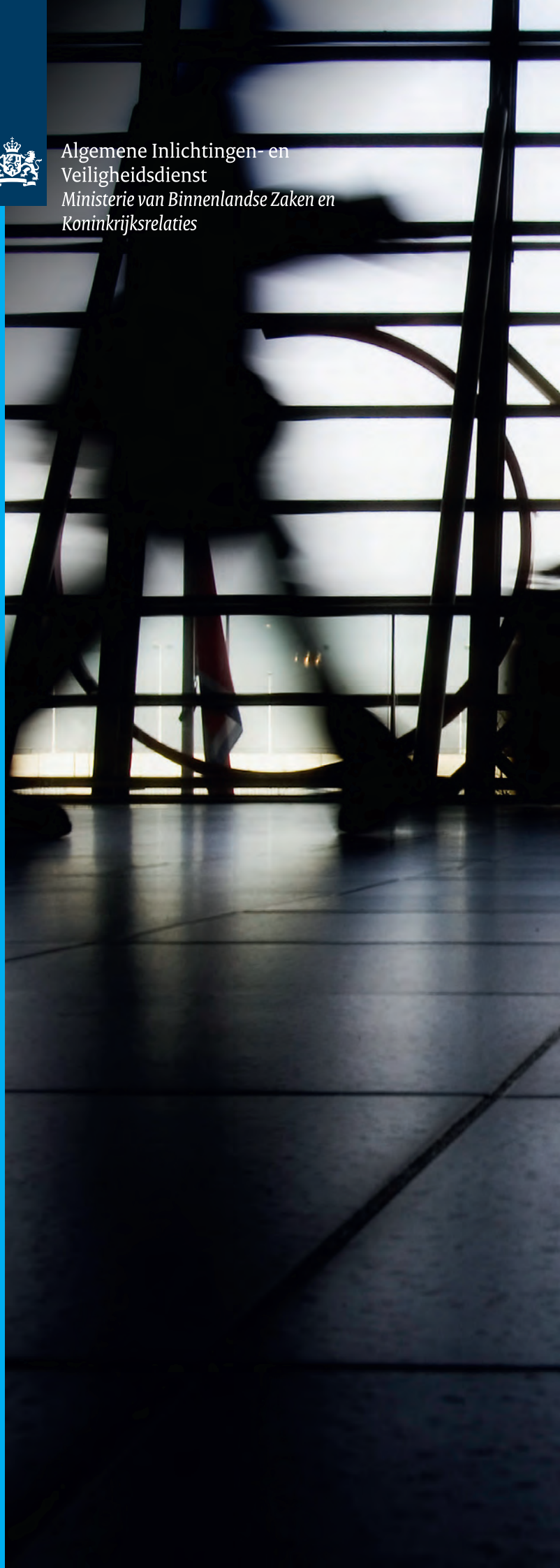
Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Kwetsbaarheids-analyse spionage

Spionagerisico's en de nationale veiligheid



Management samenvatting

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) constateert dat economische, strategische en technisch-wetenschappelijke spionage een actuele dreiging vormt voor de Nederlandse nationale veiligheid. Om deze dreiging beter in beeld te brengen en aanbevelingen te doen hoe deze dreiging (verder) te reduceren hebben de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het Directoraat-Generaal Veiligheid (DGV) van het ministerie van BZK gezamenlijk onderzoek gedaan naar spionagerisico's op het terrein van economisch welzijn & wetenschappelijk potentieel en openbaar bestuur & vitale infrastructuur. De AIVD neemt in zijn contraspionage-onderzoeken waar dat in sectoren binnen deze aandachtsgebieden, verschillende buitenlandse inlichtingendiensten actief zijn met het heimelijk vergaren van inlichtingen.

Door middel van gesprekken met partijen uit de verschillende sectoren en op basis van (operationele) informatie uit AIVD-onderzoeken is op hoofdlijnen in beeld gebracht welke informatie per sector voorhanden is, waarvan kennisname door een buitenlandse overheid de Nederlandse nationale veiligheid aantast en waarvan verondersteld kan worden dat buitenlandse inlichtingendiensten/overheden er belang bij hebben deze informatie te bezitten. Dergelijke gegevens of verzamelingen van gegevens worden in dit rapport *kernbelangen* genoemd. De verschillende wijzen waarop kernbelangen kwetsbaar zijn voor spionage worden *kwetsbaarheden* genoemd. Ook deze zijn onderzocht. Op basis van de in dit rapport beschreven inzichten en conclusies wordt door de onderzoekers een aantal algemene aanbevelingen gedaan. Deze aanbevelingen geven een eerste richting voor een beleidsopvolgingstraject binnen de kaders van de Strategie Nationale Veiligheid. In dit beleidsopvolgingstraject dienen de algemene aanbevelingen nader te worden geconcretiseerd en te worden toebedeeld aan actiehouders.

Kernbelangen

Uit het onderzoek blijkt dat in alle onderzochte sectoren kernbelangen zijn te vinden. Deze zijn grofweg te verdelen in de categorieën:

- Datasets en blauwdrukken: hierbij gaat het om in organisaties aanwezige gegevensbestanden, ontwerpen en bouwtekeningen;
- Standpunten en strategie: bijvoorbeeld beleidsstandpunten, langjarige visies en onderhandelingsstrategieën;
- Opkomende kernbelangen en infrastructuur: bijvoorbeeld wetenschappelijke innovaties die in de toekomst in concrete toepassingen belangrijke bijdragen aan de Nederlandse economie kunnen leveren.

Kwetsbaarheden

De belangrijkste aangrijpingspunten voor spionageactiviteiten van buitenlandse inlichtingendiensten worden gevormd door de factoren 'mens' en 'techniek'. Inlichtingendiensten proberen voor hen relevante informatie te verkrijgen via mensen die (indirect) toegang hebben tot deze informatie of via de inzet van technische middelen zoals door hacken, tappen of afluisteren. De verschillende mogelijkheden om telecommunicatieverkeer te onderscheppen, vormen in dit verband een belangrijke kwetsbaarheid. Uit het onderzoek blijkt ook dat de toenemende verwevenheid en complexiteit van computersystemen alsmede het koppelen van dataopslagsystemen, de gevoelige gegevens in systemen kwetsbaar maakt. Het uitbesteden van activiteiten als systeem- en serverbeheer, *datawarehousing* en gegevensverwerking brengt eveneens spionagerisico's met zich mee.

Met gericht beleid, in zowel de private als de publieke sectoren, kan de weerstand tegen spionage worden versterkt en kunnen Nederlandse kernbelangen beter worden beveiligd. De kwaliteit van dit beleid is bepalend voor de mate waarin kernbelangen kwetsbaar zijn voor inlichtingenactiviteiten. Uit het onderzoek blijkt dat bepaalde beleidsbeslissingen de kwetsbaarheid voor spionageactiviteiten in enkele sectoren onbedoeld hebben vergroot. Zo heeft de bevordering van kennismigratie van en naar Nederland als ongewenst neveneffect dat inlichtingenofficieren zich relatief eenvoudig in de studentenpopulatie kunnen verschuilen.

Het tegengaan van inlichtingenactiviteiten vereist dat diegenen, die risico lopen om bespioneerd te worden, op de hoogte zijn van het feit dat zij mogelijk interessant zijn voor buitenlandse diensten en dat zij daarnaast weten hoe inlichtingenactiviteiten worden uitgevoerd. Uit het onderzoek blijkt dat de *awareness* in de betrokken sectoren ten aanzien van spionage vaak laag is. Het beperkte bewustzijn wordt zichtbaar op drie niveaus:

- *Waardebewustzijn*: organisaties en individuele medewerkers realiseren zich soms niet of onvoldoende wat de waarde is van de informatie waarover zij beschikken of waartoe zij toegang kunnen verschaffen;
- *Beveiligingsbewustzijn*: beveiliging en veiligheid van kernbelangen hebben niet altijd voldoende aandacht binnen organisaties; in het beleid zijn andere overwegingen vaak prioritair;

- *Belangenafweging*: organisatiebelangen en/of overheidsbelangen op korte termijn prevaleren (vaak) over de belangen op lange termijn. Het naar het buitenland weglekken van strategische kennis of bedrijvigheid die relevant is voor de Nederlandse nationale veiligheid op lange termijn krijgt onvoldoende aandacht.

Aanbevelingen

Naar aanleiding van deze conclusies worden drie hoofdaanbevelingen gedaan voor (verdere) versterking van de weerbaarheid tegen spionage:

- Versterk actief het bewustzijn (onder managers en medewerkers) van overheden, bedrijven en instellingen met betrekking tot de waarde van de informatie waarover zij beschikken en van de mogelijke interesse van buitenlandse overheden in deze informatie.
- Werk aan een cultuurverandering op het gebied van beveiliging. Daarbij zijn gebruikers, de inrichting van gegevensstromen en databases en de gebruikte technieken voor detectie van incidenten belangrijke aandachtspunten.
- Besteed bij beleidsvorming nadrukkelijk aandacht aan de bescherming van kernbelangen en de effecten van beleid op de belangen van Nederland op langere termijn.

Deze aanbevelingen zijn in hoofdstuk 10 geïllustreerd met een aantal mogelijke, meer concrete handelingsperspectieven. De nadere concretisering en toedeling van acties behoort niet tot de reikwijdte van het onderzoek en zal in een beleidsopvolgingstraject moeten plaatsvinden door de belanghebbende beleidsdepartementen.

Inhoud

Aanleiding

Onze samenleving is kwetsbaar. De nationale veiligheid kan op verschillende manieren bedreigd worden. De nationale veiligheid is in het geding als vitale belangen van de Nederlandse staat en/of samenleving zodanig worden bedreigd dat sprake is van – potentiële – maatschappelijke ontwrichting. Sommige gevaren zijn overduidelijk, zoals het risico van natuurrampen of een terroristische aanslag. Voor andere gevaren is dit niet zo duidelijk omdat die zich sluipenderwijs manifesteren of zich grotendeels of geheel aan het oog onttrekken, zelfs voor waarnemers met een geoefend oog. Spionage is hier een voorbeeld van.

Met de Strategie Nationale Veiligheid kan het kabinet bepalen welke dreigingen de nationale veiligheid in gevaar kunnen brengen en hoe te anticiperen op die dreigingen, ongeacht de aard ervan. De Strategie Nationale Veiligheid is een integrale, kabinetsbrede aanpak, onder regie van de minister van Binnenlandse Zaken en Koninkrijksrelaties. Het Directoraat-Generaal Veiligheid is verantwoordelijk voor de (samenhang in de) uitvoering van de strategie. De AIVD heeft in het kader van de bescherming van de nationale veiligheid een taak als het gaat om het onderkennen en tegengaan van inlichtingenactiviteiten van andere landen. In het kader van deze taak heeft de AIVD, in samenwerking met het Directoraat-Generaal Veiligheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, onderzocht welke soorten informatie (in dit rapport kernbelangen genoemd) voor de nationale veiligheid van belang zijn en waarvan kan worden aangenomen dat buitenlandse mogendheden deze door middel van spionage willen verzamelen.

De volledige betekenis van spionage voor de nationale veiligheid is vanuit dit perspectief nog niet eerder in beeld gebracht. Deze verkennende, brede inventarisatie heeft tot doel de risico's van spionage beter in kaart te brengen en enkele algemene aanbevelingen te doen, zodat de geschetste risico's zo veel mogelijk kunnen worden gereduceerd.

Dreiging

Spionage

Inlichtingenactiviteiten

Veiligheidsinbreuken

Strategie Nationale Veiligheid

1. Inleiding

De minister van Binnenlandse Zaken en Koninkrijksrelaties constateert dat economische, strategische en technisch-wetenschappelijke spionage[1] door verschillende landen, een actuele dreiging vormt voor Nederland. Het grote belang van technologische ontwikkelingen leidt tot zorg over de intentie van andere landen om deze kennis door middel van spionage te stelen, en de gevolgen daarvan voor de huidige en toekomstige Nederlandse kenniseconomie.

Ook de vitale infrastructuur in Nederland, waaronder bijvoorbeeld de telecom- en energiesector, kan door spionage worden bedreigd. De gevolgen hiervan kunnen uiteenlopen van het in verkeerde handen raken van beschermde klantgegevens tot grootschalige digitale veiligheidsinbreuken bij overheid en/of bedrijfsleven. De AIVD constateerde verschillende gevallen van deze vorm van spionage. Er is onder meer vastgesteld dat buitenlandse inlichtingendiensten gevoelige informatie proberen te verkrijgen over de infrastructuur van de telecomsector ten behoeve van hun inlichtingenwerkzaamheden.

Buitenlandse inlichtingendiensten proberen verder ook gerubriceerde en andere vertrouwelijke (overheids) informatie te bemachtigen op politiek, militair en economisch terrein om deze informatie voor hun eigen nationale belangen te kunnen gebruiken. In diverse landen is het vergaren van dit soort inlichtingen zelfs expliciet verankerd in de wettelijke taak van de inlichtingendiensten.

De AIVD constateert dat andere landen structurele belangstelling hebben voor genoemde aandachtsgebieden en daarom blijft aandacht voor het fenomeen spionage en de risico's die dit met zich mee brengt meer dan nodig. Bij elke vorm van inlichtingenactiviteiten door een vreemde mogendheid in Nederland worden Nederlandse belangen geschaad. Alle heimelijke inlichtingenactiviteiten uitgevoerd door buitenlandse inlichtingendiensten op Nederlands grondgebied vormen namelijk een inbreuk op de Nederlandse soevereiniteit.[2] Daarnaast kunnen ze de politiek-bestuurlijke en ambtelijke integriteit; het Nederlandse (technisch-)wetenschappelijk, economisch en militair potentieel; of de rechten van Nederlandse ingezetenen aantasten. Om die reden vormen inlichtingenactiviteiten, waaronder spionage, een bedreiging voor de Nederlandse nationale veiligheid.

Spionage en nationale veiligheid

Wanneer de schade van buitenlandse inlichtingenactiviteiten leidt tot *een zodanige aantasting van de vitale belangen van onze samenleving en/of staat dat er sprake is van (potentiële) maatschappelijke ontwrichting, komt de nationale veiligheid van Nederland in het geding*. Deze definitie van het begrip nationale veiligheid is geformuleerd in het kader van de door de ministerraad vastgestelde Strategie Nationale Veiligheid.[3] Met dit interdepartementale traject wil de Nederlandse overheid zorg dragen voor een integrale en samenhangende aanpak van interne en externe dreigingen die zich richten tegen de samenleving en de bevolking op het eigen grondgebied. Met de werkwijze die in de strategie wordt beschreven kan de Nederlandse overheid beter dan voorheen bepalen welke dreigingen de nationale veiligheid in gevaar kunnen brengen en hoe daarop kan worden geanticipeerd. Gezien het feit dat spionage een bedreiging vormt voor de nationale veiligheid is het van belang ook deze dreiging een plek te geven binnen de strategie. Dit rapport vormt daartoe een aanzet.

In de Strategie Nationale Veiligheid zijn vijf 'vitale belangen' gedefinieerd die Nederland dient te beschermen met het oog op de nationale veiligheid. Aantasting van één of meerdere van deze vitale belangen, door interne of externe dreigingen, leidt (of kan leiden) tot maatschappelijke ontwrichting. De vijf vitale belangen zijn:

- *Territoriale integriteit*: het ongestoord functioneren van Nederland als onafhankelijke staat, en specifieker de territoriale integriteit van Nederland. De territoriale integriteit is in het geding bij bijvoorbeeld een dreigende bezetting van het grondgebied van het Rijk door een andere mogendheid, maar ook bij een terroristische aanslag;

[1] Over het algemeen gebruikt de AIVD de bredere term 'inlichtingenactiviteiten'. Inlichtingenactiviteiten zijn te omschrijven als ongewenste activiteiten van buitenlandse mogendheden (doorgaans inlichtingendiensten) op Nederlands grondgebied. Met spionage worden uitsluitend die inlichtingenactiviteiten bedoeld die gericht zijn op het heimelijk of onder valse voorwendselen verwerven van informatie (en dus niet de activiteiten beïnvloeding, disruptie of andere heimelijke, ongewenste activiteiten). Deze studie richt zich op spionage en daarom zal in dit stuk altijd die term gebruikt worden in plaats van het bredere begrip inlichtingenactiviteiten. Alleen als nadrukkelijk (ook) een *andere* vorm van inlichtingenactiviteiten bedoeld wordt dan spionage, zal het woord inlichtingenactiviteiten gekozen worden.

[2] De enige uitzondering hierop wordt gevormd door inlichtingenactiviteiten die van te voren zijn gemeld aan de Nederlandse overheid en waarvoor toestemming is verleend.

[3] Tweede Kamer, 2006-2007, 30821, nr. 3

- *Fysieke veiligheid*: het ongestoord functioneren van de mens in Nederland en zijn omgeving. De fysieke veiligheid komt bijvoorbeeld in gevaar als de volksgezondheid wordt bedreigd door de uitbraak van een epidemie, maar ook bij een grootscheepse dijkdoorbraak of een ongeluk in een chemische fabriek.
- *Economische veiligheid*: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. De economische veiligheid kan bijvoorbeeld aangetast worden als het handelsverkeer met een belangrijke buitenlandse partner uitvalt.
- *Ecologische veiligheid*: het beschikken over voldoende zelfherstellend vermogen van de leefomgeving bij aantasting. De ecologische veiligheid kan in het geding komen door bijvoorbeeld verstoringen in het beheer van het oppervlaktewater of klimaatveranderingen.
- *Sociale en politieke stabiliteit*: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden. De sociale en politieke stabiliteit kan in het geding zijn als veranderingen optreden in de demografische opbouw van de samenleving, de sociale cohesie en de mate van deelname van de bevolking aan maatschappelijke processen.

Spionage als gevaar voor de nationale veiligheid

Inlichtingenactiviteiten kunnen deze door de Nederlandse overheid vastgestelde 'vitale belangen' en daarmee de nationale veiligheid schaden. Het heimelijk beïnvloeden van het democratisch proces, kan de sociale en politieke stabiliteit aantasten. In een nog extremer geval biedt een land ondersteuning aan een terroristisch netwerk dat een aanslag pleegt in Nederland. In dat geval brengen inlichtingenactiviteiten de fysieke veiligheid van mensen in Nederland en de territoriale integriteit van Nederland in gevaar. Ten slotte kunnen inlichtingenactiviteiten van andere landen de Nederlandse economische veiligheid aantasten, bijvoorbeeld als door spionage waardevolle bedrijfsgeheimen worden ontvreemd, met als gevolg verlies van concurrentiepositie en een grootschalig verlies van inkomsten voor Nederland.

Onderzoek

Spionage is de afgelopen jaren door de AIVD onder andere waargenomen op terreinen als het economisch welzijn en technisch-wetenschappelijk potentieel, het openbaar bestuur en de vitale infrastructuur van Nederland. In die wetenschap is het wenselijk binnen al deze aandachtsgebieden zicht te krijgen op de belangrijkste *informatie, waarvan kennisname de nationale veiligheid aantast en waarvan verondersteld kan worden dat buitenlandse inlichtingendiensten/overheden er belang bij hebben deze te bezitten*.[4] Dergelijke gegevens of verzamelingen van gegevens worden in dit rapport kernbelangen genoemd. De wijze waarop kernbelangen kwetsbaar zijn voor spionage, hierna 'kwetsbaarheden' genoemd, zijn in dit rapport gedefinieerd als *de voornaamste factoren die aantasting van een kernbelang door spionage mogelijk maken*.

Vanuit deze behoefte aan kennis over belangen en kwetsbaarheden hebben de AIVD en DGV gezamenlijk onderzoek uitgevoerd naar deze aandachtsgebieden. Hiervoor is een groot aantal vertegenwoordigers uit sectoren binnen de aandachtsgebieden (economisch welzijn en technisch-wetenschappelijk potentieel, openbaar bestuur en vitale infrastructuur) bevraagd. Deze gesprekken vormen de basis van dit rapport. Daarnaast is gebruik gemaakt van informatie uit AIVD-onderzoeken.

1.1 Doel

Met deze rapportage willen de AIVD en DGV op hoofdlijnen een beeld schetsen van de belangrijkste geïdentificeerde kernbelangen en bijbehorende kwetsbaarheden in de onderzochte sectoren. Het is nadrukkelijk *niet* de ambitie om een uitputtend beeld te geven van alle Nederlandse kernbelangen en kwetsbaarheden. Dat is ook nauwelijks mogelijk gezien het hoge tempo van met name technologische ontwikkelingen en innovaties. Daarnaast worden niet alle bevindingen in deze openbare publicatie gedetailleerd weergegeven om te voorkomen dat ongewild richting gegeven wordt aan de inlichtingenactiviteiten van buitenlandse inlichtingendiensten.

De resultaten van het onderzoek en de op basis daarvan gedane algemene aanbevelingen bieden aanknopingspunten voor de verdere beleidsontwikkeling om onderkende Nederlandse kernbelangen beter te beschermen. Zo kunnen de hier besproken resultaten worden gebruikt in verdere beleidsontwikkeling in het kader van de Strategie Nationale Veiligheid. Verder stelt dit rapport de verantwoordelijke professionals binnen bedrijven en overheden in staat om eigen kernbelangen en kwetsbaarheden beter te kunnen identificeren en te beschermen.

[4] Kernbelangen kunnen tevens worden geschaad door niet-statelijke actoren (terroristische organisaties, in Nederland opererende buitenlandse oppositiegroeperingen, enzovoort). Deze vallen buiten de reikwijdte van dit onderzoek. In veel gevallen zullen overigens de bedreigde kernbelangen en kwetsbaarheden voor statelijke en niet-statelijke actoren hetzelfde zijn. Er kan wel verschil bestaan in de doelen en modi operandi van deze actoren.

1.2 Onderzoeksmethode en afbakening

De analyse van kernbelangen en kwetsbaarheden in dit rapport is in belangrijke mate gebaseerd op gesprekken met tientallen vertegenwoordigers van bedrijven en organisaties uit sectoren die prominent vertegenwoordigd zijn binnen de eerdergenoemde aandachtsgebieden (economisch welzijn en technisch-wetenschappelijk potentieel, openbaar bestuur en vitale infrastructuur). Deze rapportage spitst zich daarom toe op kernbelangen uit die sectoren. Voor een verdere duiding en analyse van deze informatie is ook gebruik gemaakt van bij de AIVD reeds beschikbare informatie over waargenomen inlichtingenactiviteiten, modi operandi en kwetsbaarheden.

De keuze voor de genoemde sectoren komt allereerst voort uit het feit dat de AIVD, mede als gevolg van toegenomen globalisering, internationale interdependentie en complexiteit, een behoefte aan inlichtingen over juist deze sectoren vermoedt en waarneemt.[5] De sectoren en de vormen van dreiging waar al een goed beeld van bestaat, of waarvoor de verantwoordelijkheid reeds expliciet belegd is, zijn niet in het onderzoek meegenomen. Om die reden wordt hier niet of nauwelijks aandacht besteed aan de meer traditionele doelwitten van spionage op het vlak van militaire en nucleaire technologie en kennis. Het niet, of in beperkte mate, noemen van kernbelangen op beide terreinen betekent echter niet dat op deze terreinen in Nederland op dit moment geen spionageactiviteiten plaatsvinden.

1.3 Leeswijzer

Na het inleidende hoofdstuk volgt in hoofdstuk 2 een beschrijving van de drie categorieën kernbelangen die in dit rapport worden onderscheiden. In sommige sectoren zijn alle drie categorieën kernbelangen terug te vinden, terwijl in andere sectoren slechts één of twee categorieën naar voren komen. In de daaropvolgende vijf hoofdstukken worden de onderzochte sectoren afzonderlijk besproken. Daarbij wordt de indeling van kernbelangen gehanteerd zoals beschreven in hoofdstuk 2. Hoofdstuk 8 beschrijft vervolgens de diverse kwetsbaarheden die uit het onderzoek naar voren zijn gekomen en die in meer of mindere mate raken aan alle kernbelangen die in de voorgaande hoofdstukken de revue zijn gepasseerd. De hoofdstukken 9 en 10, ten slotte, bevatten respectievelijk de conclusies en de algemene beleidsaanbevelingen.

[5] Grotere wederzijdse afhankelijkheid maakt kennis over standpunten en strategie op deze gebieden voor staten wenselijk.

Kernbelangen

Strategie

Stereotiepe doelwitten

Datasets

2. Soorten kernbelangen

Uit gesprekken met vertegenwoordigers van partijen uit het veld blijkt dat kernbelangen in de onderzochte sectoren grofweg zijn onder te verdelen in drie categorieën:

- Datasets en blauwdrukken
- Standpunten en strategie
- Opkomende kernbelangen en infrastructuur

In de volgende paragrafen worden deze drie categorieën verder toegelicht.

2.1 Datasets en blauwdrukken

De kernbelangen in de categorie Datasets en blauwdrukken vormen de meest stereotiepe doelwitten van spionage. Het gaat om feitelijke en gebundelde informatie (datasets) of gedetailleerde (technische) informatie. Dat zijn bijvoorbeeld blauwdrukken van hoogwaardige technologieën of omschrijvingen van belangrijke productieprocessen. Maar ook bestanden met privacygevoelige gegevens vallen in deze categorie. Voorbeelden hiervan zijn de adressen en contactgegevens van organisaties, de Gemeentelijke Basis Administratie (GBA) bij gemeenten en de bel- en betalingsgegevens van klanten van een telefonieprovider.

Gegevens uit deze categorie zijn vaak binnen de eigen organisatie reeds afgeschermd en worden door de organisatie als vertrouwelijk beschouwd, bijvoorbeeld omdat de informatie interessant is voor concurrenten of criminelen. Dergelijke informatie kan echter ook doelwit zijn van inlichtingendiensten. In dit geval is geen sprake meer van criminaliteit of bedrijfsspionage maar van economische spionage: het actief vergaren van bedrijfseconomische kennis door *statelijke actoren* ten bate van de eigen economie.

'Reversed Engineering'

Een buitenlandse delegatie heeft bij een bezoek aan een Nederlands bedrijf gevraagd of het mogelijk was een prototype te bekijken. Het prototype werd aan de delegatie meegegeven. Het is echter nooit teruggekomen.
Zeer waarschijnlijk is het prototype uit elkaar gehaald om door middel van '*reversed engineering*' achter de werking te komen. Vermoedelijk is het vervolgens niet meer gelukt het prototype op de juiste manier in elkaar te zetten waardoor retourneren niet meer mogelijk was.

2.2 Standpunten en strategie

Nederland kent, net als elk ander land, tal van kernbelangen in de categorie Standpunten en strategie. Deze kernbelangen komen voor bij de overheid, in het bedrijfsleven en op het snijvlak tussen beide. Voorbeelden van dit type kennis zijn onderhandelingsmarges of in te nemen standpunten in internationaal verband. Bij de overheid valt te denken aan informatie over de Nederlandse standpunten met betrekking tot uitbreiding van de Europese Unie (EU) of bij economische onderhandelingen in de Groep van 20 (G20). In het bedrijfsleven kan het gaan om voorkennis over de inhoud van offertes of vroegtijdige kennis over overnameplannen.

Het openbaar bestuur en het Nederlandse bedrijfsleven kunnen grote schade oplopen door het weglekken van gevoelige beleidsstrategieën, -visies en standpunten. De andere partij kan, gebaseerd op deze kennis, immers beter gewogen beslissingen nemen over de in te zetten strategie, ten koste van de Nederlandse overheid of het Nederlandse bedrijfsleven.

Grootste spionageschandaal in geschiedenis NAVO

In februari 2009 is de Estse oud-Defensietopman Herman Simm wegens spionage veroordeeld tot een gevangenisstraf van twaalf en een half jaar. Simm gaf jarenlang geheime NAVO-informatie door aan de Russische civiele inlichtingendienst SVR. De hoeveelheid informatie die Simm heeft doorgespeeld is zo omvangrijk dat de NAVO stelt dat het hier gaat om het grootste spionageschandaal in het zestigjarig bestaan van het bondgenootschap. Simm ontving voor zijn spionagewerk grote geldbedragen. Geld was echter niet zijn enige drijfveer. Een andere belangrijke reden voor Simm om voor de SVR te werken was het feit dat deze dienst hem effectief wist te bespelen op gevoelens van frustratie en ijdelheid. Zo werden hem door de Russen bijvoorbeeld een hoge militaire rang en een hoge Russische onderscheiding in het vooruitzicht gesteld. Simms contactpersoon bij de SVR was een Russische inlichtingenofficier die zich jarenlang succesvol uitgaf voor Zuid-Amerikaanse zakenman. Zijn cover werd ondersteund door een correcte en complete set identiteitspapieren, inschrijving in relevante overheidsdatabases en een kloppend cv.

Meer dan bij de andere categorieën wordt over dit type kernbelang gecommuniceerd via e-mail of telefoon. Conceptstukken, opmerkingen, twistpunten en andere relevante informatie worden intensief uitgewisseld tussen belanghebbenden via (draadloze) e-mailsystemen en telefoons. Kwetsbaarheden van deze communicatiesystemen raken dit type kernbelang dan ook extra. Ook vanwege de relatief korte periode waarin dergelijke informatie waardevol is, is telecominterceptie[6] één van de voor de hand liggende methodes.

Kennis van strategie en standpunten kan daarnaast leiden tot meer algemene inzichten die op lange termijn waardevol blijven en waarmee partijen kunnen anticiperen op toekomstige standpunten.

2.3 Opkomende kernbelangen en infrastructuur

De kernbelangen uit deze categorie zijn ideeën, wetenschappelijk onderzoek of inzichten en concepten die nu (nog) openbaar zijn maar het in zich hebben op termijn tot economisch of strategisch interessante toepassingen te leiden. Daarnaast behoren ook cruciale onderdelen van de Nederlandse infrastructuur tot deze categorie. Voor beide soorten kernbelangen geldt dat ze op zich niet geheim of (wettelijk) beschermd zijn, maar dat ze tegelijkertijd wel van groot belang zijn voor het (toekomstig economisch) functioneren van de Nederlandse maatschappij.

De derde categorie kernbelangen wijkt op een cruciaal punt af van de eerste twee categorieën. Kernbelangen uit deze categorie zijn namelijk in meer of mindere mate bewust toegankelijk of openbaar gemaakt door de eigenaren. Ook verschillen ze van kernbelangen uit de andere categorieën in tijdsdimensie. De (volledige) consequenties van aantasting van deze categorie kunnen pas zichtbaar worden op lange termijn. Dit in tegenstelling tot '2.2 Standpunten en strategie' en '2.1 Datasets en blauwdrukken', waar de tijdsduur voor de gevolgen van aantasting optreden onvergelijkbaar korter is.

Hoewel kernbelangen in deze categorie niet met 'klassieke' spionageactiviteiten ontvreemd hoeven worden, moet wel rekening gehouden worden met mogelijk oneerlijke intenties van onderzoekspartners of potentiële kopers. Per geval moet afgewogen worden of het gaat om een eerlijk verzoek tot samenwerking, of dat achter de voorgestelde uitwisseling een dubbele agenda zit. Deze categorie is daarmee, evengoed als de andere twee categorieën, van belang voor de nationale veiligheid. Alleen met voldoende inzicht in kwetsbaarheden van deze categorie kernbelangen kunnen betrokkenen onderbouwde kosten-batenafwegingen maken.

Spionerende studenten
Technologische kennis, ook als die niet als 'geheim' gekwalificeerd is, kan heel waardevol zijn voor andere landen. Ook Nederland is een interessant land om kennis te vergaren op wetenschappelijk en technologisch terrein.
Binnen de wetenschappelijke sector (universiteiten, onderzoeksinstituten) is vaak een internationaal publiek actief. Dat biedt extra kansen voor inlichtingendiensten. Verschillende inlichtingendiensten die door de AIVD intensief worden gevolgd zijn erg actief in het verzamelen van inlichtingen op wetenschappelijk gebied. De AIVD heeft aanwijzingen dat in het buitenland studerende studenten door de inlichtingendiensten uit het land van herkomst soms worden ingezet om te spioneren.

[6] Met interceptie wordt in inlichtingencontext het 'tappen' van telecommunicatie bedoeld.

Hoogwaardige kennis

Technologie

Kenniseconomie

Octrooi

3. Kernbelangen in het economisch welzijn en het technisch-wetenschappelijk potentieel

Organisaties en bedrijven in Nederland beschikken over waardevolle hoogwaardige kennis en expertise. De Nederlandse concurrentiepositie is voor een substantieel deel gebouwd op deze hoogontwikkelde kennis en expertise, met name op het gebied van technologie en toegepaste wetenschap. De in Nederland ontwikkelde technologische kennis resulteert niet zelden in zeer succesvolle toepassingen in de industrie. Technische universiteiten, research & developmentafdelingen (r&d) van bedrijven en publieke en private kennis- en onderzoeksinstituten maken deel uit van de Nederlandse infrastructuur van onderzoek en ontwikkeling. De hier opgebouwde kennis en expertise staan op verschillende terreinen internationaal hoog aangeschreven en leveren een belangrijke bijdrage aan de Nederlandse (economische) welvaart.

In een wereld waarin de productie van goederen steeds meer plaatsvindt in lagelonenlanden, is het voor Nederland van belang een leidende rol te blijven spelen in onderzoek en ontwikkeling. Dit maakt ook dat het kabinet de ambitie heeft uitgesproken dat Nederland zichzelf internationaal (wederom) een toppositie verschaft als innovatieve kenniseconomie. Het versterken én behouden van innovatieve kennis en inzichten ten bate van de Nederlandse economie is daarvoor van het allergrootste belang.

Zoals eerder aangegeven is economische veiligheid één van de vitale belangen die beschermd dienen te worden in het kader van de nationale veiligheid. Het ongestoord functioneren van Nederland als effectieve en efficiënte economie is een waarborg voor de economische veiligheid van ons land. Aantasting van het economisch welzijn van Nederland raakt dan ook direct aan de nationale veiligheid. Kernbelangen in dit aandachtsgebied zijn te vinden in de categorieën datasets en blauwdrukken, standpunten en strategie en opkomende kernbelangen en infrastructuur. Deze laatste categorie is in dit aandachtsgebied prominent vertegenwoordigd.

De vraag rijst wat de economische schade van spionage is. Maar de financiële gevolgen van economische spionage voor de Nederlandse economie zijn tot op heden nooit gekwantificeerd. Een indicatie voor de gevolgen van economische spionage vormt de Duitse schatting dat Duitsland per jaar ongeveer 20 miljard euro schade lijdt door economische spionage. In de VS liggen de schattingen voor de schade die geleden wordt als gevolg van economische spionage ver uit elkaar: er worden bedragen tussen de 50 en 200 miljard dollar per jaar genoemd.[7]

3.1 Datasets en blauwdrukken

De sector economisch welzijn en technisch-wetenschappelijk potentieel kent veel datasets en blauwdrukken die interessant zijn voor buitenlandse inlichtingendiensten. De belangrijkste voorbeelden daarvan zijn hieronder terug te vinden.

Hangende octrooien

Een octrooi (ook wel bekend als patent) is een exclusief recht op een uitvinding waarmee anderen verboden wordt deze uitvinding commercieel toe te passen gedurende een bepaalde periode. Om een octrooi te verkrijgen moet een procedure gestart worden bij het Nederlands of Europees Octrooicentrum. Voor de aanvraag moeten de technologie en kennis die ten grondslag liggen aan het nieuwe product of proces inzichtelijk worden gemaakt. Dit staat in het octrooidocument waarin de nieuwe uitvinding beschreven wordt. Hierbij is het belangrijk om concreet en nauwkeurig de techniek van de nieuwe vinding te beschrijven om de verschillen met reeds bestaande octrooien aan te tonen en zo een sterk octrooidocument te krijgen.

Een dergelijk octrooidocument is interessant voor derden omdat het een uitgebreide beschrijving van een nieuwe uitvinding bevat. Kennis over octrooi-aanvragen geeft dus inzicht in de richting waarin onderzoek door andere landen/bedrijven plaatsvindt. Hoewel patentinformatie uiteindelijk openbaar wordt, duurt de aanvraag 18 maanden. Die periode geeft gelegenheid om bijvoorbeeld anderhalf jaar eerder de eigen r&d bij te sturen op basis van de opgedane kennis. Dat maakt spionage op dit terrein rendabel.

(Bewust) niet-gepatenteerde kennis

Ondanks het 'monopolierecht' dat een octrooi biedt, kan de kennis in de praktijk toch door anderen gebruikt worden. De handhaving van het octrooirecht is afhankelijk van de bereidheid van individuele landen om hun nationale industrieën aan deze regels te houden. Die bereidheid is niet altijd even groot, zeker niet als het gaat om strategische producten of grote financiële belangen. Een bedrijf

[7] Dave Drab, 'White paper: *Economic Espionage and Trade Secret Theft – Defending Against Pickpockets of the New M llennium*', Xerox Global Services, augustus 2003.

kan er daarom voor kiezen een uitvinding of technologie niet te patenteren maar geheim te houden. Het hoeft hier overigens niet alleen om technische blauwdrukken te gaan; ook productieprocessen kunnen bewust geheim worden gehouden. Dergelijke niet-gepatenteerde kennis is interessant om te bemachtigen, gebruik ervan is immers zelfs mogelijk zonder openlijk inbreuk te maken op lopende patenten.

Kernbelangen in de categorie blauwdrukken en datasets liggen niet alleen op het terrein van hangende octrooien en bewust niet-gepatenteerde kennis. Dit geldt ook voor reeds ontwikkelde en toegepaste kennis en technologieën. Voor Nederland is in dit verband een aantal hoogwaardige toepassingen relevant zoals de productie en toepassing van optica, radartechnologie en lucht- en ruimtevaarttechniek. Hetzelfde geldt in zekere mate voor terreinen als toegepaste robotica, *non-intrusive-scan*-technologieën en innovatieve toepassingen voor inzet onder water. Technieken en toepassingen die nog in ontwikkeling zijn, worden in de paragraaf 3.3 Opkomende kernbelangen en infrastructuur behandeld. Ook op militair en *dualuse*[8]-vlak vinden ontwikkelingen plaats die wel kort aangehaald worden, maar buiten het bereik van dit onderzoek vallen.

Optica en optomechanica

De kennis over optiek die in de Nederlandse wetenschappelijke wereld en het Nederlandse bedrijfsleven toegepast wordt, is van een hoog niveau. Daarnaast sluit deze techniek goed aan bij tal van andere Nederlandse bedrijfsactiviteiten. Optica is van belang voor toepassingsgebieden als chipfabricage (lithografie) en geavanceerde waarnemingsapparatuur. Laatstgenoemd ontwikkelingsterrein kan van belang zijn op strategisch-militair vlak. Hoogwaardige chipfabricage behelst zowel economische als strategisch-militaire belangen, waarbij de economische belangen waarschijnlijk groter zijn dan de directe strategisch-militaire, als we in ogenschouw nemen dat inmiddels meer dan de helft van alle *integrated circuits* (ic's, chips) gemaakt wordt met Nederlandse fotonicatechnieken. Deze economische en strategisch-militaire toepassingen verklaren de waargenomen interesse van buitenlandse inlichtingendiensten in onderzoek op het terrein van *high end* optica en haar toepassingsgebieden. De interesse van buitenlandse inlichtingendiensten is ook de reden dat Nederlandse bedrijven die in deze sector actief zijn een relatief hoog risicoprofiel hebben waar het gaat om spionage.

High Tech Systems – Mechatronica en robotica

High Tech Systems (HTS) is een innovatiegebied op het raakvlak van een groot aantal disciplines: mechanica, elektronica, fotonica en besturingstechnologie. De centrale technologie wordt gevormd door mechatronica, een geavanceerde integratie van deze disciplines. Deze technologie vormt de spil van *motion & control systems* die in vrijwel alle *hightech*-systemen van belang zijn.

Mechatronische systemen vinden hun toepassing in allerlei producten, instrumenten, systemen en sectoren: fabricageprocessen, consumentenelektronica, robotica, medische systemen, de automobielsector, de lucht- en ruimtevaart en technologieën ontwikkeld voor de defensiesector.

Robotica is een opkomende technologie die de potentie heeft om op de (middel)lange termijn een stempel op de samenleving te drukken. Op bepaalde deelgebieden van de robotica heeft Nederland een koppositie. Nederlandse autonome medische robotica en mechatronica staan bijvoorbeeld hoog aangeschreven in de wereld. Speerpunt van robotica in Nederland is het op maat toepassen van robottechnologie. Hiertoe worden aangeleverde robotsystemen volledig op de eisen van de klant toegesneden.

Nederland heeft een vooraanstaande positie in de chipindustrie, een sterk cluster medische technologie en huisvest diverse internationale topspelers op het gebied van HTS. In Nederland worden relatief veel octrooien aangevraagd voor mechatronica. Het aantal zit ver boven het Europese gemiddelde en ook dat van de VS.

Zowel op economisch als millitair-strategisch gebied vertegenwoordigt mechatronica een grote waarde. Dergelijke toegepaste kennis oefent dan ook grote aantrekkingskracht uit op buitenlandse inlichtingendiensten.

Radartechnologie

Door Nederland ontwikkelde radartechnologie kan een grote waarde hebben voor buitenlandse inlichtingendiensten. Voor radartechnologie geldt dat het naast civiele toepassingen ook militaire toepassingen kent. Vanuit het oogpunt van nationale veiligheid zou bij het weglekken van dergelijke kennis dus zowel het economisch welzijn als de territoriale integriteit van Nederland bedreigd kunnen worden.

[8] De toepasbaarheid van een bepaald soort kennis of apparatuur voor zowel civiele als militaire doeleinden.

Lucht- en ruimtevaarttechnologie

Binnen Nederland is ruime kennis voorhanden over (de toepassing van) lucht- en ruimtevaarttechnologieën. Dergelijke kennis is interessant voor sommige staten. Zowel vanuit financieel als vanuit strategisch oogpunt kan het van groot belang zijn om als land (of nationale industrie) dergelijke hoogwaardige technologieën te bezitten. Belangrijke componenten uit de in Nederland aanwezige expertise zijn onder meer kennis over innovatieve materialen en (civiele) *avionica* (hard- en software). Ook kennis over satelliettechnologie moet tot deze groep worden gerekend.

De kennis over (de toepassing van) lucht- en ruimtevaarttechnologie is allereerst van economisch belang voor de Nederlandse industrietak die een bijdrage levert aan de ontwikkeling en productie van onderdelen voor vliegtuigen en satellieten. Door kennisverlies aan derden bestaat het risico dat Nederlandse bedrijven economische schade oplopen. Deelname aan internationale programma's komt in gevaar omdat de potentiële Nederlandse inbreng reeds op andere wijze bekend is geworden als gevolg waarvan concreet verlies van orders voor de industrie op kan treden.

Het weglekken van kennis kan leiden tot de productie van hoogwaardig defensiemateriaal in landen van zorg. Daarnaast kunnen partijen uit dergelijke kennis informatie afleiden over Nederlands/Europees defensiemateriaal en de potentiële zwakke punten ervan. Ook dit raakt direct aan de nationale veiligheid.

Waterbouwkunde, -technologie en -management

Nederland leeft met water en heeft hierdoor noodzakelijkerwijs veel kostbare kennis opgebouwd op het gebied van waterbouwkunde. Nederlandse kennis van waterkeringen is uniek. Niet voor niets zijn Nederlandse bedrijven na de orkaan Katrina, die in 2005 het Amerikaanse New Orleans trof, gevraagd te helpen bij het verstevigen van de dijken aldaar.

Daarnaast heeft Nederland een unieke positie in de baggerindustrie. Nederlandse baggerbedrijven hebben een voorsprong in de wereld en zijn sterk vertegenwoordigd op de wereldbaggermarkt. Al met al vertegenwoordigt dergelijke kennis een grote waarde bij omvangrijke (infrastructurele) projecten, zeker voor opkomende economieën die veel van dergelijke projecten (willen) uitvoeren. De economische schade voor het Nederlandse bedrijfsleven die door diefstal van dergelijke kennis geleden kan worden is substantieel.

3.2 Strategie en standpunten

Kernbelangen op het terrein van Strategie en standpunten liggen voor wat betreft het economisch welzijn en het technisch-wetenschappelijk potentieel van Nederland hoofdzakelijk op het terrein van internationale orders en voorgenomen fusies en overnames van grote bedrijven die een stempel drukken op de Nederlandse economie.

Internationale orders

Met opdrachten die internationaal worden aanbesteed kunnen grote bedragen gemoeid zijn. Opdrachten kunnen dermate waardevol en prestigieus zijn dat een buitenlandse mogendheid er veel aan gelegen is een dergelijke opdracht aan de nationale industrie gegund te krijgen. Als men weet of een concurrent gaat offreren, en zo ja, als men kennis heeft van de details van de offerte, kan daar bij het opstellen van een eigen offerte rekening mee worden gehouden waardoor de kans op het binnenhalen van de opdracht groter wordt.

Een bekend voorbeeld van directe economische spionage vond plaats in 1985. Een Amerikaanse vliegtuigproducent werd ernstig benadeeld door een Franse inlichtingendienst. Tijdens de onderhandelingen over levering van een gevechtsvliegtuig aan de Indiase overheid, wisten Franse inlichtingenofficieren de voorwaarden van het Amerikaanse eindbod te achterhalen en door te spelen aan een Franse concurrent voor de order. Deze slaagden er vervolgens in het contract, van meer dan twee miljard dollar, binnen te halen.

Kennis over voorgenomen fusies of overnames

Vanuit economisch perspectief kunnen buitenlandse mogendheden geïnteresseerd zijn in voorgenomen fusies en overnames van of door multinationals. Als de betrokken spelers en bedragen bekend zijn, kunnen partijen fusies en overnames beïnvloeden of er zelfs een actieve rol in spelen. Op deze manier kunnen overnames voorkomen worden of kunnen de bedragen die met een overname gemoeid zijn bewust gedrukt of juist opgedreven worden. Meer strategische motieven kunnen ook een rol spelen, zoals bijvoorbeeld de wens om belangrijke bedrijven in bezit van een moederbedrijf uit eigen land te houden. Dit alles is met name relevant wanneer één van de betrokken partijen een Nederlandse onderneming is die qua werkgelegenheid, belastingafdracht of dividenduitkering van belang is voor de Nederlandse economie. Economische schade voor een dergelijk bedrijf betekent immers indirect schade aan de Nederlandse economie.

3.3 Opkomende kernbelangen en infrastructuur

Technisch wetenschappelijke kennis, informatie en *knowhow* in een relatief vroeg stadium van ontwikkeling moet een belangrijke bijdrage gaan leveren aan de Nederlandse economie op de (middel)lange termijn. Nederland herbergt relatief veel van dit soort kernbelangen, bijvoorbeeld in zijn technische universiteiten, maar ook in technisch hoogwaardige multinationals of initiatieven als een High Tech Campus.

Het belang van dergelijke kennis voor de Nederlandse economie bestaat uit de mogelijkheden voor doorontwikkeling en vergroting van de economische waarde. Bovendien leidt het beschikbaar hebben van dit soort 'vroege' kennis vaak tot de formatie van een cluster van hoogwaardige (*spin-off*)-bedrijven. Het vormen van dergelijke clusters op Nederlands grondgebied heeft een groot economisch belang. Dit geldt ook voor de toekomst, als een vakgebied volwassen wordt. Weglekken van kennis naar concurrerende landen verkleint de kans dat clustervorming zich in Nederland voordoet, terwijl hier wel de initiële investeringen gedaan zijn.

De AIVD ziet dat buitenlandse mogendheden op verschillende manieren deze kennis en informatie proberen te verwerven om daarmee hun eigen economie te stimuleren. Dit gebeurt door traditionele economische spionage maar ook door het laten opleiden van landgenoten in Nederland (bij voorkeur aan technische universiteiten) en door de overname van hoogwaardige technologische bedrijven. Enkele van de onderzoeksterreinen die in dit verband relevant zijn worden hieronder besproken.

Voor veel van deze ontwikkelingen geldt dat het potentiële *dual use* niet wordt herkend, waardoor de ontwikkelingen minder goed beschermd worden dan wanneer men zich wel bewust is van de mogelijkheid van een strategisch-militaire toepassing.

Innovatieve materialen

Nederland loopt voorop in de ontwikkeling van innovatieve materialen. Dit kennisgebied sluit nadrukkelijk aan bij de eerder beschreven lucht- en ruimtevaarttechnologie maar strekt zich breder uit dan alleen dat onderwerp. Deze kennis kan rekenen op de belangstelling van buitenlandse inlichtingendiensten. Kennis over bijvoorbeeld lichtgewicht composiet of zelfherstellende materialen is niet alleen te gebruiken voor meer reguliere toepassingen, maar ook van groot belang voor toepassingen met een duidelijk strategisch-militair karakter.

De economische gevolgen van spionage kunnen op dit terrein groot zijn. Als Nederlandse bedrijven en onderzoeksinstellingen in staat zijn unieke *high-performance*-materialen te leveren, draagt dat direct bij aan de welvaart in Nederland. Bij weglekken van dergelijke kennis aan derden kunnen Nederlandse bedrijven oneerlijke concurrentie krijgen. Dit komt bijvoorbeeld tot uiting in grote internationale samenwerkingsprojecten, waar de hoogwaardige materiaalkennis een *unique selling point* voor het Nederlandse bedrijfsleven zou zijn, maar nu ineens een andere partij de uiteindelijk deelname binnensleept.
Daarnaast is hier sprake van een duidelijk strategisch belang: innovatieve materialen zijn van groot belang voor de productie van en kennis over hoogwaardig defensiemateriaal. Verlies van dergelijke kennis kan dus directe consequenties hebben voor de territoriale veiligheid en andere defensiebelangen van Nederland en onze bondgenoten.

Biotechnologie

Biotechnologie is een economisch relevant onderzoeksveld dat nog steeds in opkomst is. Het is een brede discipline waarin Nederland zich historisch gezien samen met Japan in de voorhoede bevindt, maar waarbij Nederland inmiddels wel van deze koppositie wegzakt. De implicaties van toepassingen van geavanceerde biotechnologie zijn niettemin nog groot. Gezien het grote economische potentieel en eventuele *dualuse*-toepassingen van biotechnologie is de Nederlandse kennis op dit terrein waardevol voor andere overheden.

Biobased economy

De *biobased economy* is een opkomend concept waarin het gebruik van agrarische/biologische producten als grondstof voor allerlei materialen voor non-food-toepassingen centraal staat. Het gaat daarbij om nieuwe toepassingen en vooral om veranderingen in schaalgrootte. Voor bijvoorbeeld landen als China en India is de *biobased* economie, gezien de in deze landen groeiende honger naar energie en voedsel, van toekomstig levensbelang. Door de wereldwijde verschuiving die in deze richting voorzien wordt, en de enorme (financiële) implicaties van het 'vergroenen van de economie' is het voor Nederland van economisch belang zijn goede kennispositie op dit gebied te beschermen.

Life sciences

Nederland heeft een aantal succesvolle *bioscience* parken. Het park in Leiden behoort bijvoorbeeld tot de top vijf van Europa. Er wordt fors geïnvesteerd in deze locaties en sommige, zoals die in Amsterdam en Utrecht, worden nog steeds uitgebreid. In deze parken wordt geïnvesteerd in hoogwaardig wetenschappelijk onderzoek om innovatieve medische (bio)technologieën en nieuwe medicijnen te ontwikkelen. Grote investeringen in *life sciences* worden op den duur terugverdiend; startende bedrijven kunnen uitgroeien tot nieuwe spelers in de farmaceutische industrie

en gevestigde bedrijven doen vernieuwende vondsten. Onderzoek op het gebied van *life sciences* is daarmee een waardevol onderdeel van de Nederlandse kenniseconomie. Voor *life sciences* geldt, net als voor veel andere kernbelangen in dit aandachtsgebied, dat als de kennis wegvloeit vlak voor deze economisch rendabel wordt, er alleen is geïnvesteerd zonder dat daar de vruchten van kunnen worden geplukt.

Nanotechnologie

Nanotechnologie is een breed wetenschappelijk vakgebied waarvan de toekomstige toepassingmogelijkheden zowel maatschappelijke als economische impact zullen hebben. Nanotechnologie is de verzamelnaam voor toepassingen en technieken die op zeer kleine fysieke (nano)schaal plaatsvinden. Nanotechnologie heeft implicaties en toepassingen op tal van (andere) toegepast-wetenschappelijke gebieden zoals cryptologie, biologie (bionanotechnologie), natuurkunde (photonica, quantum computing), (bio)chemie en medische technologie/farmacie. Nanotechnologie maakt een heel scala van nieuwe of verbeterde producten mogelijk en is wellicht een van de meest in het oog springende kernbelangen. Nederlandse onderzoekers op dit terrein, in zowel de private als de publieke sector, behoren tot de internationale top. Er zijn op dit moment economische belangen mee gemoeid in de vorm van investeringen in onderzoek en r&d. Een koppositie op het gebied van nanotechnologie kan op termijn resulteren in *spin-off*-bedrijven en patenten die een nog veel groter economisch belang vertegenwoordigen. Een clustervorming van hoogwaardige nanotechnologiebedrijven in Nederland zou een groot economisch belang vertegenwoordigen. In de internationale competitie om een '*Centre of Excellence*' te worden op het gebied van nanotechnologie kan verlies van informatie aan andere partijen dus grote gevolgen hebben voor de toekomstige positie van het Nederlands bedrijfsleven. Een tweede belangrijke notie is dat de technologie niet alleen een economische waarde vertegenwoordigt, maar dat ook tal van (militair-)strategische toepassingen denkbaar zijn, die door landen als vitaal voor hun nationale veiligheid gezien zullen worden.

Wetenschappelijke samenwerking hoogwaardige technologie

De AIVD heeft vastgesteld dat buitenlandse inlichtingendiensten in Nederland spioneren op het gebied van nanotechnologie, waarbij zij bereid zijn brutaal te opereren om de gezochte informatie te bemachtigen. Recent nog bleek een buitenlandse wetenschappelijke delegatie bij een bezoek aan Nederland voor meer dan de helft uit inlichtingenofficieren te bestaan. Het doel van het bezoek was om tot nadere wetenschappelijke samenwerking op het gebied van nanotechnologie te komen. De deelnemers aan de delegatie waren overigens wel degelijk 'echte' wetenschappers met verstand van het onderwerp. Ze waren echter tegelijk ook inlichtingenofficieren. In het kader van samenwerking krijgen inlichtingenofficieren zo, onder valse voorwendselen, toegang tot personen en bedrijven die actief zijn op het gebied van nanotechnologie. Dit is een vorm van klassieke spionage om bij relatief openbare informatie te komen.

Dataverkeer

Netwerkinrichting

Aantasting

Interceptie

4. Kernbelangen in de telecomsector

Bij aantasting van belangen in de telecomsector is vrijwel direct sprake van aantasting van de nationale veiligheid. Communicatie en dataverkeer is van levensbelang voor het ongehinderd functioneren van de Nederlandse maatschappij. De sector kan bovendien door inlichtingendiensten worden gebruikt als een middel om toegang te krijgen tot informatie. De AIVD signaleert dan ook dat de telecomsector een doelwit is van buitenlandse inlichtingendiensten. Telecom is als het ware een kernbelang en kwetsbaarheid ineen. De kwetsbaarheden in de sector telecommunicatie hebben direct hun weerslag op alle andere sectoren. Een aantasting van belangen in de sector telecommunicatie heeft direct effect op de belangen van de sector zelf en/of zijn gebruikers.

In het kader van de nationale veiligheid maken instanties in de veiligheidsketen (waaronder politie, AIVD en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) gebruik van telefonieverkeersgegevens en andere gebruikersinformatie. Zorgen dat uitsluitend deze (bevoegde) partijen gebruik kunnen maken van deze wettelijk bepaalde interceptie, is van belang voor de nationale veiligheid. Het is immers een aantasting van de rechten van Nederlandse burgers, als buitenlandse inlichtingendiensten of organisaties Nederlands telecommunicatieverkeer zouden kunnen tappen. Daarnaast zou het vertrouwen in de overheid ernstig aangetast worden.

De grote interesse van buitenlandse inlichtingendiensten wordt verklaard door het feit dat telecommunicatie een flessenhals is waar een groot deel van alle 'technische' spionageactiviteiten langs plaats moet vinden. Deze sector biedt naast interceptiemogelijkheden ook tal van mogelijkheden om actief aanvallen uit te voeren op gekoppelde computersystemen. Op deze manier kunnen nagenoeg alle kernbelangen bereikt worden.

Telecommunicatie is een sector die de laatste jaren een stormachtige ontwikkeling heeft doorgemaakt door de voortdurende innovatie die er plaats vindt. Hierdoor zijn kernbelangen en kwetsbaarheden in deze sector, waarschijnlijk meer dan in andere, onderhevig aan veranderingen. Wat vandaag goed beschermd is, kan morgen kwetsbaar zijn. Het continue volgen van de (technologische en digitale) ontwikkelingen is daarom van groot belang.

4.1 Datasets en blauwdrukken

Het digitale dataverkeer bevat gegevens die in potentie toegang kunnen bieden tot informatie over andere kernbelangen bij andere sectoren, zoals strategische besluitvorming bij de overheid of bedrijfsgeheimen.

Informatie op het telecomnetwerk

De AIVD heeft sterke aanwijzingen dat buitenlandse inlichtingendiensten interesse hebben in informatie op het Nederlandse telecomnetwerk. Het gaat hier om telefonische verkeersgegevens en klantgegevens (wie belt met wie, abonneegegevens gekoppeld aan telefoonnummers, MAC-adressen (unieke identificatienummers van computerapparatuur), e-mailadressen, huisadressen en IP-adressen). Dergelijke gegevens zijn relevant voor de *datamining*- en data-analyse-activiteiten van buitenlandse inlichtingendiensten.

Telecominformatie is van oudsher een van de belangrijkste bronnen van informatie voor inlichtingendiensten. Ongewenste activiteiten van buitenlandse mogendheden gericht op het verkrijgen van telecommunicatiegegevens kunnen Nederlandse belangen aantasten, ook als deze activiteiten niet direct tegen Nederland gericht zijn. Daarnaast is het inwinnen van economisch relevante informatie voorstelbaar. In sommige landen behoort het inwinnen van economische inlichtingen in het buitenland immers tot de expliciet geformuleerde opdracht van inlichtingendiensten. De aandacht kan ook nog gericht zijn op (de inhoud van) telecomdiensten die via de sector worden aangeboden aan andere sectoren, zoals de afwikkeling van betalingsverkeer in de financiële sector of administratief verkeer van de energiesector.

Dergelijke activiteiten blijven niet altijd beperkt tot in Nederland gevestigde bedrijven. Ze kunnen ook plaatsvinden bij een Nederlands bedrijf of instelling, die in het buitenland is gevestigd.

De netwerken zijn drager van grote hoeveelheden gegevens afkomstig van andere sectoren zoals de energiesector, bancaire gegevens en overheidscommunicatie met inbegrip van:

- factuurgegevens van telecomproviders;
- dataverkeer voor regulering en aansturing van de vitale infrastructuur;
- dataverkeer van het digitale financieel economisch verkeer;
- IT-infrastructuur en communicatiesystemen van de Nederlandse overheid, de EU en de NAVO in Nederland;

- bedrijfsgeheimen die over een netwerk verzonden worden.

Het oneigenlijk inzien, kopiëren of ontvreemden van informatie uit de telecomsector kan diverse consequenties hebben. Er kan bijvoorbeeld economische schade optreden als bedrijfsgeheimen in de verkeerde handen vallen. Wanneer strategische informatie, bijvoorbeeld van de Nederlandse overheid, in vreemde handen komt, wordt de positie van Nederland in internationaal opzicht mogelijk ondermijnd.

Ten slotte kan legale interceptie (door de Nederlandse overheid) gecorrumpeerd worden als buitenlandse partijen zich toegang kunnen verschaffen tot deze legale interceptiemiddelen.

Informatie over het telecomnetwerk

Met informatie over infrastructuur en inrichting van de netwerken zélf kan een buitenlandse inlichtingendienst zich een beeld vormen van kwetsbaarheden van het netwerk. Ook kan met dergelijke heimelijk verkregen informatie eventueel een economisch voordeel worden behaald. Door middel van technische inzichten over netwerkinrichting kan een buitenlandse inlichtingendienst zich toegang verschaffen tot de infrastructuur van een telecomprovider, om vervolgens kennis te kunnen nemen van verkeer op het netwerk of gebruik te maken van de diensten van die provider. Ook kan een beeld verkregen worden van partijen die betrokken zijn bij beheer en onderhoud van de netwerken. Daarmee kan inzicht worden verkregen in manieren om toegang tot de netwerken te verkrijgen.

Van grote waarde zijn knooppunten van telecommunicatiediensten en datastromen, bijvoorbeeld AMSIX (dit is het grootste switchboard van Europa, en bevindt zich in Nederland). De knooppunten kunnen voor inlichtingendiensten fungeren als toegangs- of tappunten tot de eerder genoemde informatie die zich op het netwerk bevindt.

4.2 Standpunten en strategie

Hoewel interceptie van telecommunicatie een goede manier is om strategische kennis op te doen over kernbelangen, vormt de strategische kennis over deze sector zelf waarschijnlijk geen primair doelwit van spionage. Dergelijke kennis zal vooral gezocht worden door inlichtingendiensten om ermee een positie binnen de Nederlandse telecominfrastructuur te verwerven. Marktkennis kan namelijk bijdragen aan toetreding van buitenlandse telecombedrijven en leveranciers (van bijvoorbeeld *datawarehouse*-diensten[9], *billingservices*, of hard- en software) tot de Nederlandse markt. De AIVD signaleert dat een deel van de bedrijven die in Nederland actief zijn als toeleverancier afkomstig is uit hoogrisicolanden en dat een deel (historische) banden heeft met buitenlandse inlichtingendiensten. Dit zorgt voor een verhoogd spionagerisico.

4.3 Opkomende kernbelangen en infrastructuur

Vanwege de informatie die over dit netwerk verzonden wordt, en het belang voor het ongehinderd functioneren van de Nederlandse maatschappij, is de fysieke infrastructuur van het Nederlandse communicatienetwerk een kernbelang op zichzelf. Indien niet-gerechtigde actoren toegang krijgen tot telecomnetwerken, of partijen die al toegang hebben misbruik maken van hun autorisaties, dan kan dit zowel de nationale veiligheid, als de privacy van burgers als de integriteit van de telecomsector schaden. Ook de belangen van de gebruikers van de telecominfrastructuur (overheden en bedrijven) kunnen aangetast raken.
Het bezit van (onderdelen) van telecomnetwerken door buitenlandse partijen vormt in dit licht een potentiële bedreiging. Met het eigendom neemt immers ook de toegang tot informatie over het netwerk zelf, alsmede de gegevens die er overheen verzonden worden, toe. Onder druk van een buitenlandse inlichtingendienst zouden bij dergelijke bedrijven beide typen informatie verkregen kunnen worden.

[9] Een database waarin data uit verschillende systemen worden gedupliceerd om met deze gecombineerde gegevens rapportages en analyses te kunnen maken.

Economische Veiligheid

Weglekken

Cruciaal

Oppositiegroepen

5. Kernbelangen in de financiële sector

Economische veiligheid is in de Strategie Nationale Veiligheid gedefinieerd als één van de vijf vitale belangen die beschermd dienen te worden in het kader van de nationale veiligheid. De strategie noemt het 'ongestoord functioneren van Nederland als effectieve en efficiënte economie' als waarborg voor de economische veiligheid van ons land.

Het Nederlands welzijn is in hoge mate afhankelijk van het goed functioneren van de open economie, met een efficiënt werkende financieel-economische infrastructuur voor aanbieders en afnemers, consumenten en producenten. Die faciliterende infrastructuur moet betrouwbaar zijn en voldoen aan de kwaliteitsnormen die afnemers eraan stellen. Een tweede factor die van belang is bij het bewaken van de Nederlandse economische veiligheid betreft het veiligstellen van in economisch opzicht interessante informatie zoals voornemens op het gebied van investeringen of de toewijzing van belangrijke orders. Het weglekken van informatie op dit terrein kan aanzienlijke economische schade tot gevolg hebben.

Ook het technisch functioneren van het betalingsverkeer is cruciaal voor het goed functioneren van de maatschappij. Grote verstoringen op dit gebied zouden een directe bedreiging voor de nationale veiligheid betekenen en tot maatschappelijke ontwrichting kunnen leiden. Disruptie van het betalingsverkeer valt echter buiten de reikwijdte van dit onderzoek en wordt verder niet behandeld.

In de volgende paragrafen worden de kernbelangen binnen de sector puntsgewijs behandeld. Uit het onderzoek blijkt dat deze alleen zijn te vinden in de categorie Datasets en blauwdrukken. De andere categorieën zijn, althans binnen de afbakening van dit onderzoek, niet vertegenwoordigd.

5.1 Datasets en blauwdrukken

Inzicht in het betalingsverkeer

Buitenlandse inlichtingendiensten zijn vooral geïnteresseerd in betalingsverkeer om inzicht te krijgen in het doen en laten van de individuen en groeperingen waarnaar ze onderzoek verrichten. Het kan dan bijvoorbeeld gaan om (leden van) een migrantengemeenschap, oppositiegroepen of jihadistische terroristen. Via het betalingsverkeer kunnen diensten eventueel ook inzicht krijgen in het betalingspatroon van hoofdrolspelers in de Nederlandse economie. Dit kan negatieve gevolgen hebben voor de concurrentiepositie van het Nederlandse bedrijfsleven. Met kennis en inzicht in het geldverkeer van en naar staatsbankrekeningen kan afgeleid worden waarin de Nederlandse overheid investeert.

De focus van buitenlandse inlichtingendiensten op het Nederlandse (deel van internationaal) betalingsverkeer is weliswaar vanuit het oogpunt van economische spionage onwenselijk, maar in het kader van terrorismebestrijding is delen van dit soort informatie juist wel wenselijk. Door informatie over financiële transacties te combineren met bestanden over personen die onderzocht worden, kunnen immers verdachte transacties gevonden worden. Bijvoorbeeld met betrekking tot de financiering van terrorisme. Deze strijdige belangen maken bescherming van het betalingsverkeer extra complex.

Persoonsgegevens bij banken

Naast het overzicht van alle financiële transacties hebben banken de beschikking over uitgebreide gegevensets van hun klanten. Deze informatie helpt inlichtingendiensten inzicht te krijgen in individuen en groeperingen waarnaar ze onderzoek verrichten. Daarnaast is inzicht in de financiële situatie en uitgavenpatronen in combinatie met de naam van de werkgever gevoelig. Hiermee kunnen bijvoorbeeld personen gespot worden die een interessante werkgever hebben en tegelijkertijd mogelijk vatbaar zijn voor omkoping of chantage.

Energievoorzieningszekerheid

Olie en gas

Concurrentiepositie

Energiebronnen

6. Kernbelangen in de energiesector

Energie en de energiesector vormen een belangrijke pijler onder de Nederlandse economie. Zo exploiteert Nederland het grootste aardgasveld van Europa, fungeert de Rotterdamse haven als hét olieknooppunt voor West-Europa en hebben grote olie(handels)bedrijven een standplaats op ons grondgebied. Naast jarenlang opgebouwde technische kennis op het gebied van olie- en gaswinning, -opslag, -bewerking en -transport beschikt Nederland ook over kennis en vaardigheden op het gebied van handel in energie, met name op het terrein van gas. Zowel de hardere (technologische) energiekennis als de zachtere kanten van de sector (vaardigheden bij het vermarkten van energie op de handelsvloer) bepalen de internationale concurrentiepositie van Nederland. Beide zijn daarmee interessant voor buitenlandse inlichtingendiensten.

Ook in de toekomst zal energie voor Nederland op een aantal vlakken van groot belang blijven. Het kabinet ondersteunt expliciet het streven om Nederland straks de 'gasrotonde' van Europa te maken en zo de Nederlandse rol als Europees energieknooppunt verder te versterken. Dit houdt in dat Nederland voor Noordwest-Europa een belangrijk logistiek knooppunt wordt voor de opslag en transport van gas. Hiermee kan Nederland zijn energievoorziening voor de toekomst zeker stellen. Daarnaast kan de functie van knooppunt een sterke stimulans zijn voor Nederlandse ondernemingen. Kennis over een eventuele strategie ter realisatie van deze knooppuntfunctie is een potentieel doelwit van inlichtingenactiviteiten, evenals de kennis die het mogelijk maakt om strategische onderdelen van de 'gasrotonde' in handen te krijgen.

De ambitie van Nederland op energiegebied strekt verder dan de 'gasrotonde'. Ook onderzoek naar groene energie, energiebesparing, en CO_2 -reductie vindt in Nederland op hoog niveau plaats. Dergelijke kennis moet Nederland de middelen bieden om ook op lange termijn een rol van betekenis te blijven vervullen op de Europese energiemarkt. De afnemende reserves van fossiele brandstoffen en de steeds breder gedragen zorg over het milieu en het klimaat, maken de kennis over processen om groene energie op te wekken, te transporteren en op te slaan van groot economisch belang. Innovatie in de energiesector op het gebied van duurzame energiebronnen en -dragers (ook wel *energy efficiency*) zijn belangrijk voor de lange termijn. Nederland heeft nu grote economische belangen in energie maar om die ook in de toekomst veilig te kunnen stellen moet Nederland aandacht houden voor ontwikkeling, exploitatie, toepassing en vermarkting van bestaande en nieuwe energiebronnen en innovatieve energieoverdracht- en transportmiddelen

Naast het louter economische belang van (de toevoer van) energie gaat er ook een politiek-strategisch belang van de sector uit. Energietoevoer heeft invloed op de internationale politieke verhoudingen. Er bestaat een groot spanningsveld tussen verschillende landen met als inzet een gunstige prijsstelling voor de af te nemen energie en grondstoffen en de leveringsvoorzieningszekerheid van deze grondstoffen. Landen met aanzienlijke energiebronnen hebben in dit krachtenveld een belangrijke positie. De potentiële invloed van energieleverende landen brengt risico's met zich mee voor de afnemende landen, waaronder Nederland. Deze landen zouden immers onder druk kunnen worden gezet met energieleveranties als pressiemiddel. Landen die hun energietoevoer veilig gesteld hebben, en niet afhankelijk zijn van één of een klein aantal leveranciers, hebben meer vrijheid om onafhankelijk te opereren in de internationale arena.

6.1 Datasets en blauwdrukken

Kernbelangen binnen de categorie Datasets en blauwdrukken raken veelal aan innovatieve technologieën ten bate van de winning van olie en gas en de transport, opslag en bewerking van fossiele brandstoffen. Ook technieken voor het benutten van alternatieve energiebronnen vallen in deze categorie.

Technieken voor olie en gaswinning

Nederland heeft een sterke kennispositie op het gebied van de winning van olie en gas. Deze technische kennis onderscheidt Nederlandse bedrijven van buitenlandse concurrenten, waardoor belangrijke contracten voor de exploitatie van olievelden binnengehaald kunnen worden. In dit kader kan bijvoorbeeld gedacht worden aan *offshore*technologie waarover Nederland veel kennis bezit. Vanwege de omvang en duur van dergelijke projecten is de economische impact van deelname groot. Voor andere landen is kennis over deze technieken uit zowel financieel als strategisch oogpunt aantrekkelijk. Technische kennis over olie- en gaswinning vormt dan ook een doelwit van inlichtingendiensten. Daarnaast is het van belang erbij stil te staan dat er extra aandacht is voor dergelijke technieken van inlichtingendiensten uit landen die onder embargoregimes vallen. De kennis en *knowhow* uit de energiesector die door hen niet commercieel ingevoerd kan worden, bijvoorbeeld vanwege een handelsembargo, kan alleen nog verkregen worden door middel van spionage of via andere heimelijke wegen.

Technieken voor transport, opslag en bewerken van olie en gas

Naast kennis over de technische kant van het winnen van olie en gas, is er in Nederland ook veel kennis aanwezig over aanpalende processen, zoals technieken om olie en gasproducten te bewerken, te transporteren en op te slaan. Ook waardevol is kennis op het gebied van het vloeibaar maken (*liquification*), het behandelen en transporteren van Liquid Natural Gas (LNG). In de Nederlandse ambitie om een internationaal knooppunt te zijn voor de doorvoer van energie(producten) kunnen dergelijke technologieën een belangrijke troef zijn. Weglekken van deze kennis verzwakt de Nederlandse positie in de internationale competitie voor het verwezenlijken van een dergelijke economisch zwaartepunt.

Technieken voor alternatieve opwekking van energie en CO_2-opslag

Naast de kennis over het winnen van conventionele energie is in Nederland ook veel kennis voorhanden op het gebied van alternatieve opwekking van energie. Nederland bezet een vooraanstaande positie in het onderzoek naar en de productie van zonneceltechnologie. Hoogwaardige innovatieve vondsten, zoals flexibele folies met zonnecellen en efficiënte windenergie-opwekking, hebben hun oorsprong in Nederland.

Nucleaire energie

Kennis op het gebied van nucleaire energie is niet diepgaand onderzocht in het kader van deze analyse omdat dit reeds een regulier onderwerp van onderzoek vormt van de Nederlandse inlichtingen- en veiligheidsdiensten in het kader van met name non-proliferatie. Toch wordt het kernbelang in dit rapport kort benoemd omdat Nederland een hoog kennisniveau heeft op dit gebied en er grote (economische) belangen mee gemoeid zijn. Zo wordt in Nederland een aanzienlijk aandeel van het wereldwijd gebruikte verrijkt uranium geproduceerd met behulp van, in Nederland ontwikkelde, centrifugetechnieken. Daarnaast is bijvoorbeeld meer dan de helft van alle medische isotopen die in Europa gebruikt worden afkomstig uit Nederland.

6.2 Standpunten en strategie

Nederland wil in de toekomst een belangrijke rol blijven spelen op de internationale energiemarkt, deels uit economische overwegingen, deels ook vanuit strategische overwegingen die raken aan energievoorzieningszekerheid. Om deze ambities waar te maken werkt Nederland, deels in internationaal verband, aan langjarige energiestrategieën, -visies en -beleid. Belangrijke onderdelen daarvan zijn kernbelangen in de categorie 'standpunten en strategie'.

Energiebeleid van Nederland en de EU

De in Nederland aanwezige kennis over het meerjarige energiebeleid van ons land, alsmede dat van Europese gremia als de EU, vormt een kernbelang. Een onderdeel daarvan zijn de visiestukken, strategische documenten en andere informatie die raken aan de Nederlandse ambitie om gasstromen in Europa te verbinden. Nederland is echter niet het enige land dat deze ambitie heeft; andere Europese landen manifesteren zich ook als knooppunten van gasstromen van Europa, of willen daar in ieder geval zo veel mogelijk grip op blijven houden. Alle kennis over de Nederlandse strategie ter realisatie van de 'gasrotonde' en andere vergelijkbare strategische beleidslijnen kan dan ook als waardevol voor inlichtingendiensten gezien worden.

Strategische bedrijfsinformatie

Strategische bedrijfsinformatie van grote bedrijven in de olie- en gassector is interessant voor buitenlandse inlichtingendiensten. Het gaat ondermeer om kennis over voorraden, reken- en analysemodellen en biedingen bij aanbestedingen. Ook de financiële situatie en de investerings- en bedrijfsstrategieën, bijvoorbeeld met betrekking tot de ontwikkeling van nieuwe olie- en gasvelden, zijn zaken waar inlichtingendiensten in geïnteresseerd zijn. Dit speelt mede omdat een aanzienlijk deel van de internationaal opererende bedrijven in de sector staatsbedrijven zijn of zeer nauwe banden met een nationale overheid onderhouden. Het weglekken van dit soort kennis heeft een verslechtering van economische positie van de getroffen bedrijven tot gevolg. Daarmee wordt ook de economische positie van Nederland geraakt, bijvoorbeeld door verlies van werkgelegenheid, belastinginkomsten en dividenden. Bovendien kan de energieleveringszekerheid voor Nederland (indirect) geraakt worden.

Handelsvaardigheid (cultuur en structuur van de markt)

Traditionele partijen in het Nederlandse energielandschap beschikken over een combinatie van handelsvaardigheden en kennis van de culturele en structurele inrichting van de Nederlandse energiemarkt. De wijze waarop de Nederlandse markt is ingericht en functioneert is een verworvenheid. Buitenlandse partijen kunnen een voordeel behalen door (heimelijk) kennis te nemen van de cultuur en structuur van de Nederlandse markt om deze zo op een juiste manier te kunnen betreden. Deze vaardigheden zijn grotendeels cultureel en commercieel.

Buitenlandse partijen kunnen zich, openlijk en heimelijk, oriënteren op de cultuur en structuur van de Nederlandse gashandel. Bijvoorbeeld door samenwerkingsverbanden voor te stellen, *joint ventures* aan te gaan of investeringen op Nederlandse bodem te doen. Buitenlandse energiebedrijven kunnen met deze samenwerkingsverbanden eerste stappen zetten op de Nederlandse energiemarkt waarbij niet

uitgesloten kan worden dat enkele van deze partijen dit als opmaat zien in hun ambitie om op termijn een belangrijke bepalende stempel te drukken op de West-Europese energiemarkt.

6.3 Opkomende kernbelangen en infrastructuur

De invoering van de Wet Onafhankelijk Netbeheer (WON) heeft geleid tot een snelle opeenvolging van gebeurtenissen in de energiesector. Door de WON zijn productie en levering van energie gesplitst en is onafhankelijk netbeheer ontstaan. Hierdoor zijn een groot aantal partijen die van belang zijn voor de Nederlandse energievoorzieningszekerheid meer onder invloed gekomen van ontwikkelingen op de vrije markt en minder van de Nederlandse overheid. Hierdoor kunnen controle op en bescherming van kernbelangen in deze sector door de Nederlandse overheid verminderen, met mogelijk ongewenste gevolgen.

Energie-infrastructuur, -levering en -opslag

Kennis en informatie die de energievoorzieningszekerheid van Nederland garanderen, vormen een kernbelang. In het geval van energieschaarste is het belangrijk om zeker te zijn dat Nederland toegang blijft houden tot de door Nederlandse partijen gereserveerde energievoorraden. Het is echter de vraag wat de mogelijkheden zijn voor Nederland als een (niet-Nederlands) commercieel bedrijf zijn contractuele verplichtingen niet aan alle partijen kan nakomen en besluit het Nederlandse deel van zijn energieleveranties niet na te komen, om de voorziening van een grotere klant, of het vestigingsland zelf, veilig te stellen. Door niet alleen de energie-infrastructuur, maar ook cruciale onderdelen voor de beheersing van energieproductie en -levering in Nederlandse handen te houden maakt Nederland zich met betrekking tot zijn energievoorzieningszekerheid minder afhankelijk van anderen. Kennis waarmee buitenlandse energiebedrijven cruciale componenten van de Nederlandse energiesector in handen kunnen krijgen, vormt een kernbelang. Het concentreren van cruciale elementen van de ‘gasrotonde’ in Nederland brengt namelijk kansen voor ons land met zich mee maar zorgt tevens voor risico’s, mocht het eigendom en daarmee de zeggenschap van (cruciale onderdelen van) de Nederlandse energiesector in handen vallen van buitenlandse (staats)energiebedrijven.

Het bezit en beheer van een infrastructureel netwerk is echter slechts een deel van de garantie op energievoorziening; het bezit van een netwerk zegt niets over de vraag welke partij daar, tegen welke prijs, energie op wil leveren. De veronderstelling dat energie beschikbaar is, en dat aangekochte energie ook daadwerkelijk geleverd wordt, is alleen houdbaar bij een normaal functionerende markt. Ten tijde van energieschaarste, of bij spanningen of conflicten, kan het verkrijgen van energie echter niet meer vanzelfsprekend worden geacht. De duidelijke scheiding die in Nederland bestaat tussen overheid en markt, is in andere EU-landen al minder scherp, en buiten de EU zelfs geregeld diffuus. In een gespannen markt kunnen commerciële afspraken onder druk komen te staan als de staatsbelangen zich in de buitenlandse energiepartij gaan manifesteren. Energie kan om politieke of commerciële redenen niet zoals overeengekomen aan Nederland geleverd worden, bijvoorbeeld omdat op het laatste moment een koper is gevonden die een hogere prijs biedt, of doordat het land dat energie aanbiedt volumes ‘knijpt’, om zo politieke of economische druk te forceren. Schommelingen in de energieprijs werken door naar consumenten en naar de industrie. Een hogere prijs voor gas of elektriciteit voor Nederland betekent onmiddellijk een achterstelling in economische positie, doordat de productie hier duurder wordt.

Kennis met betrekking tot alternatieve energiebronnen

Nederland beschikt over hoogwaardige technologische kennis over renewables, alternatieve energiebronnen en systemen om energieverbruik zuiniger en efficiënter te maken. Hier investeert Nederland fors in. Ook buitenlandse overheden zijn in deze kennis geïnteresseerd. Er is op dit moment in Nederland weinig aandacht voor het behoud van deze potentieel zeer waardevolle kennis. Kennis kan daardoor op heimelijke wijze weglekken naar landen die, net als Nederland, op termijn genoodzaakt zullen zijn over te gaan op andere energiebronnen. Zo verdwijnt het onderliggend onderzoekswerk van meer fundamentele aard, en de Nederlandse investeringen in de ontwikkeling ervan, naar het buitenland.

Overheidsbeleid

Manipulatie

Rechtsstaat

Integriteit

Infiltratie

7. Kernbelangen in het openbaar bestuur

De Rijksoverheid speelt een rol in de bescherming van de vijf 'vitale belangen' die in de Strategie Nationale Veiligheid zijn benoemd. De rijksoverheid is bovendien een symbool van de onafhankelijkheid van Nederland als staat. Daarmee vervult de rijksoverheid een belangrijke vertrouwensrol ten opzichte van de burgers. De integriteit en de betrouwbaarheid van de Nederlandse overheid komen onder druk te staan als buitenlandse inlichtingendiensten heimelijk inlichtingen kunnen verzamelen bij de overheid, of het overheidsbeleid actief en heimelijk proberen te beïnvloeden. De Nederlandse burger vertrouwt erop dat de overheid zorg draagt voor bescherming van de veiligheid en de rechten van haar burgers, zonder ongewenste bemoeienis van buitenaf. De betekenis van de sector 'openbaar bestuur', als onderdeel van de (rijks)overheid voor de nationale veiligheid is derhalve groot.

De Nederlandse overheid is om een aantal redenen een voor de hand liggend doelwit van spionageactiviteiten van buitenlandse mogendheden. Zij beschikt in de eerste plaats over een grote hoeveelheid gegevens die interessant kunnen zijn voor andere mogendheden. Deze gegevens variëren van strategisch-tactische beleidsvoornemens van de regering tot de persoonsgegevens van burgers en economische data van bedrijven en sectoren. In de tweede plaats worden door overheidsfunctionarissen belangrijke beslissingen genomen die richtinggevend zijn voor de rol die Nederland speelt in internationale gremia. Bewindslieden en hoge ambtenaren beschikken over gevoelige informatie (standpunten, onderhandelingsruimte en strategie) voorafgaand aan internationale onderhandelingen en besprekingen. Ten slotte is de overheid schakelpunt naar bedrijven en instellingen, worden op overheidsniveau gelden toegekend aan sectoren in de Nederlandse economie (in de vorm van subsidies) en faciliteert en bemiddelt de overheid in het veld tussen bedrijven en burgers. Hiermee speelt de overheid een invloedrijke financieel-economische rol, en ook hier kan een buitenlandse mogendheid belang hebben bij het heimelijk aansturen van deze rol in een bepaalde richting.

Politie en justitie vertegenwoordigen de Nederlandse rechtsstaat in de meest concrete vorm. Spionage en buitenlandse inmenging op dit onderdeel van openbaar bestuur raken dus direct aan de integriteit en onafhankelijkheid van de rechtsstaat. Een buitenlandse mogendheid kan belang hebben bij het verkrijgen van informatie over (voormalige) landgenoten bij politie en justitie. Een economisch motief voor infiltratie of manipulatie is het onderhouden van banden met de migrantengemeenschap in Nederland met als achterliggend doel het op gang houden van geldstromen vanuit Nederland naar het land van herkomst.

Tot slot beschikt de overheid over het geweldsmonopolie en hebben politie en justitie in deze hoedanigheid bevoegdheden die andere organisaties niet hebben (verrichten van arrestaties, bijzondere opsporingsmiddelen). Kennis over technieken van onderzoek door politie en justitie kan voor andere mogendheden interessant zijn omdat deze de kans op ontdekking van heimelijke activiteiten kan verkleinen. Het weglekken van informatie kan op deze wijze de kwetsbaarheden van kernbelangen ook in andere sectoren vergroten.

In de volgende paragrafen worden de kernbelangen van het openbaar bestuur afzonderlijk behandeld.

7.1 Datasets en blauwdrukken

Databanken

De Nederlandse overheid beschikt, al dan niet gecentraliseerd, over veel gegevens van Nederlandse burgers, bedrijven en organisaties. Verschillende van deze databanken kunnen in meer of mindere mate op de belangstelling van buitenlandse inlichtingendiensten rekenen.

Enkele voorbeelden van interessante databestanden in beheer van de Nederlandse overheid zijn:

- (inkomsten)gegevens van personen, bedrijven en organisaties bij de Belastingdienst;
- informatie uit de gegevensbestanden van de Gemeentelijke Basis Administratie (GBA);
- personeelsgegevens van overheidspersoneel, in het bijzonder onderdelen als het ministerie van Buitenlandse Zaken, Algemene Zaken of Defensie;
- informatie uit politie informatiesystemen zoals Herkenningsdienst-systeem (HKS) en Xpol;
- informatie uit tal van andere informatiesystemen zoals die van de Sociale Verzekeringsbank (SVB), Dienst Uitvoer Onderwijs (DUO), Immigratie- en Naturalisatiedienst (IND), Douane.

De steeds verdergaande koppeling van databestanden van verschillende overheidsorganisaties leidt enerzijds tot meer gebruiksvriendelijkheid voor de overheid en de burger, maar maakt deze databestanden ook kwetsbaarder voor inzage door onbevoegden. Er ontstaan namelijk meerdere ingangen om het systeem te benaderen. Via het minst beveiligde systeem kan toegang worden verkregen tot gegevens die moeilijker direct te benaderen zijn: de hele keten is immers slechts zo sterk als de zwakste schakel.

Uit deze, al dan niet aan elkaar gekoppelde, bestanden is veel specifieke informatie te halen over individuen en organisaties. Hoewel niet elke genoemde databank op zichzelf een letterlijk kernbelang is, geldt wel dat de verschillende bestanden, bijvoorbeeld met behulp van *datamining*, waardevolle inzichten kunnen bieden.

Gegevens uit deze databanken kunnen inlichtingendiensten informatie verschaffen over personen en/of organisaties waarvoor zij belangstelling hebben. Daarnaast bieden de gegevens in de databanken toegang tot andere kernbelangen omdat mensen op interessante posities, en hun mogelijke kwetsbaarheden (zoals hun financiële situatie, gezinssituatie, strafrechtelijk verleden), doeltreffend geïdentificeerd kunnen worden.

Daarnaast zijn de gegevens die over burgers en organisaties of bedrijven in de verschillende systemen staan privacygevoelig en kwetsbaar. Het zijn gegevens die in Nederland niet zomaar met mensen gedeeld mogen worden. Weglekken van deze informatie naar buitenlandse mogendheden zou het vertrouwen van de burger in de (rijks) overheid dan ook ernstig aantasten en zo een bedreiging vormen voor de nationale veiligheid.

Kennis over beveiligingssystemen

Op diverse plekken binnen de overheid wordt onderzoek gedaan naar weerstandsverhogende maatregelen voor ICT-systemen en naar veiligheidssystemen als cryptografie en biometrie. Zowel deze kennis op zichzelf, als kennis over de toepassing ervan in Nederlandse beveiligingsmaatregelen, kan van grote waarde zijn voor inlichtingendiensten. Het biedt immers kansen om de eigen beveiliging te verhogen, of de beveiliging bij andere Nederlandse kernbelangen te omzeilen. De kennis helpt inlichtingendiensten bovendien om beter in te schatten met welke 'afbreukrisico's' het uitvoeren van inlichtingenoperaties gepaard gaat.

7.2 Standpunten en strategie

De Nederlandse standpunten in internationale beleidskwesties, de Nederlandse strategie bij onderhandelingen met internationale partners en de langjarige visie op de inrichting van vitale sectoren vormen een verzameling kernbelangen die traditioneel gezien op veel interesse van buitenlandse inlichtingendiensten kunnen rekenen. De aanwezigheid van een groot aantal internationale instellingen in Nederland – met name in Den Haag – trekt eveneens buitenlandse inlichtingenactiviteiten aan.

Standpunten van de Nederlandse overheid in internationale kwesties

Kennis over het standpunt en de strategie die Nederland wenst in te zetten in internationale overleggen kan door andere landen gebruikt worden om hun eigen standpunten en strategie vorm te geven. Een voorbeeld is het standpunt van de Nederlandse overheid over EU-beleid en -strategie. Behalve de negatieve effecten die het weglekken van informatie over deze standpunten kan hebben op de onderhandelingsruimte van Nederland in internationale gremia, kan deze informatie bovendien gebruikt worden om heimelijk andere partijen te mobiliseren. Voorbeelden daarvan zijn de Nederlandse standpunten ten aanzien van de EU, energievoorzieningszekerheid en handelsbelangen.

Informatie over de EU en NAVO

De Europese Unie (EU) is met 27 lidstaten en bijna een half miljard inwoners een (economisch) invloedrijk partnerschap en daarmee doelwit van spionage door niet-EU-lidstaten. Hetzelfde geldt voor de Noord-Atlantische Verdragsorganisatie (NAVO). Inlichtingendiensten zijn buitengewoon geïnteresseerd in informatie over de interne verhoudingen binnen internationale organisaties. Met name standpunten in onderlinge meningsverschillen tussen EU-lidstaten of NAVO-lidstaten vormen voor buitenlandse partijen interessante informatie, bijvoorbeeld over uitbreiding van de EU of de NAVO. Informatie over eventuele onderlinge meningsverschillen kan gebruikt worden om partijen uit elkaar te spelen, en zo de organisatie te verzwakken in haar internationale optreden. Dit vergroot de manoeuvreerruimte voor andere partijen in de internationale arena. Een verzwakking van de EU of de NAVO kan de internationale positie van Nederland en Nederlandse belangen, op bijvoorbeeld economisch gebied, schaden.

Daarnaast bestaat er interesse in gerubriceerde informatie van internationale organisaties, zoals de voorgenomen strategie op een bepaald dossier. Alle deelnemende landen met toegang tot dergelijke informatie hebben de verantwoordelijkheid om deze afdoende te beveiligingen. Inlichtingendiensten zullen, om ingangen te vinden, zoeken naar een zwakke plek bij de verschillende deelnemende partijen. Los van het belang van deze informatie loopt Nederland in internationaal verband politieke schade op als een eventuele zwakke plek zich in Nederland blijkt te bevinden.

Nederland huisvest tal van internationale organisaties. Dat gastheerschap brengt de verantwoordelijkheid met zich mee deze internationale organisaties een ongehinderd functioneren te garanderen. Het tegengaan van spionage bij dergelijke organisaties valt dus ook onder de verantwoordelijkheid van de Nederlandse overheid. Spionage-incidenten bij een dergelijke organisatie hebben daarmee negatieve gevolgen voor de internationale positie van Nederland.

Technische route

Zwakste schakel

Afluisteren

Inlichtingendienst

Cultiveren

8. Hoe lekt informatie weg? Risico's en kwetsbaarheden voor spionage

In de voorgaande hoofdstukken zijn voor diverse sectoren kernbelangen benoemd die interessant zijn voor buitenlandse inlichtingendiensten. Deze diensten kunnen de betreffende kernbelangen op grofweg twee manieren proberen te bemachtigen.
De eerste manier is om via mensen informatie in te winnen. De andere methode is om met technische middelen informatie te onderscheppen. Alle factoren die aantasting van kernbelangen door spionage mogelijk maken, hangen samen met deze twee routes – mens en techniek.

Buitenlandse inlichtingendiensten hanteren uiteenlopende methodes om via mensen toegang te verkrijgen tot voor hen interessante informatie of gegevens. Elke inlichtingendienst heeft daarbij een eigen wijze van opereren, maar gemene delers kunnen wel onderscheiden worden. Deze komen terug in paragraaf 8.2.

De technische route wordt eveneens door bijna alle diensten toegepast. Er zijn op dit gebied echter grote verschillen in capaciteiten van de verschillende diensten. In paragraaf 8.1 wordt aandacht besteed aan deze technische kwetsbaarheden. In inlichtingenoperaties wordt overigens vaak een heel scala aan methodes en middelen gecombineerd ingezet, om elkaar aan te vullen, te verifiëren en te versterken. Er bestaan dus talloze mengvormen van 'opereren'.

Ook in de toekomst zullen inlichtingendiensten zich blijven richten op de twee toegangsroutes, mens en techniek. Dit zijn bij het beschermen van kernbelangen dan ook altijd de zaken waarop de aandacht primair gericht moet zijn. Het is het echter goed om te beseffen dat ontwikkelingen in de inlichtingenwereld soms snel gaan; er is een continue wedloop van aanvalstechnieken en tegenmaatregelen op beide terreinen gaande, waardoor er feitelijk een continue noodzaak tot het evalueren van kwetsbaarheden is. Wat kort geleden nog afdoende bescherming was, kan vandaag niet langer toereikend zijn.
Uit het onderzoek komen drie belangrijke ontwikkelingen naar voren die op dit moment de kwetsbaarheid van de Nederlandse kernbelangen beïnvloeden. Dit zijn beleid, uitbesteding en verwevenheid. Deze ontwikkelingen worden later in dit hoofdstuk in meer detail besproken.

De wijze waarop een inlichtingendienst bij voorkeur zal trachten de informatie te achterhalen hangt af van een aantal factoren, zoals de 'specialiteit' van de betreffende inlichtingendienst en hoeveel risico deze bereid is te nemen. De belangrijkste afweging zal echter altijd zijn wat de zwakste schakel in de beveiliging is, ofwel de grootste kwetsbaarheid van een kernbelang. En die zwakste schakel -techniek of mens, verwevenheid met andere systemen of uitbesteding- hangt sterk samen met het kernbelang dat een buitenlandse mogendheid wil ontvreemden.

8.1 Toegangsroute 1: technische toegang

De eerste methode om toegang tot kernbelangen te krijgen, is via technische middelen. Informatie ligt opgeslagen in documenten, in de vorm van prototypes of is terug te vinden in het ontwerp van een fabriek. De informatie wordt digitaal bewaard op computersystemen, en er wordt over gecommuniceerd via post, e-mail en telefoon. Al deze vormen van informatieopslag en -overdracht kunnen op technische wijze aangegrepen worden, om de gewenste informatie te bemachtigen.

Interceptie van vaste en draadloze telecommunicatie

De voornaamste vormen van telecommunicatie zijn vaste en mobiele telefonie, VOIP-telefonie (bellen 'via internet') en e-mail.

Ongeacht welke vorm van telecommunicatie gebruikt wordt, zodra het telecomnetwerk van een buitenlandse partij gebruikt wordt omdat vanuit of naar het buitenland gebeld wordt, is het onmogelijk de veiligheid van de informatie te garanderen. Voor elke vorm van internet en e-mail gebruik (draadloos en kabelgebonden) is dat sowieso het geval. Het is namelijk niet duidelijk langs welke route de informatie over het internet reist. Als informatie langs buitenlandse 'knooppunten' komt, kan deze dus door inlichtingendiensten onderschept worden. Niet of onvoldoende versleutelde e-mails, documenten of webconferenties kunnen zo onderschept en uitgelezen worden. Er mag vanuit gegaan worden dat door meerdere partijen – structureel en geautomatiseerd – dataverkeer van het internet onderschept, geanalyseerd, opgeslagen en gebruikt wordt voor inlichtingendoeleinden. Het voldoende beveiligen, door middel van encryptie, van vertrouwelijke informatie

vóór verzending over internet, is dan ook van groot belang, evenals de afweging of gebruik van een dergelijk – relatief onveilig – medium wel opportuun is.

Tenslotte zijn er mobiele systemen die gebruik maken van eigen separate opslagservers in het buitenland waar bijvoorbeeld e-mails tijdelijk worden opgeslagen. Vanwege dergelijke centrale opslagsystemen is dit soort apparatuur *per definitie* kwetsbaar voor inlichtingenactiviteiten van buitenlandse diensten. Deze laatstgenoemde vorm van communicatie is extra zorgwekkend doordat juist dit soort systemen door de hogere managementlagen van zowel overheid als bedrijfsleven worden gebruikt: dus door de mensen op sleutelposities als het gaat om beslissingen over standpunten en strategie, en ten aanzien van kennis en toegang tot informatie.

Het is daarnaast niet uit te sluiten dat buitenlandse inlichtingendiensten erin slagen om communicatie die over Nederlandse netwerken loopt te onderscheppen. Inlichtingendiensten zijn immers goed in staat om hard- of software zo te manipuleren dat zij op afstand toegang krijgen tot systemen. Bovendien kunnen ze proberen draadloze en kabelgebonden communicatie ter plaatse te onderscheppen. Communicatie over vaste lijnen, via pda's, smartphones en ook dect telefoons is dan ook *niet per definitie* veilig.

Smartphone
De Amerikaanse president Barack Obama maakt graag gebruik van zijn smartphone. Uit veiligheidsoogpunt werd hem het gebruik van deze telefoon in eerste instantie verboden. Na maanden van discussie werd bekend gemaakt dat Obama deze pda mocht blijven gebruiken, maar dat hij er een veilige door de geheime dienst ontwikkelde *smartphone* bij kreeg waarop hij zijn staatszaken moest afhandelen.

Potentieel interessante datastromen zijn bijvoorbeeld communicatie van en naar ambassades, ministeries als Defensie, Binnenlandse Zaken en Koninkrijksrelaties, Justitie, Economische Zaken en Algemene Zaken en de datastromen van het interdepartementale communicatiesysteem 'de Haagse Ring'. Ook draadloze en kabelgebonden telecommunicatie van en naar NAVO- en EU-vertegenwoordigingen in Nederland vragen in dit verband om aandacht.

Digitale aanvallen

Naast interceptiemogelijkheden biedt het internet ook tal van mogelijkheden om actief aanvallen uit te voeren op gekoppelde computersystemen. Door directe aanvallen, of door via het internet de medewerkers te bereiken, kunnen inlichtingendiensten allerlei informatie verwerven. Via het internet kan een organisatie het doelwit worden van aanvallen door middel van *hacken*, *phishing*,[10] of *trojan horses (trojans)*. *Trojans* bijvoorbeeld zijn programma's die ogenschijnlijk aan oorspronkelijk bonafide boodschappen zijn gehecht en die zich na het openen nestelen in het systeem van de geadresseerde om, na te zijn geactiveerd, in diens pc onopgemerkt informatie te vergaren en te versturen. Vaak krijgen medewerkers in een dergelijke situatie een persoonlijke e-mail met als bijlage een document op hun eigen interessegebied. Ook andere digitale gegevensdragers kunnen dergelijke kwalijke bestanden met zich mee dragen die zichzelf direct activeren zodra ze in een computer worden gestoken. Voorbeelden van zulke gegevensdragers zijn usb-sticks en cd-rom's van onduidelijke origine.

GhostNet
Begin 2009 werd duidelijk dat een NAVO-basis in Nederland doelwit was geworden van een omvangrijk internetspionagenetwerk dat werd aangestuurd met computers die bijna allemaal te herleiden zijn tot Chinees grondgebied. Het spionagenetwerk, GhostNet genoemd, heeft computers bespioneerd in meer dan honderd landen. Via gerichte e-mails met daaraan geïnfecteerde Word- en pdf-bestanden, infecteerden hackers computers van ambassades, ministeries en internationale instellingen. Van de geïnfecteerde computers werd informatie verzameld door documenten te kopiëren en door via webcams en microfoons gesprekken af te luisteren.

Observatie, afluisteren en fysiek stelen

Het via de telefooncentrale tappen van telefoongesprekken is niet de enige manier om gesprekken af te luisteren. Gesprekken zijn bijvoorbeeld ook af te luisteren middels de inzet van afluisterapparatuur of richtmicrofoons. Zo kunnen microfoons in muren of meubilair verborgen worden. Informatie die is opgeslagen in de vorm van documenten of op computerhardware kan natuurlijk ook letterlijk gestolen worden, door in te breken in een kantoor en ze mee te nemen of te kopiëren.

[10] Phishing is het vragen om gevoelige informatie via digitale middelen, die ogenschijnlijk van een betrouwbare partij afkomstig zijn.

Afluisteren
In 2004 is in het kantoor van de VN in Genève afluisterapparatuur aangetroffen in de ruimte waar videoconferenties met het VN-hoofdkwartier in New York plaatshebben. De apparatuur heeft er vermoedelijk vier jaar gezeten. Een jaar eerder werd ook al geavanceerde en uitgebreide afluisterapparatuur aangetroffen in het gebouw van de Europese Raad in Brussel.

8.2 Toegangsroute 2: menselijke toegang

Mensen die direct dan wel indirect toegang hebben tot (informatie over) kernbelangen, zijn een middel om bij het kernbelang te komen. Mensen kunnen gevoelige kennis in hun hoofd hebben, de wachtwoorden kennen die toegang geven tot digitale bestanden, of beschikken over de sleutel van een kluis. In sommige gevallen zijn mensen de enige manier om toegang te krijgen tot informatie, bijvoorbeeld wanneer (data)systemen niet aan het internet verbonden zijn (*stand-alone*-computers of netwerken).

Inlichtingendiensten gaan op verschillende manieren te werk wanneer ze via mensen informatie willen bemachtigen. Soms gaan ze langzaam en voor veel mensen ongemerkt te werk, andere diensten zijn brutaler en kiezen voor een confronterende aanpak. Dit hangt ook af van de urgentie om bepaalde informatie te bemachtigen en van de positie van de toekomstige bron.

Voordat mensen met relevante kennis benaderd worden door een buitenlandse inlichtingendienst moet deze wel van het bestaan van betrokkenen op de hoogte zijn. Dat kan via allerlei manieren. 'Spotplekken' zijn traditioneel gezien beurzen, symposia, conferenties en bepaalde (migranten) verenigingen. In toenemende mate vervult ook internet hierin een rol. Netwerksites als LinkedIn en Facebook zijn belangrijke informatiebronnen voor buitenlandse inlichtingendiensten op zoek naar potentiële agenten en informanten bij Nederlandse bedrijven of overheidsorganisaties.

Ten slotte is het een factor van belang of iemand zich bewust is van het feit dat hij over interessante informatie beschikt. Iemand zonder dit bewustzijn beseft ook minder dat buitenlandse diensten interesse in hem kunnen hebben. Iemand die wel het besef heeft dat hij geheimen met zich meedraagt, is waarschijnlijk meer op z'n hoede.

Waardebewustzijn

Uit dit onderzoek blijkt dat werknemers en bestuurders in relevante organisaties zich lang niet altijd realiseren dat zij over kernbelangen beschikken en dat hun bedrijf, werk of kennis de aandacht heeft van buitenlandse inlichtingendiensten. Mensen kunnen onbewust belangrijke informatie prijsgeven als ze zich niet realiseren dat de informatie waarover ze beschikken interessant is voor een buitenlandse inlichtingendienst. Medewerkers die verantwoordelijk zijn voor de beveiliging van een organisatie, zijn zich vaak wel sterk bewust van de verschillende risico's en potentiële kwetsbaarheden. Echter, zolang niet de hele organisatie een zekere mate van bewustzijn heeft, blijven tal van mogelijke kwetsbaarheden bestaan.

Het inzicht in waardebewustzijn blijkt onder zowel bestuurders als medewerkers sterk te wisselen binnen en tussen de sectoren. De medewerkers met het hoogste bewustzijn hoeven echter niet per se de medewerkers te zijn die het meest direct toegang hebben tot kernbelangen. Het al dan niet aanwezig zijn van besef onder medewerkers van de waarde van de informatie waar ze mee werken, is voor een groot deel afhankelijk van de bedrijfscultuur. Als een medewerker niet op de hoogte is het feit dat de informatie waar hij mee werkt gevoelig is voor spionage, zal hij er ook logischerwijze niet automatisch als beschermenswaardig mee omgaan. Omgekeerd kan het evenzeer zo zijn dat medewerkers een sterker besef kunnen hebben van de waarde van de informatie dan bestuurders, juist omdat ze meer inzicht hebben in de informatie. In een dergelijke situatie zal men op de werkvloer voorzichtiger willen omgaan met informatie dan het beleid van de organisatie voorschrijft of wellicht zelfs opdringt.

Pas als het besef van de waarde van informatie in de complete organisatie is doordrongen, zowel *top-down* als *bottom-up*, kan er een bedrijfscultuur ontstaan waarin te beschermen kennis ook daadwerkelijk als zodanig wordt behandeld door alle lagen van een organisatie.

Onbekend met spionage

Zoals al geconstateerd zijn veel mensen zich onvoldoende bewust van de waarde van de informatie waarover zij beschikken. Mensen overschatten bovendien de veiligheid van technische toepassingen (bijvoorbeeld pda's) die zij in hun dagelijkse werk gebruiken, waardoor hun gebruikersgedrag het kernbelang nóg kwetsbaarder maakt. Hierbij kan gedacht worden aan het uitwisselen van gevoelige informatie over de telefoon of via e-mail. Men laat het gebruikersgemak prevaleren boven de veiligheid van de informatie, met als gevolg dat bijvoorbeeld een op een congres verkregen usb-stick meteen in de computer op het werk wordt gestoken.

Ook van de manieren waarop inlichtingendiensten mensen inzetten om aan gevoelige informatie te komen, is niet iedereen zich bewust. Er lijkt geen noodzaak te bestaan voor mensen om terughoudend zijn met het in detail bespreken van onderzoeksresultaten met een collega-onderzoeker, die al jarenlang dezelfde symposia bezoekt. Weinigen zullen er bij stil staan dat deze immer geïnteresseerde, vriendelijke buitenlandse collega wel eens een inlichtingenofficier zou kunnen zijn. Maar men kan ook verleid worden tot het onbewust weggeven van informatie, via *phishing*, of tijdens een gesprek in de kroeg, na afloop van een vergadering.

Spionage via e-mail
Een aantal rijksambtenaren is geabonneerd op een nieuwsservice van de Europese Unie. Als zij een e-mail met bijlage ontvangen die afkomstig lijkt te zijn van de nieuwsservice, wordt dit bericht zonder aarzelen geopend. In een recent geval bleek dat de e-mail van een derde partij afkomstig was en een *trojan* bevatte. Blijkbaar was de verzender op de hoogte van de e-mailadressen van de abonnees van de nieuwsservice en heeft hij deze gebruikt bij het versturen van de *trojan*.

Methodes van inlichtingendiensten

Cultivering (social engineering)
Het verkrijgen van informatie van personen begint meestal met het langzaam winnen van vertrouwen, vaak in de vorm van een individuele vriendschap, waarbij de attenties voornamelijk van de inlichtingenzijde komen en waarbij haast als vanzelfsprekend op een gegeven moment tegenprestaties dienen te worden verleend. Het handelen van de inlichtingenofficier bestaat daarbij uit een aantal logische stappen in een zorgvuldig gefaseerd omgangsplan.

Chantage
Chantage is één van de brutalere, en minder vaak gebruikte, manieren om aan informatie te komen. Een voorbeeld van een klassieke methode is het in een chantabele positie manoeuvreren van een persoon die een interessante positie bekleedt, bijvoorbeeld door amoureuze escapades uit te lokken. Wanneer eenmaal chantabele feiten voorhanden zijn, wordt gevraagd mee te werken met de buitenlandse inlichtingendienst.

Overigens moeten zowel mannen als vrouwen behoedzaam zijn voor de charmes van buitenlandse inlichtingenofficieren en hun agenten. Iedereen kan doelwit worden van amoureuze cultiveringspogingen.

Daten met spionnen
Tijdens een officieel bezoek aan het buitenland bracht een Britse hoge ambtenaar de nacht door met een lokale dame, waarna zijn *BlackBerry* verdwenen bleek te zijn. Hoewel het apparaat waarschijnlijk geen geheime gegevens bevatte, bestond het risico dat met het toestel werd ingebroken op de server van de ambtswoning van de premier.

Soms begint chantage net als bij cultivering op een onschuldige wijze, de eerste keren wordt slechts om een klein beetje informatie gevraagd, of om een klein, ogenschijnlijk onschuldig, detail. Nadat gedurende een periode van *nurturing* een vertrouwensband is opgebouwd, wordt uiteindelijk om informatie gevraagd die weliswaar niet geheim is, maar wel net over de grens van onschuldig ligt. Als die grens eenmaal is gepasseerd, kan iemand het gevoel krijgen niet meer terug te kunnen en is een dergelijk persoon langzaam en doelbewust in de val van een chantabele positie gelokt. Melding maken bij de bedrijfsbeveiliging is immers niet meer erg aanlokkelijk, omdat de (interne) regels reeds zijn overschreden. Door als inlichtingenofficier zorgvuldig door te bouwen aan het steeds lastiger parket waarin een persoon zich gaat bevinden, weet hij deze uiteindelijk in een positie te manoeuvreren, waarin hij ronduit om geheime gegevens kan vragen.

Bewust lekken
Informatie kan uiteraard ook bewust door werknemers worden prijsgegeven. Uiteenlopende motieven als geld, persoonlijk gewin, erkenning/ego, persoonlijke overtuiging, of gevoelens van onvrede of wraak kunnen hier een rol bij spelen. Inlichtingenofficieren spelen, zeker als er achtergrondinformatie over iemand beschikbaar is, bewust in op dergelijke gevoelens, om ze uiteindelijk voor hun eigen doeleinden aan te wenden.

Menselijke toegang tot bestanden
De AIVD heeft in 2008 geconstateerd dat de Marokkaanse inlichtingendienst politiefunctionarissen heeft ingezet om toegang te krijgen tot gesloten gegevensbestanden. Op aangeven van de AIVD is naar aanleiding van deze kwestie een aantal in Nederland gestationeerde Marokkaanse diplomaten teruggeroepen naar Marokko. Tevens zijn betrokken politiefunctionarissen uit hun functie ontheven en is er een strafrechtelijk onderzoek gestart. Deze zaak vormde de aanleiding om het bewustzijn over spionagerisico's binnen de Nederlandse politiesector te verhogen.

8.3 De mens als centraal punt

In bovenstaande paragrafen is beschreven hoe de factor 'techniek' en de factor 'mens' invloed hebben op de toegankelijkheid en daarmee ook de kwetsbaarheid van kernbelangen, ongeacht de sector waarin deze te vinden zijn. Omdat veel technische hulpmiddelen zoals laptops, thuiswerkplekken en pda's vaak onvoldoende beveiligd zijn om bescherming te bieden tegen de activiteiten van inlichtingendiensten, valt of staat de beveiliging van kernbelangen ook met het gebruikersgedrag van de mens. Medewerkers moeten zich realiseren dat ze geen gevoelige informatie kunnen uitwisselen over onveilige systemen. Het menselijke gedrag wordt echter niet uitsluitend bepaald door zijn besef van de waarde van de informatie waar hij over beschikt. Gebruiksvriendelijkheid, snelheid en gemak zijn ook van invloed op de mate waarin een mens zich houdt aan afspraken die ten behoeve van de veiligheid van een kernbelang zijn gemaakt.

Het nemen van bepaalde veiligheidsmaatregelen en het zich ook daadwerkelijk conformeren aan deze maatregelen zijn bepalende factoren voor het succes van elk veiligheidsbeleid. Uit het onderzoek zijn verschillende ontwikkelingen naar voren gekomen die de kwetsbaarheid van een kernbelang kunnen vergroten als organisaties zich niet bewust zijn van de risico's die aan deze ontwikkelingen zijn verbonden.

8.4 Ontwikkeling 1: beleid

De eerste belangrijke factor is (de actualiteit en volledigheid aan) veiligheidsgerelateerd beleid. Beleid kan zich richten op bijvoorbeeld informatiebeveiliging bij de overheid of op de *clean desk policy* bij een bedrijf. Ook keuzes op tal van (beleids)terreinen die niet direct met beveiliging te maken hebben, kunnen de kansen van inlichtingendiensten beïnvloeden, zoals bijvoorbeeld het uitbesteden van onderhoud aan ICT-systemen.

De gevolgen kunnen zich laten gelden in de vorm van economische schade tot aan aantasting van de fysieke, of zelfs de territoriale integriteit van de Nederlandse staat. Dergelijke activiteiten benutten kwetsbaarheden van Nederlands beleid. Hoewel dus Nederlandse belangen geschaad kunnen worden, wordt op dit moment bij beleidsformulering vaak heel weinig rekening gehouden met mogelijke veiligheidsimplicaties. Veel beleid is op dit moment niet ingericht op het voorkomen van dreiging tegen de nationale veiligheid, of werkt deze zelfs onbewust in de hand. Het gaat hierbij ondermeer om beleid ten aanzien van de opleiding van buitenlandse studenten en de liberalisering en privatisering van bedrijven in enkele vitale sectoren.

Prioritering van beveiliging

Gezien de vermogens van inlichtingendiensten om zwakke plekken in beveiliging te vinden en te benutten, is een organisatiebreed, structureel gehandhaafd en breed gedragen beveiligingsbeleid de enige manier om kernbelangen afdoende te beschermen. Om deze benodigde maatregelen te realiseren moet de interne beveiliging ook op een voldoende hoog bestuurlijk niveau geagendeerd zijn. De prioriteit die aan (informatie)beveiliging gegeven wordt verschilt erg tussen organisaties. De positie van de beveiligingsverantwoordelijke afdeling binnen een organisatie is hiervan een voorbeeld. Vaker wel dan niet lijkt beveiliging een sluitpost op de begroting te zijn, met slechts een beperkte mogelijkheid om op afdoende hoog bestuurlijk niveau aandachtspunten aan te kaarten. In bredere zin kan dit tot gevolg hebben dat beveiliging niet alleen onvoldoende middelen, maar met name ook onvoldoende draagvlak heeft binnen de organisatie.

Bewuste aandacht van de hogere bestuurslagen is zowel vanuit het oogpunt van de te nemen bedrijfsbrede maatregelen, als vanuit het oogpunt van beeldvorming binnen de organisatie van belang. Hiertoe is het noodzakelijk dat een beveiligingsverantwoordelijke afdeling binnen een organisatie over voldoende slagkracht en bevoegdheden beschikt. Men kan echter ook denken aan beleid waarbij bepaalde processen of werkstromen standaard dienen te worden geaccordeerd door deze afdeling. Alleen als het belang van beveiligingsbewustzijn nadrukkelijk wordt uitgedragen door bestuurders op het hoogste niveau, zal het bewustzijn in de rest van de organisatie doordringen en toenemen.

Opleiding en onderzoek

De wetenschappelijke wereld is op een bijzondere manier kwetsbaar. Aan de ene kant vormt vrije uitwisseling van onderzoeksresultaten en informatie de basis van wetenschap, aan de andere kant vormt wetenschappelijk onderzoek vaak de voorloper van kennis met economische en/of strategische waarde. Het punt waarop kennis van wetenschappelijk open, naar waardevol, of wellicht zelfs geheim, gaat is niet altijd goed vast te stellen. Ook het scheidsvlak tussen normale informatie- en kennisuitwisseling ten bate van de wetenschap enerzijds en heimelijke informatievergaring ten bate van economisch of strategisch gewin van een ander land anderzijds, is niet altijd eenduidig en eenvoudig te bepalen.

Juist door de inherente openheid van wetenschap is wetenschappelijke spionage relatief eenvoudig. De open cultuur van universiteiten en de aanwezigheid van veel buitenlandse studenten en onderzoekers maakt het voor inlichtingendiensten relatief eenvoudig om relevante inlichtingen te verzamelen. Bovendien blijkt in de praktijk gevoelige informatie slecht afgeschermd, en zijn de faculteiten zeer toegankelijk. Er heerst een cultuur van open

kamerdeuren, open kasten en relatief eenvoudig toegankelijke computernetwerken.

De universiteiten vormen daarnaast ook een voorportaal voor nog verdergaande activiteiten. Ook buitenlandse studenten krijgen via de universiteit vaak gemakkelijk stageplaatsen bij bedrijven, en niet zelden bij bedrijven die beschikken over kernbelangen. Bij technische studies zijn dit bijvoorbeeld plaatsen op r&d-afdelingen.

Een andere belangrijke bijdrage van kennisinstellingen is dat zij, behalve kennis, ook kenniswerkers voortbrengen. Er studeren bijvoorbeeld jaarlijks ongeveer een miljoen Chinese ingenieurs af. Dat gebeurt niet alleen aan opleidingen in China, maar ook aan buitenlandse (top)universiteiten waaronder Nederlandse. Wetenschap heeft een traditie van vrije uitwisseling van kennis en mensen, en landen als China maken daar dankbaar gebruik van. China probeert immers op zo kort mogelijke termijn zijn internationale concurrentiepositie te verbeteren. Nederland is in dat opzicht een interessante opleidingsplek voor studenten uit China en andere landen. Het overgrote deel van deze studenten keert na hun opleiding terug naar China en hun land van herkomst met de hier opgedane kennis en inzichten.

Het huidige Nederlandse onderwijsbeleid bevordert kennis migratie en het aantrekken van buitenlandse studenten nadrukkelijk. Begrijpelijk want buitenlandse studenten leveren tijdens hun verblijf in Nederland natuurlijk een bijdrage aan de ontwikkeling van het Nederlandse kennispotentieel, en daarmee uiteindelijk zelfs aan de economische ontwikkeling van Nederland. Bovendien geldt dat niet alle wetenschappelijke kennismigratie onwenselijk is: zo wordt in het kader van ontwikkelingssamenwerking kennismigratie gestimuleerd die geen schade toebrengt aan het economisch welzijn. Nadeel is echter dat studenten en promovendi zich ten behoeve van hun land van herkomst ook met heimelijke intenties kunnen toeleggen op het verkrijgen van inzicht in onderzoekstechnieken, toepassingen en wetenschappelijke inzichten die ontwikkeld worden op Nederlandse universiteiten en grotendeels gefinancierd worden door de Nederlandse overheid. Innovatieve kennis die ten goede zou moeten komen aan het Nederlandse economisch welzijn kan zo weglekken naar onze concurrenten.

Privatisering en liberalisering strategische infrastructuur

Het is binnen Europa van groot belang economische grenzen open te stellen, en marktpartijen de kans te bieden eerlijk te concurreren op de Europese markt. Een onderdeel van eerlijke (Europese) concurrentie is ook het terugbrengen van de rol van de staat in de markt. In het geval van enkele belangrijke onderdelen van de vitale infrastructuur is het echter de vraag of het wenselijk het is de bedrijfstak te privatiseren en liberaliseren. Dit kan in potentie namelijk nadelige consequenties hebben voor de Nederlandse nationale veiligheid. Private ondernemingen kunnen immers overgenomen worden door niet-Nederlandse (of zelfs niet-Europese) bedrijven. De infrastructuur komt op dat moment in handen van een partij die geen binding heeft met Nederland. Dit terwijl de keuzes over bijvoorbeeld onderhoud of gebruik van deze infrastructuur van grote invloed kunnen zijn op het functioneren van de Nederlandse maatschappij. Tegelijk is echter, zeker in het geval van een niet-Europese overname, de invloed die door de Nederlandse regering uitgeoefend kan worden op die keuzes gering.

Een voorbeeld hiervan is dat bandbreedtes, zendmasten of andere onderdelen van het telecomnetwerk in buitenlandse handen komen. Hiermee krijgen deze partijen immers meer toegang tot informatie over het netwerk zelf, alsmede tot de data die er overheen verzonden wordt. Andere voorbeelden zijn te vinden in de energiesector en in de transportsector (luchthavens, zeehavens). Nederland heeft één van de meest geliberaliseerde energiesectoren van Europa. Andere landen denken op dit punt meer strategisch en houden meer rekening met de eigen nationale veiligheid.

Nederland is traditioneel een open handelsnatie die gericht is op zo min mogelijk protectionisme. Dit heeft veel welvaart gebracht. Keerzijde is wel dat Nederland in vergelijking met andere landen weinig besef heeft van en beleid maakt rond de bescherming van strategische industrieën en strategische kennis voor nu en in de toekomst.[11] Andere landen hebben dat wel, in meer of mindere mate. Daar vindt bijvoorbeeld een toets plaats voordat buitenlandse investeerders een belang kunnen nemen in een bedrijf. Ook heeft Nederland strategische kennisorganisaties (deels) geprivatiseerd. Andere landen beschikken nog wel over dergelijke publieke onderzoeksinstituten.

Dual use

Een extra aandachtspunt is het feit dat veel technologieën hier in Nederland worden ontwikkeld met als gebruikersdoeleinde de consument, terwijl dezelfde technologie kan worden 'misbruikt' voor strategisch-militaire doeleinden (bijv. *self healing materials*, *coatings* of medische ontwikkelingen zoals scans). Deze toepassingen van technologieën met consumentendoeleinden worden minder goed beschermd dan technologieën voor strategisch-militaire doeleinden. In Nederland is men zich meestal niet bewwust

[11] In een buitenlands onderzoeksrapport (*'Laws and Policies Regulating Foreign Investment in 10 Countries'*, GAO, februari 2008) wordt Nederland vermeld als één van de weinige landen die geen beleidskaders hebben die moeten borgen dat strategische economische kennis en bedrijven voor Nederland behouden blijven.

van dit mogelijk 'misbruik' van de technologie. In sommige andere landen worden dit soort zogenaamde *dual-use*-technologieën wegens hun militaire toepassingsmogelijkheden onder het motto van nationale veiligheid afgeschermd van de buitenwereld.

8.5 Ontwikkeling 2: uitbesteding & *offshoring*

De tweede ontwikkeling die aandacht verdient is de groei van (grootschalige) inkoop van technische apparatuur uit het buitenland, het uitbesteden aan derden en het *offshoren* (uitbesteden naar het buitenland) van activiteiten op verschillende gebieden (ICT-onderhoud maar ook dataopslag en data-entry, personeelsadministratie of factureren). Als een externe partij zo dicht bij informatie van de eigen organisatie kan komen, zeker als die externe partij zich in het buitenland bevindt waar ook nog andere waarborgen (wet- en regelgeving) gelden, is het moeilijk afdoende controle te houden op de bescherming van de informatie.

Hard- & software

Bedrijven en instellingen maken veel gebruik van hard- en software die in het buitenland is ontwikkeld en/of vanuit het buitenland wordt onderhouden. Veelvuldig worden computers en andere apparatuur uit het buitenland aangekocht, omdat een buitenlands bedrijf de aanbestedingsprocedure wint. Het draaiend houden van complexe hard- en software wordt bovendien regelmatig overgelaten aan de specialisten van het ontwerpende bedrijf, of een gespecialiseerde andere externe partij. Juist door het specialisme dat vereist is voor productie en onderhoud van deze producten is het moeilijk om als organisatie zelf zicht te houden op wat er exact gebeurt in en op de eigen systemen, en wie toegang heeft tot welke informatie. Buitenlandse onderhoudsbedrijven kunnen (nauwe) banden onderhouden met hun overheid en inlichtingendiensten. Mogelijkerwijs zijn er onderlinge afspraken gemaakt over het leveren van informatie. Op deze wijze kunnen kernbelangen in handen komen van een ander land.

Bij de aankoop van buitenlandse hard- en software moet dus rekening gehouden worden met beveiligingsrisico's. Het is voorstelbaar dat inlichtingendiensten bedrijven uit eigen land achterdeurtjes laten inbouwen waardoor zijzelf ongezien kunnen binnendringen.

Servers

Voor (back-up)servers die zich in het buitenland bevinden, geldt hetzelfde als voor software die vanuit het buitenland wordt beheerd. Partijen in Nederland hebben vaak geen zicht op wie er toegang heeft tot de gegevens die op deze servers staan, als men zich al bewust is van het feit dat eigen vertrouwelijke gegevens in het buitenland zijn opgeslagen.

Bij spionage via servers is het lastig om vast te stellen of gegevens gecompromitteerd worden. Bij het leeghalen van een server hoeft geen 'vermomd' dataverkeer van het netwerk naar het buitenland verstuurd te worden, zoals bij heimelijk geïnstalleerde software vaak wel het geval is. Inlichtingendiensten moeten dan ook in staat geacht worden ongemerkt de volledige inhoud van een computerserver op hun grondgebied te kopiëren, zeker als deze in een lokaal datacentrum staat. Als een computerserver bijvoorbeeld binnen het regionale hoofdkantoor van een multinational staat, wordt die opgave ingewikkelder.

Een ontwikkeling die extra gevolgen kan hebben, is het toenemende aanbod van internetdiensten met online geheugencapaciteit. Online geheugencapaciteit bevindt zich uiteindelijk ook ergens fysiek op servers die op het grondgebied van een land staan. Automatische back-up/synchronisatieprogramma's voor pc's, laptops, telefoons en pda's vallen hieronder, net als (gratis) online e-mailprogramma's en applicaties waarmee online door meerdere mensen tegelijk aan documenten gewerkt kan worden. Ontwikkelingen zoals *cloud computing* (het massaal verwerken van data via internet, in plaats van fysiek op de eigen computer) maken aandacht voor de potentiële kwetsbaarheid van dit soort applicaties alleen maar belangrijker.

Ondersteunende dienstverlening

Taken als het factureren van klanten, het beheer van de personele administratie, het vertalen van teksten, het omzetten van documenten naar digitale (doorzoekbare) teksten of data-entry in databases zijn allemaal vormen van activiteiten die door organisaties grotendeels uitbesteed (kunnen) worden. Vaak wordt niet stil gestaan bij het feit dat dergelijke dienstverleners daarmee toegang krijgen tot informatie van de organisatie. Het is bovendien relatief eenvoudig om via dergelijke dienstverleners, waar wellicht niet dezelfde strenge veiligheidsregimes gelden als bij het aanleverende bedrijf, spionage te plegen. Ook hier geldt weer dat als het betreffende bedrijf in het buitenland gevestigd is, in ieder geval de controlemogelijkheden op de toegang tot de informatie door de eigenaar van deze informatie beperkt zijn.

Daarnaast moet ook nog rekening gehouden worden met de ketenwerking die kan optreden. Niet alleen de partij waaraan werkzaamheden uitbesteed worden is van belang, ook dat bedrijf kan zelf (delen van) werkzaamheden uitbesteden aan onderaannemers (waaronder externe partijen). Op deze manier ontstaat een keten van bedrijven die allemaal op een of andere manier toegang tot de informatie krijgen. Om informatie goed te beveiligen moeten duidelijke afspraken bestaan en moeten alle bedrijven uit deze

keten bekend en betrouwbaar bevonden zijn. Om hierover uitspraken te kunnen doen, is niet alleen kennis vereist over de directe partij waaraan uitbesteed wordt, maar ook over diens ondersteunende organisaties.

Rol van inlichtingendiensten

In alle bovenstaande voorbeelden van uitbesteding is het goed stil te staan bij het verschil tussen de activiteiten van inlichtingendiensten en de bedreigingen die uitgaan van bedrijfsspionage. Hoewel in beide gevallen geprobeerd wordt gevoelige informatie te bemachtigen, is in het geval van economische spionage een inlichtingendienst de spionerende partij. Daarmee is de inzet van een breed scala aan inlichtingenmiddelen voorstelbaar. Zelfs gerenommeerde bedrijven, die een naam hoog te houden hebben op het gebied van beveiliging tegen bedrijfsspionage, kunnen of willen niet altijd bescherming bieden tegen de activiteiten van een inlichtingendienst. Het kan bijvoorbeeld zo zijn dat een bedrijf is opgericht door een inlichtingendienst, met als doel op deze wijze aan informatie te komen. Daarnaast kan een staat op een bedrijf, dat binnen zijn grenzen gevestigd is, druk uitoefenen om mee te werken. Het verkrijgen van vergunningen, aanklachten wegens aantasting van nationale veiligheid, of het mislopen van lucratieve overheidsorders zijn instrumenten waarvoor bedrijven buitengewoon gevoelig kunnen zijn. Ten slotte kan het zo zijn dat de overheid in kwestie eigenaar is, of in ieder geval ongehinderde toegang heeft tot alle infrastructuur rondom een bedrijfspand dat op zijn grondgebied staat. Post, digitale datastromen en telefonie zijn alle te onderscheppen, zonder dat het bedrijf in kwestie hiervan weet hoeft te hebben. Ook zo kan informatie dus relatief eenvoudig gecompromitteerd worden. Kortom: het is goed mogelijk dat (in de regel betrouwbare) bedrijven die fysiek in het buitenland gevestigd zijn, een 'uitnodiging' tot samenwerken met hun nationale inlichtingendienst niet zo gemakkelijk af kunnen slaan.

8.6 Ontwikkeling 3: verwevenheid van netwerken

Een andere invloedrijke factor voor de kwetsbaarheid is het feit dat, door de voortschrijdende ontwikkelingen van internet en ICT-toepassingen, steeds meer netwerken, systemen en bestanden aan elkaar en aan het internet gekoppeld raken. Dit heeft grote praktische voordelen in de dagelijkse bedrijfsvoering, maar creëert wel een steeds groter netwerk van mogelijke 'toegangspunten' voor buitenlandse inlichtingendiensten. Een gerelateerde kwetsbaarheid is de doorontwikkeling van datamining.[12] De mogelijkheid om uiteenlopende databestanden te verzamelen en te combineren tot één gevoelig totaalbestand stelt extra eisen aan informatiebeveiliging.

Verwevenheid van netwerken

In het huidige digitale tijdperk treedt een extra complicatie op in de beveiliging van informatie. Omdat steeds meer systemen en bestanden gekoppeld zijn, gaat steeds nadrukkelijker het 'zwakste schakel'- principe gelden. Als een serie netwerken of systemen gekoppeld is, wordt het mogelijk binnendoor van systeem naar systeem te *hacken*. De slechtst beveiligde schakel in de keten van gekoppelde systemen vormt dan een logische ingang tot het geheel aan netwerken. Omdat met toenemende vertakkingen steeds minder helder wordt welke bestanden inmiddels (indirect) aan elkaar verbonden zijn, neemt het risico op een zwak punt in de keten toe.

Datamining

Met een verdergaande koppeling van steeds meer informatie aan het internet wordt Nederland kwetsbaarder voor *datamining*, zeker gezien de toenemende technische mogelijkheden van volledig geautomatiseerde *datamining*. Informatie is ook via steeds meer commerciële partijen beschikbaar (marketingbureaus, verzekeraars, kredietwaardigheidregistratiebureaus). Met *datamining* kan strategische informatie gehaald worden uit verschillende databanken gevuld met relatief onbruikbare stukjes deelinformatie. Voor *datamining* geldt nadrukkelijk dat het geheel aan informatie groter is dan de som der delen. Beperkte of geanonimiseerde bestanden met informatie worden zo meer gevoelig voor spionage.

[12] Datamining is het extraheren van gestructureerde informatie uit een groter geheel van ongekoppelde informatie.

Weerbaarheid

Beperkt beschermd

Beveiligingsbewustzijn

Kwetsbaar

9. Conclusies

Spionage door buitenlandse inlichtingendiensten brengt Nederland schade toe. De exacte omvang van de schade kan niet op basis van dit onderzoek worden vastgesteld. Wel is getracht langs deze weg beter inzicht te krijgen in de kernbelangen en kwetsbaarheden binnen de aandachtsgebieden economisch welzijn en technisch-wetenschappelijk potentieel, openbaar bestuur en vitale infrastructuur.
Het begrip kernbelang is daarbij gedefinieerd als informatie, waarvan kennisname de nationale veiligheid aantast en waarvan verondersteld kan worden dat buitenlandse inlichtingendiensten/overheden er belang bij hebben deze te bezitten.

In het voorgaande gedeelte zijn de binnen de sectoren geïdentificeerde kernbelangen gerapporteerd en de kwetsbaarheden rond deze kernbelangen geschetst. Uit dit geheel komt een aantal conclusies naar voren. In dit hoofdstuk worden kort de belangrijkste conclusies samengevat en enkele daaruit voortvloeiende (beleids)aanbevelingen behandeld.

9.1 Awareness als overkoepelend thema

De voornaamste conclusie die uit het onderzoek getrokken kan worden is dat de *awareness* in de betrokken sectoren ten aanzien van spionage vaak laag is. Het beperkte bewustzijn wordt zichtbaar op drie niveaus.
De weerbaarheid van een organisatie tegen spionage wordt bepaald door het bewustzijn van die organisatie dat zij beschikt over een of meerdere kernbelang(en) en het bewustzijn dat andere partijen daarin interesse kunnen hebben. Dat bewustzijn wordt zichtbaar op drie niveaus:

- *Waardebewustzijn*: organisaties en individuele medewerkers realiseren zich soms niet of onvoldoende wat de waarde is -ook voor anderen- van de informatie waarover zij beschikken of waartoe zij toegang kunnen verschaffen;
- *Beveiligingsbewustzijn*: beveiliging en veiligheid van kernbelangen hebben niet altijd voldoende aandacht binnen organisaties en in het beleid zijn andere overwegingen vaak prioritair;
- *Belangenafweging*: organisatiebelangen en/of overheidsbelangen op korte termijn prevaleren (vaak) over de belangen op lange termijn. Het weglekken naar het buitenland van strategische kennis of bedrijvigheid die relevant is voor de Nederlandse nationale veiligheid op lange termijn krijgt onvoldoende aandacht.

9.2 Kernbelangen en kwetsbaarheden

In alle sectoren is sprake van kernbelangen
Uit het onderzoek blijkt dat in alle genoemde sectoren sprake is van kernbelangen. Deze zijn grofweg te verdelen in de categorieën:

- Datasets & Blauwdrukken: in organisaties aanwezige gegevensbestanden, ontwerpen en bouwtekeningen;
- Standpunten & Strategie: bijvoorbeeld beleidsstandpunten, langjarige visies en onderhandelingsstrategieën;
- Opkomende kernbelangen & Infrastructuur: bijvoorbeeld wetenschappelijke innovaties die in de toekomst in concrete toepassingen winstgevend kunnen worden.

De belangrijkste factoren die de kwetsbaarheid van een kernbelang voor spionage bepalen zijn de factoren 'techniek' en 'mens'.
Inlichtingendiensten proberen informatie te verkrijgen via de inzet van technische middelen zoals *hacken*, tappen of afluisteren of via mensen die (indirect) toegang hebben tot deze informatie. Kwetsbaarheden op deze twee terreinen worden niet allemaal onderkend door de organisaties die hebben meegewerkt aan dit onderzoek. Wanneer een kernbelang niet als zodanig wordt onderkend, krijgen de kwetsbaarheden voor spionage geen aandacht. Uit het onderzoek kan een aantal specifieke conclusies worden getrokken ten aanzien van de waargenomen kwetsbaarheden. Ter illustratie volgen er enkele, waarbij moet worden aangetekend dat deze opsomming niet uitputtend is.

Kwetsbaarheid: onbekendheid van de waarde van informatie
Uit het onderzoek blijkt dat instellingen en bedrijven zich niet altijd bewust zijn van het feit dat zij over informatie of kennis beschikken die van waarde is voor inlichtingendiensten. Dit komt vooral omdat de focus ligt op het realiseren van hoogwaardige resultaten, niet op bescherming van informatie tegen onvermoede dreigingen. Kennis over spionage is beperkt. Spionage lijkt iets te zijn uit de tijd van de Koude Oorlog. Voor zover er bij stil wordt gestaan, is de inschatting dat spionage alleen de nationale veiligheid bedreigt als het leidt tot ernstige verstoring van onderdelen van de vitale infrastructuur (bijvoorbeeld energievoorziening of betalingsverkeer) of gericht is op militaire toepassingen. De meeste respondenten weten weinig over de mate waarin spionage in Nederland voorkomt, hoe het in de praktijk werkt en welke informatie voor buitenlandse inlichtingendiensten belangrijk is. Mensen zijn zich niet altijd bewust wat de consequenties van spionage kunnen zijn voor de eigen organisatie en de Nederlandse nationale veiligheid. Het ontbreken van een reëel beeld van wat spionage inhoudt, hoe het zich manifesteert en wat

het betekent voor Nederland, maakt Nederland als geheel kwetsbaar.

Kwetsbaarheid: kernbelangen zijn beperkt beschermd
De kwetsbaarheid van een kernbelang wordt onder andere bepaald door de mate van bescherming dat een kernbelang geniet: hoe goed is het kernbelang beschermd? Een aantal in dit rapport genoemde kernbelangen zijn niet, of niet goed genoeg beschermd. Met name kernbelangen die door de sector zelf niet voldoende als kernbelang worden onderkend, kennen een hoge kwetsbaarheid. Kernbelangen die ook direct gevoelig zijn voor bedrijfsspionage of die anderszins aantrekkelijk zijn voor criminelen, zijn doorgaans beter beschermd dan kernbelangen die dat niet zijn. Dit wil echter niet zeggen dat de bescherming dan ook afdoende is tegen spionage door inlichtingendiensten.

Kwetsbaarheid: onwetendheid medewerkers
Onwetendheid van individuele medewerkers over de doelen en werkwijzen van inlichtingendiensten maakt organisaties als geheel kwetsbaar voor spionage. Individuele medewerkers kunnen zonder het te weten waardevolle informatie prijs geven. Er kan echter ook chantage of manipulatie van medewerkers worden toegepast, waardoor dergelijke informatie in verkeerde handen geraakt. Medewerkers die zich niet van de bestaande risico's bewust zijn, zijn voor dergelijke praktijken kwetsbaarder dan degenen die wel op de hoogte zijn.

Kwetsbaarheid: interceptie telecommunicatie
Een van de voornaamste technische kwetsbaarheden is de mogelijkheid van data-interceptie. Dit geldt voor draadloze en kabelgebonden telefonie en internet. Er wordt op grote schaal gebruik gemaakt van uiterst onveilige communicatiesystemen terwijl van verschillende landen inlichtingenactiviteiten op het gebied van telecommunicatie geconstateerd worden. Telecom is daarom niet alleen onderzocht als (vitale) sector, maar ook als een kwetsbaarheid, vanwege de instrumentele waarde voor spionage. Door zich toegang te verschaffen tot de telecomsector kunnen diensten namelijk toegang verkrijgen tot nagenoeg alle andere kernbelangen. Kwetsbaarheid van de telecomsector verhoogt de kwetsbaarheid voor alle kernbelangen althans voor zover informatie wordt opgeslagen op systemen verbonden aan, danwel verzonden wordt over, telecommunicatienetwerken.

Kwetsbaarheid: verwevenheid computersystemen
De verwevenheid van computersystemen en het koppelen van databanken maakt gegevens op die systemen kwetsbaar; koppeling met minder of niet-beschermde systemen zorgt voor toegangmogelijkheden via de slechtst beveiligde schakel in dit systeem. Dit geldt met name bij gekoppelde systemen waar meer partijen bij betrokken zijn; de zwakste schakel kan de toegang zijn tot álle verbonden systemen, netwerken en databases. Wanneer deze zwakste schakel zich buiten het zicht van de eigenaar van een kernbelang bevindt, is de kwetsbaarheid van het kernbelang groter dan de eigenaar zou vermoeden op grond van de beveiliging op het eigen systeem.

De ruime beschikbaarheid van fragmenten van informatie verhoogt ook de kwetsbaarheid van een kernbelang. Het gaat daarbij vaak ook om niet-geheime informatie die te verkrijgen is via commerciële partijen, overheden of (netwerk)sites op het internet. Door deze losse datasets te koppelen en met behulp van computers te analyseren, ontstaan verrijkte datasets. De informatie die hieruit is af te leiden, is vele malen rijker dan de som der delen en kan de kwetsbaarheid van een kernbelang substantieel verhogen.

Kwetsbaarheid: uitbesteden
Het uitbesteden en *offshoren* van activiteiten als systeem- en serverbeheer, *datawarehousing* en gegevensverwerking brengt spionagerisico met zich mee. Het zicht op welke externe partijen toegang hebben tot de systemen en gegevens wordt door uitbesteden belemmerd. Hetzelfde geldt voor het inhuren van extern personeel indien aan deze medewerkers niet dezelfde veiligheidseisen worden gesteld als aan het eigen personeel. Bij uitbesteden moet bovendien rekening gehouden worden met de ketenwerking die kan optreden. Niet alleen de partij waaraan direct uitbesteed wordt, is van belang, ook diens aanleverende of ondersteunende partijen zijn dat. Als de primaire partij waaraan een organisatie bijvoorbeeld personeelsbestanden toevertrouwt wel betrouwbaar is, maar de partij die bij hen ICT-onderhoud uitvoert dat niet is, kunnen gegevens alsnog gecompromitteerd raken.

Kwetsbaarheid: beleid
Met gericht beleid, in zowel de private als de publieke sectoren, kan de weerbaarheid tegen spionage worden verhoogd en kunnen Nederlandse kernbelangen worden beveiligd. De kwaliteit van beleid en beleidsimplementaties beïnvloedt de kwetsbaarheid van kernbelangen voor inlichtingenactiviteiten in belangrijke mate. Ook overheidsbeleid dat is opgesteld om niet-veiligheidsgerelateerde belangen te behartigen, kan van invloed zijn op de kwetsbaarheid van kernbelangen. Privatisering, liberalisering en antiprotectionismebeleid bevorderen een openmarktwerking en daarmee de Nederlandse welvaart. Vrijemarktwerking kan er echter ook toe leiden dat strategische onderdelen van de Nederlandse economie door buitenlandse (overheids) bedrijven worden overgenomen. Als ondernemingen, die werken met hoogwaardige technologische toepassingen, voortkomend uit met publieke middelen gefinancierd fundamenteel onderzoek, opgekocht worden door buitenlandse partijen, vloeien de toegepaste kennis en de bijbehorende economische waarde, naar het buitenland. Zeker in het geval het onderdelen van de vitale infrastructuur betreft, kan dat raken aan de nationale veiligheid.

Zowel vanuit dit perspectief als tegen de achtergrond van de economische impact moet in dergelijke trajecten rekening worden gehouden met spionageactiviteiten. Na een buitenlandse overname ontstaat vervolgens een situatie waarin de kwetsbaarheid voor spionage is verhoogd. De overgenomen onderdelen van de Nederlandse economie zijn dan immers (deels) aan het zicht en de controle van de Nederlandse overheid onttrokken.

Belangenafweging

Waardebewustzijn

Voorlichting

Cultuurverandering

10. Aanbevelingen

De resultaten van het onderzoek leiden tot drie algemene aanbevelingen met als doel de Nederlandse kernbelangen beter te beschermen. Bij de algemene aanbevelingen wordt met enkele (niet-limitatieve) voorbeelden geïllustreerd hoe die aanbeveling in praktijk vorm kan krijgen. Er is bewust voor gekozen te volstaan met enkele voorbeelden en suggesties om te voorkomen dat de onderzoekers op de stoel van de beleidsmakers gaan zitten. De verdere uitwerking van de aanbevelingen in acties en de toedeling hiervan aan actiehouders wordt nadrukkelijk aan de belanghebbende departementen, instellingen en bedrijven overgelaten. De hieronder genoemde aanbevelingen geven richting aan de beleidsopvolging. Zo kunnen de aanbevelingen worden gebruikt in verdere beleidsontwikkeling in het kader van de Strategie Nationale Veiligheid.
Verder stelt dit rapport de verantwoordelijke professionals in bedrijven en overheden in staat om eigen kernbelangen en kwetsbaarheden beter te identificeren en te beschermen. De drie thema's uit de conclusies bevatten aangrijpingspunten voor (verdere) versterking van de weerbaarheid tegen spionage.
Hoewel het onderzoek zich beperkt tot statelijke spionage op de terreinen van economisch welzijn & wetenschappelijk potentieel en openbaar bestuur & vitale infrastructuur zijn de aanbevelingen breed toepasbaar, ook binnen andere sectoren. Daarnaast kan een verhoogde bescherming tegen statelijke spionage ook de kwetsbaarheid voor bedrijfsspionage reduceren.

10.1 Waardebewustzijn

Uit het onderzoek blijkt dat organisaties en individuele medewerkers van organisaties zich soms niet of onvoldoende realiseren wat de waarde is van de informatie waarover zij beschikken of waartoe zij toegang kunnen verschaffen. Gevolgen daarvan kunnen zijn het onbewust weg laten lekken van kernbelangen, onvoldoende beveiliging van kernbelangen of juist het niet serieus nemen of naleven van beveiligingsmaatregelen wanneer deze zijn ingesteld. Het weglekken van kernbelangen kan, maar hoeft niet direct, schade toebrengen aan de organisatie. Het weglekken van kernbelangen kan bovendien ook een aantasting van de nationale veiligheid betekenen.

Op basis van het uitgevoerde onderzoek wordt daarom de volgende algemene aanbeveling gedaan: **Versterk actief het bewustzijn (onder managers en medewerkers) van overheden, bedrijven en instellingen met betrekking tot de waarde van de informatie waarover zij beschikken en van de mogelijke interesse van buitenlandse overheden in deze informatie**

Overheden, bedrijven en instellingen zijn zelf verantwoordelijk voor het waardebewustzijn over de informatie als kernbelang. Op basis van de uitkomsten van het onderzoek kan wel een aantal concrete suggesties worden gedaan op welke wijze het waardebewustzijn van organisaties en de individuele medewerkers kan worden vergroot:

- Verzorg sectorspecifieke *awareness*-presentaties (op managementniveau én medewerkersniveau), waarbij gezamenlijk op specifiek voor die sector geldende kernbelangen en kwetsbaarheden wordt ingegaan.

- Geef voorlichting of laat voorlichting geven bij hoogrisico-organisaties over de wijze van rekruteren en cultiveren van menselijke bronnen door buitenlandse inlichtingendiensten. Doel hiervan is dat betrokkenen in deze organisaties beter leren herkennen wanneer zij te maken hebben met een buitenlandse inlichtingenofficier.

- Maak inzichtelijk welke schade Nederland en Nederlandse bedrijven (kunnen) lijden als gevolg van spionage door buitenlandse inlichtingendiensten. Doe dit bijvoorbeeld aan de hand van een scenario in de nationale risicobeoordeling (onderdeel van de Strategie Nationale Veiligheid).

- Begin bij het versterken van het waardebewustzijn bij bestuurders op het hoogste niveau in de organisatie, opdat dit bewustzijn onderdeel wordt van het beleid.

- Stel een checklist op waarmee bedrijven en instellingen kunnen nagaan of technieken die zij ontwikkelen voor wetenschappelijke of consumentendoeleinden eventueel ook waardevol zouden kunnen zijn voor buitenlandse inlichtingendiensten, mede in verband met hun toepassing op andere terreinen (zoals *dualuse*-toepassingen). Pas hier eventueel regelgeving op aan.

- Breng in kaart welke Nederlandse technisch-wetenschappelijke studierichtingen en onderzoeksterreinen een verhoogd spionagerisico hebben. Een eerste aanzet hiertoe is terug te vinden in dit rapport. Voor deze studierichtingen kunnen vervolgens *awareness*-trajecten worden gestart.

- Maak afspraken tussen de overheid en bedrijven en instellingen wanneer en op welke wijze medeoverheden, bedrijven en instellingen worden gealerteerd op verhoogde belangstelling van een buitenlandse inlichtingendienst.

- Zorg voor een zichtbaar en herkenbaar meldpunt waar overheden, bedrijven en instellingen terecht kunnen met vragen over en vermoedens van spionage door buitenlandse inlichtingendiensten.

10.2 Veiligheidsbewustzijn

Uit het onderzoek blijkt dat beveiliging niet altijd wordt meegenomen bij bijvoorbeeld de keuze voor een bepaald softwaresysteem, uitbesteding van de fysieke beveiliging of externe inhuur van medewerkers. De randvoorwaarden voor beveiliging van kernbelangen hebben niet altijd voldoende aandacht binnen organisaties. Beperkte aandacht voor beveiliging en veiligheid kan tot onbegrip van individuele medewerkers leiden, die niet accepteren dat ze te allen tijde hun pasje zichtbaar moeten dragen of mensen van buiten de organisatie niet zomaar mee naar binnen mogen nemen. De afweging tussen beveiliging en gebruiksvriendelijkheid wordt vaak in het voordeel van gebruiksvriendelijkheid gemaakt. Gecombineerd met een gebrekkig waardebewustzijn kan het zelfs gebeuren dat mensen bewust veiligheidsmaatregelen ontwijken, omdat deze niet zo gebruiksvriendelijk zijn als zij zouden willen.

Daarnaast is het vertrouwen van gebruikers in de veiligheid van de door hen gebruikte technieken en ICT-toepassingen (te) groot. Dit uit zich vaak in het gedrag van mensen: bijvoorbeeld bij ICT-gebruik (het openen van e-mailbijlagen, of het downloaden van bestanden van internet). Maar het kan ook gaan om het meenemen van een laptop op reis, het voeren van telefoongesprekken in openbare ruimtes en het gebruik van *smartphones* en pda's voor werken met gevoelige informatie.

Hieruit vloeit de volgende aanbeveling voort:
Werk aan een cultuurverandering op het gebied van beveiliging. Daarbij zijn gebruikers, de inrichting van gegevensstromen en databases en de gebruikte technieken voor detectie van incidenten belangrijke aandachtspunten.

Om het beveiligingsbewustzijn (verder) te versterken kunnen de volgende acties worden ondernomen:

- Houd binnen overheden, bedrijven en instellingen periodieke *security audits* en systeempenetratietesten waarin nadrukkelijk aandacht wordt besteed aan spionagerisico's.

- Zorg in hoogrisico-organisaties voor (verdere) compartimentering van gevoelige informatie.

- Maak afspraken met ICT-dienstverleners dat datasystemen (servers) die gevoelige, vertrouwelijke of geheime informatie bevatten fysiek in Nederland moeten zijn geplaatst en beschikken over de juiste beveiligingsvoorzieningen.

- Versterk de positie van beveiligingsverantwoordelijke afdelingen, beveiligingsambtenaren en -medewerkers. Zorg dat bij besluiten op het terrein van bedrijfsvoering altijd vooraf advies wordt ingewonnen bij een beveiligingsexpert binnen de organisatie. Op deze wijze wordt voorkomen dat omissies in het beveiligingsbeleid ontstaan die duurder zijn om op een later moment te herstellen of wellicht zelfs nooit zichtbaar worden.

- De positie van de beveiligingsverantwoordelijke afdeling kan worden versterkt door het onderwerp te laten opnemen in de portefeuille van een persoon uit het topmanagement of Raad van Bestuur.

- Vergroot de kennis over de kwetsbaarheden van ICT-technieken en -toepassingen. Maak daarbij duidelijk waar zich specifieke kwetsbaarheden voordoen, hoe deze zijn te herkennen en te voorkomen.

- Stel een overzichtelijk afwegingskader op voor overheden, bedrijven en instellingen ten aanzien van de verzending van gevoelige informatie. Met dit afwegingskader kan gekozen worden welke informatie (kernbelang of niet), op welke wijze (versleuteld of niet), via welke weg (internet, telefonisch of anders) het best verzonden kan worden.

- Stel bij het verlenen van subsidies en budgetten aan onderzoeksinstellingen met een verhoogd risicoprofiel de voorwaarde dat deze instellingen vooraf inzicht geven in de te nemen beveiligingsmaatregelen en waardebewustzijnverhogende activiteiten. Maak een risicoanalyse op het terrein van spionage door een buitenlandse inlichtingendienst. Een dergelijke risicoanalyse helpt de kernbelangen rond het onderzoek alsmede de daarbij behorende risico's in kaart te brengen. Eenzelfde 'spionagerisicoanalyse' kan worden gevraagd als voorwaarde voor het toekennen van innovatiesubsidies door SenterNovem en andere subsidieverstrekkers op innovatiegebied.

- Versterk de positie van toezichthoudende organen, zoals het Agentschap Telecom voor de telecomsector, bij het onderkennen en beperken van spionagerisico's in de genoemde sectoren.

- Laat het eerder genoemde meldpunt advies geven aan overheden, bedrijven en instellingen over de manier waarop zij zich tegen spionage door buitenlandse inlichtingendiensten kunnen beschermen.

- Geef als overheid zelf het goede voorbeeld:
  - Draag zorg voor een adequate naleving van geldende beleidskaders zoals het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR) en het Voorschrift Informatiebeveiliging Rijksdienst bijzondere informatie (VIR-BI) uit 2004.
  - Bevorder het eigen gebruik van kwalitatief hoogwaardige en voor het doel geschikte beveiligingsproducten. Voor bescherming van gerubriceerde informatie kan gebruik gemaakt worden van door AIVD/NBV geëvalueerde, door de minister van BZK goedgekeurde beveiligingsproducten. Voor niet-gerubriceerde informatie zijn ook beoordelingssystemen voor ICT-middelen beschikbaar, zoals de internationaal geaccepteerde 'Common Criteria'.
  - Gebruik op politiek en (hoog)ambtelijk niveau geen pda's met uitsluitend door de producent ingebouwde beveiligingssystemen om e-mail te verzenden met een gevoelig tot geheim karakter. Op dit moment worden deze nog steeds op grote schaal gebruikt, ook voor het versturen van gevoelige en vertrouwelijke informatie.
  - Verplicht loggen van systemen die gevoelige, vertrouwelijke of geheime informatie bevatten. Dit is nog niet overal het geval.

10.3 Belangenafweging

Belangen op korte termijn versus belangen op lange(re) termijn:
Uit het onderzoek blijkt dat organisatiebelangen en/of overheidsbelangen op korte termijn (vaak) prevaleren over de belangen op lange termijn. Als de verkoop van een bedrijf(sonderdeel) op korte termijn geld oplevert, wordt soms nauwelijks aandacht besteed aan het feit dat het uit handen geven van dit bedrijf(sonderdeel) in de toekomst een veiligheidsprobleem kan vormen. Drie voorbeelden:

Marktwerking versus nationale belangen

De verkoop van Nederlandse bedrijven aan buitenlandse bedrijven stuit op dit moment op weinig weerstand of belemmeringen. Dit past in het Nederlandse beleid van liberalisering en antiprotectionisme. Het in buitenlandse handen doen overgaan van dergelijke bedrijven kan (op termijn) schade toebrengen aan de Nederlandse nationale veiligheid. De liberalisering van de energiemarkt heeft ertoe geleid dat sommige energieleveranciers onderdeel zijn geworden van grote, buitenlandse organisaties. De vraag kan gesteld worden of in de belangenafweging van een dergelijk bedrijf de Nederlandse energievoorzieningszekerheid voorop staat. Andere westerse landen zien dergelijke risico's ook en hebben om die reden eigen nationale toetsingskaders met behulp waarvan buitenlandse overnames worden goed of afgekeurd.

Kennis delen versus kennis beschermen

Op dit moment worden op grote schaal buitenlandse studenten aangetrokken om onderzoek te verrichten in technisch-wetenschappelijke studierichtingen waar Nederlandse kernbelangen zijn te vinden en waarvan het weglekken schade zou toebrengen aan het economisch welzijn van Nederland. Na deze studie vertrekt het merendeel van deze studenten weer naar het land van herkomst met medeneming van de kennis en vaardigheden opgedaan in Nederland. Strategisch-economische kennis die moet bijdragen aan het economisch potentieel van de toekomstige Nederlandse kenniseconomie kan zo wegvloeien naar buitenlandse concurrenten. De economische schade die hieruit ontstaat kan de nationale veiligheid aantasten.

Uit handen geven versus in handen houden

Veel bedrijven en instellingen kiezen ervoor om activiteiten als systeem- en serverbeheer, datawarehousing en gegevensverwerking uit te besteden of te *offshoren*. Dit brengt spionagerisico's met zich mee. Het zicht op welke externe partijen toegang hebben tot de systemen en gegevens wordt door uitbesteden belemmerd. De mogelijke kostenbesparing op korte termijn wordt lang niet altijd afgezet tegen de mogelijke (economische) risico's waaraan het bedrijf of instelling wordt blootgesteld als zo gegevens toegankelijk worden voor spionage-activiteiten.

Op basis van deze overwegingen wordt de volgende aanbeveling gedaan:
Besteed bij beleidsvorming nadrukkelijk aandacht aan de bescherming van kernbelangen en de effecten van beleid op de belangen van Nederland op langere termijn.

Om een betere balans te vinden in het afwegen van belangen op de korte en de lange(re) termijn kunnen bijvoorbeeld de volgende acties worden ondernomen:

- Breid batenanalyses voor het Nederlandse economisch welzijn van het delen van technisch-wetenschappelijke kennis uit met de kostenanalyses als gevolg van het weglekken van deze kennis.

- Besteed in de afweging om activiteiten uit te besteden of te *offshoren* nadrukkelijk aandacht aan de risico's van spionage en de (economische/financiële) gevolgen hiervan.

Colofon
Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

Postbus 20010 | 2500 EA Den Haag

Grafische verzorging
Zijlstra Drukwerk B.V., Rijswijk

februari 2010