Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

30 821 Nationale Veiligheid

32 852 Grondstoffenvoorzieningszekerheid

Nr. 302

BRIEF VAN DE MINISTERS VAN ECONOMISCHE ZAKEN EN VAN JUSTITIE EN VEILIGHEID EN DE STAATSSECRETARIS VAN BUITENLANDSE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 juli 2025

Met deze brief informeren wij u, conform de toezegging aan uw Kamer, mede namens de Ministers van Defensie en Onderwijs, Cultuur en Wetenschap, over de status en voortgang van het economische veiligheidsbeleid van Nederland.[1]

Belang van economische en nationale veiligheid

Machtsverhoudingen veranderen in hoog tempo, de internationale veiligheidssituatie is de afgelopen jaren sterk verslechterd en een open en op regels gebaseerde wereldeconomie is niet langer vanzelfsprekend. We ontlenen een belangrijk deel van ons verdienvermogen aan onze internationale verbondenheid. Die verbondenheid willen we zoveel mogelijk behouden. We zien echter dat toegang tot kennis, technologie en kritieke grondstoffen in toenemende mate bepalend is voor het waarborgen van onze nationale veiligheid. Statelijke actoren schromen niet om economische middelen in te zetten als geopolitiek drukmiddel, bijvoorbeeld door (het dreigen met) het afknijpen van toeleveringsketens van geneesmiddelen of grondstoffen. Tegelijkertijd staat ons nationale en Europese concurrentievermogen onder druk. We moeten niet naïef zijn, en onze nationale en Europese capaciteiten beschermen en versterken, waar het aan onze nationale veiligheid raakt. Dit vraagt om actie.

De inlichtingen- en veiligheidsdiensten typeren de huidige veiligheidssituatie als een *«grey zone»* waar statelijke actoren met een scala van heimelijke en digitale methoden een bedreiging vormen voor onze nationale veiligheid. Hierbij zijn het Nederlandse bedrijfsleven en kennisinstellingen steeds vaker doelwit.[2] Door gebruik van zowel legale als illegale middelen, waaronder gerichte investeringen, spionage,

[1] TZ202411-021
[2] MIVD jaarplanbrief 2025.

kst-30821-302
ISSN 0921 - 7371
's-Gravenhage 2025

sabotage en cyberaanvallen, proberen statelijke actoren toegang te verwerven tot sensitieve kennis en technologie, alsook vitale processen.

Zorgen voor onze economische veiligheid is dan ook urgenter en actueler dan ooit. Dit draagt ook bij aan onze open strategische autonomie, doordat het Nederland en de EU in staat stelt om zelf keuzes te blijven maken om publieke belangen te borgen. Het kabinet heeft de afgelopen jaren dan ook gewerkt aan een robuust beleid en instrumentarium.

Beleidsaanpak economische veiligheid

Economische veiligheid is een van de nationale veiligheidsbelangen zoals uiteengezet in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden en benoemd in de Aanpak Statelijke Dreigingen.[3] In de Veiligheidsstrategie is een actielijn opgenomen om de weerbaarheid van de economie te vergroten en de wetenschap te beschermen. De afgelopen jaren is economische veiligheid uitgegroeid tot een eigenstandig beleidsterrein. Het kabinet zal zich blijvend inzetten om onze economische veiligheid te waarborgen.

Nederland is uitgegroeid tot voorloper in Europa op het gebied van economische veiligheid.[4] Het Nederlandse economische veiligheidsbeleid ziet toe op het weerbaar maken van onze economie tegen de inzet van economische activiteiten of instrumenten, die een risico vormen voor de nationale veiligheid, door of in opdracht van statelijke actoren. De te beschermen belangen en daarmee de hoofddoelen zijn:

- het tegengaan van ongewenste kennis- en technologieoverdracht;
- het borgen van de continuïteit van vitale processen;[5]
- het verminderen en voorkomen van risicovolle strategische afhankelijkheden.

Hierbij wordt onder meer ingezet op het verkrijgen van inzicht in dreigingen en het voorkomen van ongewenste zeggenschap en spionage. Verder gaat het hierbij ook om het vergroten van de fysieke en digitale veiligheid, om gerichte ondersteuning van het bedrijfsleven alsmede om veilig inkopen en aanbesteden. Daarnaast zijn versterking van het concurrentievermogen en samenwerkingsverbanden – zowel publiek-privaat als Europees en internationaal – noodzakelijk.

Conform de motie van het lid Thijssen is onderzocht of bovenstaande drie hoofddoelstellingen voor het brede economische veiligheidsbeleid specifieker gemaakt kunnen worden.[6] Het specificeren van doelen op gebied van economische veiligheid is zeer complex.[7] Economische veiligheid is immers een dynamisch streven waar geopolitieke ontwikkelingen en dreigingen directe invloed op hebben. Daarnaast maakt het vaak heimelijke karakter van de dreiging het formuleren van een kwantitatief doel moeilijk. Op basis van nieuwe inzichten over de nationale veiligheidsdreiging en de weerbaarheid van de Nederlandse economie alsook beleidsontwikkelingen in binnen- of buitenland, kunnen de doelstellingen worden aangescherpt. Naar verwachting worden dit najaar de resultaten van een nulmeting van het bedrijfsleven op het gebied van economische veiligheid opgeleverd. Op basis van de nulmeting zullen de doelstellingen waar mogelijk geconcretiseerd en gekwantificeerd worden.

---

[3] Kamerstuk 30 821, nr. 178, bijlage en Kamerstuk 30 821, nr. 175

[4] Clingendael en SEO (2025): Verkenning_Internationaal_EV_Instrumentarium.pdf p. 92.

[5] Specifiek ten aanzien van de vitale processen in de digitale infrastructuur is naast het borgen van de continuïteit ook het borgen van de integriteit van het proces een centrale doelstelling.

[6] Kamerstuk 32 852, nr. 327

[7] Specifiek voor grondstoffen, zie Aanhangsel Handelingen II 2024/25, nr. 2062

De kabinetsaanpak economische veiligheid kent verschillende uitgangspunten. Het instrumentarium bevindt zich primair op nationaal niveau, waarbij coördinatie en samenwerking in Europees en internationaal verband de inzet versterkt. Het kabinet streeft daarom bij maatregelen op het gebied van economische veiligheid (en kennisveiligheid) naar samenhang op EU- en internationaal niveau. Dit komt de effectiviteit van maatregelen ten goede en is belangrijk voor een gelijk speelveld. Het beleid is landenneutraal, conform internationale principes, rechtsbeginselen en verplichtingen zoals het non-discriminatiebeginsel. Ook is het beleid adaptief en risico-gebaseerd, om de nationale veiligheidsbelangen zo goed mogelijk te waarborgen en marktverstoring te minimaliseren. Het credo voor de economie hierbij blijft: «open waar het kan; gesloten waar het moet». Het kabinet ziet het economische veiligheidsbeleid nauw verwant aan het bredere innovatie-, industrie- en handelsbeleid en de aanpak maatschappelijke weerbaarheid tegen militaire en hybride dreigingen.[8]

Naar analogie van het EU-kader vereist het realiseren van de doelstellingen een geïntegreerde aanpak langs drie sporen: *protect* (beschermen), *promote* (versterken) en *partner* (samenwerken), die worden versterkt door actieve ondersteuning van het bedrijfsleven en kennisopbouw op dit thema.[9] De beleidsinitiatieven en -instrumenten binnen het economische veiligheidsbeleid van de Rijksoverheid (zie bijlage) raken aan één of meerdere van deze sporen.

Protect

Beschermende maatregelen zijn nodig om kwetsbaarheden op het gebied van kennis en technologie, vitale processen en risicovolle strategische afhankelijkheden te verminderen. Zo voorkomen we dat deze kwetsbaarheden tegen ons worden gebruikt. Dat doen we onder andere via het stelsel van investeringstoetsing (bestaande uit sectorale wetgeving en de Wet veiligheidstoets investeringen, fusies en overnames), exportcontrolebeleid van strategische goederen en diensten, gerichte (beveiligings-)maatregelen in het vitaal stelsel en de Beschermingsvoorziening Economische Veiligheid.[10]

Hoewel hiermee een goede en stevige basis is gelegd, vragen de toegenomen dreiging en geopolitieke ontwikkelingen om aanscherping en aanvulling. Daarom zijn onderstaande acties in gang gezet.

Box 1: *Protect*-initiatieven die in ontwikkeling zijn
- Voorstel om de reikwijdte van de Wet veiligheidstoets investeringen, fusies en overnames uit te breiden naar meer sensitieve technologieën en vitale aanbieders;
- Sectorale investeringstoets voor de defensie-en veiligheid gerelateerde industrie (voorziene inwerkingtreding medio 2026);
- Onderzoek naar de eventuele risico's van *greenfield*- en uitgaande investeringen;
- Herziening van de *Foreign Direct Investments*-screeningsverordening;

[8] Kamerstuk 30 821, nr. 249

[9] Het instrumentarium bestaat niet alleen uit initiatieven die specifiek voor economische veiligheid zijn ontwikkeld, maar ook uit instrumenten die voor een ander doel zijn ontwikkeld en ook bijdragen aan de versterking van de economische veiligheid.

[10] De Wet veiligheidstoets investeringen, fusies en overnames en Beschermingsvoorziening Economische Veiligheid worden dit jaar geëvalueerd.

- Herzien van de regelgeving rondom overheidsaanbestedingen middels de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten;
- Verkenning naar economische veiligheidsrisico's bij subsidies die het Ministerie van Economische Zaken aan het bedrijfsleven verstrekt;
- Onderzoek naar hoe risico's op ongewenste kennis- en technologieoverdracht door internationale kenniswerkers kan worden tegengegaan.

Promote

Een sterke, innoverende en concurrerende economie is beter bestand tegen dreigingen voor de nationale veiligheid.[11] Daarom zijn, naast het creëren van de juiste randvoorwaarden, in specifieke gevallen actieve en gerichte stimulerende maatregelen nodig om (technologische) leiderschapsposities en essentiële capaciteiten in strategische waardeketens te verkrijgen en behouden. Dit stelt ons in staat om te blijven innoveren, de concurrentie voor te blijven en ons verdienvermogen veilig te stellen en daarmee onze weerbaarheid te vergroten. De Nationale Technologiestrategie, de Defensie Strategie voor Industrie en Innovatie 2025–2029 en de Agenda Digitale Open Strategische Autonomie zijn hier voorbeelden van.

Box 2: *Promote*-initiatieven die in ontwikkeling zijn
- Nauwere samenwerking met private partijen, Invest-NL en de regionale ontwikkelingsmaatschappijen op gebied van economische veiligheid;
- Invest International is voornemens een publiek-privaat investeringsfonds op te zetten om Nederland betere toegang te geven tot kritieke grondstoffen;
- Verder integreren van economische veiligheid in het industriebeleid. Naar verwachting volgt oplevering vernieuwd industriebeleid in Q3 2025;
- Oplevering actieagenda's voor alle tien de technologiegebieden binnen de Nationale Technologie Strategie eind 2025;
- Ontwikkeling van een *roadmap* voor elk van de vijf NLD gebieden uit de Defensie Strategie voor Industrie en Innovatie 2025–2029 (kwantum, slimme materialen, ruimtetechnologie, intelligente systemen en sensoren);
- Een actieplan om toe te werken naar de 3% R&D-uitgaven van het BBP;
- Het Pact Ondernemingsklimaat om de randvoorwaarden voor ondernemen in Nederland aantrekkelijker te maken.

Partner

Ten derde is samenwerking met (internationale) publieke en private partners benodigd voor behoud van een gelijk speelveld, versterking van onze internationale positie en vergemakkelijking van de toegang tot technologie, producten en kritieke grondstoffen die we zelf niet in huis hebben. Zo draagt deze pilaar ook bij aan een succesvolle *protect*- en *promote*-inzet. De Nederlandse inzet op *partner*-beleid op Europees niveau vormt een integraal onderdeel van ons economisch veiligheidsbeleid.[12] Ook is Nederlandse deelname aan andere multilaterale gremia zoals de WTO en OESO van belang, evenals de samenwerking met bilaterale partners buiten de EU en het bedrijfsleven. Voorbeelden van

[11] Zoals toegelicht in de Kabinetsvisie EU-Concurrentievermogen, Kamerstuk 21 501-30, nr. 621.
[12] O.a. Economische Veiligheidsstrategie (juni 2023) en het Europees Economische Veiligheidspakket (januari 2024).

partner-initiatieven zijn EU-handels- en partnerschapsovereenkomsten, bilaterale grondstoffenpartnerschappen, en de Semicon Board NL.

Box 3: *Partner*-initiatieven die in ontwikkeling zijn
- Intensivering van de dialoog met het bedrijfsleven;
- De beleidsagenda Buitenlandse Handel waar het vergroten van onze weerbaarheid een belangrijke pijler is. Deze is op 28 mei jl. met uw Kamer gedeeld;
- Grondstoffenpartnerschappen en onderhandelingen over handelsakkoorden met grondstofrijke landen, ten behoeve van de leveringszekerheid van kritieke grondstoffen;
- Internationale samenwerkingsverbanden ter versterking van het Nederlandse halfgeleiderecosysteem, zoals de Semicon Coalition.

Ondersteuning bedrijfsleven

Ondersteuning van het bedrijfsleven bij het omgaan met economische veiligheidsrisico's is noodzakelijk. Ondernemingen, zeker het kennisintensieve mkb, zijn over het algemeen nog onvoldoende toegerust om de risico's adequaat het hoofd te kunnen bieden. Niet alleen bedrijven zijn daar op termijn de dupe van, het zorgt er ook voor dat Nederland kwetsbaar wordt voor kwaadwillende actoren en daarmee de nationale veiligheid in gevaar komt. De komende jaren gaat de Minister van Economische Zaken extra inzetten op het actief stimuleren en ondersteunen van het bedrijfsleven bij het nemen van maatregelen ter versterking van hun weerbaarheid tegen economische veiligheidsdreigingen. In lijn met het Actieprogramma mkb-dienstverlening staat hierin het perspectief van ondernemers centraal.[13] Een belangrijk instrument in dit kader is het Ondernemersloket Economische Veiligheid (OLEV).

Box 4: Ondersteuning bedrijfsleven-initiatieven die in ontwikkeling zijn
- Doorontwikkeling van het OLEV, o.a. met fysieke aanwezigheid in hightech ecosystemen (intensivering in Brainport en uitbreiding naar Delft);
- Nulmeting economische veiligheid van het bedrijfsleven;
- Communicatiecampagne voor ondernemers om hen bewuster te maken van economische veiligheidsrisico's en te activeren om maatregelen te nemen;
- Ontwikkeling van het Cyberweerbaarheidsnetwerk door het Nationaal Cyber Security Centrum, het Digital Trust Centrum en Cyber Security Incident Response Team voor digitale diensten.

Kennisopbouw

Voor een proportioneel en effectief economisch veiligheidsbeleid is kennisopbouw randvoorwaardelijk. Om zicht te krijgen op de toenemende dreiging en de complexiteit van de dreigingen, is een solide en eigenstandige inlichtingenpositie onmisbaar. Dit vereist goed toegeruste inlichtingen- en veiligheidsdiensten. Ook is het van groot belang risicovolle strategische afhankelijkheden in kaart te brengen en bijbehorende handelingsopties te ontwikkelen om deze op proportionele wijze te verminderen of te voorkomen. De interdepartementale Taskforce Strategische Afhankelijkheden (TFSA) ziet hierop toe.[14] Op het gebied van kritieke grondstoffen en daarmee samenhangende strategische materialen en producten brengt het Nederlands Materialen Observatorium (NMO) de

[13] Op 31 maart is uw Kamer geïnformeerd over de voortgang van het Actieprogramma mkb-dienstverlening, gericht op het stroomlijnen van ondernemersdienstverlening.
[14] Kamerstuk 30 821, nr. 244

risicovolle strategische afhankelijkheden in kaart. Het NMO analyseert en monitort op structurele basis de aanvoer en beschikbaarheid van kritieke grondstoffen en toeleveringsketens die van belang zijn voor Nederland en het Nederlandse bedrijfsleven. De nadruk ligt daarbij op de impact van mogelijke verstoringen in toeleveringsketens.[15] Daarnaast wordt, door en in opdracht van het kabinet, veelvuldig onderzoek gedaan om nieuwe risico's te herkennen, en de impact daarvan en van potentiële maatregelen op de economie te kunnen duiden.

Box 5: Kennisopbouw-initiatieven die in ontwikkeling zijn
- Het kabinet verkent of de inlichtingen- en veiligheidsdiensten extra bevoegdheden nodig hebben ter bevordering van de economische veiligheid;
- Doorontwikkeling van de aanpak tegen statelijke dreigingen.

Tot slot

Het is belangrijk dat we blijven investeren in het beschermen van onze economische veiligheid, zeker in deze geopolitiek turbulente tijd. Hiermee maken we onze bedrijven, kennisinstellingen en economie in zijn geheel weerbaarder tegen dreigingen van buitenaf. In de bijlage staat een uitgebreider overzicht van bestaande beleidsinitiatieven en -instrumenten. Ook wordt hierin invulling gegeven aan de toezegging aan uw Kamer en de motie Idsinga over specifieke onderdelen van de beleidsaanpak economische veiligheid.[16]
Conform de motie Idsinga, zal uw Kamer jaarlijks worden geïnformeerd over de nadere voortgang op het gebied van economische veiligheid.[17] De eerstvolgende brief zal in de zomer van 2026 volgen, of eerder indien nodig.

De Minister van Economische Zaken,
V.P.G. Karremans

De Minister van Justitie en Veiligheid,
D.M. van Weel

De Staatssecretaris Buitenlandse Handel,
J.C. Boerma

[15] Kamerstuk 32 852, nr. 317
[16] TZ202411-022 en Kamerstuk 32 852, nr. 333
[17] Kamerstuk 32 852, nr. 333

Bijlage 1:

Overzicht beleidsinitiatieven en instrumenten economische veiligheid

Protect

Om de Nederlandse economie te beschermen tegen economische veiligheidsdreigingen neemt het kabinet verschillende beschermende maatregelen.

Investeringen, fusies en overnames

De afgelopen jaren is er gebouwd aan een robuust stelsel van investeringstoetsing waarmee risico's voor de nationale veiligheid voortkomend uit ongewenste zeggenschap worden geadresseerd. Het gaat hierbij om verwervingsactiviteiten zoals investeringen, fusies en overnames. Sectorale investeringstoetsen bestaan binnen de Gaswet en Elektriciteitswet (vanaf 2026 gebundeld in de Energiewet) en de Telecommunicatiewet. Ook beschikt het kabinet over de Wet veiligheidstoets investeringen, fusies en overnames (vifo), die op 1 juni 2023 in werking is getreden. Het kabinet werkt momenteel aan verdere uitbreiding van het toepassingsbereik van de Wet vifo, zodat investeringen in bepaalde sectoren zoals kunstmatige intelligentie en biotechnologie[18] ook onder de Wet vifo getoetst kunnen worden. Dit jaar worden de Wet vifo en de Wet ongewenste zeggenschap telecommunicatie (tussentijds) geëvalueerd. Daarnaast wordt er gewerkt aan een investeringstoets voor de defensiegerelateerde industrie, de Wet weerbaarheid defensie- en veiligheid gerelateerde industrie, waarvan de inwerkingtreding is voorzien voor medio 2026. Ook is een investeringstoets voor zogenaamde *greenfield*-investeringen voor nieuwe windparken op zee gestart om sectorspecifieke risico's te beheersen.[19] Momenteel wordt er op EU-niveau gewerkt aan een herziening van de *Foreign Direct Investments*-screeningsverordening, die streeft naar harmonisatie en verbetering van samenwerking op het gebied van investeringstoetsing in de EU.[20] Nederland draagt hier actief aan bij om te zorgen dat deze herziening zo goed mogelijk aansluit bij het Nederlandse stelsel van investeringstoetsing. Voorts publiceerde de Europese Commissie op 15 januari 2025 een aanbeveling over de evaluatie van uitgaande investeringen in technologiegebieden die van cruciaal belang worden geacht voor de economische veiligheid van de EU.[21]

In 2023 heeft het kabinet een vangnetregeling geïntroduceerd, de Beschermingsvoorziening Economische Veiligheid (BEV). Dit biedt het kabinet de mogelijkheid om in uiterste gevallen, per direct, een belang te nemen in bedrijven van strategisch belang. Dit gebeurt wanneer voorziene investeringen door statelijke actoren, of partijen die handelen op aanwijzing van statelijke actoren, een bedreiging vormen voor de nationale veiligheid.[22] De voorziening dient als laatste redmiddel en kan worden ingezet als bestaande instrumenten, zoals de Wet vifo, ontoereikend zijn om risico's voor de nationale veiligheid af te dekken. De voorziening en Wet vifo zien beide toe op het ondervangen van risico's voor de nationale veiligheid uitgaande van voorziene investeringen.[23] De Wet vifo kan in uiterste gevallen ongewenste investeringen blokkeren, terwijl de BEV daarvoor een vervangende investering in de plaats kan

[18] Kamerstuk 32 852, nr. 317
[19] Wet windenergie op zee
[20] Kamerstuk 22 112, nrs. 3905 en 3988
[21] Kamerstuk 22 112, nr. 4007
[22] Kamerstuk 30 821, nr. 199
[23] TZ202411-022

stellen, en zo fungeert als slot op de deur van het stelsel van investeringstoetsing. De BEV kan worden ingezet wanneer een onderneming van strategische waarde (nog) buiten de reikwijdte van de Wet vifo valt of wanneer een geblokkeerde investering ertoe leidt dat een bedrijf in financiële problemen komt. Dit mechanisme voorkomt risico's voor de nationale veiligheid in het geval dat Nederlandse bedrijven van strategisch belang in verkeerde handen vallen of failliet gaan door een gebrek aan alternatieve investeringen. De eerste evaluatie van deze regeling wordt eind 2025 verwacht.

Beschermen fysieke en digitale veiligheid vitale infrastructuur

Het kabinet werkt onder coördinatie van de Minister van Justitie en Veiligheid, samen met bedrijven, andere departementen, organisaties en inlichtingen- en veiligheidsdiensten aan de Aanpak Vitaal voor een verbeterde bescherming van de Nederlandse vitale infrastructuur. Op deze manier verhogen we zowel de fysieke als digitale en economische weerbaarheid. Uw Kamer is in mei 2023 geïnformeerd over de Aanpak Vitaal[24] en zal voor de zomer geïnformeerd worden over de voortgang ervan. Vanwege de grensoverschrijdende verbondenheid van de vitale infrastructuur is inzet ook op Europees en internationaal niveau noodzakelijk. In dit kader zijn eind 2022 twee Europese richtlijnen die een (wettelijk) kader bieden voor het versterken en waarborgen van de digitale en fysieke weerbaarheid van onder meer de vitale infrastructuur aangenomen: de herziening van de richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de richtlijn veerkrachtige kritieke entiteiten (de CER-richtlijn).[25] Deze CER- en NIS2-richtlijnen worden op dit moment geïmplementeerd in Nederlandse wetgeving, te weten de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet en vormen een belangrijk onderdeel van de Aanpak Vitaal en de versterking van de digitale weerbaarheid van Nederland.[26] De wetsvoorstellen zijn op begin juni 2025 bij uw Kamer ingediend. Op dit moment zijn de inspanningen erop gericht dat beide wetten alsook de bijbehorende lagere regelgeving zo snel als mogelijk in werking treden. Voor de digitale infrastructuur zijn al langer specifieke beschermingsmaatregelen van kracht, gericht op aanbieders van mobiele communicatienetwerken.

Digitale weerbaarheid is een essentiële randvoorwaarde voor het functioneren van de samenleving en de economie. In het jaarlijks gepubliceerde Cybersecuritybeeld Nederland (CSBN) wordt inzicht geboden in de ontwikkeling van de digitale dreiging, de belangen die daardoor kunnen worden aangetast en de digitale weerbaarheid.[27] In de Nederlandse Cybersecuritystrategie 2022–2028 (NLCS)[28] en het bijbehorende actieplan is geformuleerd welke maatregelen het kabinet neemt om deze dreiging het hoofd te bieden en de weerbaarheid te verhogen. De strategie is gebaseerd op vier pijlers, waarlangs strategische doelen zijn geformuleerd. Indien nodig wordt het actieplan jaarlijks geactualiseerd op basis van onder andere het CSBN en inzichten van publieke, private en wetenschapspartijen. Mede ter uitwerking van pijler 3 uit de NLCS, is de Internationale Cybersecuritystrategie tot stand gekomen.[29] Hierin is de diplomatieke inzet die nodig is om te werken aan een open, vrij en veilig digitaal domein beschreven.

---

[24] Kamerstuk 30 821, nr. 182
[25] Zie Richtlijn - 2022/2557 - EN - EUR-Lex en Richtlijn - 2022/2555 - EN - EUR-Lex.
[26] Zie ook de website van de NCTV: https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen.
[27] Zie voor de meest recente CSBN 2024 Kamerstuk 26 643, nr. 1229
[28] Kamerstuk 26 643, nr. 925 en voor de voortgangrapportages, Kamerstuk 26 643, nrs. 1072 en 1229
[29] Kamerstuk 26 643, nr. 1036 en voor de voortgangsrapportage zie Kamerstuk 26 643, nr. 1252

Veilig inkopen en aanbesteden

Het kabinet is van mening dat Nederland en de EU in beginsel baat hebben bij open aanbestedingsmarkten. Binnen het aanbestedingsstelsel bestaat een aantal instrumenten om veiligheidsrisico's bij aanbestedingen te mitigeren. Zo kent de Aanbestedingswet (Aw) 2012 een bepaling op basis waarvan ondernemers uit landen die zijn aangesloten bij de Overeenkomst inzake overheidsopdrachten (GPA) en landen met een bilaterale overeenkomst niet minder gunstig mogen worden behandeld dan EU-landen, maar voor overige landen staat het de aanbestedende dienst vrij om wel extra voorwaarden te stellen. In de Aw 2012 is daarnaast bepaald dat aanbestedende diensten en speciale-sectorbedrijven uit het Verdrag betreffende de werking van de Europese Unie kunnen inroepen om opdrachten uit te zonderen van de Europese aanbestedingsplicht, wanneer het volgen van normale aanbestedingsprocedures niet kan om nationale veiligheid te beschermen.

De Aanbestedingswet op Defensie- en Veiligheidsgebied[30] (ADV) is een wettelijk kader dat is toegesneden op het aanbesteden van opdrachten op het gebied van defensie en veiligheid. In principe kan elke aanbestedende dienst gebruik van deze wet maken, mits de opdracht onder toepassing van de ADV voldoet. Onder de ADV zijn er meer mogelijkheden tot het uitsluiten van partijen, het beperken van toegang van (onder)aannemers en het stellen van eisen over gegevensbeveiliging en leveringszekerheid.

Het kabinet past sectorale wetgeving aan om meer beveiligingseisen op te leggen aan inkoop en aanbesteden zodat de aanbestedende dienst meer maatregelen kan nemen tegen risico's. Zo is in de Energiewet geregeld dat netbeheerders gebruik kunnen maken van de ADV. Daarnaast zet het kabinet zich in Europa, bij het dit jaar voorziene voorstel van de Europese Commissie tot herziening van de aanbestedingsrichtlijnen, in om betere en makkelijkere inzetbare regels voor overheden bij aanbesteden. Daarbij wordt ook gekeken naar de manieren waarop deze regels kunnen bijdragen aan het voorkomen of verminderen van risicovolle strategische afhankelijkheden. Bij het voorbereiden van een aanbesteding is het belangrijk na te gaan of er risico's voor de nationale veiligheid zijn. Door de Rijksoverheid is de Toolbox veilig inkopen vernieuwd.[31] De instrumenten uit de Toolbox (een *quickscan*, risicoanalyse en *quickguide)* helpen om stil te staan bij eventuele risico's van een aanbesteding voor de nationale veiligheid. PIANOo, het Expertisecentrum Aanbesteden van het Ministerie van Economische Zaken, heeft als taak het inkopen en aanbesteden bij overheden te professionaliseren. Hierbij betrekt zij ook Toolbox veilig inkopen.

Er gaan nieuwe beveiligingseisen gelden voor bedrijven die opdrachten uitvoeren voor de Rijksoverheid die raken aan de nationale veiligheid.[32] De eisen staan in de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO 2025). De eisen worden ontwikkeld om ervoor te zorgen dat de nationale veiligheid voldoende gewaarborgd blijft wanneer er contracten met externe partijen gesloten worden. Dit ABRO-voorschrift wordt door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Defensie doorontwikkeld vanuit de Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO) van het Ministerie van Defensie.[33] De nieuwe regeling zal beveiligingseisen stellen aan opdrachtnemers op het gebied van bestuur en organisatie, personeel, de

[30] https://wetten.overheid.nl/BWBR0032898/2019-04-18.
[31] Https://www.nctv.nl/onderwerpen/economische-veiligheid/toolbox-veilig-inkopen.
[32] Industrieveiligheid - ABRO: nieuwe beveiligingseisen voor bedrijven.
[33] Kamerstuk 26 643, nr. 1007

fysieke omgeving, cyber en cloud. ABRO 2025 vervangt de ABDO. De ABRO worden niet in één keer ingevoerd maar in zogenoemde tranches. Tranche 1 betreft de departementen, de agentschappen en de politie. De eerste organisaties van tranche 1 starten naar verwachting vanaf deze zomer met het toepassen van ABRO. De volledige tranche 1 past naar verwachting binnen twee jaar ABRO geleidelijk toe. De indeling van andere overheidsorganisaties in opvolgende tranches wordt voorbereid. Dat gaat in tranches 2 en 3 voornamelijk om zelfstandige bestuursorganen, decentrale overheden, bedrijven uit de vitale sectoren en Hoge Colleges van Staat. De uitbreiding naar tranches 2 en 3 vergt besluitvorming binnen het kabinet.

Kennismigranten, erkend referenten en uitleenconstructies

Een internationale kennismigrant kan onder voorwaarden naar Nederland komen om te werken en daarmee bij te dragen aan kennis- en technologieontwikkeling in Nederland. Momenteel wordt door het Ministerie van Economische Zaken onderzocht hoe risico's op ongewenste kennis- en technologieoverdracht door individuele internationale kenniswerkers kunnen worden tegengegaan, waarbij nationale veiligheid en een aantrekkelijk ondernemingsklimaat in balans worden gehouden. Daarnaast worden onder leiding van het Ministerie van Asiel en Migratie maatregelen uitgewerkt om te voorkomen dat statelijke actoren met kwade bedoelingen via de erkend referentstatus van bedrijven vreemdelingen kunnen inzetten om op zoek te gaan naar informatie over sensitieve kennis en technologie. Hiervoor is een conceptbeoordelingskader ontwikkeld dat momenteel, middels hypothetische testcasussen binnen een pilot, nader wordt uitgewerkt en getest. Uw Kamer is hier in november 2024 voor het laatst over geïnformeerd,[34] en zal na de zomer van dit jaar nader over de bevindingen bij deze trajecten worden geïnformeerd. Daarnaast werkt het Ministerie van Asiel en Migratie er met de Ministeries van Economische Zaken en Sociale Zaken en Werkgelegenheid aan om uitleenconstructies van kennismigranten in te perken en zo potentieel misbruik tegen te gaan.

Exportcontrole dual-use en militaire goederen en technologie

Het Nederlandse exportcontrolebeleid voor strategische goederen en diensten, verantwoordelijkheid van de Staatssecretaris Buitenlandse Handel, is ook een instrument om ongewenste kennis- en technologieoverdracht tegen te gaan. Bij exportcontrole is nationale veiligheid een belangrijk uitgangspunt, onder meer zodat Nederland niet bijdraagt aan de ontwikkeling en verspreiding van massavernietigingswapens en om te voorkomen dat gevoelige goederen en technologieën in handen komen van partijen die een risico vormen voor onze veiligheid. Het kabinet zet zich in voor meer coördinatie tussen EU-lidstaten waar het gaat om exportcontrole van zogeheten *dual-use* goederen, oftewel goederen die voor zowel civiele als militaire doeleinden worden gebruikt. Het uitgangspunt hierbij blijft uiteraard dat het kabinet zijn nationale bevoegdheid behoudt. Ook bij exportcontrole op militaire goederen is het kabinet een voorstander van meer samenwerking en eenduidige toepassing van onder andere wapenexportbeleid in Europa.

Anti-dwang instrument

De EU beschikt sinds 2023 over het anti-dwang instrument *(Anti-Coercion Instrument*, ACI) dat als doel heeft om de EU en haar lidstaten te beschermen tegen economische dwang door derde landen en zo nodig

[34] Kamerstuk 30 573, nr. 218

onder voorwaarden tegenmaatregelen te treffen. Daarbij verwijst economische dwang naar een situatie waarin een derde land de EU of een lidstaat met handelspolitieke of investering gerelateerde maatregelen onder druk probeert te zetten om een bepaalde beleidskeuze te maken. Tot op heden heeft de EU het ACI nog niet ingezet.

Investeren aanpak spionage

Vanwege de toenemende kwetsbaarheid van Nederland voor spionage is een aanvullende strafbaarstelling voor spionageactiviteiten tot stand gekomen. Het doel ervan is om onze nationale veiligheid, de veiligheid van personen, vitale infrastructuur en ook hoogwaardige technologieën beter te beschermen.
Er bestond al wetgeving die klassieke spionage strafbaar stelt, zoals het delen van staatsgeheimen. Echter veranderen vormen en inzet van spionage. Het is nu ook strafbaar als een persoon gevoelige informatie lekt die niet staatsgeheim is, of als iemand handelingen uitvoert voor een buitenlandse overheid waarbij Nederlandse belangen ernstig worden geschaad. Voorbeelden daarvan zijn het delen van gevoelige bedrijfsinformatie die een ander land kan misbruiken, of het doorgeven van persoonsgegevens aan buitenlandse overheden. Personen die spionageactiviteiten uitvoeren voor een buitenlandse overheid kunnen een maximale gevangenisstraf van acht jaar krijgen. In ernstigere situaties geldt een maximum gevangenisstraf van 12 jaar. Dat is bijvoorbeeld als spionageactiviteiten de dood tot gevolg hebben. Vanwege de opkomst van digitale spionage kunnen ook computermisdrijven zwaarder worden bestraft als deze begaan zijn voor een buitenlandse overheid. Het strafmaximum wordt ook verhoogd bij een aantal andere strafbare feiten die samengaan met spionageactiviteiten en begaan worden voor buitenlandse overheden, zoals omkoping.
Op 15 mei jl. is de wet uitbreiding strafbaarheid spionageactiviteiten in werking getreden.[35]

Kennisveiligheid

Kennisveiligheid is een eigenstandig beleidsterrein.[36] Kennisveiligheid ziet onder andere op het voorkomen van ongewenste overdracht van gevoelige kennis en technologie bij kennisinstellingen (universiteiten, hogescholen en toepaste onderzoeksinstellingen, ofwel de TO2), daar waar economische veiligheid zich richt op bedrijven. Het kabinet zet zich met het kennisveiligheidsbeleid samen met de kennissector in voor het verder vergroten van de weerbaarheid van Nederlands onderzoek en wetenschap. Daarbij wordt steeds de balans gezocht tussen enerzijds het benutten van kansen in open internationale samenwerking en anderzijds het beschermen van de nationale veiligheid en de hoogwaardige technologische kennis die onze kennisinstellingen ontwikkelen. Er wordt ingezet op bewustwording en zelfregulering van de sector. Het doel hierbij is dat kennisinstellingen weten welke kwetsbaarheden er zijn, de risico's herkennen en kunnen mitigeren, en tegelijkertijd kansen kunnen blijven benutten.

De inzet bestaat uit een continue dialoog over hoe de aanpak verder verbeterd kan worden, welke dilemma's daarbij opspelen en hoe we die gezamenlijk kunnen oplossen. De Nationale Leidraad Kennisveiligheid, die de Rijksoverheid samen met de kennissector heeft opgesteld, biedt handvatten om internationale samenwerking op een open en veilige manier vorm te geven. Ook is er het Loket Kennisveiligheid dat kennisin-

[35] Staatsblad 2025, 100
[36] Kamerstuk 31 288, nr. 894

stellingen adviseert over risico's bij internationale samenwerkingen, en proactieve kennisdeling via de *learning community* faciliteert. Om het gelijk speelveld te bevorderen en te leren van *best practices* elders is er ook inzet op EU en internationaal niveau. De EU Raadsaanbeveling kennisveiligheid[37] draagt daaraan bij, het bevat een overkoepelend kader voor alle lidstaten en de Europese Commissie om kennisveiligheid te versterken. Uw Kamer is op 13 juni 2025 geïnformeerd over de stand van zaken van een aantal moties en toezeggingen op dit beleidsterrein.[38]

Op dit moment wordt gewerkt aan het wetsvoorstel screening kennisveiligheid, dat ziet op screening van masterstudenten en onderzoekers die toegang gaan krijgen tot sensitieve technologieën. Het wetsvoorstel is op 7 april 2025 in consultatie gegaan.[39]

Promote

Een sterke economie is doorgaans een weerbaardere economie, waardoor het kabinet verschillende beleidsinitiatieven onderneemt ter versterking van de economie.

Versterken concurrentievermogen

Bij het versterken van het nationaal en Europees concurrentievermogen en gerichte sectorenbeleid ligt de aandacht vooral op strategische markten en een beperkte set (digitale) sleuteltechnologieën die bijdragen aan toekomstige economische groei en onze weerbaarheid.

- *Nationale Technologiestrategie (NTS)*
  De NTS, die in 2024 is gelanceerd, richt zich op het stimuleren van innovatie en het versterken van Nederland als technologisch leider op tien technologiegebieden zoals kwantumtechnologie, kunstmatige intelligentie en fotonica.[40] Het kabinet investeert in deze sectoren om de technologische soevereiniteit van Nederland te waarborgen. Nationale veiligheid is een van de grondslagen waarop deze strategie is ingegeven. Eind 2025 zullen er actieagenda's liggen voor alle tien de technologiegebieden.
- *Agenda Digitale Open Strategische Autonomie*
  De Agenda Digitale Open Strategische Autonomie maakt de balans op van onze autonomie in het digitale domein.[41] Conclusie: we zijn sterk asymmetrisch afhankelijk van derde landen. Hiertoe zijn tien technologieën aangewezen die geopolitiek het meest cruciaal zijn om onze positie in te versterken.
- *Sectorenbeleid*
  De gerichte programma's in het sectorenbeleid van het Ministerie van Economische Zaken focussen zich op ecosystemen, zoals de defensie-industrie, maritieme maakindustrie en halfgeleiders (onder andere met de Semicon Coalition). In het nieuwe industriebeleid zal meer focus komen te liggen op het verdienvermogen en weerbaarheid, naast de bestaande aandacht voor maatschappelijke missies.[42] Uw Kamer zal naar verwachting in Q3 2025 geïnformeerd worden over het nieuwe industriebeleid van het Ministerie van Economische Zaken.
- *Defensie- en veiligheid gerelateerde industrie*
  Ook werkt het kabinet aan de versterking van de defensie en veiligheid gerelateerde industrie. Deze inzet is uiteengezet in de Defensie

---

[37] Https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf.
[38] Kamerstuk 31 288, nr. 1205
[39] Overheid.nl | Consultatie Wet screening kennisveiligheid.
[40] Kamerstuk 33 009, nr. 140
[41] Kamerstuk 36 259, nr. 21
[42] Kamerstuk 33 009, nr. 63

Strategie voor Industrie en Innovatie 2025–2029 (D-SII)[43] en de Defensienota.[44] In deze Kamerstukken wordt ook de Wet weerbaarheid defensie- en veiligheid gerelateerde industrie aangekondigd, waarvan het marktreguleringshoofdstuk ook zal fungeren als sluitstuk op het beleid om de industrie te versterken.

- *Lange-termijn Ruimtevaartagenda (LTR)*
  De kabinetsreactie op de Lange-termijn Ruimtevaartagenda[45] geeft aan dat de samenleving sterk afhankelijk is van ruimtevaarttechnologie, met name op het gebied van aardobservatie, plaats- en tijdsbepaling en communicatie. Door gerichte keuzes die aansluiten op de bovengenoemde NTS zet het kabinet in op een belangrijke bijdrage van Nederland aan Europese autonomie op ruimtevaarttechnologie en daarmee het versterken van de economische veiligheid.
- *Start-up en scale-upbeleid*
  Het kabinet heeft de ambitie om van Nederland het nummer 1 startup- en scale-up ecosysteem van Europa te maken. Daarbij wordt extra ingezet op het stimuleren van kennisintensieve *(deeptech)* bedrijven. De regeling voor medewerkersparticipatie en het versterken van Invest-NL met aanvullende middelen dragen hier sterk aan bij. Bovendien werken we aan het mobiliseren van institutioneel kapitaal voor startups en scale-ups, onder meer via een *blended finance* faciliteit. Uw Kamer zal naar verwachting in Q3 geïnformeerd worden over de beleidsinzet om het ondernemingsklimaat voor startups en scale-ups te versterken.

Het doel van deze activiteiten is om sterke posities op te bouwen in waardeketens, om (technologische) leiderschapsposities te versterken en ook te profiteren van de kansen onder andere geboden door groene en digitale transities aan grote bedrijven, mkb en start-ups. Om dezelfde reden wordt ook in brede zin ingezet op het verhogen van de R&D-intensiteit van Nederland, in 2025 in het bijzonder met het reeds aangekondigde actieplan om toe te werken naar de 3% R&D-uitgaven van het BBP. In dit plan zullen beleidsopties geschetst worden voor het verhogen van (private) R&D-uitgaven, zodat we als Nederland bij de top van de wereld blijven horen op het gebied van onderzoek en ontwikkeling. Ook vergt het hebben van een sterke en concurrerende economie aantrekkelijker maken van de randvoorwaarden voor ondernemen in Nederland. In dit kader wordt er gewerkt aan het Pact Ondernemingsklimaat.

Kabinetsaanpak risicovolle strategische afhankelijkheden

Binnen deze kabinetsaanpak richten verschillende departementen zich doorlopend op het in kaart brengen van risicovolle strategische afhankelijkheden. Daarnaast werken de departementen voor de reeds geïdentificeerde risicovolle strategische afhankelijkheden op hun beleidsterreinen handelingsopties uit. Uw Kamer is afgelopen najaar laatstelijk geïnformeerd over de voortgang.[46] In 2022 is de interdepartementale Taskforce Strategische Afhankelijkheden (TFSA) opgericht. De TFSA speelt een centrale rol door de samenwerking tussen departementen te bevorderen en de identificatie en aanpak van risicovolle strategische afhankelijkheden aan te jagen. Mogelijke maatregelen binnen deze aanpak zijn zowel te typeren als *protect*, *promote*, *partner* als kennisopbouw.

---

[43] De DSII wijst vijf NLD gebieden aan: kwantum, slimme materialen, ruimtetechnologie, intelligente systemen en sensoren.
[44] Kamerstuk 31 125, nr. 134 en Kamerstuk 36 592, nr. 1
[45] Kamerstuk 24 446, nr. 90
[46] Kamerstuk 30 821, nr. 244

In lijn met de motie van het lid Idsinga, die verzoekt tot een aanpak met betrekking tot strategische voorraden,[47] werkt het kabinet in het kader van de TFSA reeds per geïdentificeerde risicovolle strategische afhankelijkheid handelingsopties uit. Het aanleggen van strategische voorraden is hierbij één van de mogelijke handelingsopties om risicovolle strategische afhankelijkheden te mitigeren. Over de invulling van de aanpak van de verdere versterking van onze vitale infrastructuur in het licht van militaire en hybride dreigingen verwacht het kabinet uw Kamer voor de zomer te informeren. Ook komt binnen de Wet weerbaarheid defensie- en veiligheid gerelateerde industrie de mogelijkheid om enkele ondernemingen aanwijzingen te geven ten aanzien van voorraadvorming.

Relevant is ook de motie van het lid Thijssen. Deze vraagt te onderzoeken welke ongewenste strategische afhankelijkheden er in de windenergiesector zijnen in de toekomst kunnen ontstaan, en hoe we deze afhankelijkheden kunnen afbouwen dan wel voorkomen.[48] Het kabinet voert een kosten-batenanalyse uit voor het afbouwen van strategische afhankelijkheden, zoals ook is gemeld in voornoemde Kamerbrief van 31 oktober 2024.[49] Het kabinet zal hierbij ook de windenergiesector betrekken. Indien gewenst kan uw Kamer na de zomer vertrouwelijk geïnformeerd worden over de eerste resultaten.

Verder zet het kabinet onder de Nationale Grondstoffenstrategie (NGS) op een aanpak om de leveringszekerheid van kritieke grondstoffen te vergroten, en risicovolle strategische afhankelijkheden in toeleveringsketens te verminderen, want ook de controle over kritieke grondstoffen wordt inmiddels geopolitiek ingezet. Het kabinet zet onder de NGS in op publiek-private routekaarten om waardeketens van productgroepen die essentieel zijn voor Nederland weerbaarder te maken, onder andere voor de digitale en energietransitie, defensie-industrie, vitale sectoren en strategische sectoren in groeimarkten. In lijn met de motie van het lid Van der Werf[50] zet het kabinet ook expliciet in op een aanpak om risicovolle afhankelijkheden voor de defensie-industrie te verminderen en het risico van mogelijke disrupties binnen die toeleveringsketens te mitigeren. Het kabinet werkt in dat kader ook aan het opzetten van twee pilots voor trajecten rondom voorraadvorming van kritieke grondstoffen, waarvan één voor de defensie-industrie. Het kabinet richt zich tevens op het vergroten van de verwerkingscapaciteit van kritieke grondstoffen, op hergebruik van kritieke grondstoffen en op het afsluiten van strategische partnerschappen met grondstofrijke landen, zowel bilateraal als in Europees verband. Zo zijn er bilaterale grondstoffenpartnerschappen afgesloten met Vietnam en Québec en draagt Nederland bij aan nadere invulling van de EU-partnerschappen met bijvoorbeeld Chili en Australië. Ook richt het kabinet zich op verduurzaming van internationale grondstoffenketens om stabiele(re) toeleveringsketens met minder disrupties te realiseren. Om effectieve keuzes te kunnen maken, is het nodig om inzicht te hebben in de waardeketens van kritieke grondstoffen en waar precies kwetsbaarheden zitten. Het Nederlands Materialen Observatorium (NMO) is met dat doel opgericht, om kennis over waardeketens van kritieke grondstoffen en hun belang voor Nederland op te bouwen, ontwikkelingen daarin structureel te analyseren en monitoren, en daarover advies te geven aan de overheid en bedrijven.

---

[47] Kamerstuk 32 852, nr. 333
[48] Kamerstuk 32 852, nr. 329
[49] Kamerstuk 30 821, nr. 244
[50] Kamerstuk 36 600 X, nr. 25

Op Europees niveau wordt ook ingezet op een aanpak voor het vergroten van Europese leveringszekerheid van kritieke grondstoffen, via de *Critical Raw Materials Act* (CRMA). Onder andere door de ontwikkeling van Europese kritieke grondstoffenketens, in samenwerking met grondstofrijke partnerlanden. Hiervoor zijn streefdoelen opgenomen in de CRMA, voor eigen winning, verwerking en recycling van kritieke grondstoffen door de EU. Een Europese aanpak is ook essentieel vanwege de Europese verwevenheid van de industrie. De activiteiten van het NMO sluiten ook aan bij de verplichte stresstesten, (risico)analyses en monitoring van waardeketen in Europees verband onder de CRMA.

Op het gebied van geneesmiddelen streeft het kabinet ernaar de risico's van strategische afhankelijkheden te verminderen. Zowel op nationaal als Europees niveau lopen analyses om risicovolle strategische afhankelijkheden in de geneesmiddelenketen te identificeren en mitigeren. Hierin neemt het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) het voortouw.[51] Mogelijke handelingsopties zijn het stimuleren van de productie van kritieke geneesmiddelen in Nederland en Europa en diversificatie van toeleveringsketens van geneesmiddelen. In het kader van *Important Projects of Common European Interest Med4Cure* zijn subsidies verstrekt, waaronder aan een project dat zich richt op de ontwikkeling van innovatieve productieprocessen voor geneesmiddelen en werkzame stoffen. Daarnaast draagt het Ministerie van VWS binnen de *Critical Medicines Alliance* bij aan een gezamenlijk plan om de productie van geneesmiddelen in Europa te stimuleren en het aantal aanbieders van geneesmiddelen voor Europa te vergroten. De Europese Commissie heeft op 11 maart jl. de *Critical Medicines Act* gepubliceerd. Daarin zijn een aantal aanbevelingen uit de *Critical Medicines Alliance* verwerkt. Het doel van dit voorstel is onder andere om de leveringszekerheid en beschikbaarheid van kritieke geneesmiddelen te verbeteren en daarmee open strategische autonomie van de Europese Unie te versterken. Het volledige kabinetsstandpunt op de *Critical Medicines Act* is aan uw Kamer via het gebruikelijke Beoordeling Nieuwe Commissievoorstellen (BNC)-proces voorgelegd.[52] Naast deze twee *promote*-initiatieven wordt in het kader van *partner* gewerkt aan het verder versterken van relaties met grote producerende landen van geneesmiddelen, zoals India.

Partner

Economische veiligheid vraagt om nauwe samenwerking tussen overheden, bedrijven en internationale partners.

Europese en internationale samenwerking

Nederland werkt bilateraal, in EU-verband en internationaal intensief samen om economische veiligheidsrisico's gezamenlijk aan te pakken. Daarbij hoort ook een positieve grondhouding ten opzichte van handelsakkoorden en strategische partnerschappen met derde landen, bijvoorbeeld omdat deze bijdragen aan de diversificatie van toeleveringsketens. De waardeketens van de industrie zijn over het algemeen Europees en internationaal georganiseerd, daarom heeft sterke Europese samenwerking de voorkeur en wordt bij het aangaan van partnerschappen in eerste instantie gezamenlijk opgetrokken binnen EU-verband. Een voorbeeld zijn de partnerschappen op het gebied van strategische technologieën, waaronder halfgeleiders. Door intensieve samenwerking met onze Europese partners en de implementatie van deze gezamenlijke beleidsinitiatieven, bouwen wij aan een veilige en concurrerende

[51] Kamerstuk 29 477, nr. 918
[52] Kamerstuk 22 112, nr. 4078

economische omgeving die ook in tijden van geopolitieke onzekerheden houvast biedt.

Publiek-private samenwerking

Het kabinet zet in op nauwe samenwerking met bedrijven op gebied van economische veiligheidsvraagstukken. Er zijn diverse tafels waarin het kabinet met het bedrijfsleven over het thema economische veiligheid spreekt. Zo organiseert het Ministerie van Economische Zaken sinds 2019 op periodieke basis op ministerieel en (hoog-)ambtelijk niveau sessies met het bedrijfsleven over economische veiligheid. De dialoog richt zich op het vergroten van de bewustwording, het signalen van risico's, het uitwisselen van *best practices* en het ontwikkelen van gezamenlijk handelingsperspectief. Deze dialoog zal de komende tijd worden voortgezet en geïntensiveerd.

Verder is recentelijk de Semicon Board Nederland opgericht, met vertegenwoordigers op ministerieel niveau, uit het kennis- en innovatie-ecosysteem en het bedrijfsleven. Tijdens de eerste bijeenkomst is met de leden afgesproken dat een gezamenlijke sectoragenda voor de halfgeleiderindustrie, inclusief een investeringsstrategie wordt opgesteld. De sectoragenda beoogt vorm en inhoud te geven aan de opgaven, ambities en investeringen die nodig zijn voor een internationaal toonaangevende en duurzame kennis- en industriepositie van de sector in 2035. Onderdeel van de board is een actietafel Europese weerbaarheid.

Daarnaast werken departementen en bedrijven in de nationale cryptostrategie samen om Nederland als crypto producerend land in het hoge vertrouwenssegment te behouden en te versterken. Het gaat hierbij om de ontwikkeling en productie van cryptografische beschermingsmiddelen op eigen bodem. Daarbij is een doel van de strategie om de overheid op de middellange en lange termijn te verzekeren van goede en duurzame middelen voor informatiebeveiliging.

Tot slot is aangekondigd dat een publiek-privaat geopolitiek en weerbaarheidsberaad wordt ingericht, waarvan de eerste bijeenkomst na deze zomer zal plaatsvinden.[53] Dit beraad heeft als doel leden van het kabinet, bedrijfsleven, kennisinstellingen en maatschappelijke partners in wisselende samenstelling regulier samen te brengen in een informele en vertrouwelijke setting om relevante ontwikkelingen te bespreken met het oog op versterking van onze weerbaarheid. Deze overleggen hebben een niet-besluitvormend karakter.

Ondersteuning bedrijfsleven

Om ondernemers wegwijs te maken in tijden van geopolitieke spanningen en EV-dreigingen is in opdracht van het Ministerie van Economische Zaken het Ondernemersloket Economische Veiligheid (OLEV) opgericht. Het OLEV, belegd bij de Rijksdienst voor Ondernemend Nederland (RVO), is het Rijksbreed aanspreekpunt economische veiligheid voor ondernemers. Het OLEV informeert actief over de dreigingen en het nemen van preventieve of mitigerende maatregelen, zoals op het gebied van personeelsbeleid, inkoop, cybersecurity, toeleveringsketens, investeringen, informatieveiligheid en de export van dual-use goederen. Ook vervult het loket een belangrijke adviesfunctie, waarbij het bedrijven voorziet van deskundige informatie. Het OLEV zal de komende jaren verder ontwikkeld worden om haar digitale toegankelijkheid en fysieke aanwezigheid in hightech ecosystemen te vergroten.

[53] Kamerstuk 30 821, nr. 249

Ook werken het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Centrum (DTC) gezamenlijk aan een Nederlands cybersecuritystelsel dat optimaal functioneert. Een Cyberweerbaarheidsnetwerk wordt ontwikkeld waarin met een brede groep aan publieke en private partners gecoördineerd samen zal worden gewerkt. Momenteel wordt gewerkt aan de integratie van het DTC, NCSC en Cyber Security Incident Response Team for Digital Service Providers (CSIRT-DSP), die eind 2025 is afgerond, zodat er één cybersecurity organisatie ontstaat. Via onder andere toegankelijke en praktische websites bieden het NCSC en DTC actuele en betrouwbare informatie over digitale dreigingen en kwetsbaarheden, en kennis voor het preventief verhogen van de weerbaarheid, aangevuld met concrete adviezen die bedrijven direct kunnen toepassen. Tevens faciliteren zij actieve *communities*, waar ondernemers met en van elkaar kunnen leren en samenwerken, waaronder in het Cyberweerbaarheidsnetwerk en de online DTC-community. Het Cyberweerbaarheidsnetwerk richt zich op 1) informatiedeling; 2) doelwit- en slachtoffernotificatie; 3) incidentenafhandeling; 4) opleiden/trainen/oefenen; en 5) kennisuitwisseling. Het programma Cyclotron richt zich op publiek-private samenwerking tussen overheid, bedrijfsleven en maatschappelijke organisaties. Het moet leiden tot een platform waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen.

Kennisopbouw

Effectieve en proportionele maatregelen op het gebied van economische veiligheid vragen een sterke kennispositie van de Rijksoverheid. Kennisopbouw is dan ook integraal onderdeel van de hiervoor genoemde beleidsinitiatieven. Daarnaast zijn er nog enkele governancestructuren die zich hier specifiek op richten:

- Het onder de Nationale Grondstoffenstrategie opgerichte Nederlands Materialen Observatorium (NMO) monitort structureel de waardeketens van voor Nederland belangrijke kritieke grondstoffen, en kwetsbaarheden daarin. Hiertoe werkt het NMO samen met andere kennisinstellingen, universiteiten, maatschappelijke organisaties en het bedrijfsleven, alsmede met andere Europese observatoria. De activiteiten van het NMO sluiten ook aan bij de verplichte stresstesten, (risico)analyses en monitoring van waardeketens in Europees verband onder de Europese *Critical Raw Materials Act*. Het NMO draagt daarmee bij aan de identificatie van (nieuwe) risicovolle strategische afhankelijkheden.
- Binnen de Kennisunit Sensitieve Technologie van de RVO ondersteunen technologisch experts het Ondernemersloket Economische Veiligheid, het Loket Kennisveiligheid en departementen desgevraagd bij specifieke vragen over sensitieve technologieën.
- Het Dreigingsbeeld Statelijke Actoren is een gezamenlijke analyse van de AIVD, MIVD en NCTV en heeft tot doel het bewustzijn te vergroten over de aard en omvang van de dreiging op nationale veiligheid vanuit statelijke actoren, waarop overheidsorganisaties, bedrijven en kennisinstellingen, hun beleid tegen statelijke dreigingen kunnen baseren.[54]

[54] Kamerstuk 30 821, nrs. 125 en 175