formulering van de belangen is steeds aansluiting gezocht bij al bestaande (strafrechtelijke) begrippen – zo komt het begrip «vitale infrastructuur» nu al voor in artikel 138b Sr – en bij het normaal spraakgebruik. Daarmee bieden deze begrippen, in combinatie met daarbij behorende toelichting, voldoende houvast voor de rechtspraktijk. Voorts zijn naar aanleiding van de adviezen ter nadere onderbouwing en verduidelijking aanvullingen gedaan ten aanzien van de nut en noodzaak van de strafbaarstelling (paragraaf 3; adviezen NOvA en NVvR), de samenwerking met het bedrijfsleven (paragraaf 3; advies vanuit het bedrijfsleven) het handelen ter uitvoering van buitenlandse wettelijke plichten (paragraaf 5.1; advies NOvA), de verhouding tot hoger recht (paragraaf 7; adviezen NOvA, Rvdr en NVvR), het beschermingsbeginsel dat centraal staat in het kader van de rechtsmacht (artikelsgewijze toelichting op de artikelen I en II, onderdeel A; advies NOvA) en de plaats van de nieuwe strafbaarstelling in het wetboek (artikelsgewijze toelichting op de artikelen I en II, onderdeel B; advies NVvR).
Zoals hiervoor al kort aangestipt pleiten politie, OM en NVvR er in hun adviezen voor om het opzetvereiste – voor zover dat ziet op het in het leven roepen van gevaar voor de in de strafbaarstelling opgesomde belangen – te laten vervallen dan wel daaraan een culpoze variant toe te voegen. De NOvA daarentegen meent dat door de invulling die wordt gegeven aan het voorwaardelijk opzet «een lage lat» is gelegd. Organisaties uit het bedrijfsleven onderschrijven in hun advies het uitgangspunt dat sprake moet zijn van (voorwaardelijk) opzet en wijzen daarbij op het belang van goede voorlichting voor medewerkers binnen bedrijven uit de vitale infrastructuur en de topsectoren. Deze adviezen afwegende, meent het kabinet dat met het geformuleerde opzetvereiste een goede balans is gevonden tussen enerzijds het belang om personen die laakbaar hebben gehandeld te kunnen bestraffen en anderzijds het belang om de strafbaarheid te beperken tot personen aan wie dit handelen vanuit een oogpunt van redelijke en proportionele aansprakelijkheidstelling aangerekend kan worden. In paragraaf 5.1 wordt nader ingegaan op het opzetvereiste en de afwegingen die daarbij zijn gemaakt. Met betrekking tot het punt van voorlichting wordt opgemerkt dat voorlichtingsmateriaal worden ontwikkeld over spionage en dit wetsvoorstel, niet alleen om bekendheid te geven aan de nieuwe strafbaarstelling, maar ook om de bewustwording en alertheid te vergroten. Zie hierover ook paragraaf 3.

3. 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 worden vergroot? Voor de dreiging van spionage door statelijke actoren is tot op heden vooral ingezet op het verhogen van de weerbaarheid. Belangrijke elementen in deze aanpak zijn de Wet veiligheidstoets investeringen, fusies en overnames alsmede maatregelen die zijn getroffen op het terrein van kennisveiligheid en inkoop- en aanbesteding en de aanpak van ongewenste buitenlandse inmenging om beïnvloeding van diasporagemeenschappen tegen te gaan.

Zoals ook in de inleiding werd geduid volgt uit het Cybersecuritybeeld Nederland 2022 dat spionage en (voorbereidingen tot) sabotage van statelijke actoren het grootste digitale risico vormen voor de nationale veiligheid. 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. Zie Kamerstukken II 2019/20, 26 643, nr. 695. In dit kader heeft de AIVD in juni 2019 «Offensief cyberprogramma, een ideaal businessmodel voor staten» gepubliceerd.[1] 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. Ook wordt getracht om de weerbaarheid van potentiële slachtoffers te verhogen door aan de hand van voorlichting de bewustwording en alertheid te vergroten. Zo heeft de AIVD op 8 februari 2022 bijvoorbeeld een waarschuwingscampagne gelanceerd om Nederlandse werknemers en ambtenaren bewust te maken van gevaren voor spionage via sociale media. Met deze campagne «Check voor je connect» probeert de AIVD mensen alert te maken op online contactverzoeken en handvatten te bieden voor het herkennen van valse profielen (Zie Kamerstukken II 2021/2022, 30977, nr. 163). Om er voor zorg te dragen dat organisaties goed inzicht hebben en goed weten om te gaan met de bestaande dreigingen en risico's is het van belang dat daar goede informatie over beschikbaar is. Samenwerking tussen overheidsorganisaties om te komen tot een goede communicatie over het beeld van risico's, dreigingen en handelingsperspectief maakt onderdeel uit van het beleid inzake vitale infrastructuur en cybersecurity. In de Nederlandse Cybersecurity Strategie is bijvoorbeeld nadrukkelijk aandacht voor intensieve publiek-private informatie-uitwisseling die zoveel mogelijk aansluit bij de behoefte van de doelgroep.

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 zowel in februari 2021 als in november 2022 een 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) 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 op de inzet op het vergroten van de weerbaarheid 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)(hierna ook: DBSA), de beleidsreactie op het DBSA, de voortgang van de aanpak statelijke dreigingen (Kamerstukken II 2020/21, 30821 nr. 125) en de Kamerbrief aanpak statelijke dreigingen en aanbieding dreigingsbeeld statelijke actoren 2 (brief van 28 november 2022 met kenmerk 2022Z23347) (hierna ook: tweede DBSA). Deze strafrechtelijke aanpak wordt met dit wetsvoorstel van een nadere invulling voorzien.

[1] Zie: https://www.aivd.nl/documenten/publicaties/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten.

Het Wetboek van Strafrecht bevat verschillende bepalingen die kunnen worden ingezet om strafrechtelijk op te treden tegen gedragingen die samenhangen met spionage. In het bijzonder 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. Het bestanddeel «inlichting waarvan de geheimhouding door het belang van de staat of zijn bondgenoten wordt geboden» (hierna ook wel: staatsgeheim) in artikel 98 Sr wordt daarbij materieel ingevuld. Dat betekent dat de rechter niet is gebonden aan de rubricering die het document heeft gekregen binnen de overheidsorganisatie. Dat geldt zowel voor gerubriceerde als voor ongerubriceerde informatie. Dat neemt niet weg dat er een grote hoeveelheid overheidsinformatie is die weliswaar gevoelig is, maar niet als een zodanige inlichting kan worden aangemerkt. Voor een illustratie wordt verwezen naar: ECLI:NL:GHDHA:2014:2419 (bekrachtigd in cassatie; zie ECLI:NL:HR:2016:168). In deze zaak ging het onder andere om documenten over de werkwijze en inrichting van de inlichtingenstructuur bij de NAVO ("intelligence reform") en verslagen van ontmoetingen van de Noord Atlantische Raad. Deze informatie werd niet aangemerkt als een «inlichting waarvan de geheimhouding door het belang van de staat of zijn bondgenoten wordt geboden».
Ook ongerubriceerde overheidsinformatie 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 of personen te beïnvloeden of om economisch voordeel te behalen en de eigen concurrentiepositie te versterken. Dat geldt niet alleen voor informatie die verband houdt met militair optreden, maar ook voor andere (vooralsnog) ongerubriceerde, maar wel cruciale of kwetsbare (politiek gevoelige) overheidsinformatie.
Niet alleen gevoelige overheidsinformatie kan buiten de reikwijdte van artikel 98 Sr vallen, maar ook zeer gevoelige informatie van bedrijven die werkzaam zijn binnen vitale processen, evenals informatie die beschikbaar is binnen kennisinstellingen. De artikelen 272 e.v. Sr kunnen in voorkomende gevallen weliswaar een mogelijkheid bieden om strafrechtelijk op te treden tegen degene die dergelijke vertrouwelijke informatie aan een buitenlandse mogendheid verstrekt, maar deze strafbepalingen richten zich primair tot personen die een bepaalde functie verrichten waaraan een geheimhoudingsplicht is verbonden, zoals ambtenaren en werknemers. Dat betekent dat andere (tussen)personen die dergelijke gevoelige informatie bemachtigen en doorgeven aan een buitenlandse mogendheid niet strafbaar zijn op grond van deze strafbaarstellingen.
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. In voorkomende gevallen zou de strafbaarstelling van ambtelijke en niet-ambtelijke omkoping nog een handvat kunnen bieden om hiertegen op te treden, maar dat vergt dan wel dat daarvan sprake is en dat dit bewezen kan worden. Dit hoeft niet altijd het geval te zijn, bijvoorbeeld als de betrokkene vanuit een diepgevoelde overtuiging of loyaliteit samenwerkt met een buitenlandse mogendheid. Bovendien beogen die bepalingen een ander belang te beschermen, te weten de zuiverheid van de dienstbetrekking, het vertrouwen tussen werknemer en werkgever en de publieke moraal en – bij ambtelijke corruptie – de integriteit van het overheidsoptreden. Ook is de feitelijke gedraging – het delen van bepaalde informatie met een buitenlandse mogendheid – op zichzelf niet strafbaar op grond van deze bepalingen, terwijl in dergelijke gevallen zwaarwegende belangen van Nederland, Nederlandse bondgenoten, volkenrechtelijke organisaties gevestigd in Nederland of Nederlandse burgers ernstig geschaad kunnen worden.
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. Op basis van dergelijke informatie kunnen personen binnen een gemeenschap of familieleden van dergelijke personen in het land van herkomst worden gediscrimineerd, belasterd of bedreigd. Hoewel dit soort gedragingen strafbaar zijn, geldt dat niet zonder meer voor het delen van de daarvoor benodigde informatie met de buitenlandse mogendheid. Diasporaspionage kan niet alleen leiden tot fysiek

gevaar voor personen, maar ontwricht ook in Nederland aanwezige gemeenschappen, doordat mensen binnen deze gemeenschap of gemeenschappen onderling tegen elkaar worden opgezet. Bovendien kan ontwrichting binnen een gemeenschap schadelijk zijn voor de sociale en politieke stabiliteit van Nederland. Zie ook *Kamerstukken II* 2017/18 30821 en 26643, nr. 42.
Voorgaande illustreert dat er verschillende categorieën informatie zijn, waarvan het delen met een buitenlandse mogendheid niet strafbaar is, terwijl daardoor wel fundamentele Nederlandse belangen kunnen worden geschaad. Inlichtingendiensten zijn niet meer 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" staatgeheime informatie.

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 in heimelijk contact met een buitenlandse mogendheid ondersteunen of faciliteren van die mogendheid met bijvoorbeeld het ophalen en bezorgen van pakketjes, het volgen van personen, het plegen van sabotage en het verspreiden van schadelijke 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.

Met dit wetsvoorstel wordt dan ook – in aanvulling op de bovengenoemde inzet op het vergroten van de weerbaarheid – invulling gegeven aan het belang om ruimer dan op basis van de huidige wetgeving strafrechtelijk te kunnen optreden tegen de zich ontwikkelende dreiging die uitgaat van spionageactiviteiten.

4. 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 (staats)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. De wetgeving van enkele landen met vergelijkbare rechtssystemen is in het bijzonder bij de voorbereiding van dit wetsvoorstel in ogenschouw genomen.
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 en beschikbaar stellen aan en verzamelen van voorwerpen en inlichtingen voor 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 organisatie 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. Zie: https://www.gov.uk/government/consultations/legislation-to-counter-state-threats. In mei 2022 heeft de Britse overheid een "National Security Bill" ingediend (Bill 165 2022-23). Zie https://bills.parliament.uk/bills/3154. Op grond van het wetsvoorstel worden verschillende gedragingen strafbaar gesteld. Naast klassieke spionage («espionage»), sabotage, buitenlandse inmenging («foreign interference») en het ontvangen van giften («benefits») van een buitenlandse inlichtingendienst. In het kader van «espionage» wordt in het wetsvoorstel niet alleen het delen van «protected information» terwijl de betrokkene weet dat de veiligheid of belangen van het Verenigd Koninkrijk daardoor in gevaar komen strafbaar gesteld, maar ook het delen van bedrijfsgeheimen («trade secrets») met een buitenlandse mogendheid (economische spionage). Bij «foreign interference» gaat het onder andere om het manipuleren van verkiezingen en personen in publieke functies, maar ook andere gedragingen («conduct») dat de veiligheid of belangen van het Verenigd Koninkrijk in gevaar brengen («prejudicing the safety or interest of the United Kindom») ten behoeve van een buitenlandse mogendheid («for or on behalf of a foreign power»).
Net als in Nederland is er dus ook in andere landen behoefte om ten aanzien van wat in deze memorie van toelichting als "spionageactiviteiten" wordt aangeduid strafrechtelijk te kunnen optreden. Het is van belang dat het Nederlandse strafrechtelijk instrumentarium op een vergelijkbaar niveau met wetgeving van ons omringende landen blijft, om te voorkomen dat Nederland een aantrekkelijk(er) doelwit voor spionage wordt.

5. 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 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 3 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.

5.1 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 schadetoebrengende handelingen in heimelijke betrokkenheid met en ten behoeve van een buitenlandse mogendheid, wetende dat daarvan gevaar is te duchten voor een of meerdere van de opgesomde belangen.

Schadetoebrengende handelingen (sub 1º)

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. Het moet daarbij gaan om «schadetoebrengende» handelingen. Deze beperking is aangebracht om duidelijker tot uitdrukking te brengen dat niet iedere gedraging ten behoeve van een buitenlandse mogendheid onder de strafbaarstelling valt. Bij schade gaat het om de situatie waarin nadeel of verlies is geleden. Daarbij kan worden gedacht aan fysieke en vermogensschade, maar ook aan schade die wordt toegebracht aan andere te beschermen belangen, zoals de persoonlijke levenssfeer en persoonlijke vrijheid, de integriteit en waarachtigheid van (overheids)handelen of van informatie en de openbare orde. Met «schadetoebrengend» wordt dus niet (enkel) verwezen naar de in de aanhef opgesomde belangen. Blijkens de delictsomschrijving moet de schadetoebrengende handeling wel zijn gepleegd wetende dat er (ook) gevaar voor die belangen is te duchten.
Bij schadetoebrengende handelingen kan onder meer gedacht worden aan het plegen van sabotage, maar ook bijvoorbeeld het in de gaten houden, volgen of intimideren van in Nederland verblijvende personen en het openbaar maken of het verspreiden van schadelijke informatie, bijvoorbeeld over personen.

Verstrekken van inlichtingen, een voorwerp of gegevens (sub 2º)

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 3) 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.

In verband met de gekozen strafmaat is niet alleen poging tot plegen van schadetoebrengende handelingen als bedoeld in sub 1º of het verstrekken van informatie als bedoeld in sub 2º strafbaar (artikel 45 Sr), maar zijn voorbereidingshandelingen dat eveneens (artikel 46 Sr). Dat betekent dat ook personen die inlichtingen nog niet hebben verstrekt, maar wel al hebben verzameld of voorhanden hebben (bijvoorbeeld omdat zij een pakketje onder zich hebben met daarin een gegevensdrager), of die nog geen sabotage hebben gepleegd, maar wel voorwerpen voor handen hebben om sabotage te plegen, in voorkomende gevallen strafbaar zijn.

In heimelijke betrokkenheid met en ten behoeve van een buitenlandse mogendheid

Het verrichten van schadetoebrengende gedragingen en het verstrekken van inlichtingen is strafbaar als deze handelingen «in heimelijke betrokkenheid met een buitenlandse mogendheid» worden gepleegd. Een belangrijk kenmerk van spionageactiviteiten is immers dat zij zijn omgeven met een bepaalde mate van heimelijkheid. «betrokkenheid» moet ruim worden opgevat. Het gaat niet alleen om situaties waarin de buitenlandse mogendheid de gedragingen aanstuurt of de gedragingen faciliteert, maar ook waarin deze meer op de achtergrond betrokken is als begunstigde van de gedraging. Dat een buitenlandse mogendheid in het bijzonder bevoordeeld wordt door de gedraging kan dan ook een aanwijzing zijn van diens betrokkenheid. Zoals hierna bij de bespreking van het opzetvereiste nog aan de orde komt, dient de pleger wetenschap te hebben van deze heimelijke betrokkenheid. Van «heimelijke betrokkenheid» kan ook sprake zijn als op zichzelf kenbaar is dat de pleger een band heeft met de buitenlandse mogendheid, bijvoorbeeld omdat hij in dienst is van een buitenlandse overheid of anderszins blijk heeft gegeven van betrokkenheid bij een buitenlandse overheid. Centraal staat de heimelijke betrokkenheid bij de schadetoebrengende gedraging. Gedacht kan worden 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 of waarin de betrokkene een functie verricht waarin het ongebruikelijk is dat de informatie die hij verkrijgt ook wordt gedeeld met die buitenlandse mogendheid. Dat de betrokkenheid heimelijk is, betekent niet dat gedragingen zelf (volledig) heimelijk hoeven te worden verricht. Het bezorgen van pakketjes of het verzamelen van bepaalde informatie kan immers in redelijke openheid plaatsvinden. Dat bepaalde personen (binnen een groep of gemeenschap) op de hoogte zijn van de betrokkenheid van de buitenlandse mogendheid, hoeft er evenmin aan af te doen dat sprake is van "heimelijke betrokkenheid". Dat daarvan sprake is, kan worden afgeleid uit de in het geding zijnde belangen waarin besloten ligt dat heimelijkheid door de buitenlandse mogendheid wordt nagestreefd. Dat kan blijken enerzijds uit het heimelijke karakter waarmee de strafbare gedraging gepaard gaat, anderzijds uit het achterwege laten van enige kennisgeving van de buitenlandse mogendheid aangaande haar betrokkenheid aan de Nederlandse overheidsinstanties.

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 de 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. Er is niet gekozen voor aansluiting bij het bestanddeel «dan wel een zodanig persoon of lichaam dat gevaar ontstaat dat de inlichting of de gegevens aan een buitenlandse mogendheid bekend wordt» zoals opgenomen in artikel 98a Sr, omdat de hier voorgestelde strafbaarstelling niet alleen betrekking heeft op informatieverstrekking, waardoor die formulering minder bruikbaar is, terwijl door het gebruik van «middellijk» en «ten behoeve van» eveneens kan worden bereikt dat «indirecte

spionageconstructies», waarbij niet statelijke dekmantels of facilitators worden gebruikt, strafbaar zijn. Evenmin is voorzien in een nadere afbakening om welke buitenlandse mogendheden het kan gaan. Het Wetboek van Strafrecht maakt op dit moment slechts onderscheid tussen staten waarmee Nederland niet en staten waarmee Nederland wel in een gewapend conflict is gewikkeld (zie artikel 87a Sr). Dit onderscheid is voor de strafbaarstelling van spionage niet geschikt, nu spionageactiviteiten (tegen Nederland) ook plaatsvinden buiten de context van een gewapend conflict. In verschillende andere misdrijven tegen de staat, opgenomen in Titel I van het Tweede Boek van het Wetboek van Strafrecht is evenmin een onderscheid gemaakt tussen verschillende buitenlandse mogendheden. Het maken van een onderscheid in de nieuwe strafbaarstelling zou ook niet aansluiten bij de landenneutrale benadering die de basis vormt voor de bestaande aanpak van statelijke dreigingen.

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. Bij andere delicten zoals opzettelijke geweldpleging tegen de beschermde goederen van een internationaal beschermd persoon (artikel 117b Sr) of brandstichting (157 Sr) wordt niet vereist dat het opzet van de betrokkene ook is gericht op het in het leven roepen van het in die bepalingen genoemde gevaar. Dat gevaar is «geobjectiveerd». Voor die delicten geldt echter dat de gedraging die de betrokkene pleegt (geweldpleging, brandstichting) ook zonder dat dat gevaar ontstaat strafbaar is. Voor onderhavige bepaling geldt echter dat de door de betrokkene gepleegde gedragingen – die ook kunnen bestaan uit op het oog meer alledaagse handelingen zoals het bezorgen van pakketjes – op zichzelf niet zonder meer onder een strafbaarstelling vallen. Zij ontlenen hun strafwaardigheid aan het gevaar dat daardoor in het leven wordt geroepen voor zwaarwegende Nederlandse belangen. Nu het in het leven roepen van het gevaar een wezenlijk onderdeel vormt van de strafbaarstelling en het verwijt dat de betrokkene wordt gemaakt, ligt in de rede dat ook wordt vereist dat zijn opzet daarop is gericht. Daarmee wordt een te ruime strafrechtelijke aansprakelijkheid voorkomen. 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 de aard van de gedraging en de omstandigheden waaronder deze is verricht (de «uiterlijke verschijningsvorm van de gedraging») een rol spelen. Hierbij kan worden gedacht aan omstandigheden zoals de heimelijkheid van het contact of de handelingen, het handelen in strijd met integriteitscodes, pogingen het gedrag te verhullen, 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; zij zijn 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.
De omstandigheid dat de spionageactiviteiten worden gepleegd ter uitvoering van een (buitenlands) wettelijk voorschrift of een ambtelijk bevel (gegeven door een buitenlandse autoriteit) (vgl. de artikelen 42 en 43 Sr) vormt in beginsel geen beletsel voor strafbaarheid. Alleen indien in dergelijke gevallen sprake is van een situatie vergelijkbaar met «overmacht», zoals hiervoor beschreven, en geen sprake is van «culpa in causa» kan een succesvol beroep worden gedaan op de omstandigheid dat de activiteiten werden gepleegd ter uitvoering van een wettelijke voorschrift of ambtelijk bevel. Vgl. J. de Hullu, *Materieel Strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht*, Deventer: Wolters Kluwer 2021, blz. 331-332 en 334. Nu de artikelen 42 en 43 Sr in beginsel zien op Nederlandse wettelijke voorschriften en internationale voorschriften waaraan Nederland gebonden is respectievelijk bevelen gegeven door Nederlandse ambtsdragers, zal een beroep op een buitenlands voorschrift of bevel via de band van artikel 40 Sr beoordeeld moeten worden.

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 toe nam 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. Deze belangen worden (limitatief) opgesomd in de bepaling. 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. Bij de formulering van de belangen is aansluiting gezocht bij bestaande (strafrechtelijke) begrippen.

Het eerste belang dat genoemd wordt is de «veiligheid van de staat, van zijn bondgenoten of van een volkenrechtelijke organisatie». Voor de invulling van dit begrip kan worden aangesloten bij de invulling die elders in het Wetboek van Strafrecht aan dit begrip wordt gegeven. Dit zijn de belangen die door Titel I van Boek 2 van het wetboek worden beschermd, met inbegrip van 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 betreft de «vitale infrastructuur». Deze term komt op dit moment al in het Wetboek van Strafrecht voor, namelijk in artikel 138b Sr, en heeft dezelfde betekenis. 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. Blijkens de bestaande jurisprudentie over artikel 138b Sr wordt voor de invulling van dit begrip ook gekeken naar welke processen zijn gecategoriseerd als vitaal.[2] Zie bijvoorbeeld Rb. Den Haag 4 januari 2022, ECLI:NL:RBDHA:2022:22. Zie ter illustratie ook Rb. Rotterdam 14 april 2010, ECLI:NL:RBROT:2010:BM1172 en Rb. Zeeland-West Brabant 22 februari 2022, ECLI:NL:RBZWZB:2022:848. 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 tweede DBSA van november 2022 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 van levensbedreigende ziektes. Veel technologie en kennis heeft grote innovatieve waarde en levert daarmee een belangrijke bijdrage aan de Nederlandse welvaart. 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

[2] Zie voor een overzicht van processen die op dit moment in Nederland zijn geïdentificeerd als vitaal: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

met betrekking tot vitale processen en de veiligheid van personen, maar ook voor de economische en strategische positie van Nederland. Spionageactiviteiten leiden niet alleen tot schade voor het Nederlandse bedrijfsleven en kennisinstellingen. Door het weglekken van hoogwaardige kennis en technologie kan Nederland haar voorsprong en daarmee strategische positie verliezen. Dit kan gevolgen hebben voor het verdienvermogen van Nederland en kan de concurrentiepositie en geopolitieke positie negatief beïnvloeden. Bovendien kan hoogwaardige technologie ook kwaadaardig worden ingezet tegen Nederland, andere landen of burgers (bijvoorbeeld door gebruik voor sabotage of spionage of door versterking van de militaire capaciteit van een ander land). Om die reden zijn de integriteit en exclusiviteit van hoogwaardige technologieën als afzonderlijk belang opgenomen in de voorgestelde bepaling.
De term «hoogwaardige technologieën» omvat allereerst technologieën die ook wel als «sensitief» worden aangemerkt. Voor de invulling van dit begrip kan worden gekeken naar de Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo). Blijkens die wet worden als sensitieve technologieën aangeduid: militaire technologieën, technologieën die een «dual use» toepassing hebben[3]; (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; technologieën die worden gekenmerkt door een breed toepassingsbereik binnen verschillende vitale processen of processen die raken aan de nationale veiligheid (vgl. artikel 8 van de Wet vifo). Daarnaast worden onder «hoogwaardige technologieën» begrepen (andere) innovatieve technologieën die (ook) kwaadaardig kunnen worden toegepast tegen Nederland, andere landen en burgers of die van groot belang zijn voor de economische en strategische positie van Nederland. Voorbeelden zijn kunstmatige intelligentie, hoogwaardige micro-elektronica (waaronder semi-conductoren), DNA-technieken en agrarische innovaties als zaadveredeling.

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

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

hij een beroep op een strafuitsluitingsgrond kon doen. Deze strafbaarstelling omvat daarmee ook vormen van «doen plegen».

5.2 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 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.

6. Opsporing en vervolging

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 rekening te houden met, dan wel een afweging te maken tussen de wettelijke plicht tot het beschermen van eigen bronnen, het voortzetten van inlichtingenonderzoek ten faveure van bijvoorbeeld de kennis van modus operandi van de betrokken buitenlandse mogendheid en 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. Hoewel deze nieuwe strafbaarstelling vanwege de bovengenoemde redenen vermoedelijk tot een beperkt aantal zaken zal leiden, biedt de bepaling – 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.

7. 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. De beperking tot «schadetoebrengende» handelingen die worden verricht «in heimelijke betrokkenheid met een buitenlandse mogendheid» waarborgt dat alleen gedragingen die samenhangen met spionageactiviteiten onder het bereik van de strafbaarstelling valt. Het moet bovendien gaan om gedragingen waardoor gevaar ontstaat voor de in de delictsomschrijving genoemde fundamentele Nederlandse belangen. Zoals in paragraaf 5.1 aan de orde is gekomen, is er bewust voor gekozen om deze belangen afzonderlijk in de delictsomschrijving te benoemen om zo meer handvatten te geven voor de beoordeling welke gedragingen onder de strafbaarstelling vallen. Bij de formulering van de belangen is aansluiting gezocht bij bestaande (strafrechtelijke) begrippen en het normaal spraakgebruik. Daarmee bieden deze begrippen, in combinatie met daarbij behorende toelichting, voldoende houvast voor de

rechtspraktijk. 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 (aanvullend) 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 de belangen 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 acht jaar gevangenisstraf doet recht aan de ernst van het feit en is afgewogen tegen 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 de gedraging 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 niet aan de delictsomschrijving 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 voorafgaand 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 en buitenlandse overheidsfunctionarissen

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. Dat de gedragingen blijkens de voorgestelde delictsomschrijving alleen strafbaar zijn als zij «in heimelijke betrokkenheid met een buitenlandse mogendheid» worden verricht, waarborgt eveneens dat het verrichten van gebruikelijke gedragingen in het diplomatieke verkeer niet onder het bereik van deze strafbaarstelling vallen. Hoewel ook gedragingen in het diplomatieke verkeer met vertrouwelijkheid omgeven kunnen zijn, zal (ook voor de andere betrokkenen) duidelijk zijn dat de desbetreffende diplomatieke en consulaire vertegenwoordiger werkzaam is voor een buitenlandse mogendheid. Er is dan geen sprake van «heimelijke betrokkenheid». Zie over de uitleg die aan dit bestanddeel wordt gegeven paragraaf 5.1. Overigens zal veelal ook sprake zijn van diplomatieke onschendbaarheid of immuniteit.

Voor buitenlandse overheidsfunctionarissen die niet de diplomatieke status hebben, geldt dat zij onder omstandigheden eveneens immuniteit kunnen hebben. Het gaat dan om buitenlandse staatshoofden, regeringsleiders en ministers van buitenlandse zaken. Aan hen komt persoonlijke immuniteit toe zolang zij in functie zijn. Daarnaast komt aan leden van officiële missies op grond van het internationale gewoonterecht functionele immuniteit toe. Dat wil zeggen dat leden van dergelijke missies (slechts) immuniteit genieten voor handelingen verricht in het kader van hun officiële hoedanigheid. Er is sprake van een officiële missie indien aan een aantal voorwaarden is voldaan. Die voorwaarden zijn dat sprake is van een missie met een tijdelijk karakter, de missie een andere staat vertegenwoordigt, de missie op bezoek komt bij de overheid van de ontvangende staat – in dit geval Nederland – en de ontvangende staat daarmee heeft ingestemd. Vgl. Kamerstukken II 2011/12, 32635, nr. 5.

Indien buitenlandse functionarissen een beroep kunnen doen op diplomatiek onschendbaarheid of een immuniteit, kunnen zij in overeenstemming met het internationale recht niet worden vervolgd voor strafbare feiten ten aanzien waarvan zij die onschendbaarheid of immuniteit kunnen inroepen, zo kwam in paragraaf 6 al aan de orde.

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

8. 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 6 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 begroot op €4 miljoen vanaf 2024 structureel en worden gedekt uit de uit het coalitieakkoord verkregen middelen. Hierin worden tevens eventuele kosten voor de BES die uit dit wetsvoorstel voortvloeien afgedekt.
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. Dat betekent niet dat in alle gevallen waarin spionageactiviteiten worden verricht buiten Nederland zal worden opgetreden. Aan de opname van de nieuwe strafbaarstelling in deze rechtsmachtbepalingen ligt het beschermingsbeginsel (en niet het universaliteitsbeginsel) ten grondslag. Zowel de nieuwe strafbaarstelling als het gewijzigde onderdeel a van de rechtsmachtbepalingen richt zich immers in eerste instantie op de bescherming van gewichtige nationale rechtsbelangen (vgl. Kamerstukken II 2012/13, 33572, nr. 3, p. 4). Dat betekent dat de uitoefening van rechtsmacht in beginsel alleen aan de orde is als het gaat om spionageactiviteiten vanuit het buitenland gericht tegen Nederland, dat wil zeggen 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). De gewichtige nationale rechtsbelangen 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. Dit betekent dat er dus steeds sprake zal zijn van aanknopingspunten met de Nederlandse rechtssfeer, daaronder begrepen de Nederlandse verantwoordelijkheid voor het bevorderen van de internationale rechtsorde. 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 van een nieuwe bepaling waarin handelingen die samenhangen met spionage afzonderlijk strafbaar worden gesteld. Deze strafbaarstelling is toegelicht in paragraaf 5.1 van het algemeen deel van deze memorie van toelichting.

De nieuwe bepalingen zijn ingevoegd in de titel over misdrijven tegen de veiligheid van de staat (Tweede Boek, Titel I). In deze titel zijn misdrijven bij elkaar gebracht die de Nederlandse staat rechtstreeks in gevaar brengen. Zij hebben met elkaar gemeen dat zij strekken tot bescherming van (belangen van) de Nederlandse staat en zijn staatsinrichting, ook tegen buitenlandse mogendheden. Het belang van de Nederlandse staat is daarbij niet per definitie beperkt tot de veiligheid van de staat in de zin van fysieke veiligheid, zoals ook blijkt uit bijvoorbeeld artikel 99 Sr dat ziet op het benadelen van onderhandelingspositie van de staat in zijn contacten met buitenlandse mogendheden. De inhoud van de nieuw voorgestelde bepaling, waarmee wordt beoogd fundamentele Nederlandse belangen te beschermen ten opzichte van buitenlandse mogendheden, past daarmee in deze titel, die bijvoorbeeld ook de bepalingen inzake de schending van staatsgeheimen omvat.

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 5.2 van het algemeen deel van deze memorie.

Artikelen III en IV

Op grond van deze bepalingen wordt de nieuwe strafbaarstelling toegevoegd aan artikel 551 Sv en 123 WvSv BES. Dat betekent dat – net als bij een aantal andere misdrijven tegen de staat – een aantal verruimde bevoegdheden voor de opsporing van dit feit beschikbaar komen. Het gaat dan om de bevoegdheid voor opsporingsambtenaren om te vorderen dat voorwerpen die vatbaar zijn voor inbeslagneming worden uitgeleverd en om de bevoegdheid zich de toegang te verschaffen tot alle plaatsen waar redelijkerwijs vermoed kan worden dat dit strafbare feit wordt begaan.

Artikel V

De datum van inwerkingtreding zal bij koninklijk besluit worden bepaald.

De Minister van Justitie en Veiligheid,