



Dep. **VERTROUWELIJK**

Contactpersoon

[REDACTED]
[REDACTED]

5.1.2e

Datum
9 juli 2019

Bijlagen
4

agenda

Task Force Economische Veiligheid

Omschrijving	Task Force Economische Veiligheid
Vergaderdatum en -tijd	11 juli 2019, 12:00-14:00 uur
Vergaderplaats	ICCb/MCCb zaal, NCTV

1. Opening en mededelingen

2. Vaststellen verslag 22-05-2019

3. Terugblik besluitvorming en parlementair proces (vertrouwelijke briefing, plenair debat)

Bijlage 1: TK Brief AIVD over Nationale veiligheid en concessies 5G

4. Uitwerking maatregelen

Mondelinge toelichting NCTV

5. Herooverweging voorzorgsmaatregel Kaspersky

Bijlage 2: TK Brief Reactie Kaspersky Lab inzake rol van de overheid en IT-branche in cybersecurity

Bijlage 3: Brief aan Kaspersky Lab

6. Internationaal

Bijlage 4: ~~Volgt 10-07~~ Input Europees risico-assessment 5G

7. Rondvraag en w.v.t.t.k.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

Kaspersky Lab

Papendorpseweg 79
3528 BJ Utrecht

5.1.2e

5.1.2e

Ons kenmerk
2481812

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 9 juli 2019

Onderwerp Uw brief van 1 maart 2019

Geachte [REDACTED],

5.1.2e

Op 1 maart 2019 heeft u, naar aanleiding van een gesprek tussen u en [REDACTED]

5.1.2e

[REDACTED], op 17 januari jl., een brief gestuurd aan het NCSC, [REDACTED], met als onderwerp "**Reactie: voorzorgsmaatregel uitfaseren gebruik antivirussoftware Kaspersky Lab, 27 juni 2018**". In dit gesprek heeft u aangegeven reden te zien voor heroverweging van de vorig jaar door het kabinet genomen voorzorgsmaatregel ten aanzien van de antivirussoftware van Kaspersky Lab.

5.1.2e

Deze voorzorgsmaatregel houdt, zoals is toegelicht in de brief aan de Tweede Kamer van 14 mei 2018 en de brief aan uw bedrijf van 27 juni 2018, in dat, vanwege de mogelijke risico's voor de nationale veiligheid, het gebruik van antivirussoftware van Kaspersky Lab bij de rijksoverheid wordt uitgefaseerd en dat aan vitale en ABDO-bedrijven wordt geadviseerd hetzelfde te doen.

In uw brief van 1 maart 2019 schetst u ten eerste de inspanningen van Kaspersky Lab ten behoeve van de digitale weerbaarheid van Nederland en de gevolgen voor Kaspersky Lab van bovenbedoelde voorzorgsmaatregel. Ten tweede verduidelijkt u in uw brief, aan de hand van de drie factoren waarvan onder meer in mijn brief aan uw bedrijf van 27 juni 2018 is vermeld dat die aanleiding zijn geweest voor genoemde voorzorgsmaatregel, waarom u meent dat deze aanleiding berust op verkeerde aannames. Die verduidelijking en de opening van een Transparency Center in Zurich waar diverse onderdelen van uw producten onder de loep genomen kunnen worden, geven volgens u reden tot heroverweging van deze maatregel.

Op 15 maart 2019 is de ontvangst van deze brief schriftelijk aan u bevestigd. Op 3 juni is aan u een brief gestuurd waarin, naar aanleiding van uw opmerking dat deze op verzoek zal worden verstrekt, om het rapport van de heer K. Hober, waarnaar u in uw brief verwijst, is verzocht. Bij brief van 19 juni 2019 is u bericht dat streven erop is gericht om binnen uiterlijk vier weken na ontvangst van uw reactie op de brief van 3 juni, te reageren op uw verzoek om heroverweging.

Ik heb het in uw brief vermelde verzoek om heroverweging van bovenbedoelde voorzorgsmaatregel bestudeerd. Naar aanleiding hiervan ben ik tot het oordeel gekomen dat er geen aanleiding is tot heroverweging van die voorzorgsmaatregel. Ik licht dit graag ter motivering als volgt toe.

Programma Nederland
Digitaal Veilig

Datum
9 juli 2019

Ons kenmerk
2481812

Uitgebreide en diepgaande toegang tot ICT-systemen

In uw brief schrijft u het ermee oneens te zijn dat antivirussoftware uitgebreide en diepgaande toegang tot ICT-systemen heeft en dat dergelijke software vanwege de uitgebreide toegang die deze biedt, ook misbruikt kan worden om digitale spionage en sabotage mogelijk te maken. U geeft daarvoor enkele redenen.

Uw stelling onder punt I dat antivirussoftware slechts op één systeem draait en daarom geen diepe en brede toegang tot ICT-systemen heeft, deel ik niet. Bij bedrijfsmatige netwerk- en informatiesystemen is antivirussoftware doorgaans geïnstalleerd op meerdere servers of werkstations die met elkaar in verbinding staan dan wel op een centrale plek in die systemen waar al het dataverkeer doorheen komt. Antivirussoftware heeft vergaande rechten op een systeem om goed te kunnen functioneren. Zonder die rechten zou de effectiviteit beperkt zijn. Om te kunnen doen wat het moet doen, heeft antivirussoftware diepgaande toegang tot systemen, onder meer de bestanden die erop staan, en moet deze die bestanden kunnen scannen en in quarantaine kunnen zetten bij detectie van malware of virussen.

De door u onder punt II genoemde maatregelen die Kaspersky Lab treft om de integriteit van producten te waarborgen sluiten de risico's op spionage en sabotage niet uit. Ook zonder telemetrie is compromittering van netwerk- en informatiesystemen bijvoorbeeld nog steeds mogelijk. In de broncode is niet na te gaan of de AV-handtekeningen kwetsbaarheden bevatten. Inzage in de softwarebroncodes biedt geen soelaas, gelet op de omvang van de code, de veranderlijkheid daarvan bij updates en de kleine, moeilijk vast te stellen afwijkingen daarin die zouden kunnen duiden op kwetsbaarheden of backdoors. Daaraan toegevoegd de omstandigheid, dat voor een betrokken organisatie die gebruik maakt van de antivirussoftware onder meer onvoldoende controleerbaar is welke data door die software wordt verzameld en waarnaar die wordt verstuurd, maakt dat de geschetste maatregelen uitgebreide en diepgaande toegang van antivirussoftware tot de systemen waarop deze geïnstalleerd is niet uitsluiten, noch dat deze toegang gebruikt kan worden ten behoeve van digitale spionage en sabotage. De opening van een Transparency Center in Zurich, waarvan u in uw brief melding maakt, doet aan het voorgaande niet af.

De Russische wetgeving

In uw brief geeft u, onder verwijzing naar een rapport van de heer Hober, aan dat uw bedrijf niet krachtens Russische wetgeving verplicht is om de Russische inlichtingendiensten desverzocht te ondersteunen in de uitvoering van hun taken.

In zijn rapport bespreekt de heer Hober het rapport van de heer P.B. Maggs, die wetgeving van de Russische Federatie heeft benoemd op grond waarvan onder meer private organisaties verplicht kunnen worden om medewerking te verlenen aan activiteiten van de Russische inlichtingendiensten. Over de toepasselijkheid van enkele wetsartikelen verschillen Hober en Maggs van mening. Het rapport van

de heer Hober betwist echter niet dat verschillende andere wetsartikelen wel van toepassing zijn. Dit rapport doet dan ook niet af aan de conclusie dat ondernemingen in de Russische Federatie de verplichting hebben om, bijvoorbeeld door het ophalen van digitale gegevens, de Russische inlichtingendiensten assistentie te verlenen. Daarbij wijs ik in het bijzonder op artikel 15 van de Wet op de federale veiligheidsdienst (no. 40-FZ) en artikel 6 van de Wet op operationele onderzoeksactiviteiten (no. 144-FZ). Hierdoor kan ook Kaspersky Lab daartoe verplicht worden. Dit geldt niet alleen voor bijvoorbeeld organisatoren van verspreiding van informatie, daargelaten of Kaspersky Lab al dan niet als zodanig kan worden aangemerkt.

Programma Nederland
Digitaal Veilig

Datum
9 juli 2019

Ons kenmerk
2481812

Het offensieve cyberprogramma van de Russische Federatie

Tenslotte benadrukt u in uw brief, ten aanzien van de capaciteiten die de Russische Federatie in het digitale domein ontwikkelt en hun onder meer op Nederland gerichte cyberprogramma, dat Kaspersky Lab een privaat en onafhankelijk bedrijf is en dat de meerderheid van uw activiteiten buiten Rusland plaatsvindt.

De jaarverslagen van de AIVD en de MIVD over 2018 schetsen – net als vorig jaar – het beeld dat de Russische Federatie een actief en offensief cyberprogramma heeft, dat zich onder meer richt op spionage en gericht is tegen Nederland en Nederlandse belangen. Het Cybersecuritybeeld Nederland 2019 bevat ditzelfde beeld. Dit wordt in uw brief ook niet betwist.

Voorts merk ik, in reactie op uw opmerking dat de afwegingen van een aantal landen inzake het gebruik van de antivirussoftware van Kaspersky Lab verschillen, op dat het kabinet, onder kennisneming daarvan, een eigenstandige beoordeling heeft uitgevoerd en vanwege de op basis daarvan gebleken mogelijke risico's voor de nationale veiligheid de bovengenoemde voorzorgsmaatregel heeft genomen. Van belang is dat deze afweging een risico-afweging is en dat, zoals in de Kamerbrief van 14 mei 2018 is benadrukt, er geen concrete gevallen van misbruik in Nederland bekend zijn.

Tenslotte verzoekt u om een besprekingsverslag van het gesprek dat op 17 januari 2019 tussen u en [REDACTED] heeft plaatsgevonden. Ten aanzien daarvan wordt u verwezen naar de brief van 1 februari 2019 die aan u is verstuurd en die de inhoud van dit gesprek weerspiegelt.

5.1.2e

Op grond van het voorgaande zie ik in uw brief geen aanleiding de voorzorgsmaatregel, zoals die u bij brief van 27 juni 2018 is medegedeeld, te heroverwegen.

Ik hecht er hierbij aan duidelijkheidshalve op te merken dat de vorig jaar genomen voorzorgsmaatregel alleen betrekking heeft op het gebruik van de antivirussoftware van Kaspersky Lab en er derhalve geen belemmering is als het gaat om het gebruik van andere producten van, of het aangaan van een samenwerking met, uw bedrijf door de rijksoverheid, vitale bedrijven en ABDO-bedrijven.

Daarnaast geldt uiteraard dat wanneer er in de aankomende periode sprake zal zijn van een wijziging van de omstandigheden op basis waarvan tot het nemen van bovengenoemde voorzorgsmaatregel is besloten, dit aanleiding kan zijn om dat besluit te heroverwegen.

Ik hoop u hiermee voldoende geïnformeerd te hebben.

Hoogachtend,
De Minister van Justitie en Veiligheid,

Programma Nederland
Digitaal Veilig

Datum
9 juli 2019

Ons kenmerk
2481812

Ferd Grapperhaus



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep-**VERTROUWELIJK**
TFEV leden

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon



5.1.2e

Datum
3 september 2019

Ons kenmerk

nota

Stand van zaken TFEV

1. Maatregel 1 en 2

Hieronder wordt de aanpak geschetst rond de volgende aangescherpte beveiligingsmaatregelen zoals opgenomen in de Kamerbrief van 1 juli:

1. Algehele aanscherping beveiligingsmaatregelen om de digitale weerbaarheid van mobiele communicatienetwerken & -diensten te verhogen;
2. Hogere eisen stellen aan de leveranciers van producten en diensten in de kritieke onderdelen in het telecomnetwerk.

Uitwerking maatregelen 1 en 2

- De algehele aanscherping van de beveiligingsmaatregelen en de hogere eisen aan de leveranciers worden verankerd in een algemene maatregel van bestuur (amvb) onder artikel 11a.1 van de Telecommunicatiewet. Hierin is namelijk bepaald dat aanbieders van openbare elektronische communicatienetwerken- en diensten passende technische en organisatorische maatregelen moeten treffen om de risico's voor de veiligheid en integriteit van hun netwerken en diensten te beheersen.
- Maatregel 1 wordt als volgt uitgewerkt: de amvb bevat een delegatiebepaling om bij ministeriële regeling nadere regels te kunnen stellen met betrekking tot de passende technische en organisatorische maatregelen. De daadwerkelijke technische en organisatorische maatregelen voor de mobiele netwerkaanbieders worden vervolgens in een ministeriële regeling opgenomen.
- Maatregel 2 wordt als volgt uitgewerkt: de amvb geeft de minister van EZK de bevoegdheid bij beschikking aan een telecomaandbieder een verbod op te leggen om in bepaalde, door de minister aangewezen onderdelen van het netwerk, gebruik te maken van producten of diensten van een 'aangewezen partij'. Gelijktijdig met deze beschikking wordt de nadeelcompensatie vastgesteld.



5.1.2i en
5.1.2a

Planning aanscherping maatregelen 1 en 2

- De amvb wordt in de periode van 26 augustus - 11 september interdepartementaal afgestemd en vervolgens in de Taskforce EV van 18 september, de Ambtelijke Commissie Economie en Veiligheid (ACEV) van 26

september en de Ministeriële Commissie Economie en Veiligheid (MCEV) van 8 oktober behandeld. De Ministerraad kan dan op 11 oktober besluiten de amvb voor spoedadvies aan de Raad van State voor te leggen. Publicatie van de amvb in het Staatsblad is begin december voorzien.

- Parallel aan de totstandkoming van de amvb wordt gewerkt aan de ministeriële regeling en de beschikkingen. Voor het opstellen van de ministeriële regeling met een aanscherping van technische en organisatorische maatregelen (maatregel 1) wordt in september een werkgroep onder leiding van EZK bijeengeroepen met deelname van leden van de technische werkgroep, mobiele netwerkaanbieders en [REDACTED]
- [REDACTED]
[REDACTED] De Taskforce wordt van het verloop hiervan op de hoogte gehouden. Planning is de concept-beschikkingen in november voor te leggen aan de Taskforce. [REDACTED]
[REDACTED]
[REDACTED]
- Het streven is om het gehele pakket aan regelgeving begin december af te ronden, vóór aanvang van de aanvraagtermijn voor de frequentieverdeling.

5.1.2i
5.1.2i en
5.2.1

5.1.2i

2. Communicatie richting Kamer

In de volgende Taskforce EV (18-09) wordt besproken hoe en wanneer de Kamer verder wordt geïnformeerd over maatregel 1 en 2/de AMvB.

3. Maatregel 3

- Deze maatregel betreft het opzetten van een structurele samenwerking met telecomproviders, waarbij ontwikkelingen in dreiging en techniek in samenhang worden gezien, passend bij de huidige verantwoordelijkheden en rollen.
- [REDACTED]
- [REDACTED]
- De uitwerking van deze maatregel wordt ter besluitvorming aan de Taskforce voorgelegd. De ambitie is om dit tegelijkertijd met het van kracht worden van de amvb, in december, vast te stellen.

5.1.2i

5.1.2i en
5.1.2

¹ Een Advanced Persistent Threat (APT) Aanvaller die instaat is langdurige geavanceerde cyberaanvallen uit te voeren. Veelal gelieerd aan overheden.

4. Voortgang EU traject

- De komende maanden wordt toegewerkt naar het EU-brede risk assessment (deadline 1 oktober). Het proces daarvoor ziet er als volgt uit:
 - Begin september zal de Commissie een concept-EU risico assessment delen met de co-voorzitters (NL, FRA, EST, TSJ, ROE, FIN).
 - De co-voorzitters, de Commissie en ENISA zullen 12 september gezamenlijk aan het concept werken, zodat een definitief concept in de week van 16 september aan de lidstaten verzonden kan worden.
 - Op 24 september zullen alle Lidstaten vergaderen over het concept, zodat ter goedkeuring kan worden voorgelegd aan de plenaire Cooperation Group (25 september).
 - Na afronding van het risk assessment zal worden gestart met ontwikkelen van de toolbox met mogelijke mitigerende maatregelen te nemen door Lidstaten en bedrijven.

Het verwerken van de ontvangen input vanuit de Lidstaten bleek meer werk voor de Commissie en ENISA dan door hen was voorzien. De planning is daarmee krap gebleken, en is de tijd voor afstemming met en tussen de Lidstaten zeer beperkt. Er leven bij de co-voorzitters vragen of het huidige tijdspad niet met enkele weken zou moeten worden opgerekt. Een dergelijke kleine verlenging, brengt het inhoudelijke traject niet in gevaar, maar zal naar verwachting wel leiden tot meer draagvlak bij de lidstaten. Nederland steunt de deadline van 1 oktober.

[REDACTED] De samenhang met andere lopende trajecten (o.a. EU 5G traject, bijeenkomsten van januari en mei 2019 met gelijkgezinde landen) wordt hierin meegenomen. Afhankelijk van wanneer de uitgewerkte Nederlandse maatregelen openbaar worden moet deze verklaring idealiter gereed zijn. [REDACTED]

5.1.2a

[REDACTED]

5.1.2a

5. Vervolgtrajecten

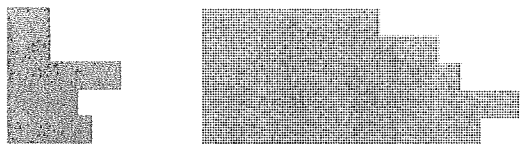
[REDACTED] NCTV schrijft hiervoor een voorstel voor en stemt dit interdepartementaal af.

5.1.1b

Eveneens wordt er een roadmap gemaakt voor de beoordeling van de overige vitale processen. Dit zal worden opgepakt binnen het bredere raamwerk van de aanpak zoals geformuleerd in de Kamerbrief van 1 juli (*Het ontwikkelen van een versterkte aanpak van bescherming van de vitale infrastructuur waarin kennis, kunde en expertise wordt gebundeld om nationale veiligheidsrisico's ten behoeve van de vitale infrastructuur, nu en in de toekomst, adequaat te adresseren*).

6. Overig

- Er zijn Kamervragen gesteld door GroenLinks (Buitenweg en Bromet) over 'het advies van de AIVD over de nationale veiligheid en veiling 5G'. De beantwoording is interdepartementaal afgestemd. De antwoorden hierop liggen nu voor bij MinJenV.
- Er is een WOB-verzoek ingediend door Politico waarin is verzocht om alle geschreven correspondentie en verslagen van vergaderingen tussen ministeries en agentschappen die verantwoordelijk zijn voor het telecommunicatie- en cybersecuritybeleid met Huawei Technologies in de periode van 1 december 2018 tot 8 juli 2019. Dit verzoek is aanvankelijk alleen ingediend bij EZK, maar inmiddels ter behandeling ook doorgestuurd naar JenV (NCTV) en BuZa.



[Redacted]

Van: [Redacted]

Verzonden: vrijdag 6 september 2019 16:52

5.1.2e

Aan: [Redacted]

[Redacted]

CC: [Redacted]

5.1.2e

[Redacted]

Onderwerp: TFEV: Schriftelijke update

Geachte Taskforce leden,

Hierbij ontvangt u een nota over de voortgang op het 5G-traject, dit ter vervanging van de Taskforce van afgelopen woensdag die geannuleerd werd. Er staat inmiddels een nieuwe TFEV gepland op woensdag 18 september, daarvoor heeft u vandaag een uitnodiging ontvangen.

We zullen in deze bijeenkomst de concept AMvB bespreken die de basis vormt voor maatregel 1 en 2 in het 5G traject. Daarnaast bespreken we hoe en wanneer de Kamer verder wordt geïnformeerd over deze maatregelen.

Vriendelijke groet en fijn weekend,

[Redacted]

5.1.2e

Ministerie van Justitie en Veiligheid

Turfmarkt 147 | 2511 DP | Den Haag

Postbus 20301 | 2500 EH | Den Haag

[Redacted]

5.1.2e



Dep. **VERTROUWELIJK**
leden van de TFEV

Contactpersoon

██████████

██████████

5.1.2e

Datum

13 september 2019

Bijlagen

3

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	18 september 2019, 13:30-15:00 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Vaststellen verslag 11-07-2019

Bijlage 1. Verslag TFEV 11072019

3. AMvB: inhoudelijke behandeling

Bijlage 2. Concept besluit veiligheid en integriteit telecommunicatie

4. Bespreken proces informeren Kamer en planning

Bijlage 3. Pakket juridische producten en planning

4. Parlementair

5. Internationaal

6. Rondvraag en w.v.t.t.k.

Vergaderschema Task Force

DATUM	TIJDSTIP
05-11-2019	15:00-17:00
09-01-2020	10:00-12:00



Dep.-VERTROUWELIJK

Datum
30 juli 2019

verslag

Task Force Economische Veiligheid

Omschrijving	Task Force Economische Veiligheid
Vergaderdatum en -tijd	11 juli 2019, 12:00-14:00 uur
Aanwezig	AIVD, AZ, BZ, BZK, DEF, EZK, FIN, NCTV, MIVD, Nationale Politie
Afwezig	BHOS

1. Opening en mededelingen

In het kader van de eerste bijeenkomst van de TFEV na het Kamerdebat over 5G begint de NCTV eerst met complimenten aan allen voor een succesvol doorlopen proces dat als blauwdruk voor toekomstige werkwijze kan dienen voordat de agenda wordt vastgesteld. Er zijn geen mededelingen of toevoegingen aan agenda.

2. Vaststellen verslag 22-05-2019

Met een enkele correctie wordt het verslag vastgesteld.

3. Terugblik besluitvorming en parlementair proces (vertrouwelijke briefing, plenair debat)

Bijlage 1: TK Brief AIVD over Nationale veiligheid en concessies 5G

Debat

De NCTV blikt terug op de besluitvorming rond 5G. De besluitvorming en het debat zijn goed verlopen. Bij het debat was een dunne bezetting maar de meeste partijen waren wel aanwezig. De NCTV spreekt zijn waardering uit richting de TFEV leden voor een soepele afstemming voor en tijdens debat. De vertrouwelijke briefing aan de Kamer heeft geholpen de Kamerleden goed te informeren waardoor het debat ook inhoudelijk goed gevoerd kon worden in afwachting van de AMvB. Bij de AMvB zal het debat scherper gevoerd kunnen worden. Tijdens het debat zijn verschillende moties aangenomen. De NCTV ligt de moties kort toe en zegt toe de moties aan het verslag toe te voegen (zie bijlages). Alle moties waren gericht aan EZK of JenV en het is helder wie wat doet.

EZK geeft aan dat bijna alle moties passen binnen het voorgenomen besluit en oplosbaar zijn de AMvB (m.u.v. motie van den Berg over eisen aan bij 5G betrokken bedrijven en aan de aandeelhouders van bij 5G betrokken bedrijven –

deze wordt deels opgepakt binnen de WOZT). Op hoofdlijnen kan gesteld worden dat de moties het Kabinetsbeleid ondersteunen.

Vertrouwelijke briefing

Ten aanzien van de vertrouwelijke briefing meldt de NCTV dat deze goed verliep zonder verrassingen. Het was een informatieve sessie voor de Kamerleden hoewel het niet duidelijk was of alle aanwezige Kamerleden ook alle stukken hebben (kunnen) lezen. Niet alle partijen waren vertegenwoordigd. Aanwezig waren VVD, D66, Groen Links, CDA en PvdA. De Kamerleden spraken in ieder geval hun waardering uit voor de briefing. Geen van de aanwezige Kamerleden heeft vraagtekens gezet bij het proces en de vertrouwelijkheid van de briefing. Hier is ook geen punt van gemaakt in het plenaire debat.

Kamerbrief met brief AIVD en MIVD

De NCTV licht toe dat afgelopen week de Volkskrant kopte met artikel over het advies van de AIVD en MIVD ten aanzien van 5G dat niet bij de Kamerbrief was gevoegd. Hierover ontstond in de media en politiek ophef waarbij de minister van JenV onder vuur kwam te liggen met het verwijt dat deze de Kamer onvolledig zou hebben geïnformeerd. Dit zorgde ervoor dat er in de loop van de dag grote politieke druk ontstond resulterend in een instructie dat er een Kamerbrief met de brief van AIVD en MIVD binnen een ½ uur, voor het 20:00 uur journaal, uit moest.

5.2.1

EZK voegt hier aan toe dat het Kamerlid Verhoeven op Radio 1 heeft aangegeven dat hij een hoorzitting wil naar besluit kabinet.

5.2.1 en
5.1.2i

5.2.1 en 5.1.2i

5.1.2a

4. Uitwerking maatregelen

Mondelinge toelichtingen

Maatregel 1 en 2 (EZK)

EZK licht toe dat maatregel 1 en maatregel 2 van het Taskforce advies uitgevoerd worden in lagere wetgeving (AMvB). In de AMvB wordt de mogelijkheid opgenomen van een ministeriele regeling waardoor aanvullende of gewijzigde veiligheidsmaatregelen kunnen worden opgelegd aan de telecomsector. De planning voor het in werking treden van de AMvB is afhankelijk van de besluitvormende en behandelende gremia. De planning ziet er ruwweg als volgt uit:

- Ambtelijke afstemming is voorzien van half augustus – 2 september;
- Afstemming voor de MCEV is voorzien in de eerste helft van september;
- Voor de Raad van Staten is een spoedprocedure van 4 weken voorzien;
en
- Planning is om begin november in het staatsblad te publiceren.

Er wordt geen rekening gehouden met nog een debat in de Kamer en er is niet voorzien in een formele consultatie. Er wordt wel afgestemd met de telco's.

Afgesproken wordt de TFEV te gebruiken om het ambtelijk proces te bewaken.

NCTV vraagt m.b.t. AMvB of Groen Links er niet van uit gaat dat er nog een debat over het AMvB komt. Men wil geen onomkeerbaar besluit voordat er een debat heeft plaatsgevonden. De behandeling van het AMvB zou dat moment moeten zijn. Zou dit niet op zijn minst politiek moeten worden gesondeerd in de coalitie?

[REDACTED]

5.2.1

EZK geeft verder aan dat de AMvB zeer technisch is. Vraag is wat de Kamer wil. Wil men ingaan op de technische details of de discussie op hoofdlijnen voeren?

[REDACTED]

5.1.2i en
5.2.1

[REDACTED]

Afgesproken wordt dat de Taskforceleden komende maand in de eigen lijn sonderen of een politieke behandeling wenselijk is en zo ja, in welke vorm. In de volgende TFEV zal dit punt terugkeren.

Afgesproken wordt dat de technische werkgroep meekijkt en participeert op de uitwerking van maatregel 1 en 2.

Maatregel 3 (NCTV)

Onder coördinatie van de NCTV is er een werkgroep van start gegaan bestaande uit AIVD, MIVD, EZK, AT, NCSC en NCTV. Planning is om telecomaanbieders in een later stadium te betrekken. Momenteel wordt er een concept procesvoorstel voor een doorlopende aanpak uitgewerkt. [REDACTED]

5.1.2i

[REDACTED] In de komende periode zal dit verder worden uitgewerkt met EZK, AT, AIVD, MIVD en NCSC en aan de TFEV worden voorgelegd. Bij de uitwerking van maatregel 3 wordt er rekening mee gehouden dat het proces ook bruikbaar is voor andere vitale sectoren. Kanttekening die hier wel bij moet worden gemaakt, is dat implementatie van het proces kan variëren al naar gelang de sectorale wetgeving die van toepassing is.

Het tijdpad voor het uitwerken van maatregel 3 loopt gelijk op met het tijdpad van de AMvB.

BZK vraagt of de TFEV een positie krijgt in het proces.

NCTV geeft aan dat in de aanpak die wordt vormgegeven de TFEV een positie krijgt in het proces van het bepalen van de veiligheidsmaatregelen voor de vitale sectoren.

Defensie wijst op het ABDO kader dat werkt via contracten en is een privaatrechtelijke constructie. Keuze voor een dergelijke constructie kan vrijblijvend werken.

NCTV licht toe dat de aanpak die wordt uitgewerkt geen privaatrechtelijke constructie is. De maatregelen voor de telecomsector worden vastgesteld middels de ministeriele aanwijzingen, een voorziening die in de AMvB wordt geregeld.

EZK vraagt hoe AT in de aanpak van maatregel 3 wordt gepositioneerd.

NCTV geeft aan dat AT meewerkt aan het uitwerken van maatregel 3 en er daarbij op toeziet dat de positie van AT goed wordt geborgd. Er wordt voor gewaakt dat er geen dingen dubbel gebeuren.

Afgesproken wordt dat de NCTV na de zomer een routeplan voor het doorlopen van de andere vitale sectoren zoals in het 5G traject in de TFEV agendeert.

De Politie vraagt of het mogelijk is dat de Technische werkgroep van de TFEV kennis en kunde deelt met de werkgroep opsporing ([REDACTED]). Doel zou moeten zijn om samen, op het niveau van medewerkers, processen te doorlopen t.b.v. kennisniveau. Het wordt door de Politie als een grote winst beschouwd hoe de TFEV het 5G proces met alle partijen heeft doorlopen. De werkwijze is onderdeel van de aanpak. De werkgroep opsporing valt niet onder de TFEV maar de vertegenwoordiger van de Politie kan wel een link leggen.

5.1.2i

Afgesproken wordt dat de werkgroep opsporing het initiatief neemt om een overleg in te plannen tussen de werkgroep opsporing en de technische werkgroep 5G.

5. Heroverweging voorzorgsmaatregel Kaspersky

Bijlage 2: TK Brief Reactie Kaspersky Lab inzake rol van de overheid en IT-branchen in cybersecurity

Bijlage 3: Brief aan Kaspersky Lab

De NCTV licht toe dat Kaspersky schriftelijk heeft gevraagd om de maatregel ten aanzien van Kaspersky antivirussoftware (advies uit te faseren bij Rijk, vitaal en ABDO bedrijven) te heroverwegen. Bij de stukken zijn twee concept-brieven gevoegd betreffende het verzoek van Kaspersky om heroverweging van de vorig jaar mei door het kabinet genomen voorzorgsmaatregel:

- een schriftelijke reactie aan Kaspersky Lab op hun verzoek, en
- een Kamerbrief o.v.v. de VKC J&V n.a.v. een e-mail van Kaspersky Lab

Deze brieven zijn reeds op werkniveau met de aanwezige departementen afgestemd. In die afstemming zijn geen inhoudelijke verschillen van inzicht uit naar voren gekomen.

Na de TFEV zullen beide stukken met de eventuele laatste wijzigingen van de Taskforceleden de lijn in gaan richting de minister JenV. Hoewel het reces al begonnen is, heeft Kaspersky gedreigd met het treffen van rechtsmaatregelen als zij niet binnen twee weken een reactie ontvangen. Schriftelijk is aan Kaspersky, naar aanleiding hiervan, medegedeeld dat ernaar wordt gestreefd om binnen vier weken, dat wil zeggen uiterlijk op 15 juli a.s., een inhoudelijke reactie op het verzoek om heroverweging te zullen sturen. Om de Tweede Kamer gelijktijdig te informeren, wordt diezelfde week, en dus in het reces, ook de Kamerbrief verzonden, gelet op de mogelijke publiciteit die Kaspersky zal zoeken naar aanleiding van dit besluit.

De brief aan Kaspersky Lab behandelt de inhoudelijke bezwaren die Kaspersky Lab heeft geuit ten aanzien van de drie factoren die vorig jaar de reden hebben gevormd voor het nemen van de voorzorgsmaatregel. Deze brief bevat, na bespreking hiervan, de conclusie dat er geen aanleiding wordt gezien voor heroverweging van die maatregel.

De Kamerbrief bevat een toelichting op de motivering van de maatregel van vorig jaar, de vermelding van de reactie op het verzoek om heroverweging, en een reactie op het verwijt van Kaspersky dat het kabinet geen objectieve richtlijnen heeft gehanteerd.

De brieven zijn afgestemd met de landsadvocaat, dit met name ook met het oog op de rechtszaak die Kaspersky Lab heeft aangekondigd waarschijnlijk te zullen starten als de maatregel niet wordt teruggedraaid. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

5.1.2i

[REDACTED]

5.1.2i

[REDACTED]

5.1.2i

[REDACTED]

5.1.2i

De TFEV heeft geen opmerkingen bij de brieven.

Afgesproken wordt dat de TFEV wordt meegenomen in verdere ontwikkelingen ten aanzien van Kaspersky

6. Internationaal

Bijlage 4: Input Europees risico-assessment 5G

Op basis van de aanbeveling van de Europese Commissie dienen alle EU-landen een nationaal risk assessment voor 5G-netwerken te doen en de uitkomsten hiervan aan te leveren. De deadline hiervoor is 15 juli. Bijgevoegd sjabloon bij de TFEV stukken is ingevuld op basis van de nationale risico-inschatting 5G. Verschillende departementen (EZK, NCSC, AIVD) hebben input geleverd op deze sjabloon en die is vervolgens samengevoegd door de NCTV in samenwerking met TNO. [REDACTED]

5.1.2a

BZ geeft aan dat het de voorkeur heeft uitgebreid te rapporteren. Nederland heeft een voortrekkersrol in dit traject. Dat creëert verplichtingen.

Afgesproken wordt dat BZ na gaat hoe andere landen de uitvraag invullen. Op basis daarvan zal worden bepaald wat er wordt aangeleverd bij de Europese Commissie.

7. Rondvraag en w.v.t.t.k.

Geen WVTTK

Pakket juridische producten en planning

Het pakket juridische producten waarin de maatregelen 1 en 2 uit de Taskforcerapportage worden uitgewerkt bestaat uit:

- **Amvb Besluit veiligheid en integriteit telecommunicatie**
 - ACEV 26 september
 - MCEV 8 oktober
 - Ministerraad 11 oktober
 - Spoedadvies Raad van State (4 weken: omstreeks 15 november ontvangst advies)
 - Vertrouwelijke bespreking TK eind november (*is afhankelijk van bespreking TFEV*)
 - *Publicatie amvb in Staatsblad: eerste week december*
 - Directe inwerkingtreding
- **Beschikkingen Agentschap Telecom aan aanbieders van mobiele netwerken**
 - Geen openbare publicatie, bekendmaking uitsluitend door vertrouwelijke toezending aan de betreffende netwerkaanbieder (kritieke onderdelen STG).
 - Voor de rechtmatigheid van de beschikking is duidelijkheid over nadeelcompensatie (het beoordelingskader) vereist.
 - Grondslag = artikel 2, lid 2, van de amvb, toezending moet daarom gelijk met of na inwerkingtreding van de amvb (december 2019).
 - [REDACTED] 5.1.2i
 - [REDACTED]
 - [REDACTED]
- [REDACTED] 5.1.2i
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- **Ministeriële regeling EZK beveiligingsmaatregelen (maatregel 1 Taskforcerapportage)**
 - Afhankelijk van de precieze invulling van de beveiligingsmaatregelen zal de regeling technische voorschriften bevatten die genotificeerd moeten worden. Hiervoor geldt in beginsel een stand still-periode van 3 maanden, waarin de regeling nog niet kan worden vastgesteld. Hierop is een uitzondering mogelijk in geval van urgente situaties, zoals onderhavige. Of de stand still hier daadwerkelijk niet in acht hoeft worden genomen is echter ter beoordeling aan de Europese Commissie.
 - Publicatie en inwerkingtreding van de overige juridische stukken is niet afhankelijk van de ministeriële regeling. Een stand still zou dus uitsluitend leiden tot latere inwerkingtreding van de aanvullende beveiligingsmaatregelen als bedoeld in maatregel 1 uit de Taskforcerapportage.
 - *Publicatie regeling in Staatscourant: eerste week december (tenzij stand still in acht moet worden genomen)*
 - Directe inwerkingtreding



Dep. **VERTROUWELIJK**
leden van de TFEV

Datum
11 oktober 2019

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	5 november 2019, 15:00-17:00 uur
Vergaderplaats	NCTV

- | | | |
|--|---------------|--------|
| 1. Opening en mededelingen | 5 min | |
| 2. Vaststellen verslag TFEV 18-09-2019 | 5 min | |
| <i>Verslag TFEV 18092019 is eerder verspreid via de beveiligde lijn.</i> | | |
| 3. Voortgang AMvB, MR en beschikkingen | 20 min | |
| <i>Mondeling door ██████████.</i> | | 5.1.2e |
| 4. Voortgang Structurele samenwerking | 25 min | |
| <i>Mondeling door ██████████.</i> | | 5.1.2e |
| 5. Internationaal | 10 min | |
| <i>Mondeling door ██████████.</i> | | 5.1.2e |
| 6. Parlementair | 5 min | |
| 7. Rondvraag en w.v.t.t.k. | 10 min | |



Ministerie van Economische Zaken

Stand van zaken

Maatregel 1 en 2 TFEV

7 november 2019



Doel

- Kamerbrief 1 juli (**maatregel 1**):

*"De Taskforce heeft met medewerking van de drie grote telecomaانبieders (KPN, T-Mobile en VodafoneZiggo) een risicoanalyse uitgevoerd naar de kwetsbaarheid van telecommunicatienetwerken voor misbruik via leveranciers van technologie. Telecomaانبieders treffen al verscheidene maatregelen hiertegen. **Op basis van deze analyse zullen telecomaانبieders worden verplicht om aanvullende beveiligingsmaatregelen te nemen om de weerbaarheid tegen bovenbedoelde dreiging te verhogen.**"*



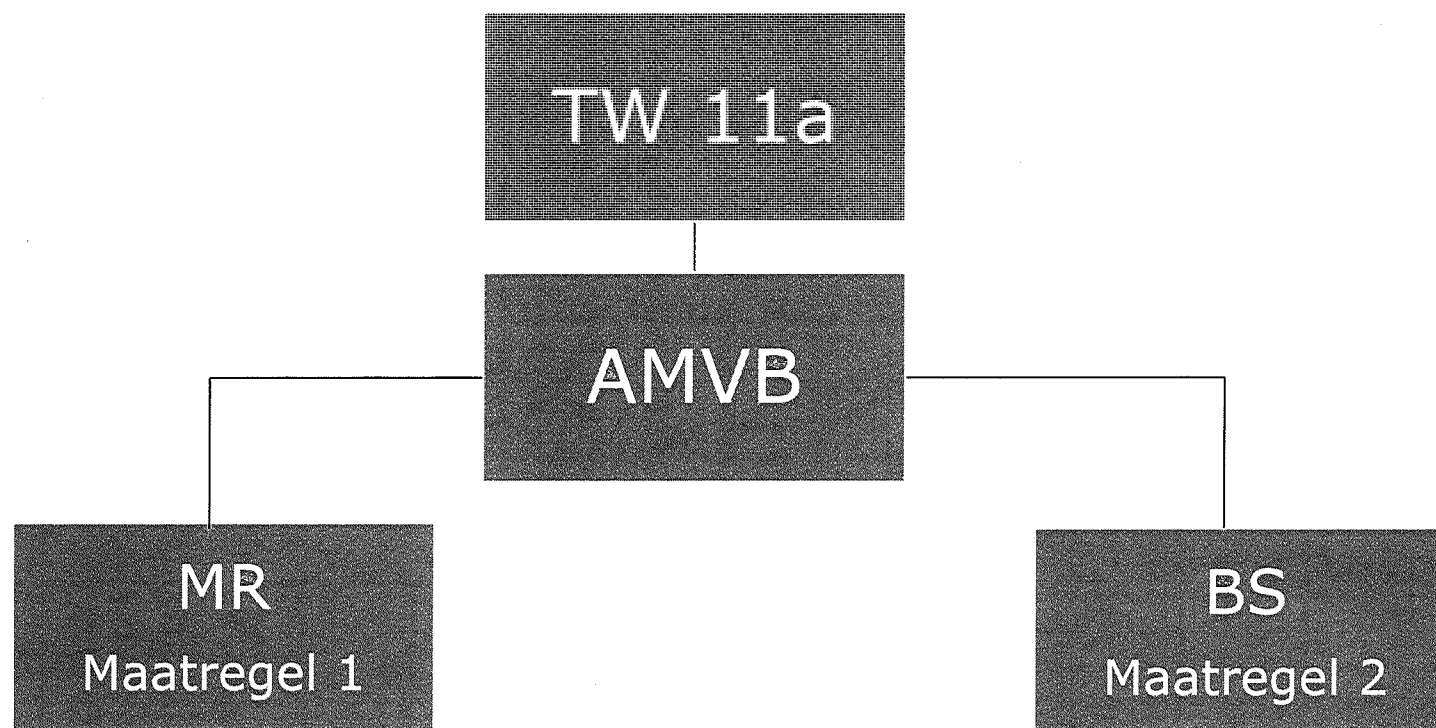
Doel

- Kamerbrief 1 juli (**maatregel 2**):

Daarnaast worden er extra hoge eisen gesteld aan leveranciers van diensten en producten in de kritieke onderdelen in het telecomnetwerk.



Juridische inbedding maatregel 1 en 2





AMVB

- Regelt bevoegdheden voor MEZK voor het stellen van nadere regels als bedoeld in maatregel 1 en 2
- Medio oktober voorgelegd voor spoedadvies aan RvS
- Advies RvS ontvangen 31 oktober
- Na verwerking advies RvS (vertrouwelijke) briefing TK
- Publicatie in Staatsblad voorzien in december/januari

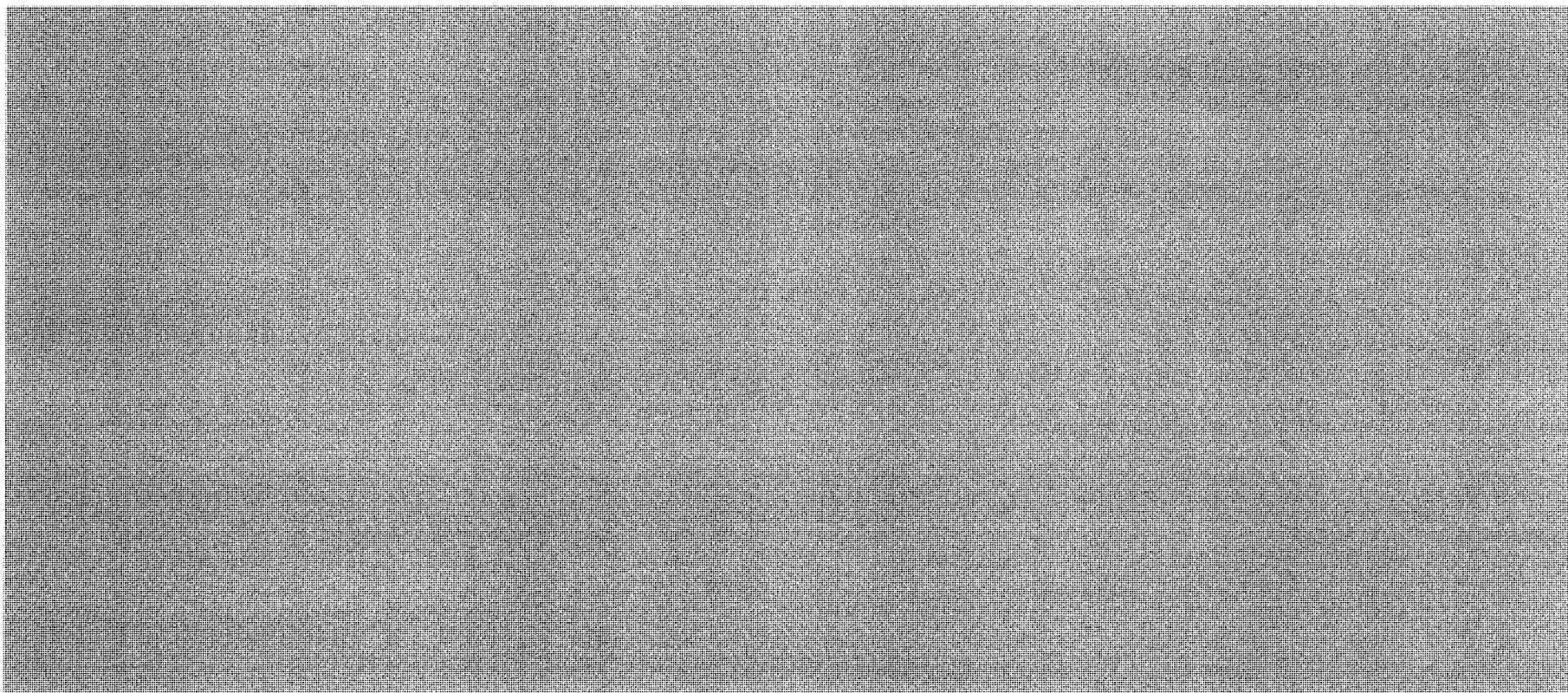


Maatregel 1: uitgangspunten

- Zowel bestaande als aanvullende maatregelen 5.1.2i
- Behoud eigen verantwoordelijkheid operator en flexibiliteit (zoals aan kunnen sluiten op specifieke situatie operator)
- Toekomstbestendig
- Uitvoerbaar & handhaafbaar
 - ✓ Waar mogelijk erkende normen gebruiken (ISO, NIST, ...)
 - ✓ Eenduidig en toetsbaar
 - ✓ Orthogonaal (geen overlap, niet tegenstrijdig)



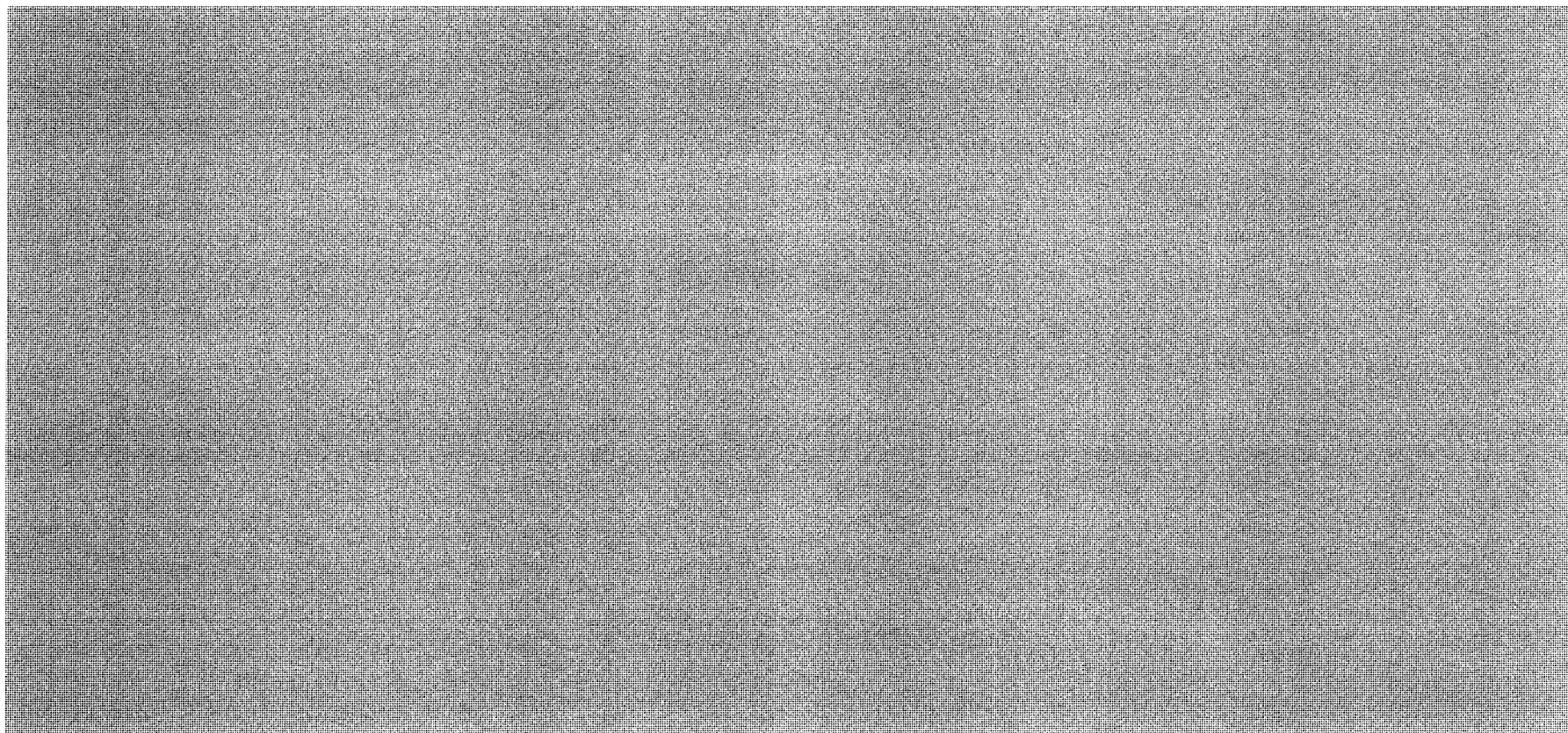
5.2.1





Uitwerking (2)

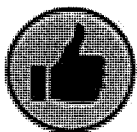
5.2.1





Planning

- | | | |
|--|------------------|--------|
| • Afstemming aanpak met MNO's | 10 oktober | |
| • Afstemming aanpak interdepartementaal | 17 oktober | |
| • Uitwerking maatregelen | oktober/november | |
| ✓ Sessies met technische wg en MNO's | | 5.1.2i |
| • Concept rapport uitwerking maatregelen | 1 december | 5.1.2i |
| • Bespreking MR interdepartementaal | begin december | |



- Bespreking MR in TFEV
- U&H toets AT, internetconsultatie
- Notificatie EC
- Publicatie Staatscourant



Maatregel 2

Stellen van extra hoge eisen aan leveranciers van diensten en producten in de kritieke onderdelen in het telecomnetwerk.



Stappen

- Opstellen concept beschikkingen
- Opstellen nadeelcompensatiekader
- Vragen zienswijze MNO's op beschikkingen en kader
- Definitieve beschikkingen (met kader) versturen

• [Redacted]

5.1.2i en 5.2.1

[Redacted]

[Redacted]



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**
leden van de TFEV

Datum
11 december 2019

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	18 december 2019, 12:30-14:30 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Vaststellen verslag TFEV 05-11-2019

Verslag TFEV 18092019 is eerder verspreid via de beveiligde lijn.

3. Voortgang AMvB, MR en beschikkingen

Bijlage 1. Ministeriele regeling beveiligingsmaatregelen

4. Voortgang structurele samenwerking

5. Inventarisatie versterkingsmaatregelen EV, vitaal & cyber

Bijlage 2. Inventarisatie versterkingsmaatregelen EV, Cyber en vitaal

6. Internationaal

7. Parlementair

8. Rondvraag en w.v.t.t.k.

Bijlage 3. Woordvoeringslijnen AMvB 5G nationaal en internationaal

Ministeriële regeling beveiligingsmaatregelen

Aanleiding

In de vorige Taskforce Economische Veiligheid (TFEV) van 5 november vroeg de MIVD wat er wordt verstaan onder 'threat hunting capability' (één van de door [REDACTED] voorgestelde beveiligingsmaatregelen en vermeld in de presentatie van EZK). Ook kwam in de vorige TFEV de vraag aan de orde voor welke aanbieders de ministeriële regeling zou moeten gelden. Op beide punten wordt hieronder ingegaan.

5.1.2i

1. **Wat is threat hunting capability?** Aanbieders monitoren normaliter realtime hun systemen. Dit wordt ook gelogd. Als er afwijkingen worden geconstateerd, dan kunnen analisten dit verder onderzoeken en indien nodig worden maatregelen getroffen.
Bij "threat hunting" worden de loggegevens van de systemen - bijvoorbeeld over een bepaalde periode - nader geanalyseerd vanuit een nieuw gesignaleerde risico of dreiging. De historische systeemgegevens worden dus bekeken vanuit de invalshoek van dat nieuwe risico of die dreiging. Het kan zijn dat alsnog afwijkingen worden gesignaleerd. Ook dan kunnen die worden onderzocht en kunnen maatregelen worden getroffen.

2. De reikwijdte van de ministeriële regeling

[REDACTED]

[REDACTED]

[REDACTED]

5.1.2i

Toelichting

Op dit moment wordt de ministeriële regeling nader uitgewerkt:

- Het op 5 december gepubliceerde besluit "veiligheid en integriteit telecommunicatie" bevat de grondslag om bij ministeriële regeling beveiligingsmaatregelen aan alle "aanbieders van een openbaar elektronisch communicatienetwerk en/of -dienst" op te kunnen leggen.
- In het dit voorjaar door de TFEV verrichtte onderzoek is er gekeken naar "aanbieders van mobiele telecomdiensten die daarvoor een eigen technische infrastructuur onderhouden". Het zijn aldus de MNO's, de mobiele netwerk operators KPN, VodafoneZiggo en T-Mobile die bij de totstandkoming van het TFEV-rapport (middels een risico-analyse) waren betrokken en nu bij de uitwerking van de ministeriële regeling. De beveiligingsmaatregelen die met de ministeriële regeling aan de MNO's worden opgelegd zijn te rechtvaardigen vanuit (nationale) veiligheid.

- [REDACTED]

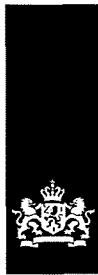
5.1.2i

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Dep. **VERTROUWELIJK**
TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

nota

Inventarisatie versterkingsmaatregelen EV, Cyber en
vitaal

Datum
9 december 2019

Ons kenmerk
-

Aanleiding

- Vorige Taskforce Economische Veiligheid (5 november) is gesproken over de structurele samenwerking die wordt opgericht voor telecom en de benodigde middelen hiervoor. Er is toen besloten om in de volgende Taskforce een bredere verkenning uit te voeren naar een 'vitaal brede' structurele samenwerking.
- Gezien de nauwe verwevenheid van deze structurele samenwerking met maatregelen op het gebied van economische veiligheid, cyber security en de bescherming van vitale infrastructuur, is een eerste interdepartementale inventarisatie van geplande en mogelijke aanvullende maatregelen voor deze onderwerpen uitgevoerd.
- In de bijlage zijn de uitkomsten van deze eerste verkenning opgenomen. Deze zijn opgeknipt in twee delen:
 1. Maatregelen die voorzien of mogelijk zijn op de korte termijn (2020 en 2021) en
 2. Maatregelen op de langere termijn (2022 – nieuwe kabinet).

Gevraagd besluit

1. Kennisnemen van de inventarisatie van geplande en mogelijke aanvullende maatregelen op het gebied van economische veiligheid, cybersecurity en vitaal.
2. Akkoord gaan met nadere uitwerking van dit traject op basis van deze inventarisatie van maatregelen.
3. Vaststellen welke aanvullende (in bijlage aangegeven als 'nog niet geplande') maatregelen verder uitgewerkt kunnen worden.
4. Afspraken maken over verdere uitwerking en financiering voor korte termijn maatregelen. Hierbij zijn de volgende opties van toepassing:
 - A. Reeds geplande en mogelijk aanvullende maatregelen opvangen binnen eigen begroting.
 - B. Gezamenlijke claim uitwerken voor begroting 2020/2021. *N.B. zeer kort dag, formele deadlines voor aanleveren al gesloten.*
5. Akkoord gaan met voorstel om de lange termijn maatregelen gezamenlijk uit te werken richting het Regeerakkoord.

Toelichting

Onderbouwing voor aanvullende maatregelen

- De kern van de Nederlandse vitale processen – telecom, data-communicatie en energie – is in toenemende mate afhankelijk van digitale technologie.
- Statelijke actoren maken vanuit geopolitieke motieven steeds vaker misbruik van digitale kwetsbaarheden. Dat doen ze rechtstreeks maar ook via *supply chain attacks*, zoals o.a. beschreven in het meest recent CSBN en het WRR-rapport "Voorbereiden op digitale ontwrichting". Daarnaast worden overnames en investeringen ingezet voor geopolitieke doeleinden.
- De afgelopen jaren is door de diverse veiligheidspartners flink geïnvesteerd in cyber security en zijn stappen gezet in de aanpak van statelijke dreigingen. Hierdoor is er beter inzicht ontstaan in onze te beschermen belangen, de dreiging en kwetsbaarheden.
- De casussen met betrekking tot het gebruik van Kaspersky antivirussoftware, Pulse-VPN-kwetsbaarheden en de uitrol van een nieuw 5G netwerk in Nederland illustreren de kwetsbaarheden in Nederland.
- Op casuïstiekbasis zijn nu maatregelen genomen. De aard en omvang van de dreiging vragen om structurele borging en uitbouw van deze maatregelen. Zoals het WRR-rapport ook aantoont, zijn daarnaast structurele maatregelen nodig om de basis op orde te brengen, inclusief herstelvermogen.
- Daarmee zijn op korte termijn maatregelen nodig, toewerkend naar de lange termijn.

Toelichting begrotingsproces en opties

Op dit moment worden de voorjaarsnota van 2020 en de begroting van 2021 voorbereid (loopt parallel). In maart 2020 gaan de beleidsbrieven uit. Naar verwachting is de voorjaarsnota in 2021 beleidsarm vanwege de verkiezingen. De voorjaarsnota van 2020/begroting van 2021 lijkt daarmee het enige moment om op korte termijn structureel extra middelen te ontvangen.

Voor optie B en C geldt dat er duidelijkheid moet zijn over hoe de betrokken departementen eventueel nieuw beleid binnen de huidige budgettaire kaders gaan dekken of dat aanvullende middelen geclaimd worden.

Korte termijn

Er is een aantal maatregelen waarbij op korte termijn al extra middelen noodzakelijk of gewenst zijn. Optie A (binnen eigen begroting opvangen) zal (moeten) leiden tot herprioritering bij de betrokken departementen. Bij optie B (een gezamenlijke claim) daarentegen worden er extra middelen vrijgemaakt, maar kan wel het risico ontstaan dat toekomstig gerelateerde claims minder kans maken. Ook geldt hiervoor een zeer korte deadline; op dit moment loopt de voorbereiding voor de voorjaarsnota al.

Lange termijn

Maatregelen voor de lange termijn verdienen nog verdere uitwerking. Door dit gezamenlijk uit te werken richting het regeerakkoord is er tijd om een integrale en goed onderbouwde claim op te stellen. Hierbij is ruimte voor game changers (grote investeringen) en kan worden aangesloten bij de uitkomsten van de Brede Maatschappelijke Heroverwegingen.

Relatie met eerder ontvangen gelden

- Bij Regeerakkoord zijn aanvullende middelen voor cybersecurity beschikbaar gesteld, die oplopen tot 95 miljoen structureel. Deze middelen worden besteed aan capaciteit en expertise bij operationele diensten, zoals Defensie, beide inlichtingen- en veiligheidsdiensten en het Nationaal Cyber Security Centrum (NCSC). Daarnaast worden de middelen ingezet voor capaciteit, awareness-building, kennisontwikkelingen en onderzoek bij IenW (Rijkswaterstaat) en EZK. Deze middelen zijn toegekend naar aanleiding van een (grotere, +- 330 mln.) gezamenlijke cyberclaim onder coördinatie van de NCTV.
- HGIS gelden met betrekking tot China notitie: In het voorjaar van 2019 is de China notitie gepresenteerd. Er is toen 24 miljoen toegewezen voor bijstelling van het Nederlandse Chinabeleid. Bij het verder uitwerken van een claim voor EV, cybersecurity en vitaal wordt nagegaan voor welke onderwerpen reeds aanvullende middelen zijn toegewezen.
- Innovatiefonds: Kan onder meer zien op stimuleren onderzoek en ontwikkeling. Bij vervolg uitwerken van de hiervoor gestelde claim voor EV, cybersecurity en vitaal kan nader gekeken worden naar mogelijke overlap.

Woordvoeringslijn 5G nationaal

- Het kabinet (uitkomsten Taskforce Economische Veiligheid) heeft in juli zijn aanvullende maatregelen aangekondigd om telecommunicatiediensten, zoals de toekomstige 5G-netwerken, te beschermen tegen dreigingen als spionage en sabotage.
- Eén van deze maatregelen is de mogelijkheid van het stellen van extra hoge eisen aan leveranciers van diensten en producten.
 - Telecomaanbieders zullen verder worden verplicht om aanvullende beveiligingsmaatregelen te nemen om de weerbaarheid tegen bovenbedoelde dreiging te verhogen.
 - Een structurele aanpak is nodig omdat er continu ontwikkelingen zijn in het dreigingsbeeld, omdat technologische ontwikkelingen binnen de telecomsector razendsnel gaan en omdat het belangrijk is om goed zicht te hebben op de (technische) werking van de telecomnetwerken om te identificeren waar maatregelen nodig zijn.
- Binnen de EU is de afgelopen periode een gezamenlijke Europese aanpak van de veiligheid en integriteit van telecomnetwerken uitgewerkt.
 - Het gaat onder meer om Raadsconclusies van de EU Telecomraad van 3 december. Zie <https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/>
 - Daarnaast heeft de EU een gecoördineerde risicoanalyse tot stand gebracht.
- In de EU Telecomraad is door alle lidstaten afgesproken dat kritieke onderdelen van telecomnetwerken alleen afkomstig mogen zijn van betrouwbare leveranciers.
- Het 5 december genomen Nederlandse besluit (AMvB) is hierop gebaseerd en in lijn met maatregelen van andere lidstaten.
 - Dit is ook eerder zo met de Tweede Kamer afgesproken n.a.v. diverse aangenomen moties.
- Aanbieders van mobiele telecommunicatie in Nederland kan worden opgedragen conform deze AMvB dat zij bepaalde leveranciers zullen moeten uitsluiten op basis van criteria zoals vermoedens van misbruik of spionage.
 - Uitsluiting van een onbetrouwbare leverancier kan conform de AMvB plaatsvinden als het vermoeden bestaat dat deze de Nederlandse telecominfrastructuur- en diensten kan misbruiken of uit kan laten vallen.
 - Of als er sprake is bij deze partij van nauwe banden met of wettelijke controle door buitenlandse overheden dan wel derde partijen zoals bedrijven en inlichtingendiensten die vermoedelijk betrokken zijn bij spionage, beïnvloeding of sabotage.
 - De beoordeling hiervan gaat in overleg met de NCTV en de Nederlandse inlichtingendiensten.
- Er is dus nog geen besluit aan aanbieders opgedragen dat bepaalde partijen (of landen) worden geweerd.



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep.-VERTROUWELIJK

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

23 januari 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	28 januari 2020, 15:30-17:00 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Vaststellen verslag TFEV 18-12-2019

Verslag TFEV is nogmaals verspreid via de beveiligde lijn op 23 januari

3. Begrotingsvoorstel 2020-2021

Bijlage 1. Input beleidsbrief en overzicht versterkingsmaatregelen

4. Voortgang structurele samenwerking

Bijlage 2. Oplegnota structurele samenwerking

Bijlage 3. Plan van aanpak

5. One-pager Economische Veiligheid

[REDACTED]

5.1.2a

[REDACTED]

[REDACTED]

5.1.2a

6. Derubricering kritieke onderdelen

Bijlage 5. De-rubriceren kritieke onderdelen

7. Internationaal

8. Parlementair

9. Rondvraag en w.v.t.t.k.

Dep.-VERTROUWELIJK



Aan
Leden van de Taskforce Economische Veiligheid

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Behandeld door

[REDACTED]

[REDACTED]

[REDACTED]

5.1.2e

Datum
16 januari 2020

Kenmerk
DGBI-DE / 20015469

Kopie aan

memo

De-rubriceren kritieke onderdelen telecom

Bijlage(n)

Gevraagd besluit

EZK is bezig met de uitwerking van beschikkingen ter implementatie van eerdere besluitvorming in de Taskforce Economische Veiligheid rondom kritieke onderdelen van mobiele netwerken. De lijst met kritieke onderdelen is als onderdeel van het voor de TFEV gemaakte rapport [REDACTED] STG-C geclassificeerd. Deze rubricering leidt er toe dat het in de praktijk onuitvoerbaar is invulling te geven aan de uitwerking van de beschikkingen. Daarbij geldt dat o.i. het alleen noemen van de lijst met kritieke onderdelen van dien aard is dat er geen overwegende bezwaren zijn om deze op een lager niveau te rubriceren. Om de balans te vinden tussen werkbaarheid en vertrouwelijkheid wordt instemming gevraagd de lijst met kritieke onderdelen te de-rubriceren naar dep-v (het voornoemde rapport zelf zal STG-C blijven).

5.1.1b

Toelichting

In de beschikkingen die aan de drie mobiele netwerkaanbieders (MNO's) worden gestuurd moet een termijn worden opgenomen waarbinnen aan de verplichting rond kritieke onderdelen moet zijn voldaan. Tevens moet de nadeelcompensatie die het gevolg is van de verplichting worden vastgesteld. Om de termijn en nadeelcompensatie vast te kunnen stellen, is het nodig dat EZK de kritieke onderdelen kan delen met de drie MNO's en dat de MNO's deze vervolgens op een 'need to know' basis kunnen delen met personen die zij nodig hebben voor het inschatten van de door hun benodigde termijn en geleden nadeelcompensatie. Deze informatie heeft EZK nodig om de beschikkingen vast te kunnen stellen.

Anders dan bij andere staatsgeheime stukken gaat het hier niet enkel om informatie die door een enkel persoon binnen een MNO moet worden gelezen, maar gaat het om het door de MNO actief kunnen verwerken en delen van informatie met meerdere benodigde (niet gescreende) betrokkenen. Ter illustratie. EZK heeft MNO's gevraagd gemotiveerd aan te geven welke termijn zou moeten worden aangehouden om enerzijds aan het veiligheidsrisico het hoofd te kunnen bieden en anderzijds de continuïteit van hun dienstverlening te waarborgen. Om dit te kunnen doen en verdere uitvoering te kunnen geven aan het besluit van de overheid, hebben MNO's aangegeven diverse experts te moeten inschakelen. Daarnaast worden MNO's voor het op te stellen nadeelcompensatiekader gevraagd gemotiveerd aan te geven voor welk bedrag aan nadeelcompensatie zij in aanmerking menen te komen. Ook hier zullen diverse (boekhoudkundige en technische) experts voor moeten worden ingeschakeld. Aan de MNO's wordt

gevraagd de informatie vergezeld te laten gaan van een accountantsverklaring die moet aangeven dat de verstrekte gegevens boekhoudkundig juist en volledig zijn. Dit impliceert dat ook externe relaties weet krijgen van kritieke onderdelen.

Zoals hierboven geschetst, moeten de MNO's meerdere mensen inschakelen om de informatie aan te leveren die nodig is voor het slaan van de beschikkingen. Er wordt vanuit gegaan dat dit grotendeels met experts van binnen de MNO's kan worden gedaan, maar verwacht wordt dat ook externe expertise is benodigd. De STG classificatie van de kritieke onderdelen maakt het niet mogelijk deze informatie onder de voor de uitvoering benodigde mensen te delen.


Een de-rubricering naar dep-v maakt het voor EZK mogelijk richting de MNO's te communiceren dat zij de lijst met kritieke onderdelen moeten behandelen volgens het bij hen bekende TLP (Traffic Light Protocol¹) AMBER. Met dep-v blijven de eisen van het Virbi rond het delen van informatie buiten de overheid van toepassing.

TLP AMBER houdt in dat ontvangers TLP AMBER-informatie alleen mogen delen binnen hun eigen organisatie op een need-to-know basis. Met in dit geval de aanvulling dat deze informatie ook gedeeld kan worden met externe relaties van de MNO's waar die noodzakelijk zijn voor de uitvoering van de beschikkingen (zoals een externe accountant).

Tegelijkertijd moet hierbij gerealiseerd worden dat het beschermen van de informatie over kritieke onderdelen onderdeel is van de veiligheidsstrategie tegen APT's. Met bredere verspreiding nemen de risico's op het bekend worden van onze tegenmaatregelen bij APT's toe. Het is daarom zaak om daar bij de verspreiding van deze informatie rekening mee te houden.

Ons inziens geldt dat alleen het noemen van de kritieke onderdelen van dien aard is dat er geen overwegende bezwaren zijn om deze op een lager niveau als dep-v te rubriceren. Het rapport waar zij uitkomen is STG-C omdat daar expliciet ook op dreigingen wordt ingegaan. Tegelijkertijd is het wel van belang om de lijst een rubricering te geven om redenen als in de vorige alinea benoemd. Om een balans te vinden tussen vertrouwelijkheid van gegevens en het uit kunnen voeren van het besluit van de TFEV rond kritieke onderdelen, wordt dep-v voorgesteld met de aan het eind van de memo benoemde aanvullende voorwaarden. De MNO's zijn akkoord met de-rubricering van de kritieke onderdelen.

Tot nu toe is de lijst met kritieke onderdelen niet gedeeld met buitenstaanders. Met de TK is deze alleen op hoofdlijnen gedeeld in een vertrouwelijke briefing. Met de voorgestelde wijze van werken wordt de informatie weliswaar breder, echter nog steeds niet openbaar gepubliceerd. Dit betekent politiek gezien dat, als daar om gevraagd wordt, de lijst met kritieke onderdelen alleen in vertrouwelijke setting wordt gedeeld met de Tweede Kamer.

Concluderend, aan u wordt gevraagd om de kritieke onderdelen zoals opgenomen in figuur 3.1 van het  rapport *Veiligheid telecomapparatuur en software* van 16 mei 2019, te de-rubriceren naar dep-v en deze te kunnen delen met de MNO's (KPN, VodafoneZiggo en T-mobile) onder TLP AMBER met de volgende aanvullende voorwaarden:

5.1.2i

¹ <https://www.first.org/tlp/docs/tlp-v1-nl.pdf>

- Met een ontvanger wordt alleen die informatie uit de lijst van kritieke onderdelen gedeeld die noodzakelijk is voor de uitvoering van een taak door desbetreffende ontvanger ("need to know").
- De MNO zorgt ervoor dat onbevoegden (anderen dan voornoemde doelgroep) geen toegang kunnen krijgen tot de lijst met kritieke onderdelen.

**Contactpersoon**

Dep. ~~VERTROUWELIJK~~

Datum
25 maart 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum	25 maart 2020
Vergaderplaats	Digitaal – schriftelijke ronde via e-mail

1. algemeen

Vanwege de maatregelen nav COVID-19 is besloten dit overleg niet fysiek door te laten gaan, maar te kiezen voor een schriftelijke ronde. Dit betekent concreet dat in deze agenda de stand van zaken per onderwerp wordt weergegeven, net als de verwachte planning en eventuele aandachtspunten. Alle leden van de taskforce krijgen de mogelijkheid om via e-mail op deze agenda te reageren, bij voorkeur voor vrijdag 27 maart 12.00u.

Er is één beslispunt, opgenomen onder ministeriële regeling.

Het is belangrijk, ook in tijden van COVID-19, te beseffen dat het traject rondom 5G hoog op de prioriteitenlijst staat. Hiermee worden immers de risico's die met de dreiging gepaard gaan gemitigeerd. Het is daarom belangrijk dat deze trajecten doorgang vinden. Waar mogelijk vinden afspraken telefonisch of per e-mail plaats. Indien noodzakelijk (bijvoorbeeld vanwege de aard en de vertrouwelijkheid) kunnen bijeenkomsten doorgang vinden, daarbij worden de maatregelen (social distancing en hygiëne) vanzelfsprekend wel in acht genomen.

2. Beschikkingen

- Er wordt gewerkt aan het concept voornemen van de beschikking. Op 12/3 is er een bijeenkomst geweest met NCTV, FIN, AT, EZK (DE & WJZ). Op 20/4 is een vervolgbijeenkomst om een nieuw concept en vervolgstappen te bespreken.
- Na het versturen van een definitief voornemen, krijgen de telco's de gelegenheid om hun zienswijze te geven, waarna de definitieve beschikking zal volgen. Streven is vooralsnog voor de zomer tot een definitieve beschikking te komen.
- NCTV en EZK (met input van de diensten) werken verder aan de geopolitieke paragraaf.

- Het blijkt lastig om een termijn voor uitfasering te bepalen. Input van de telco's is nodig. Dit is reeds mondeling aan de telco's verzocht, en zal ook per brief worden verzocht.
- Om onzekerheid voor telco's te reduceren hebben de landsadvocaat en economen in opdracht van AT/EZK een abstract nadeelcompensatiekader opgesteld. Dit kader wordt op korte termijn ter consultatie aan de telco's voorgelegd.
- De lijst met kritieke onderdelen is gederubriceerd en wordt onder voorwaarden met de telco's gedeeld.

3. Ministeriële regeling

- De beveiligingsmaatregelen die momenteel voor de ministeriële regeling worden uitgewerkt zijn ontleend aan de maatregelen uit het [REDACTED] onderzoeksrapport (STG rapport van [REDACTED] 16 mei 2019). 5.1.2i
- Onder leiding van [REDACTED] zijn de afgelopen maanden de maatregelen verder uitgewerkt en hieraan worden concrete implementatievereisten verbonden. Hierover heeft sinds het najaar intensief overleg plaatsgevonden met de NBV, NCSC, AT en de mobiele aanbieders en het voorstel is in de eindfase beland.
- Parallel hieraan werkt EZK aan de ministeriële regeling, waarbij de maatregelen uit het [REDACTED] voorstel als een bijlage aan de regeling wordt toegevoegd. EZK voert ook overleg met de sector. Verwacht wordt dat eind april een versie gereed is die ook met partijen kan worden gedeeld. Gegeven de consultatie, de uitvoerings- en handhavingstoets door AT en de notificatie in Brussel die nog moeten plaatsvinden, zal de regeling naar verwachting eind van de zomer kunnen worden gepubliceerd. 5.1.2i

Technische sessie:

- Er bestaat behoefte bij de technische werkgroep om de beveiligingsmaatregelen die zijn geformuleerd ten behoeve van de ministeriële regeling theoretisch te toetsen;
 - d.w.z. als een soort eindtoets om te beoordelen in hoeverre deze maatregelen bijdragen aan de dreigingsscenario's die zijn opgesteld door de technische werkgroep. Om dit te kunnen beoordelen is expertise vanuit de technische werkgroep nodig (NBV, AT, EZK, [REDACTED] MIVD, NCSC, NCTV). 5.1.2i
 - de technische werkgroep wil de dreigingsscenario's doornemen en hierbij zal staatsgeheime informatie worden besproken. Vanwege de urgentie (betreft maatregelen die toezien op de huidige dreiging in de huidige telecomnetwerken) vindt J&V het noodzakelijk dat deze beoordeling op korte termijn plaatsvindt en dat hiervoor fysiek moet worden bijeengekomen.
- EZK vindt dat er een goed pakket aan maatregelen ligt, zeker ook bezien in samenhang met het beschikkingentraject; de beveiligingsmaatregelen die in het [REDACTED] rapport waren opgenomen als mitigerende maatregelen bij de verschillende dreigingsscenario's zijn adequaat uitgewerkt. 5.1.2i
- EZK is wel bereid om een technische sessie te organiseren, maar gezien de huidige COVID-19 crisis en de op maandag 23 maart jl. aangescherpte maatregelen is het de vraag of een dergelijke sessie op korte termijn kan plaatsvinden: Voor EZK is aanwezigheid van [REDACTED] randvoorwaardelijk om een zinvolle technische sessie te kunnen houden. Echter, [REDACTED] is niet bereid hierbij aanwezig te zijn. [REDACTED] heeft wel aangegeven dat wanneer de wens bestaat dat deze sessie toch op korte termijn moet plaatsvinden, er een verzoek met onderbouwing richting het management van [REDACTED] moeten komen, wat vervolgens door [REDACTED] zal worden beoordeeld. 5.1.2i
5.1.2e
5.1.2i

- In het geval er een technische sessie moet plaatsvinden (op korte termijn of middellange termijn) dan zal aan de hand van de uitkomsten moeten worden gezien wat de vervolgstappen worden en of het noodzakelijk is dat eea binnen de ministeriële regeling moet worden opgelost of dat er alternatieve oplossingsrichtingen zijn, zoals meenemen in de structurele aanpak. Voor de ministeriële regeling zal er naar verwachting gevolgen zijn voor de planning en het draagvlak bij de sector.

Gevraagd besluit:

Akkoord gaan met het op korte termijn laten plaatsvinden van een technische sessie, waarvoor een verzoek bij [REDACTED] moet worden ingediend. Vanzelfsprekend worden maatregelen rondom hygiëne en *social distancing* toegepast tijdens deze sessie.

5.1.2i

3. Structurele samenwerking – stand van zaken

- Er worden op dit moment uitgangspunten voor de structurele samenwerking uitgewerkt met de telecomaandieners door AT, NBV en NCSC op basis van het plan van aanpak wat in de TFEV van 28 januari voorlag. Daarnaast wordt ook in opdracht van EZK gewerkt aan een inventarisatie van mogelijkheden om meer investeringszekerheid te bieden in de vormgeving van de structurele aanpak (ook besproken in TFEV van 28 januari). Hierbij wordt onder andere gekeken naar nadeelcompensatie en mogelijkheden om aan te sluiten bij investeringscyclussen. Een uitwerking hiervan wordt eind april verwacht en zal met u worden gedeeld.
- Bij het uitwerken van de uitgangspunten is wat verwarring ontstaan over de scope en doelstelling bij [REDACTED]. Dit wordt momenteel afgestemd, hierover ontvangt u in de volgende TFEV een terugkoppeling.

5.1.2i

4. Parlementair (Kamerbrief en briefing)

- In het debat op 6 februari over mogelijke spionage door Huawei in Nederland en de veiling van 5G-frequenties heeft MinJenV een brief toegezegd over hoe de Kamer geïnformeerd wordt, vertrouwelijk of openbaar, zodat democratische controle kan plaatsvinden.
- Daarnaast is aan de Kamer opnieuw een vertrouwelijke briefing aangeboden. De focus van de briefing ligt op de manier waarop de dreiging zich in de telecomnetwerken manifesteert en welke maatregelen daartegen worden genomen. In deze vertrouwelijke briefing kan uitgebreid worden stil gestaan welke onderdelen van het netwerken als kritiek zijn aangemerkt, waarom in deze gevallen beveiligingsmaatregelen onvoldoende zijn om de risico's te mitigeren en het nodig is dat hier alleen gebruik wordt gemaakt van vertrouwde leveranciers.
- Vanwege COVID-19 is dit voorlopig *on hold* gezet. In april wordt dit weer opgepakt.

5. Internationaal/Europees

- Het EU traject naar aanleiding van de mededeling van 29 januari loopt door. De inzet van Nederland is vastgelegd in BNC-fiche dat op 6 maart

door de MR is aangenomen. De eerstvolgende deadline is het aanleveren van informatie over hoe de Lidstaten op nationaal niveau opvolging hebben gegeven aan de toolbox. Het document hiertoe is in ontwikkeling. Er wordt nog gekeken met de Commissie wat de impact van COVID-19 is op de planning.

- De internationale like-minded conferentie over 5G in Praag stond gepland voor 5 en 6 mei. Het is onduidelijk of en hoe deze doorgang zal hebben.

6. Gezamenlijk begrotingsvoorstel 2020-2021

- Vrijdag 20/03 heeft de SG JenV gesproken met DG Rijksbegroting over het begrotingsvoorstel 2020/2021. Hierbij is besloten om het JenV gedeelte van deze claim niet te honoreren.
- Dit betrof €3,4 miljoen structureel voor uitvoeringscapaciteit bij de NCTV en NCSC voor structurele risicoanalyses en uitwerken maatregelen (telecom), versterking expertise en advies bij NCSC en een intersectoraal cyberoefenprogramma. NCTV kan dit bedrag niet vanuit de eigen begroting dekken, ook bij de begroting van JenV is er geen ruimte.
- Beeld is dat hiermee het gezamenlijke begrotingsvoorstel van tafel is; mocht u andere signalen hebben ontvangen of anderen ideeën hierover hebben dan horen wij dit graag.

Van:
Aan:

[Redacted]

5.1.2e

Cc:

[Redacted]

5.1.2e

Onderwerp: RE: Schriftelijke ronde TFEV 25 maart - graag reactie uiterlijk 27 maart 12.00u
Datum: maandag 30 maart 2020 12:27:24
Bijlagen: image001.png

Beste Taskforce leden,

Namens [Redacted] wil ik hierbij de schriftelijke ronde afronden. We hebben reactie ontvangen van bijna alle leden van de Taskforce, dank hiervoor.

5.1.2e

Wat betreft het gevraagde besluit: er is brede steun met het op korte termijn laten plaatsvinden van een technische sessie, waarvoor een verzoek bij [Redacted] moet worden ingediend.

5.1.2i

Het betreft een verzoek (geen verplichting) aan [Redacted] waarbij de urgentie en noodzaak van het bijeenkomen wordt benadrukt. Vanzelfsprekend worden maatregelen rondom hygiëne en *social distancing* toegepast tijdens deze sessie. Door de NCTV wordt een tekst opgesteld om de urgentie en vertrouwelijkheid te benadrukken; deze onderbouwing wordt door EZK opgenomen in het verzoek aan [Redacted]

5.1.2i

Ten aanzien van het begrotingsvoorstel (agendapunt 6) wordt hiermee inderdaad bedoeld dat het voorstel hiermee voorlopig van tafel is.

Met vriendelijke groeten,

5.1.2e

[Redacted]

Van:

[Redacted]

5.1.2e

Verzonden: vrijdag 27 maart 2020 11:15

Aan:

[Redacted]

[Redacted]

5.1.2e

CC: [Redacted]

5.1.2e

Onderwerp: RE: Schriftelijke ronde TFEV 25 maart - graag reactie uiterlijk 27 maart 12.00u

Beste Leden van de Taskforce,

Namens [Redacted] kan ik berichten dat lenW akkoord gaat met het gevraagde besluit.

5.1.2e

Met vriendelijke groet,

[Redacted]

5.1.2e

[Redacted]

Ministerie van Infrastructuur en Waterstaat

Hoofddirectie Financiën, Management en Control

Directie Bedrijfsvoering, Organisatie en Informatiebeleid

Rijnstraat 8 | Postbus 20901 | 2500 EX Den Haag

[Redacted]

5.1.2e



5.1.2e

www.rijksoverheid.nl/ienw

Van: [Redacted]

5.1.2e

Verzonden: woensdag 25 maart 2020 17:44

Aan: [Redacted]

[Redacted]

5.1.2e

CC: [Redacted]

[Redacted]

5.1.2e

Onderwerp: Schriftelijke ronde TFEV 25 maart - graag reactie uiterlijk 27 maart 12.00u

Beste leden van de Taskforce,

Zoals aangekondigd stuur ik u hierbij de geannoteerde agenda voor het schriftelijk overleg. Het werkt als volgt: per agendapunt staat een stand van zaken op genomen, met daarbij waar relevant de planning en eventuele aandachtspunten. Op 1 punt wordt specifiek om uw reactie gevraagd, zie daarvoor onder het kopje ministeriële regeling:

Gevraagd besluit: Akkoord gaan met het op korte termijn laten plaatsvinden van een technische sessie plaatsvindt, waarvoor een verzoek bij [Redacted] moet worden ingediend. Vanzelfsprekend worden maatregelen rondom hygiëne en *social distancing* toegepast tijdens deze sessie. U kunt in een reply all op deze e-mail reageren naar de andere Taskforce leden op de punten uit de annotatie en specifiek het gevraagde besluit. Bij voorkeur ontvangen we uw reactie voor vrijdag 27 maart 12.00u.

5.1.2i

Met vriendelijke groeten,

[Redacted]

5.1.2e

Van: [Redacted]

Verzonden: maandag 23 maart 2020 14:55

[illegible]

5.1.2e

[illegible]

5.1.2e

Beste leden van de Taskforce Economische Veiligheid,
Op woensdag 25 maart staat de volgende TFEV ingepland. Vanwege de maatregelen op COVID-19 hebben we besloten dit keer niet fysiek bij elkaar te komen voor een overleg. In plaats daarvan wordt het overleg schriftelijk (per e-mail) afgehandeld. Dit betekent dat u dinsdag 22 maart een geannoteerde agenda krijgt met daarin per onderwerp de voortgang, het verder proces en eventuele aandachtspunten. Er staan dit keer geen stukken geagendeerd. Heeft u punten die u graag al van te voren in de geannoteerde agenda opgenomen wilt hebben, dan kunt u dat doorgeven aan [REDACTED]. Indien de geannoteerde agenda tot vragen of opmerkingen leidt kunt u telefonisch of per e-mail contact opnemen.
Met vriendelijke groeten,

5.1.2e

Met vriendelijke groeten,

5.1.2e

Ministerie van Veiligheid en Justitie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

5.1.2e

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

Van:
Aan:

5.1.2e

Cc:

5.1.2e

Onderwerp: Schriftelijke ronde TFEV 25 maart - graag reactie uiterlijk 27 maart 12.00u
Datum: woensdag 25 maart 2020 17:44:06
Bijlagen: Agenda TFEV 25032020.docx

Beste leden van de Taskforce,
 Zoals aangekondigd stuur ik u hierbij de geannoteerde agenda voor het schriftelijk overleg. Het werkt als volgt: per agendapunt staat een stand van zaken op genomen, met daarbij waar relevant de planning en eventuele aandachtspunten. Op 1 punt wordt specifiek om uw reactie gevraagd, zie daarvoor onder het kopje ministeriële regeling: Gevraagd besluit: Akkoord gaan met het op korte termijn laten plaatsvinden van een technische sessie plaatsvindt, waarvoor een verzoek bij [REDACTED] moet worden ingediend. Vanzelfsprekend worden maatregelen rondom hygiëne en *social distancing* toegepast tijdens deze sessie. U kunt in een reply all op deze e-mail reageren naar de andere Taskforce leden op de punten uit de annotatie en specifiek het gevraagde besluit. Bij voorkeur ontvangen we uw reactie voor vrijdag 27 maart 12.00u.
 Met vriendelijke groeten,

5.1.2i

Van: [REDACTED]

5.1.2e

Verzonden: maandag 23 maart 2020 14:55

5.1.2e

Aan: [REDACTED]

5.1.2e

CC: [REDACTED]

5.1.2e

Onderwerp: TFEV woensdag

Beste leden van de Taskforce Economische Veiligheid,
 Op woensdag 25 maart staat de volgende TFEV ingepland. Vanwege de maatregelen op COVID-19 hebben we besloten dit keer niet fysiek bij elkaar te komen voor een overleg. In plaats daarvan wordt het overleg schriftelijk (per e-mail) afgehandeld. Dit betekent dat u dinsdag 22 maart een geannoteerde agenda krijgt met daarin per onderwerp de voortgang, het verder proces en eventuele aandachtspunten. Er staan dit keer geen stukken geagendeerd. Heeft u punten die u graag al van te voren in de geannoteerde agenda opgenomen wilt hebben, dan kunt u dat doorgeven aan [REDACTED]. Indien de geannoteerde agenda tot vragen of opmerkingen leidt kunt u telefonisch of per e-mail contact opnemen.
 Met vriendelijke groeten,

5.1.2e

5.1.2e


Ministerie van Veiligheid en Justitie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

5.1.2e






Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK

Contactpersoon

██████████
██████████

5.1.2e

Datum

15 mei 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	15 mei 2020

1. Algemeen

Vanwege de maatregelen nav COVID-19 is besloten dit overleg niet fysiek door te laten gaan maar te kiezen voor een schriftelijke ronde. Dit betekent concreet dat in deze agenda de stand van zaken per onderwerp wordt weergegeven, net als de verwachte planning en eventuele aandachtspunten. Voor agendapunt 3 zijn vanuit EZK twee beslispunten ingebracht. Alle leden van de taskforce krijgen de mogelijkheid om via e-mail op deze agenda te reageren, bij voorkeur voor vrijdag 22 mei.

Vanwege verwachte besluitvorming zal de eerstvolgende TFEV weer fysiek bijeenkomen. Hierbij zullen vanzelfsprekend de maatregelen (social distancing en hygiëne) in acht worden genomen. Er wordt momenteel nog gezocht naar een datum, u wordt hierover zo spoedig mogelijk geïnformeerd.

2. Beschikkingen

- Er wordt gewerkt aan het concept voornemen van de beschikkingen. In de week van 2 juni is een vervolgbijeenkomst met NCTV, FIN, BZ, AT, EZK (DE & WJZ) om een nieuw concept en vervolgstappen te bespreken.
- Streven is rond de zomer tot een voornemen voor een beschikking te komen. Dit hangt mede af van de voortgang op hieronder beschreven punten.
- Na het versturen van een voornemen, krijgen de telco's de gelegenheid om hun zienswijze te geven, waarna de definitieve beschikking zal volgen, die openstaat voor bezwaar en beroep.
- Planning is om in Q4 een definitieve beschikking te versturen.
- Het proces heeft vertraging opgelopen. Mensen waren (deels) niet beschikbaar vanwege Corona en er is meer tijd benodigd om de geopolitieke paragraaf van de beschikking vorm te geven en een realistische termijn voor uitfasering te bepalen.
- Voor dit laatste is de input van de telco's wenselijk. De telco's geven echter aan dat zij ervaren dat de vertrouwelijkheid van de lijst met

kritieke onderdelen hen hindert hier uitvoering aan te geven. [REDACTED]

• (1)

5.1.2i

5.1.2i

○

5.2.1

○

5.2.1

○

5.2.1

• (2)

5.1.2i

○

5.1.2i

○

5.1.2i

• (3)

5.1.2i

○

5.1.2i

Ter besluitvorming

1. Graag instemming van de Taskforce om binnen 3 weken besluitvorming voor te bereiden op de volgende punten:
 - a. Wanneer de telco's in gesprek kunnen met de vertrouwde leveranciers ter voorbereiding van de uitvoering van de beschikking, zonder de gerubriceerde lijst met kritieke onderdelen integraal te delen.
 - b. Wanneer de telco's in gesprek kunnen met de te weren leverancier ter voorbereiding van de uitvoering van de beschikking zonder de gerubriceerde lijst met kritieke onderdelen integraal te delen.

2.

5.1.2i

3. Ministeriële regeling

Met betrekking tot de ministeriële regeling (maatregel 1) zijn er geen beslispunten. Hieronder vindt u de terugkoppeling van de interdepartementale, technische sessie van 9 april jl. en de planning van de ministeriële regeling op hoofdlijnen. De uitwerking van de technische en organisatorische maatregelen wordt binnenkort naar u verstuurd.

Terugkoppeling technische sessie:

- Zoals besloten in de schriftelijke TFEV van eind maart 2020 heeft op verzoek van J&V op 9 april jl. een interdepartementale, technische sessie over de uitwerking van de technische en organisatorische maatregelen plaatsgevonden. Deze technische sessie diende als *eindtoets* opdat deze maatregelen kunnen worden vastgelegd in de ministeriële regeling (maatregel 1).
- De technische en organisatorische maatregelen, die in de ministeriële regeling zullen worden opgenomen zijn de afgelopen maanden door [REDACTED] uitgewerkt. Hierbij is nauw en frequent afgestemd met partijen vanuit de overheid (NBV, NCSC, Agentschap Telecom en EZK) en vanuit de markt (KPN, T-Mobile NL en VodafoneZiggo).
- Doel van deze afrondende technische sessie was na te gaan of de uitwerking van maatregelen recht doet aan de eerdere dreigingsanalyse (vastgelegd in [REDACTED] rapport d.d. mei 2019). Dienovereenkomstig waren alle partijen vertegenwoordigd die indertijd ook bij de dreigingsanalyse betrokken zijn

5.1.2i

5.1.2i

- geweest, te weten J&V (NCTV en NCSC), MIVD, NBV, Agentschap Telecom en EZK (directie Digitale Economie) en [REDACTED]
- De maatregelen zijn per dreigingsscenario uit het eerdere [REDACTED] rapport tegen het licht gehouden. Daarbij is expliciet besproken hoe de huidige detailuitwerking zich verhoudt tot de richtinggevende set van maatregelen die [REDACTED] in datzelfde onderzoeksrapport had opgenomen en hoe op specifieke punten (bijvoorbeeld met het oog op uitvoerbaarheid) voor alternatieve, eveneens veilige oplossingen is gekozen. Aanvullend hierop is teruggeblikt op het proces van de afgelopen maanden en is de beoogde reikwijdte van de regeling (zoals afgeleid uit het dreigingsbeeld) nader toegelicht. 5.1.2i
 - Conclusies:
 - De deelnemers aan de sessie hebben gezamenlijk geconcludeerd dat er een goed en solide fundament ligt van technische en organisatorische maatregelen voor de scope uit het eerdere [REDACTED] rapport. Deze uitgewerkte maatregelen – 19 in totaal – zullen worden opgenomen in de ministeriële regeling. 5.1.2i
 - Ontwikkelingen in de sector (bijvoorbeeld op het gebied van netwerktechnologie) dan wel nieuwe dreigingsbeelden zouden waar nodig in de structurele aanpak (maatregel 3) moeten worden geadresseerd. Niet uitgesloten is dat dit op termijn tot aanpassing van de ministeriële regeling zal leiden.
 - Hiermee wordt het [REDACTED] gefinaliseerd en kan verder gewerkt worden aan het ontwerpen van de ministeriële regeling. 5.1.2i

Planning

Processtap	Datum of periode
Opstellen concept-regeling	Heden tot 1 augustus
Opstellen artikelen, bijlage met technische en organisatorische maatregelen ([REDACTED]) & toelichting	
Interdepartementale afstemming	
Internetconsultatie en externe adviezen (Adviescollege Toetsing Regeldruk, Uitvoerbaarheids- & Handhaafbaarheidstoets (U&H-toets) Agentschap Telecom	
Verwerken reacties consultatie, ATR, U&H-toets	
Interdepartementale afstemming	
Notificatie Europese Commissie	1 augustus t/m 15 oktober
Notificatie periode	
Evt. verwerken reacties uit de notificatie	
Vaststelling regeling en publicatie	15 oktober t/m 1 november
Publicatie Staatscourant	1 november 2020

5.1.2i

¹ J&V: [REDACTED]; BZK: [REDACTED]; DEF: [REDACTED]; AT: [REDACTED]
[REDACTED]; [REDACTED]; EZK: [REDACTED]

5.1.2e

5.1.2i

4. Structurele samenwerking

De gesprekken tussen AT, MIVD, NBV en NCSC met de telecomaanbieders over de uitgangspunten voor de structurele samenwerking hebben vanwege COVID-19 en prioriteit op de beschikkingen en ministeriele regeling stilgelegen en worden zodra dit mogelijk is weer hervat. Voor de verdere uitwerking van de structurele samenwerking is het onder andere noodzakelijk dat de eerder toegezegde gesprekken met de telecomaanbieders op MT-niveau (CTO, CISO en evt. CEO niveau) gaan plaatsvinden. Hier wordt komende periode op ingezet.

[REDACTED]

5.1.2i

De inventarisatie van mogelijkheden om meer investeringszekerheid te bieden in de vormgeving van de structurele aanpak (aangekondigd in de vorige TFEV) heeft vanwege COVID-19 vertraging opgelopen en zal naar verwachting in de week van 22 juni worden opgeleverd. De uitwerking hiervan zal met u worden gedeeld.

5. Brandstichting zendmasten

In de afgelopen weken zijn in Nederland 27 (pogingen) tot brandstichting geregistreerd bij zendmasten. In een aantal gevallen hebben brandstichtingen geleid tot een verstoring in de continuïteit van mobiele netwerken. In andere gevallen konden omliggende zendmasten voldoende dekking bieden. EZK werkt met betrokken partijen aan een afwegingskader om de risico's voor het mobiele netwerk in kaart te brengen en eventueel gericht maatregelen te kunnen treffen. De politie doet onderzoek naar de verdachten en hun motieven. De brandstichtingen lijken verband te houden met complottheorieën die een verband suggereren tussen COVID-19 en 5G.

Ook vanuit de politiek is er veel aandacht voor dit onderwerp en zijn er Kamervragen gesteld. Dit onderwerp wordt binnen de bestaande verantwoordelijkheden opgepakt, de TFEV heeft hierin op dit moment geen rol.

6. Internationaal/Europees

De Prague Conference over 5G die gepland stond voor 5 mei is uitgesteld in verband met COVID-19 en zal naar verwachting in september (digitaal of fysiek) plaatsvinden.

Op 8 mei is de vragenlijst voor de NIS Cooperation Group naar u toegestuurd voor akkoord. Hierin staan de nationale maatregelen die worden genomen naar aanleiding van de EU toolbox. Op basis van de binnengekomen reacties zijn een aantal wijzigingen doorgevoerd, dit betreft:

- Tab A, kolom 6: meer toelichting gegeven over waarom dit als 'confidential' staat aangemerkt
- Tab A, kolom 12: verwijzing naar de Amvb toegevoegd, namen van wetgeving vertaald naar het Engels
- Tab A, kolom 14: correcte verwijzing naar AIVD en MIVD opgenomen
- Tab A, kolom 23: prioritering in lijn gebracht met eerdere inschatting die is gemaakt en naar EU-partners is gestuurd bij het aanleveren van het nationale risk assessment.
- Tab B, kolom 16: toevoeging van de zinsnede 'The assessment of threats, interests (and therefore assets) can change over time and are subject to constant monitoring. Security measures can be adjusted in light of these developments'.

In de bijlage vindt u de aangepaste vragenlijst. Deze wordt verstuurd naar de NIS Cooperation Group.

7. Vervolg gezamenlijk begrotingsvoorstel EV

Zoals in vorige TFEV gemeld is het gezamenlijk begrotingsvoorstel niet gehonoreerd. Er wordt nu door de betrokken departementen inzichtelijk gemaakt wat de gevolgen daarvan zijn, waar problemen/dilemma's met betrekking tot voortgang ontstaan en welke mogelijke oplossingen er zijn. De TFEV zal hiervan op de hoogte worden gesteld. Daarnaast wordt momenteel gewerkt aan een voorstel voor de inzet richting de nieuwe regeerperiode. Ook dit zal in de TFEV terugkomen.

Member State	Netherlands
Date	15-4-2020
Contact point	
General comments or remarks	

<i>Explanation of the TLP markings for information sharing restrictions:</i>		
<i>Marking</i>	<i>Meaning</i>	<i>How you may use it in this questionnaire</i>
TLP: Green	Limited disclosure, restricted to the community	Use this marking for information not considered to be sensitive
TLP: Amber	Limited disclosure, restricted to participants' organizations	Use this marking for information considered to be more sensitive, but still appropriate for sharing within the NIS CG WS
TLP: Red	Not for disclosure, restricted to participants only	Use this in the case where confidential information exists and could be shared through other channels (do not include any such information in this questionnaire)

For additional information about the TLP protocol please see:
<https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol>

Assessment of factors relevant for the implementation of key measures

[Toolbox §5.2, para 2]

Category	Details <i>Provide information about the current status and timeframes for 5G spectrum allocation (per frequency band)</i>		Sharing restriction
Timeframes for deploying 5G networks	3.5 GHz - expected Q3 2022 700, 1400 and 2100 MHz - expected Q1 2021		TLP:Green
Category	Assessment	Details <ul style="list-style-type: none"> - Provide information about the current presence of potentially high-risk suppliers in the critical and sensitive parts of the network. - For initial assessment of high-risk suppliers, factors to consider are as stated in the EU coordinated risk assessment: (a) The likelihood of the supplier being subject to interference from a non-EU country, (b) the supplier's ability to supply and (c) the overall quality of products and cybersecurity practices of the supplier. - For determining criticality and sensitivity of assets, categories as per the EU coordinated risk assessment could be considered (e.g. core network functions, network management and orchestration functions and access network functions). - The assessment of the level of exposure to high-risk suppliers should be based on the criteria used by national authorities; Member States are invited to provide explanations about the criteria used (e.g. whether high risk suppliers are present or not in critical network parts/functions, or their overall involvement in critical and sensitive parts of networks and/or provision of critical/sensitive services). 	Sharing restriction
Estimated level of exposure to potentially high-risk suppliers		The list of trusted suppliers will be confidential, therefore the level of exposure is also confidential	TLP:Amber
Category	Assessment	Details <i>Details may include information about the number and/or market share of MNOs considered to have a major dependency on any single supplier, as well as a description of the existing approach to diversification of suppliers by individual MNOs</i>	Sharing restriction
Estimated degree of dependency on individual supplier (for individual MNOs)		confidential	TLP:Red
Category	Assessment	Details <i>Details may include information about the overall dependency on an individual supplier at the national level</i>	Sharing restriction
Estimated degree of dependency on individual supplier (nationally)		confidential	TLP:Red
Category	Assessment	Details <i>Provide a brief description of existing legal instruments and main security requirements applicable to MNOs.</i>	Sharing restriction

Legal framework and requirements already in place		Telecommunications Act; Telecommunications Security and Integrity Decree (with regard to Telecommunications Act, art 11A.1. & 18.12); Act on undesired control telecommunications sector (Wet ongewenste zeggenschap telecommunicatie, WOZT)	TLP:Green
Category	Assessment	Details <i>Details may include information about the responsible authorities, resources currently dedicated to implementing, enforcing and supervising network security, type and level of expertise available, etc.</i>	Sharing restriction
National resources and capabilities		Enforcement of respective provisions in the Telecommunications Act : Radiocommunications Agency Organizations responsible for output of the process for developing draft measures, risk analysis based on new threats , etc.: Ministry of Economic Affairs and Climate Policy, Ministry of Justice and Security, General Intelligence & Security Service, Defence Intelligence & Security Service, National Cyber Security Center (NCSC-NL).	TLP:Green

**Prioritisation of risks according to the national and EU Coordinated Risk Assessment and
Review of effectiveness of existing mitigations in addressing the risks**
[Toolbox §5.2, Table 4 steps 1 and 1a]

Risk (from the EU coordinated risk assessment)	Risk prioritisation	Effectiveness of existing mitigation	Details - Wherever applicable, provide further explanation explaining the rationale for corresponding risk prioritisation - Include relevant details on potential existing mitigation measures in place. This may include details on legal framework and on security requirements already in place	Sharing restriction
1: Misconfiguration of networks	Medium priority	Highly effective	existing requirements are valid through legislation currently in force	TLP:Green
2: Lack of access control	Medium priority	Highly effective	existing requirements are valid through legislation currently in force	TLP:Green
3: Low equipment quality	Medium priority	No (effective) measures	planned to amend existing policy	TLP:Red
4: Dependency on a single supplier	Medium priority	No (effective) measures	planned to amend existing policy on resilience	TLP:Red
5: State interference through 5G supply chain	Very high priority	No (effective) measures	under construction; initiated because of national security risks	TLP:Green
6: Exploitation of 5G networks by organised crime	Medium priority	Moderately effective	only generic legislation in force	TLP:Red

7: Significant disruption of critical infrastructure or services	High priority	Highly effective	Existing legislation includes protective measures for critical infrastructures	TLP:Green
8: Massive failure of networks due to interruption of electricity supply	Medium priority	Reasonably effective	frameworks, policies and legislation not fully finalized yet.	TLP:Green
9: IoT exploitation	Medium priority	Moderately effective	Only generic legislation applicable; dedicated requirements to be developed	TLP:Amber

Details about the (planned) implementation of the key mitigation measures

[as per the Toolbox §5.2, Table 4, step 3 and §6, recommendation 1]

1. Powers for national authorities

1.a) Implementation planning

ID	Current status	Planned completion date	Remarks, explanations (include envisaged next steps if applicable)	Implementation details <u>For SM01:</u> - Describe the steps taken (or planned to be taken) for ensuring authorities have the powers to impose requirements and ex-ante powers to restrict/prohibit/impose requirements or conditions for the supply, deployment and operation of 5G equipment <u>For SM02:</u> - Include information about plans for conducting in-depth audits of MNOs - Specify if the authority has information on operator's plans for 5G equipment sourcing and for the involvement of third party suppliers	Sharing restriction
SM01	Implemented			Legislation already in force allows to impose requirements. (Telecommunications Act, Ch. 11a)	TLP:Green
SM02	Implemented			Legislation already in force allows to impose requirements. (Telecommunications Act, Ch. 11a)	TLP:Green

1.b) Experienced or expected implementation factors of relevance (as per the toolbox: §4.2, pg.14)

Factor:	Relevance:	Remarks, explanations:	Sharing restriction
Resource costs	Not directly relevant	already in force under existing legislation	TLP:Green
Sector-specific economic Impact	Very relevant	possible impact on equipment already in use ; replacement of components when future decisions impacts current suppliers	TLP:Green
Broader economic or society impact	Not directly relevant		

2. Restrictions for high-risk suppliers and managed service providers

2.a) Implementation planning

ID	Current status	Planned completion date	Remarks, explanations (include envisaged next steps if applicable)	Implementation details <u>For SM03:</u> - Describe the national framework used (or intended to be used) for assessing the risk profile of suppliers - Describe the national approach for identification of key assets (network and other assets, e.g. geographic areas or entities) - Describe the restrictions for high risk suppliers that will be applied for key assets - Describe the steps taken (or planned to be taken) for ensuring that MNOs have adequate controls and processes in place to manage residual risks for suppliers <u>For SM04:</u> - Describe any existing or forthcoming legal/regulatory framework allowing to limit and/or control the usage of Managed Service Providers (MSPs) and to impose strict access controls for third line support for high-risk suppliers	Sharing restriction
SM03	In progress	Q4 2020	regulation under development	Based on the current threat a set of 'interests to be protected' has been identified. Based on these interests the key assets have been identified; the key assets are specific technical components (software, hardware) that are relevant in protecting these interests [e.g. they store or process certain data]. The assessment of threats, interests (and therefore the designated key assets) can change over time and are subject to constant monitoring. Security measures can be adjusted in light of these developments.	TLP:Amber
SM04	In progress	Q4 2020	regulation under development	Telecommunications Act provides for implementing lower level regulation on organizational or technical requirements regarding resilience or security.	TLP:Green

2.b) Experienced or expected implementation factors of relevance (as per the toolbox: §4.2, pg.14)

Factor:	Relevance:	Remarks, explanations:	Sharing restriction
Resource costs	Relevant	Implementation of these measures requires additional government investments (> 1.5 million EUR annually)	TLP:Amber
Sector-specific economic Impact	Very relevant	direct impact on procurement strategies, business investments in security and organizational measures, possibly resulting in increase of less positive business cases	TLP:Green
Broader economic or society impact	Not directly relevant		

3. Diversification of suppliers

3.a) Implementation planning

ID	Current status	Planned completion date	Remarks, explanations (include envisaged next steps if applicable)	Implementation details <u>For SM05:</u> - Describe any existing or planned legal/regulatory instruments providing regulatory powers for ensuring that MNOs have appropriate multi-vendor strategies in place - Provide description of multi-vendor strategies and diversification strategy (per MNO and nationally) <u>For SM06:</u> - Provide description about measures taken to ensure resilience at national level through an adequate balance of suppliers	Sharing restriction
----	----------------	-------------------------	---	--	---------------------

SM05	No action taken yet		under investigation		TLP:Green
SM06	Planned		under investigation	Telecommunications Act Ch. 11a contains placeholder for lower level regulation to cover this measure	TLP:Green

3.b) Experienced or expected implementation factors of relevance (as per the toolbox: §4.2, pg.14)

Factor:	Relevance:	Remarks, explanations:	Sharing restriction
Resource costs			
Sector-specific economic Impact	Relevant	may impact bussiness investment plans	TLP:Green
Broader economic or society impact	Not directly relevant	could influence pricing of services	TLP:Green

4. Screening of foreign direct investment

4.a) Implementation planning

ID	Current status	Planned completion date	Remarks, explanations (include envisaged next steps if applicable)	Implementation details - If applicable, describe any steps taken or planned to be taken on the national level in regards to screening foreign direct investments across the 5G supply chain	Sharing restriction
SM07	In progress	Q3 2020	discussion on draft legislation in parliament almost finalized	Investment plans for parties targeted at critical services or organizations (telecom is included) will be screened by the government.	0

4.b) Experienced or expected implementation factors of relevance (as per the toolbox: §4.2, pg.14)

Factor:	Relevance:	Remarks, explanations:	Sharing restriction
Resource costs			
Sector-specific economic Impact	Relevant	business development of targeted company impacted	TLP:Green
Broader economic or society impact	Not directly relevant	secondary effect on market shares etc, because of attention by politicians, media or public	TLP:Green

5. Stronger security requirements for mobile network operators

5.a) Implementation planning

ID	Current status	Planned completion date	Remarks, explanations (include envisaged next steps if applicable)	Implementation details - Provide general Description of existing and/or planned mechanism or concrete steps taken (or planned to be taken) towards reinforcing existing and hardened technical security requirements for MNOs - Also include status of transposition of EECC, including any relevant dates and details, in particular with regards to the Article 40	Sharing restriction
TM01	In progress	Q4 2020		Apart from TM02, TM06 and TM11, all other measures are being implemented as enhancement of an existing measure or as a new measure under the umbrella of existing lower regulation. The scope of the lower regulation is resilience and continuity of services and is in force according to the Telecommunications Act. The basis is Article 13a of the EU Framework Directive (to be succeeded by article 40 of the EECC)	TLP:Green
TM02	Planned		awaiting EU wide approach		
TM03	In progress	Q4 2020			
TM04	In progress	Q4 2020			
TM05	In progress	Q4 2020			
TM06	Implemented		already covered by Telecommunications Act (Chapter 11a)		
TM07	In progress	Q4 2020			
TM08	In progress	Q4 2020			
TM11	Implemented		already covered by Telecommunications Act (Chapter 11a)		

5.b) Experienced or expected implementation factors of relevance (as per the toolbox: §4.2, pg.14)

Factor:	Relevance:	Remarks, explanations:	Sharing restriction
Resource costs	Relevant		
Sector-specific economic impact	Relevant	Telco's have to implement the new or expanded requirement	TLP:Green
Broader economic or society impact	Relevant	increased security for users	TLP:Green

Van:
Aan:

5.1.2e

Cc:

5.1.2e

Onderwerp:

Datum:

Bijlagen:

Schriftelijke ronde TFEV 15 mei - graag reactie uiterlijk 22 mei

vrijdag 15 mei 2020 16:57:29

Agenda TFEV 15052020.docx

Agendapunt 3.

Agendapunt 7 Ter info NL 200508 Questionnaire Toolbox implementation by MS.xlsx

5.1.2i

Beste leden van de Taskforce,

Hierbij ontvangt u de geannoteerde agenda voor het schriftelijk overleg. Per agendapunt staat een stand van zaken opgenomen. Op één punt wordt specifiek om uw reactie gevraagd; dit betreft agendapunt 3 inzake de beschikkingen, waarbij EZK twee beslispunten heeft aangedragen.

U kunt in een reply all op deze e-mail reageren naar de andere Taskforce leden op de punten uit de annotatie en specifiek de gevraagde besluiten. Graag ontvang ik uw reactie uiterlijk volgende week vrijdag 22 mei.

Met vriendelijke groet,

[Redacted signature]

5.1.2e

Ministerie van Justitie en Veiligheid

Turfmarkt 147 | 2511 DP | Den Haag

Postbus 20301 | 2500 EH | Den Haag

[Redacted contact information]

[Redacted contact information]

5.1.2e



H5

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon



5.1.2e

Datum

26 mei 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	15 mei 2020

1. Algemeen

Vanwege de maatregelen nav COVID-19 is besloten dit overleg niet fysiek door te laten gaan maar te kiezen voor een schriftelijke ronde. Dit betekent concreet dat in deze agenda de stand van zaken per onderwerp wordt weergegeven, net als de verwachte planning en eventuele aandachtspunten. Voor agendapunt 3 zijn vanuit EZK twee beslispunten ingebracht. Alle leden van de taskforce krijgen de mogelijkheid om via e-mail op deze agenda te reageren, bij voorkeur voor vrijdag 22 mei.

Vanwege verwachte besluitvorming zal de eerstvolgende TFEV weer fysiek bijeenkomen. Hierbij zullen vanzelfsprekend de maatregelen (social distancing en hygiëne) in acht worden genomen. Er wordt momenteel nog gezocht naar een datum, u wordt hierover zo spoedig mogelijk geïnformeerd.

2. Beschikkingen

- Er wordt gewerkt aan het concept voornemen van de beschikkingen. In de week van 2 juni is een vervolgbijeenkomst met NCTV, FIN, BZ, AT, EZK (DE & WJZ) om een nieuw concept en vervolgstappen te bespreken.
- Streven is rond de zomer tot een voornemen voor een beschikking te komen. Dit hangt mede af van de voortgang op hieronder beschreven punten.
- Na het versturen van een voornemen, krijgen de telco's de gelegenheid om hun zienswijze te geven, waarna de definitieve beschikking zal volgen, die openstaat voor bezwaar en beroep.
- Planning is om in Q4 een definitieve beschikking te versturen.
- Het proces heeft vertraging opgelopen. Mensen waren (deels) niet beschikbaar vanwege Corona en er is meer tijd nodig om de geopolitieke paragraaf van de beschikking vorm te geven en een realistische termijn voor uitfasering te bepalen.
- Voor dit laatste is de input van de telco's wenselijk. De telco's geven echter aan dat zij ervaren dat de vertrouwelijkheid van de lijst met

kritieke onderdelen hen hindert hier uitvoering aan te geven. [REDACTED]

- (1) [REDACTED]

5.1.2i

5.1.2i

- [REDACTED]

5.2.1

- [REDACTED]

5.2.1

- [REDACTED]

5.2.1

- (2) [REDACTED]

5.1.2i

- [REDACTED]

- (3) [REDACTED]

- [REDACTED]

5.1.2i

o

5.1.2i

Ter besluitvorming

1. Graag instemming van de Taskforce om binnen 3 weken besluitvorming voor te bereiden op de volgende punten:
 - a. Wanneer de telco's in gesprek kunnen met de vertrouwde leveranciers ter voorbereiding van de uitvoering van de beschikking, zonder de gerubriceerde lijst met kritieke onderdelen integraal te delen.
 - b. Wanneer de telco's in gesprek kunnen met de te weren leverancier ter voorbereiding van de uitvoering van de beschikking zonder de gerubriceerde lijst met kritieke onderdelen integraal te delen.

2.

5.1.2i

3. Ministeriële regeling

Met betrekking tot de ministeriële regeling (maatregel 1) zijn er geen beslispunten. Hieronder vindt u de terugkoppeling van de interdepartementale, technische sessie van 9 april jl. en de planning van de ministeriële regeling op hoofdlijnen. De uitwerking van de technische en organisatorische maatregelen wordt binnenkort naar u verstuurd.

Terugkoppeling technische sessie:

- Zoals besloten in de schriftelijke TFEV van eind maart 2020 heeft op verzoek van J&V op 9 april jl. een interdepartementale, technische sessie over de uitwerking van de technische en organisatorische maatregelen plaatsgevonden. Deze technische sessie diende als *eindtoets* opdat deze maatregelen kunnen worden vastgelegd in de ministeriële regeling (maatregel 1).
- De technische en organisatorische maatregelen, die in de ministeriële regeling zullen worden opgenomen zijn de afgelopen maanden door [REDACTED] uitgewerkt. Hierbij is nauw en frequent afgestemd met partijen vanuit de overheid (NBV, NCSC, Agentschap Telecom en EZK) en vanuit de markt (KPN, T-Mobile NL en VodafoneZiggo).
- Doel van deze afrondende technische sessie was na te gaan of de uitwerking van maatregelen recht doet aan de eerdere dreigingsanalyse (vastgelegd in [REDACTED] rapport d.d. mei 2019). Dienovereenkomstig waren alle partijen vertegenwoordigd die indertijd ook bij de dreigingsanalyse betrokken zijn

5.1.2i

5.1.2i

- geweest, te weten J&V (NCTV en NCSC), MIVD, NBV, Agentschap Telecom en EZK (directie Digitale Economie) en [REDACTED]
- De maatregelen zijn per dreigingsscenario uit het eerdere [REDACTED] rapport tegen het licht gehouden. Daarbij is expliciet besproken hoe de huidige detailuitwerking zich verhoudt tot de richtinggevende set van maatregelen die [REDACTED] in datzelfde onderzoeksrapport had opgenomen en hoe op specifieke punten (bijvoorbeeld met het oog op uitvoerbaarheid) voor alternatieve, eveneens veilige oplossingen is gekozen. Aanvullend hierop is teruggeblikt op het proces van de afgelopen maanden en is de beoogde reikwijdte van de regeling (zoals afgeleid uit het dreigingsbeeld) nader toegelicht.
 - Conclusies:
 - De deelnemers aan de sessie hebben gezamenlijk geconcludeerd dat er een goed en solide fundament ligt van technische en organisatorische maatregelen voor de scope uit het eerdere [REDACTED] rapport. Deze uitgewerkte maatregelen – 19 in totaal – zullen worden opgenomen in de ministeriële regeling.
 - Ontwikkelingen in de sector (bijvoorbeeld op het gebied van netwerktechnologie) dan wel nieuwe dreigingsbeelden zouden waar nodig in de structurele aanpak (maatregel 3) moeten worden geadresseerd. Niet uitgesloten is dat dit op termijn tot aanpassing van de ministeriële regeling zal leiden.
 - Hiermee wordt het [REDACTED] gefinaliseerd en kan verder gewerkt worden aan het ontwerpen van de ministeriële regeling.

5.1.2i

5.1.2i

5.1.2i

5.1.2i

5.1.2i

Planning

Processtap	Datum of periode
Opstellen concept-regeling	Heden tot 1 augustus
Opstellen artikelen, bijlage met technische en organisatorische maatregelen ([REDACTED]) & toelichting	
Interdepartementale afstemming	
Internetconsultatie en externe adviezen (Adviescollege Toetsing Regeldruk, Uitvoerbaarheids- & Handhaafbaarheidstoets (U&H-toets) Agentschap Telecom	
Verwerken reacties consultatie, ATR, U&H-toets	
Interdepartementale afstemming	
Notificatie Europese Commissie	1 augustus t/m 15 oktober
Notificatie periode	
Evt. verwerken reacties uit de notificatie	
Vaststelling regeling en publicatie	15 oktober t/m 1 november
Publicatie Staatscourant	1 november 2020

5.1.2i

¹ J&V: [REDACTED]; BZK: [REDACTED]; DEF: [REDACTED]; AT: [REDACTED]
[REDACTED]; [REDACTED]; EZK: [REDACTED]

4. Structurele samenwerking

De gesprekken tussen AT, MIVD, NBV en NCSC met de telecomaانبieders over de uitgangspunten voor de structurele samenwerking hebben vanwege COVID-19 en prioriteit op de beschikkingen en ministeriele regeling stilgelegen en worden zodra dit mogelijk is weer hervat. Voor de verdere uitwerking van de structurele samenwerking is het onder andere noodzakelijk dat de eerder toegezegde gesprekken met de telecomaانبieders op MT-niveau (CTO, CISO en evt. CEO niveau) gaan plaatsvinden. Hier wordt komende periode op ingezet.

[REDACTED]

5.1.2i

De inventarisatie van mogelijkheden om meer investeringszekerheid te bieden in de vormgeving van de structurele aanpak (aangekondigd in de vorige TFEV) heeft vanwege COVID-19 vertraging opgelopen en zal naar verwachting in de week van 22 juni worden opgeleverd. De uitwerking hiervan zal met u worden gedeeld.

5. Brandstichting zendmasten

In de afgelopen weken zijn in Nederland 27 (pogingen) tot brandstichting geregistreerd bij zendmasten. In een aantal gevallen hebben brandstichtingen geleid tot een verstoring in de continuïteit van mobiele netwerken. In andere gevallen konden omliggende zendmasten voldoende dekking bieden. EZK werkt met betrokken partijen aan een afwegingskader om de risico's voor het mobiele netwerk in kaart te brengen en eventueel gericht maatregelen te kunnen treffen. De politie doet onderzoek naar de verdachten en hun motieven. De brandstichtingen lijken verband te houden met complottheorieën die een verband suggereren tussen COVID-19 en 5G.

Ook vanuit de politiek is er veel aandacht voor dit onderwerp en zijn er Kamervragen gesteld. Dit onderwerp wordt binnen de bestaande verantwoordelijkheden opgepakt, de TFEV heeft hierin op dit moment geen rol.

6. Internationaal/Europees

De Prague Conference over 5G die gepland stond voor 5 mei is uitgesteld in verband met COVID-19 en zal naar verwachting in september (digitaal of fysiek) plaatsvinden.

Op 8 mei is de vragenlijst voor de NIS Cooperation Group naar u toegestuurd voor akkoord. Hierin staan de nationale maatregelen die worden genomen naar aanleiding van de EU toolbox. Op basis van de binnengekomen reacties zijn een aantal wijzigingen doorgevoerd, dit betreft:

- Tab A, kolom 6: meer toelichting gegeven over waarom dit als 'confidential' staat aangemerkt
- Tab A, kolom 12: verwijzing naar de Amvb toegevoegd, namen van wetgeving vertaald naar het Engels
- Tab A, kolom 14: correcte verwijzing naar AIVD en MIVD opgenomen
- Tab A, kolom 23: prioritering in lijn gebracht met eerdere inschatting die is gemaakt en naar EU-partners is gestuurd bij het aanleveren van het nationale risk assessment.
- Tab B, kolom 16: toevoeging van de zinsnede 'The assessment of threats, interests (and therefore assets) can change over time and are subject to constant monitoring. Security measures can be adjusted in light of these developments'.

In de bijlage vindt u de aangepaste vragenlijst. Deze wordt verstuurd naar de NIS Cooperation Group.

7. Vervolg gezamenlijk begrotingsvoorstel EV

Zoals in vorige TFEV gemeld is het gezamenlijk begrotingsvoorstel niet gehonoreerd. Er wordt nu door de betrokken departementen inzichtelijk gemaakt wat de gevolgen daarvan zijn, waar problemen/dilemma's met betrekking tot voortgang ontstaan en welke mogelijke oplossingen er zijn. De TFEV zal hiervan op de hoogte worden gesteld. Daarnaast wordt momenteel gewerkt aan een voorstel voor de inzet richting de nieuwe regeerperiode. Ook dit zal in de TFEV terugkomen.

Uitkomst schriftelijke ronde

Besluitvorming

1. Graag instemming van de Taskforce om binnen 3 weken besluitvorming voor te bereiden op de volgende punten:
 - a. Wanneer de telco's in gesprek kunnen met de vertrouwde leveranciers ter voorbereiding van de uitvoering van de beschikking, zonder de gerubriceerde lijst met kritieke onderdelen integraal te delen.
 - b. Wanneer de telco's in gesprek kunnen met de te weren leverancier ter voorbereiding van de uitvoering van de beschikking zonder de gerubriceerde lijst met kritieke onderdelen integraal te delen.

2. [REDACTED]

5.1.2i

Conclusie besluitvorming:

- TFEV is akkoord met gevraagde besluiten onder 1a en 1b. Vraag ten aanzien van dit besluitpunt is of het daadwerkelijk mogelijk is deze informatie niet te delen in de gesprekken met de leveranciers – kan dan op een juiste manier uitvoering worden gegeven aan de beschikking?
- TFEV bevestigt het beeld onder beslispoint 2 niet; er zijn een aantal vragen die eerst verduidelijkt dienen te worden. [REDACTED]
- Beide beslispointen komen terug in de eerstvolgende TFEV. De voorbereiding hiervan wordt interdepartementaal afgestemd.

5.1.2i

Wvttk:

- Verzoek vanuit diverse leden om de eerstvolgende TFEV fysiek en op korte termijn plaats te laten vinden.
- Gezamenlijke interdepartementale basispositie op het thema economische veiligheid: In de TFEV van 28 januari is uitgesproken om te zullen komen tot een gezamenlijke interdepartementale basispositie op het thema economische veiligheid. Het gaat hier om een set uitgangspunten die tevens als beknopte lijn kan dienen voor het uitdragen en duiden van de Nederlandse economische veiligheidsaanpak. BZ, EZK en NCTV hebben hiertoe een concept ontwikkeld. Graag agenderen we dit stuk voor discussie in de eerstvolgende TFEV.

- [REDACTED]

5.1.2a

Dep.-VERTROUWELIJK

[REDACTED]

Datum
15 mei 2020

5.1.2a



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

██████████
██████████

5.1.2e

Datum
22 juni 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	26 juni 2020, 08.30-10.00 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Beschikkingen 5G (EZK)

Bijlage 1. Beschikkingen 5G

3. Begrotingsvoorstel economische veiligheid: inzet 2020 en 2021 (NCTV)

Bijlage 2. Begrotingsvoorstel economische veiligheid: inzet 2020 en 2021

Bijlage 3. Begrotingsvoorstel EV voorjaarsnota 2020

4. Inzet voor de komende regeerperiode (NCTV)

Bijlage 4. Inzet voor de komende regeerperiode

5. Structurele samenwerking: verzoek regie en sturing (NCTV)

Verzoek regie en sturing: Mondelinge toelichting NCTV

Ter info: Bijlage 5. Oplegnota Rapport Dialogic, Bijlage 6. Rapport Dialogic Investeringszekerheid Telecommunicatiesector

6. Basispositie Economische Veiligheid (BZ)

Bijlage 7. Basispositie Economische Veiligheid

7. Internationaal/Europees

Bijlage 8. Oplegnota Rapport implementatie toolbox 5G

Bijlage 9. Rapport implementatie toolbox 5G

8. Parlementair

9. Rondvraag en afsluiting

Dep. **VERTROUWELIJK**

**Directoraat-generaal
Bedrijfsleven & Innovatie**

Behandeld door

5.1.2e

Datum
16 juni 2020

Kenmerk
DGBI / 20168400

Kopie aan

Bijlage(n)
1

Beschikkingen 5G, ten behoeve van besluitvorming van
de TFEV 26 juni 2020

- Bij de voorbereiding van de beschikking aan de telecomaanbieders (hierna telco's) waarin staat welke leverancier zij niet mogen gebruiken voor de kritieke onderdelen van hun telecomnetwerken en -diensten is een aantal vragen ontstaan rond de communicatie met de leverancier door de telco's [REDACTED] die wij voorleggen aan de TFEV ter besluitvorming.
- In de beschikking dient een termijn te worden opgenomen waarbinnen de niet vertrouwde leveranciers moeten worden uitgefaseerd uit de kritieke onderdelen. Aan de telco's is vanuit EZK, ten behoeve van het opnemen van die termijn in de ontwerp-beschikking, gevraagd om een inschatting hiervan. De telco's hebben aangegeven dat ze voor een goede inschatting van deze termijn (en vervolgens ook voor de daadwerkelijke uitfasering) in gesprek moeten met de nieuwe (vertrouwde) leveranciers en ook met de huidige (niet vertrouwde) leveranciers. Op deze manier zullen deze leveranciers de conclusie kunnen trekken dat zij tot de niet vertrouwde leveranciers horen, en dat bepaalde onderdelen als kritiek zullen worden aangewezen.¹ [REDACTED]

5.1.2i

5.1.2i en 5.2.1

5.1.2i

¹ De kritieke onderdelen van de telecomnetwerken zijn niet openbaar gemaakt omdat daarmee inzicht wordt gegeven in de kwetsbaarheden van het netwerk. Dit is juist informatie die voor kwaadwillende (statelijke) actoren interessant is en door hen misbruikt kan worden. N.a.v. een verzoek van de telco's heeft de TFEV besloten tot derubricering van de lijst van kritieke onderdelen en verstrekking aan de telco's onder DEP/TLP Amber en ondertekening van een verklaring door de telco's.

[REDACTED]

Ter besluitvorming

(1) Wanneer en hoe kunnen de telco's in gesprek met de vertrouwde leveranciers en de te weren leveranciers om kritieke onderdelen te kunnen vervangen?

De TFEV wordt geadviseerd om in te stemmen

- met de start van gesprekken tussen de telco's en de vertrouwde leveranciers en de te weren leveranciers om uitvoering te kunnen geven aan de voorbereiding op de verplichting.
- om deze gesprekken op korte termijn (direct na besluit TFEV) te laten starten.
- dat de telco's in deze gesprekken
 - o kunnen spreken over de kritieke onderdelen, op basis van need to know (en niet de gehele lijst)
 - o kunnen spreken over de verwachting dat de overheid maatregelen zal nemen, die bepaalde onderdelen betreffen en dat daar voorbereidingen voor worden getroffen,
 - o geen vragen zullen beantwoorden over de maatregelen, maar naar de overheid kunnen verwijzen.

[REDACTED]

5.1.2i

5.1.2a

Weging verzoek telco's vanuit verschillende perspectieven

De volgende perspectieven zijn van belang om een beslissing te kunnen nemen over gevraagde besluitvorming:

- Uitvoeringsperspectief
- Nationale veiligheidsperspectief
- Juridisch perspectief
- Diplomatiek perspectief

In de bijlagen treft u, per vraag, een nadere duiding aan van de bovengenoemde perspectieven.

BIJLAGE

Kernvragen:

- (1) Wanneer en hoe kunnen de telco's in gesprek met de vertrouwde leveranciers en de te weren leveranciers om kritieke onderdelen te kunnen vervangen?**

5.1.2i

(1) Wanneer en hoe kunnen de telco's in gesprek met de vertrouwde leveranciers en de te weren leveranciers om kritieke onderdelen te kunnen vervangen?

Om in de beschikking een realistische termijn voor uitfasering te bepalen en derhalve de continuïteit van de dienstverlening te kunnen garanderen is de input van de telco's noodzakelijk. De telco's geven echter aan dat zij ervaren dat de vertrouwelijkheid van de lijst met kritieke onderdelen hen hindert hier uitvoering aan te geven. Zij willen zo snel mogelijk in gesprek met de vertrouwde en te weren leveranciers om de kritieke onderdelen te kunnen vervangen. Ook als de telco's enkel in gesprek zullen gaan met de vertrouwde leveranciers, zal vervolgens breed in de markt (dus ook bij te weren leverancier) bekend worden dat wordt geweerd. Er is daarom besloten om deze twee vragen samen te bezien. Mogelijke momenten voor gesprekken tussen de telco's en de leveranciers kunnen zijn (a) direct na besluitvorming TFEV, (b) na uitbrengen voornemen, en (c) na uitbrengen beschikking. De telco's willen in dit gesprek kunnen spreken over de kritieke onderdelen van de lijst (niet integraal het gerubriceerde document), en zij willen kunnen aangeven dat het geen bedrijfsbeslissing is, maar verwijzen naar de overheid.

UITVOERINGSPECTIEF

- Uitgangspunt voor de telco's is dat contact met leveranciers een voorwaarde is om uitvoering te kunnen geven aan de verplichting om de onderdelen te vervangen, en een termijn voor uitfasering te bepalen.
- Vanuit uitvoeringsperspectief heeft het de voorkeur dat de telco's zo snel mogelijk in gesprek kunnen met de vertrouwde leveranciers en de te weren leverancier, om in ieder geval de relevante te vervangen producten en diensten in de kritieke netwerkonderdelen te kunnen bespreken.
- De te weren en nieuwe leverancier en de telco moeten samenwerken om te bezien hoe het oude systeem geleidelijk kan worden overgezet op het nieuwe systeem, om continuïteit bij migratie van complexe systemen voldoende te kunnen waarborgen.
- Indien de telecomaanbieders pas na het versturen van het voornemen, of na het versturen van de beschikking in gesprek kunnen gaan met de leveranciers, zullen de telco's hoogstens op basis van hun eigen informatie een inschatting (met naar verwachting ruime marges) kunnen maken voor een termijn van uitfasering.

NATIONALE VEILIGHEID

- Er is vanuit de nationale veiligheid an sich geen bezwaar om leveranciers te informeren dat het voornemen bestaat om hen, in relatie tot inzet in de kritieke onderdelen, niet meer als vertrouwde partijen aan te merken.
- Vanuit nationale veiligheid geldt dat bij het delen van TBB-kritieke onderdelen grote terughoudendheid moet gelden. Indien het nodig is voor

de uitvoerbaarheid om deze informatie breder te delen moet het belang van de veiligheid worden meegewogen. Hierbij geldt:

- Uitgangspunt: bespreking van kritieke onderdelen altijd op basis van need-to-know
- Telco's kunnen gericht de kritieke onderdelen bespreken die uitgefaseerd moeten worden. Hierbij mogen de kritieke onderdelen worden genoemd maar mogen ze niet als kritiek worden benoemd.
- Onderliggende TBB's mogen niet worden gedeeld
- De integrale lijst met kritieke onderdelen mag niet worden verstrekt
- De informatie uit onderliggende veiligheidsanalyses mag niet worden verstrekt.
- Bij doorvragen van niet-vertrouwde leveranciers over waarom ze worden uitgefaseerd kunnen de telco's aangeven dat ze daar geen nadere toelichting op kunnen geven. Hierbij kan worden doorverwezen naar de overheid.

JURIDISCH PERSPECTIEF

- Vanuit juridisch perspectief is van belang dat telco's niet reeds vóór het nemen van de ontwerp-beschikking in gesprekken met leveranciers mededelen dat zij concrete aanwijzingen hebben dat die leverancier in die ontwerp-beschikking als niet-vertrouwd zal worden aangemerkt. Die zekerheid is immers pas vanaf het moment dat er een ontwerp-beschikking is uitgebracht.
- Dit neemt niet weg dat telco's bijvoorbeeld wel op hoofdlijnen al vóór de ontwerp-beschikkingen in gesprek kunnen gaan met mogelijk te weren leveranciers over (alle) lopende contracten, om zo aan de overheid een indicatie te kunnen geven van de gewenste uitfaseertermijn, zonder daarbij gerubriceerde informatie te delen of op de voorgenomen besluitvorming vooruit te lopen. Voorstelbaar is daarbij dan bv. dat wordt verwezen naar de meer algemene mogelijkheid (gelet op het Besluit, berichtgeving in andere landen, etc.) dat de telco een (ontwerp-) beschikking gaat krijgen die strekt tot het weren van de betrokken leverancier.

DIPLOMATIEK PERSPECTIEF

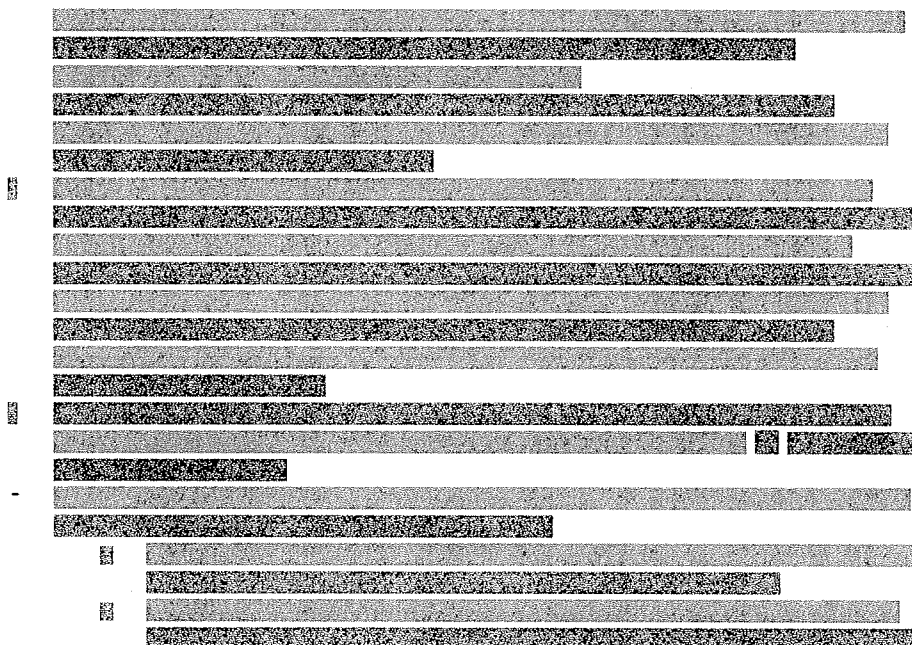
- Het uiteindelijke moment waarop de te weren partij te horen krijgt dat deze zal worden geweerd is zeer gevoelig en kan tot spanning in de bilaterale relatie met het land op de achtergrond leiden. [REDACTED]

5.1.2a

Tegelijkertijd is dit - gegeven het genomen besluit - uiteindelijk niet te vermijden. Door weloverwogen en zo zorgvuldige mogelijke timing kan wel de kans op grote schade zo veel mogelijk worden ingetoomd.

- [REDACTED]

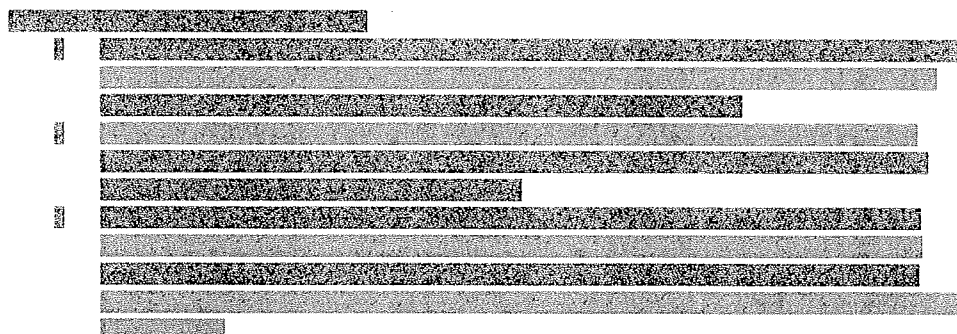
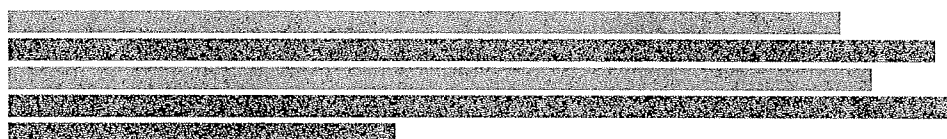
5.1.2a



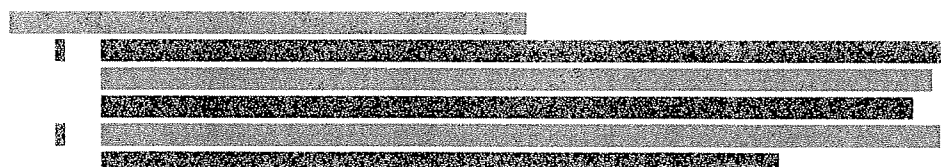
5.1.2a



5.1.2i



5.2.1i en 5.2.1



5.2.1i en 5.2.1



Category	Threat to Security (%)	Not a Threat (%)
All respondents	85	15
Male	88	12
Female	82	18
18-29	80	20
30-49	85	15
50-69	88	12
70+	90	10

A horizontal bar chart titled 'U.S. should take action to address climate change' showing the percentage of respondents who believe the U.S. should take action to address climate change. The chart is broken down by age group (18-29, 30-49, 50-69, 70+) and gender (Male, Female). The y-axis lists the age groups and genders. The x-axis represents the percentage, ranging from 0 to 100. The bars are color-coded: dark blue for 'U.S. should take action to address climate change' and light blue for 'U.S. does not need to take action to address climate change'.

Age Group	Gender	U.S. should take action to address climate change (%)	U.S. does not need to take action to address climate change (%)
18-29	Male	95	5
	Female	98	2
30-49	Male	95	5
	Female	98	2
50-69	Male	90	10
	Female	95	5
70+	Male	85	15
	Female	90	10

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

Administration	Percentage
Current Administration	85%
Previous Administration	15%

Begrotingsvoorstel economische veiligheid – inzet 2020 en 2021

Gevraagde besluiten

- Bepalen prioritaire onderwerpen voor 2020 en 2021;
- Instemmen (door desbetreffende organisaties) met het vrijmaken van middelen voor prioritaire onderwerpen voor 2020 en 2021;
- Structurele middelen voor alle onderwerpen uit het begrotingsvoorstel vanaf 2022 meenemen in de inzet richting komende regeerperiode;

Aanleiding

De afgelopen maanden is gewerkt aan een voorstel voor de voorjaarsnota 2020 met intensiveringen om de economische veiligheid, digitale weerbaarheid en vitale infrastructuur te beschermen (zie bijlage 3). Verschillende departementen zijn betrokken geweest bij de voorbereiding van dit begrotingsvoorstel (EZK, BZ, BZK, BHOS, DEF, IenW, OCW en JenV). De maatregelen kennen een nauwe afhankelijkheidsrelatie en betroffen in totaal circa €36 miljoen. Vanwege de nauwe samenhang van de verschillende maatregelen en de gemaakte afspraak tussen de departementen om het begrotingsvoorstel als één geheel in te dienen en te verdedigen heeft JenV namens betrokkenen de gesprekken met Financiën gevoerd. Hierbij is helaas het begrotingsvoorstel niet gehonoreerd. Hierdoor bestaat er een gat tussen de benodigde en beschikbare middelen.

Prioritaire onderwerpen

Per maatregel is bekeken wat de precieze kosten per organisatie zijn, of deze kosten oplosbaar zijn binnen de eigen begroting, of er een andere oplossing mogelijk is en wat de impact van beperkte middelen is (vanaf p. 3). Voor sommige maatregelen uit het begrotingsvoorstel geldt dat er acuut behoefte is aan (aangepaste) inzet van middelen doordat het een verplichting of toezegging is en inzet hiervan niet kan wachten tot de nieuwe regeerperiode. Departementen hebben daarbij onderzocht wat er mogelijk is om in aangepaste vorm toch uitvoering te geven aan de maatregel.

Onderstaande lijst is een voorstel met een aantal onderwerpen die geprioriteerd kunnen worden en de middelen die hiervoor noodzakelijk zijn in 2020 en 2021.

1. *Structurele samenwerking om dreiging vanuit geavanceerde actoren in de telecomsector tegen te gaan (intensief en gericht; maatregel TFEV)*
 - Kosten 2020 en 2021: 3.2 miljoen (2020: 1.6 mln, 2021: 1.6 mln),
 - Betrokken organisaties: AIVD, EZK, MIVD, NCSC en NCTV.
 - Voorgedragen oplossing: Herschikking van Fte's. Dit zal ten koste gaan van andere taken en verantwoordelijkheden.
2. *Uitvoeringswet Europese FDI-screeningsverordening (EU-contactpunt)*
 - Kosten 2020 en 2021: 0.6 mln (2020: 0.3 mln, 2021: 0.3 mln)
 - Betrokken organisaties: EZK, BZ, J&V.
 - Voorgedragen oplossing: EZK, J&V en BZ dragen gezamenlijk de kosten van 0.6 mln voor de operationalisering van het EU-contactpunt (afpraak MR, 0.3 mln per jaar, verdeelsleutel nog niet bepaald).
3. *Uitvoering stelsel van investeringstoetsing*
 - Kosten 2020 en 2021: 1.65 mln (2020: 0.45 mln, 2021: 1.2 mln)
 - Betrokken organisaties: EZK, J&V en betrokken vakdepartementen.
 - Voorgedragen oplossing: EZK, J&V en betrokken vakdepartementen delen kosten, verdeelsleutel nog niet bepaald.
4. *Screening ter voorkoming ongewenste kennisoverdracht (Iranverordening)*
 - Kosten 2020 en 2021: 2 mln (2020: 1 mln, 2021: 1 mln),
 - Betrokken organisaties: BZ, OCW en J&V
 - Voorgedragen oplossing: Herschikking van fte's, dit zal ten koste gaan van andere taken en verantwoordelijkheden.

- N.b. dit is vooruitlopend op het invoeren van een brede kennisregeling en gaat hierin ook t.z.t. op.

Gevraagd besluit

1. Bepalen prioritaire onderwerpen voor 2020 en 2021;
2. Instemmen (door desbetreffende organisaties) met het vrijmaken van middelen voor prioritaire onderwerpen.

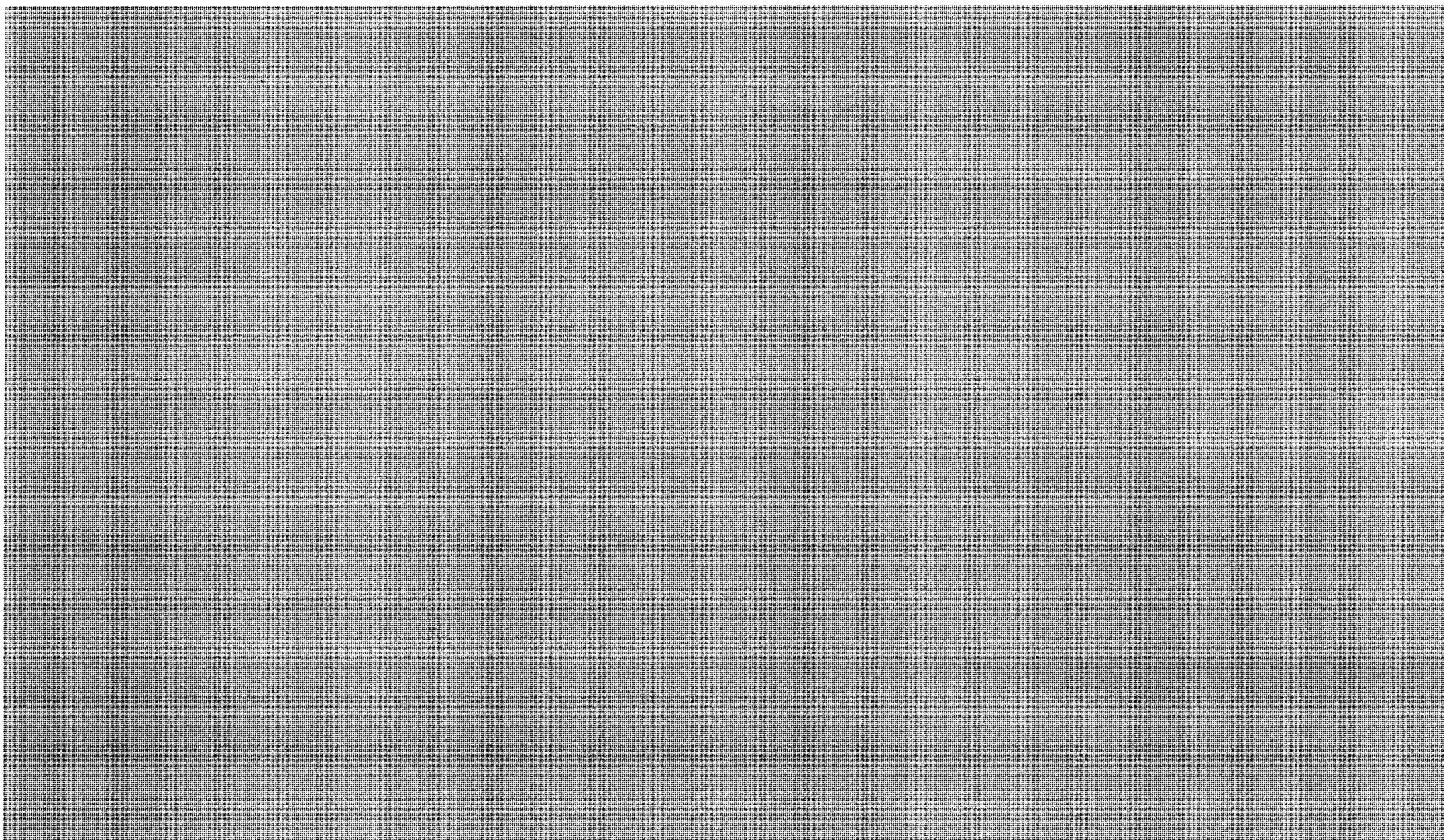
Inzet voor de komende regeerperiode

Hiernaast wordt ook gewerkt aan een voorstel voor inzet richting de komende regeerperiode (zie bijlage 4). Het voorstel is om de structurele inzet van de prioritaire onderwerpen en alle overige onderwerpen uit het begrotingsvoorstel hierin mee te nemen.

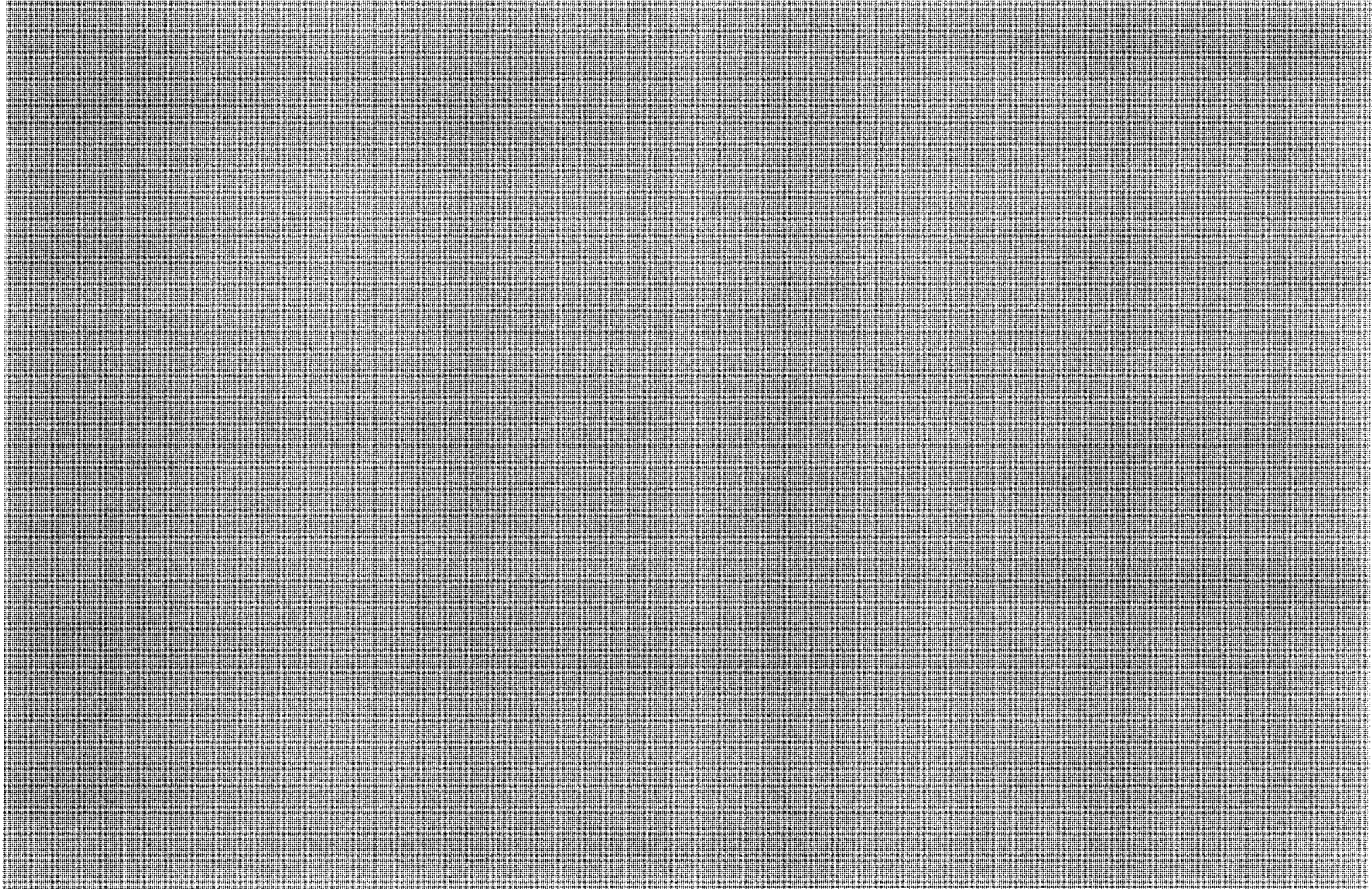
Gevraagde besluiten

- Structurele middelen voor alle onderwerpen uit het begrotingsvoorstel vanaf 2022 meenemen in de inzet richting komende regeerperiode;

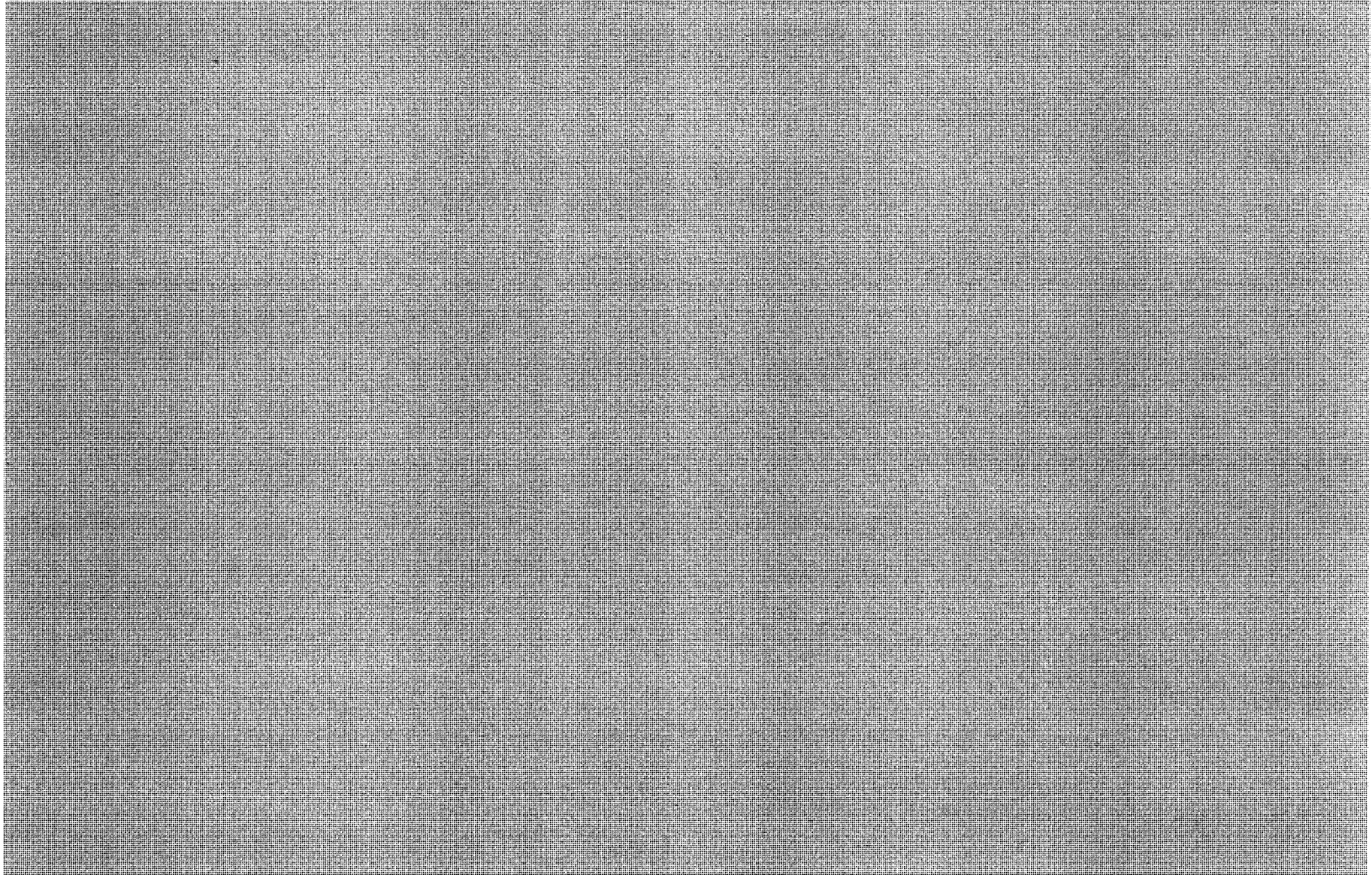
Begrotingsvoorstel EV – middelen korte termijn¹



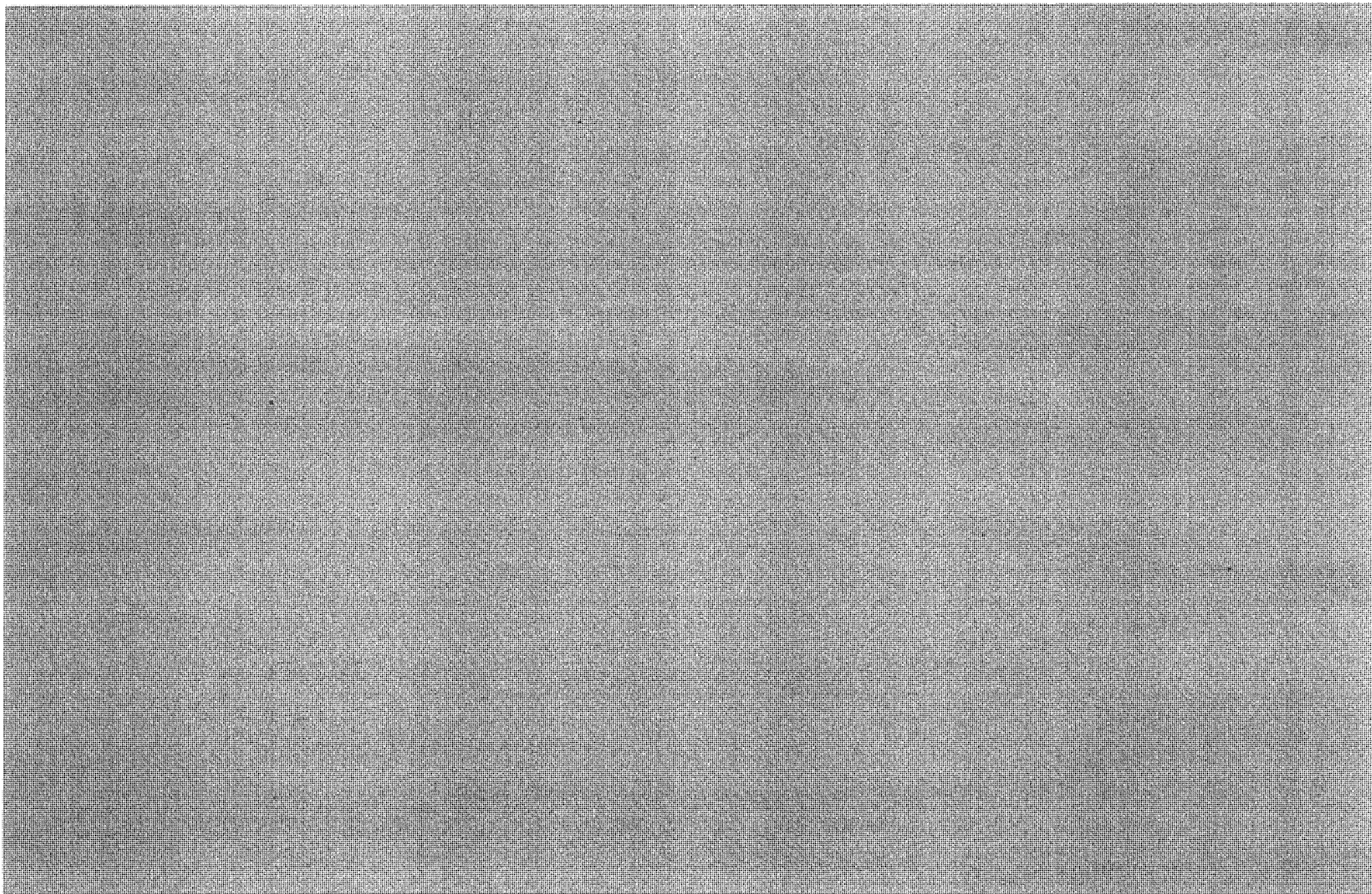
5.2.1



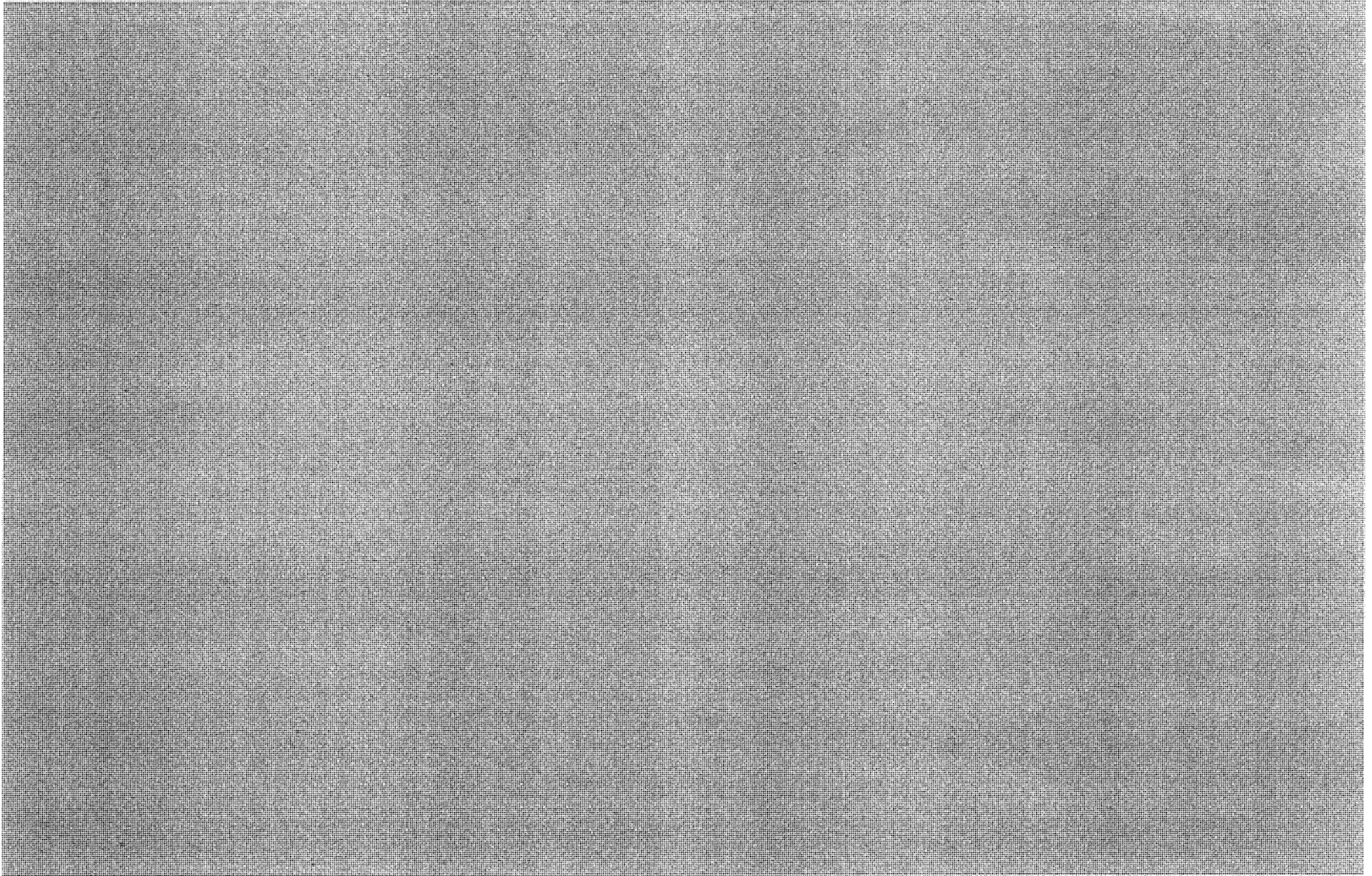
5.2.1



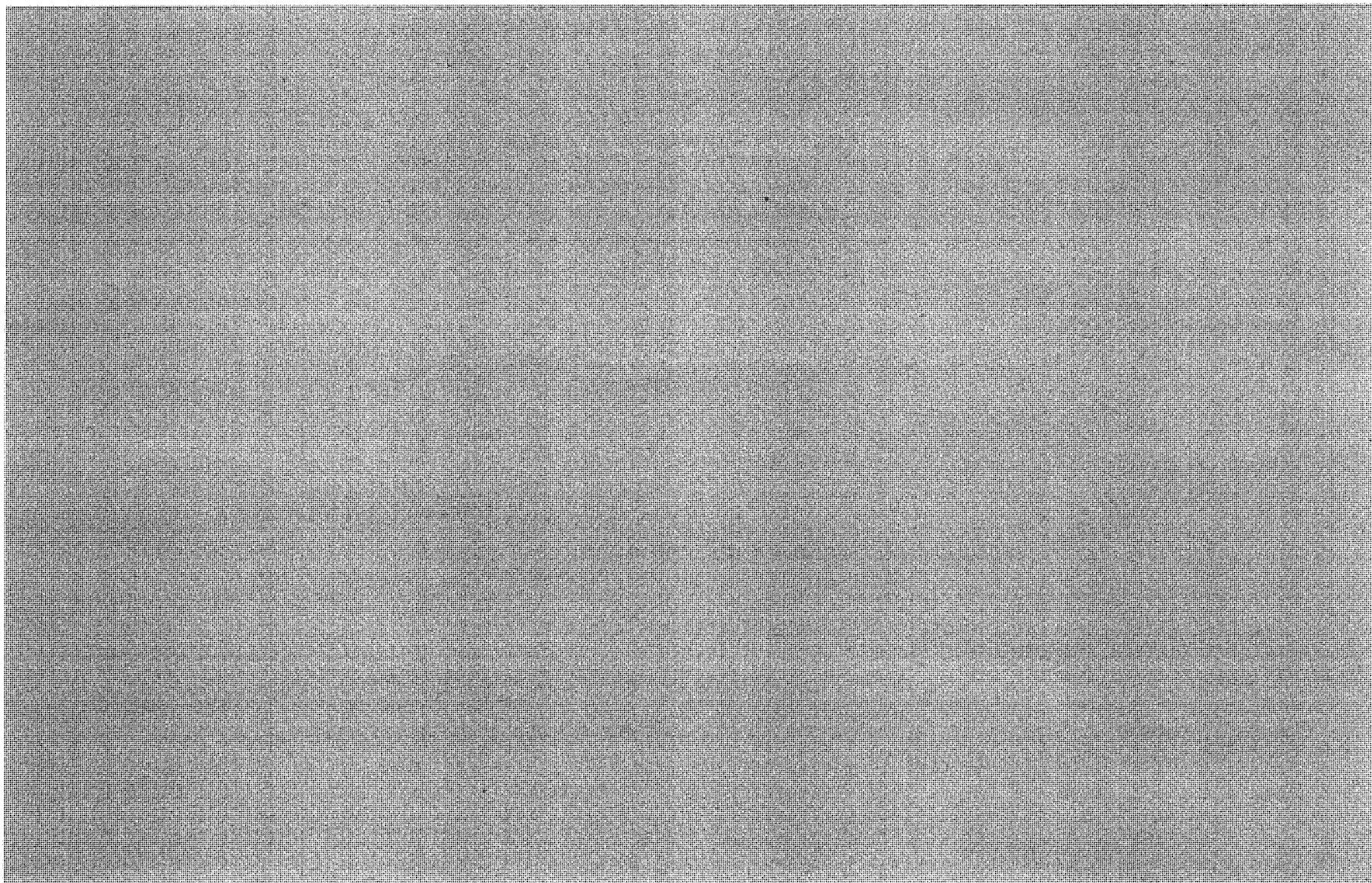
5.2.1



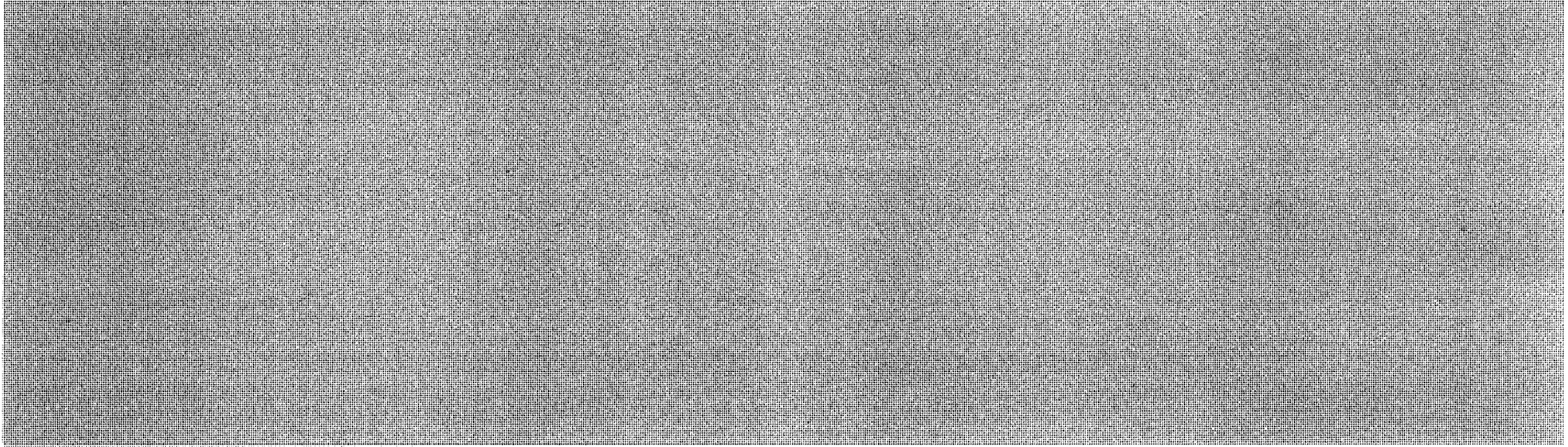
5.2.1



5.2.1



5.2.1



5.2.1

Inzet voor de komende regeerperiode

De Taskforce Economische Veiligheid heeft opdracht gegeven om te werken aan een gezamenlijk voorstel voor de inzet voor de komende regeerperiode. Hierbij is de wens uitgesproken om 'breed' in te zetten in vergelijking tot het begrotingsvoorstel voor de voorjaarsnota 2020.¹ In deze nota wordt de Taskforce Economische Veiligheid gevraagd om richting te geven aan de verdere uitwerking van dit voorstel.

De openstaande acties rondom het gezamenlijk begrotingsvoorstel voor de voorjaarsnota van 2020 worden in een separate nota behandeld (bijlage 2).

Scope en ambitie

Onderstaand schema schetst een aantal opties voor de scope en ambitie voor de inzet voor de komende regeerperiode.

Hierbij wordt voortgebouwd op het gezamenlijke begrotingsvoorstel voor de voorjaarsnota van 2020 (zie bijlage 3), waarin een groot aantal maatregelen zijn uitgewerkt en onderbouwd. De scope van dit voorstel is economische veiligheid, waarbij wel een flink aantal maatregelen gericht op cybersecurity en bescherming van vitale infrastructuur zijn meegenomen. Dit voorstel bevindt zich qua ambitie links in het schema: het omvat maatregelen die al zijn aangekondigd door het kabinet, voortkomen uit een verplichting vanuit Europese wetgeving of een logische en/of noodzakelijke toevoeging zijn van reeds genomen maatregelen.

Scope	Huidige ambitie <u>waarmaken</u> voor Economische Veiligheid, vitaal en cyber security	Huidige ambitie <u>uitbreiden</u> voor Economische Veiligheid, vitaal en cyber security	<u>Next level</u> voor Economische Veiligheid, vitaal en cyber security
	Huidige ambitie <u>waarmaken</u> voor Economische Veiligheid, vitaal	Huidige ambitie <u>uitbreiden</u> voor Economische Veiligheid, vitaal	<u>Next level</u> voor Economische Veiligheid, vitaal
	Huidige ambitie <u>waarmaken</u> voor Economische Veiligheid	Huidige ambitie <u>uitbreiden</u> voor Economische Veiligheid	<u>Next level</u> voor Economische Veiligheid
Ambitie			

Scope

In een eerste bijeenkomst van de betrokken departementen is de wens uitgesproken om een consistent en samenhangend pakket aan maatregelen op te stellen voor de inzet voor de komende regeerperiode. Vanwege de breedte van de thema's economische

¹ Verslag Taskforce Economische Veiligheid 18 december 2019. Het voorstel voor de voorjaarsnota 2020 beperkte zich tot maatregelen op economische veiligheid met uitstraling naar vitaal en cyber.

veiligheid, bescherming vitale infrastructuur en cyber security, lijkt dit proces behapbaarder te houden wanneer de voorstellen voor de verschillende thema's eerst separaat worden uitgewerkt. Op dit moment lopen er al een aantal parallelle trajecten waar ook aan deze thema's wordt gewerkt:

- In het Directeuren overleg cybersecurity (Docs) wordt gewerkt aan fiches en eventuele claims op het gebied op cybersecurity. De focus is de uitwerking van de maatregelen die zijn aangekondigd in de kabinetsreactie op het WRR-rapport: 'Voorbereiden op digitale ontwrichting'. De opbrengst richting de formatie wordt vastgesteld in de ACEV en MCEV.
- De CVIN heeft opdracht gegeven tot beleidsopvolging op het gebied van statelijke dreigingen. Deze opbrengst wordt ook behandeld en vastgesteld in de ACEV en MCEV.
- Momenteel loopt ook de jaarlijkse update van de Geïntegreerde Aanwijzing

Voorstel is om de scope van het voorstel voor de inzet voor de komende regeerperiode onder aansturing van de TFEV te richten op economische veiligheid², inclusief de maatregelen die nodig zijn om de structurele samenwerking te realiseren om dreiging vanuit geavanceerde actoren voor vitale processen tegen te gaan. Hierbij wordt afgestemd met de andere trajecten zodat maatregelen die zich op het snijvlak van de verschillende thema's bevinden niet tussen wal en schip vallen. Richting de besluitvorming in het najaar kan worden bepaald of alles samen in één voorstel wordt gevlochten met één overkoepelende boodschap of dat per thema aparte fiches worden ingediend.

Gevraagd besluit 1:

Akkoord gaan met de hierboven omschreven scope: economische veiligheid, inclusief maatregelen die nodig zijn voor structurele samenwerking vitale processen.

Ambitie:

Bovenstaand schema onderscheidt drie ambitieniveaus:³

- 1) **Huidige ambitie waarmaken:** Ambitie zoals geformuleerd in begrotingsvoorstel 2020. Dit betreffen maatregelen die al zijn aangekondigd door het kabinet of voortkomen uit een verplichting vanuit Europese wetgeving of een logische en/of noodzakelijke toevoeging zijn van reeds genomen maatregelen.
- 2) **Huidige ambitie uitbreiden:** Aanvullende maatregelen nemen, bijvoorbeeld het uitbreiden van de structurele samenwerking naar meerdere vitale processen en het updaten van faillissementswetgeving zodat er kan worden ingegrepen wanneer er nationale veiligheidsrisico's ontstaan.
- 3) **Nieuwe ambitie opstellen/'Next level':** Ambitieuze inzet waarbij de overheid een andere rol, verantwoordelijkheid of taak op zich neemt. Hierbij kan bijvoorbeeld gedacht worden aan een rijksbrede "ABDO"-regeling voor aanbestedingen en industrieveiligheid of het investeren in Europese kampioenen.

De voorbereiders van de TFEV zullen een uitgebreidere probleemanalyse uitvoeren op basis waarvan deze ambitieniveaus ingevuld, aangescherpt of eventueel bijgesteld kunnen worden. Het gevraagde besluit is bedoeld om een eerste richting te krijgen op de gewenste ambitie.

² Naast recente analyses, herbevestigt de COVID-19 crisis de noodzaak om de economische veiligheid te waarborgen. Statelijke actoren spelen in op kwetsbaarheden en afhankelijkheden; denk aan Nederlandse afhankelijkheden m.b.t. de productie en levering van persoonlijke beschermingsmiddelen en grondstoffen voor medicijnen en vaccins.

³ Het ambitieniveau is mede afhankelijk van de gekozen scope. Voor cybersecurity geldt bijvoorbeeld dat de in kamerbrieven aangekondigde maatregelen al vrij ambitieus zijn in vergelijking met de aangekondigde maatregelen op het gebied van economische veiligheid.

Gevraagd besluit 2:

Richting geven voor de inzet richting nieuwe regeerperiode:

1. Huidige ambitie waarmaken
2. Huidige ambitie uitbreiden
3. Nieuwe ambitie opstellen/'next level'

Besluitvorming

Het gezamenlijke begrotingsvoorstel voor de voorjaarsnota van 2020 is ontwikkeld onder aansturing van de Taskforce Economische Veiligheid. Destijds was de directe aanleiding dat aanvullende middelen nodig waren voor de structurele samenwerking telecom. Vervolgens is besloten om breder te inventariseren welke middelen nodig zijn op het gebied van economische veiligheid. Het lijkt logisch om besluitvorming over de inzet voor de komende regeerperiode plaats te laten vinden in de Ambtelijke Commissie Economie en Veiligheid (ACEV) en Ministeriele Commissie Economie en Veiligheid (MCEV). Hiermee kunnen de hierboven beschreven aanpalende trajecten bij elkaar worden gebracht. De TFEV stuurt op de uitwerking van het voorstel.

Gevraagd besluit 3:

Akkoord gaan met voorstel om besluitvorming in ACEV en MCEV plaats te laten vinden.

Tijdspad

Juni 2020:	Besluit TFEV scope, richting voor ambitie, planning en besluitvorming
Juli 2020:	Ambitie scherpstellen op basis van probleemanalyse
Juli 2020:	Uitwerken groslijst ⁴ maatregelen o.b.v. gekozen scope en ambitie
Okt 2020:	Uitgewerkte fiches per maatregel gereed
Nov/Dec 2020:	Besluitvorming

Gevraagd besluit 4:

Akkoord gaan met bovenstaand tijdspad.

⁴ Hiervoor kan gebruik gemaakt worden van de eerder uitgevoerde inventarisatie voor het gezamenlijk begrotingsvoorstel voor de voorjaarsnota van 2020 en van ambtelijke verkenningen zoals de Brede Maatschappelijke Heroverwegingen.



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**
TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
22 juni 2020
Ons kenmerk

oplegnota

Rapport Dialogic

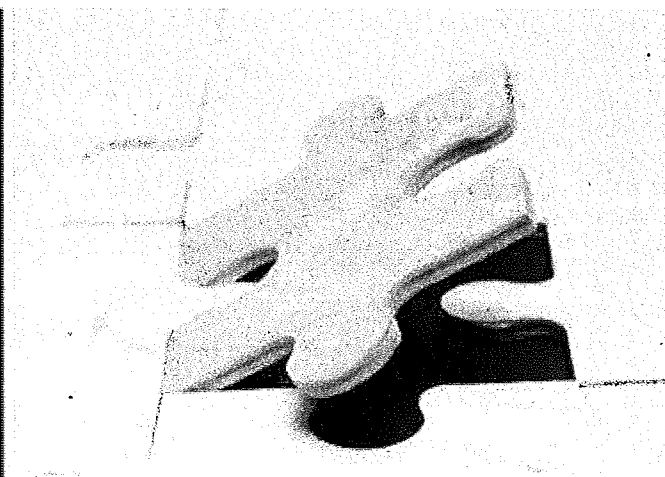
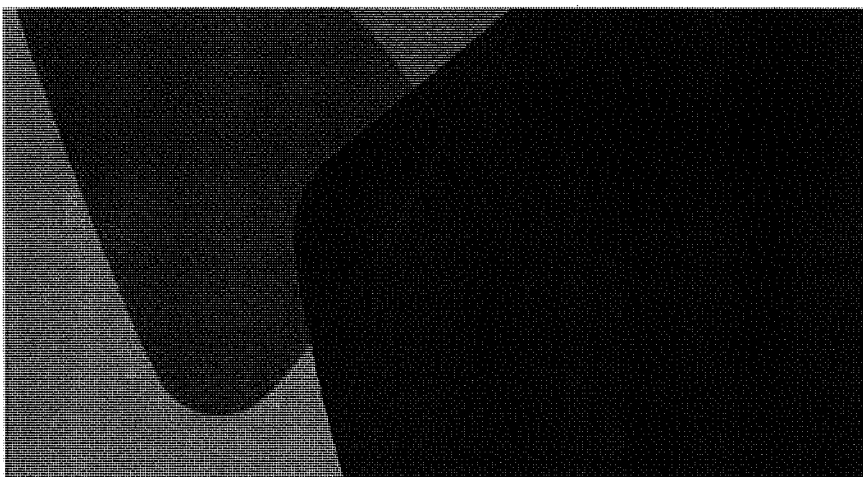
Gevraagde beslissing/doel
Samenvatting

Ter informatie

In opdracht van EZK heeft Dialogic een rapport opgesteld met een inventarisatie van mogelijkheden hoe meer investeringszekerheid te bieden in de vormgeving van de structurele aanpak.

Het rapport betreft de visie van Dialogic en is opgesteld op basis van een literatuurstudie en gesprekken met de drie mobiele netwerkaanbieders en met enkele beleidsmakers van andere landen.

Het rapport treft u hierbij ter informatie aan. Er zal interdepartementaal worden gezien hoe elementen uit dit rapport kunnen worden meegenomen in de structurele aanpak. De uitkomst hiervan zal aan u worden voorgelegd.



Investeringszekerheid in de telecommunicatiesector bij overheidsmaatregelen rondom nationale veiligheid

COMMERCEEL VERTROUWELIJK

In opdracht van:

Ministerie van Economische Zaken en
Klimaat

Project:

2020.015

Publicatienummer:

2020.015.2010 v0.9.9

Datum:

Utrecht, 22 juni 2020

Auteurs:

[Redacted]
 [Redacted]
 [Redacted]
 [Redacted]
 [Redacted]

5.1.2e



Inhoudsopgave

Managementsamenvatting	5
1 Introductie.....	9
1.1 Achtergrond	9
1.2 Onderzoeksvraag	10
1.3 Uitvoering.....	10
1.4 Leeswijzer	11
2 De relevantie van investeringszekerheid voor economische ontwikkeling.....	13
2.1 Investeringszekerheid leidt tot economische groei.....	13
2.2 Onzekerheid leidt tot lagere investeringen	16
2.3 Strategieën om de investeringszekerheid te vergroten.....	21
3 De impact van het Besluit op investeringen in de telecomsector.....	25
3.1 Reikwijdte van de impact.....	25
3.2 Bestaande marktdynamiek.....	26
3.3 Impact op investeringsbeslissingen	28
3.4 Impact op marktdynamiek	30
3.5 Impact op andere delen van het telecom-ecosysteem	31
4 Vormgeving van de structurele aanpak.....	33
4.1 Kaders van de structurele aanpak	33
4.2 Inrichten van een proces hoe met nieuwe dreigingen wordt omgegaan.....	37
4.3 Voorkomen van ongewenste investeringen.....	43
4.4 Ontwikkelen van instrumenten om marktdynamiek te verbeteren	53
5 Conclusies.....	55
Referenties	59
Bijlage 1. Landenstudies	63
5.1 Ex ante toetsing van investeringen	63
5.2 Realiseren van duidelijkheid over welke onderdelen in aanmerking komen	65
5.3 Realiseren van duidelijkheid over welke leveranciers (niet) toegestaan zijn	67
5.4 Relevante bronnen.....	68

Managementsamenvatting

De afgelopen jaren is er een discussie ontstaan over de veiligheid en integriteit van telecommunicatiesystemen. Centraal staan de systemen die afkomstig zijn van leveranciers uit landen met een naar Nederland mogelijk offensief cyberprogramma. Daarbij worden risico's gezien ten aanzien van (1) de beschikbaarheid van netwerken en (2) de confidentialiteit van de data die over deze netwerken gaat. In Nederland heeft dit onder meer geleid tot het Besluit Veiligheid en Integriteit. Daarmee kunnen telecomoperators verplicht worden bepaalde apparatuur en diensten van bepaalde leveranciers uit bepaalde delen van het netwerk te verwijderen. Daarnaast kunnen ook technische en organisatorische maatregelen worden opgelegd. Het Besluit biedt veel beleidsflexibiliteit aan de overheid. Voor telecomoperators ontstaat echter wel onzekerheid over (1) wanneer (2) welke onderdelen van de bedrijfsvoering, producten en diensten van (3) welke leverancier verwijderd moeten zijn. Voor het doen van investeringen in telecommunicatie betekent deze onzekerheid een flinke uitdaging, want hoe kun je verantwoorden dat de overheid te allen tijde je miljoeneninvesteringen in systemen uit de markt kan nemen?

Een manier om deze onzekerheid te verkleinen is het opzetten van een structurele aanpak tussen overheid en telecomoperators om de nationale veiligheid te beschermen tegen risico's die volgen uit de digitale dreiging vanuit geavanceerde (statelijke) actoren via misbruik van de telecomsector én waarin het belang van investeringszekerheid wordt meegenomen. In dit rapport staat dan ook de volgende vraag centraal: *"Hoe kan aan Nederlandse telecomoperators meer investeringszekerheid worden geboden in de vormgeving van de structurele aanpak?"*

Een goed investeringsklimaat is essentieel voor de economische ontwikkeling van een land. Investeringsbeslissingen in ICT waren de afgelopen decennia -direct en indirect- verantwoordelijk voor ruim een derde van de economische groei in Nederland. Het zorgt ervoor dat bedrijven productiever worden en nieuwe diensten ontwikkelen. Doordat het gaat om investeringen op de lange termijn, is zekerheid een essentiële voorwaarde voor bedrijven om te investeren. Overheden kunnen zekerheid bieden (bijvoorbeeld door het bieden van een goed functionerend juridisch systeem) maar kunnen ook zorgen voor onzekerheid. Beleid dat voorspelbaar, non-discriminair, begrijpelijk en transparant is zorgt voor zekerheid. Bij het maken van investeringsbeslissingen hanteren bedrijven een risico-opslag. Hoe hoger het risico, hoe hoger de opslag en hoe lager de bereidheid tot investeren, zeker in projecten met een lange tijdshorizon.

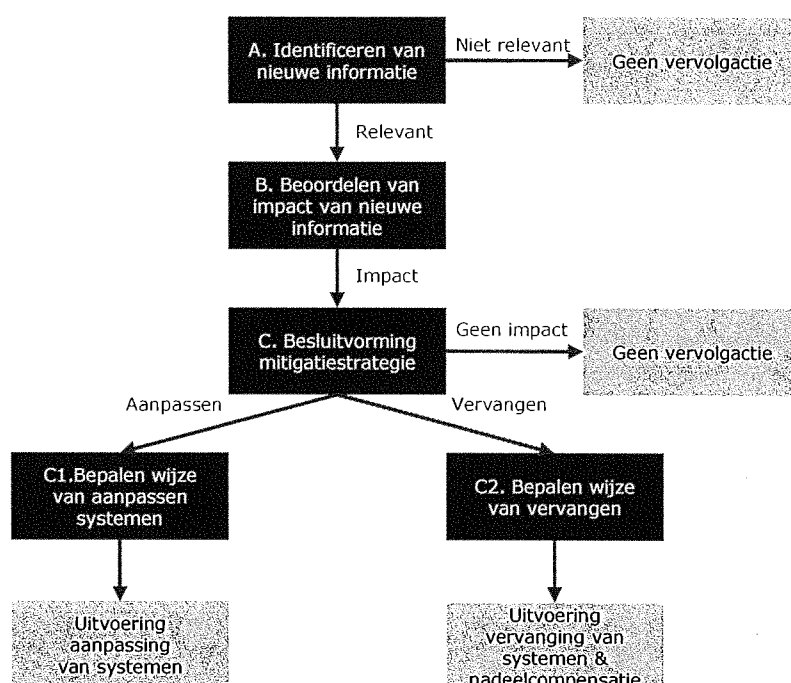
Het Besluit en hoe daar in de toekomst invulling aan wordt gegeven door de overheid introduceert onzekerheid voor telecomoperators. Welke impact dit heeft op hun investeringsbeslissingen is lastig is te schatten. Operators hebben bij investeringsbeslissingen te maken met een hoge mate van onvoorspelbaarheid welke systemen in de toekomst moeten worden verwijderd. Dit kan leiden tot een hogere risico-opslag. Er kan ook een situatie van "zelfcensuur" ontstaan waarbij operators op basis van hun *interpretatie* van het besluit bepaalde leveranciers uitsluiten. Mogelijk dempt de marktdynamiek tussen operators in Nederland de impact op investeringsbeslissingen omdat vanwege sterke concurrentie investeringen beperkt kunnen worden uitgesteld. Als de onzekerheid te groot wordt, dan bestaat echter ook de mogelijkheid dat de Nederlandse telecommarkt in een ander, minder optimaal, evenwicht belandt. Dit kan een flinke impact hebben aangezien de huidige marktdynamiek een van de redenen is dat wij in Nederland een van de beste (mobiele) netwerken ter wereld hebben. Tot slot kan er een effect ontstaan waarbij telecomoperators hun schaarse capaciteit moeten inzetten voor het wijzigen van systemen en niet voor het uitvoeren van (innovatieve) projecten.

De structurele aanpak kan Nederlandse telecomoperators meer investeringszekerheid bieden. Drie pijlers zijn hiervoor van belang:

- Er moet een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid worden gevonden. Beide aspecten zijn essentieel voor onze maatschappij. Overheden moeten accepteren dat volledige flexibiliteit niet mogelijk is en dat bedrijven investeringszekerheid nodig hebben. Bedrijven moeten accepteren dat volledige investeringszekerheid niet mogelijk is om digitale dreigingen het hoofd te bieden. Om het belang van investeringszekerheid een plek te geven in de structurele aanpak, wordt voorgesteld de huidige doelstelling te verbreden door naast nationale veiligheid ook investeringszekerheid daar in op te nemen.
- Vanuit het perspectief van meer investeringszekerheid zal moeten worden gezien hoe onderstaande tien voorwaarden in de verdere invulling van de structurele aanpak kunnen worden meegenomen:
 1. Omgeving van vertrouwen tussen samenwerkende partijen. Er moet zeer vertrouwelijke informatie tussen telecomoperators en overheid worden uitgewisseld en partijen gaan een langdurige samenwerkingsrelatie aan. Het kunnen werken in een omgeving waarin partijen elkaar vertrouwen, is daartoe essentieel.
 2. Overheidsbrede, interdepartementale insteek. De overheid is een veelkoppige entiteit met verschillende belangen. Voor eenduidige communicatie richting telecomoperators is interne afstemming en met één mond spreken door de overheid van belang.
 3. Passend binnen internationale context. Twee van de drie grote telecomoperators zijn (onderdeel van) mondiale spelers. Ons beleid zou niet te veel moeten afwijken van beleid in andere (EU)landen om te voorkomen dat ons investeringsklimaat zwak wordt.
 4. Stimuleren van een competitief concurrentiespeelveld. Concurrentie tussen telecomoperators zorgt voor uitstekende netwerken tegen acceptabele kosten. Een goede marktdynamiek waarin telecomoperators durven te investeren moet behouden blijven.
 5. Leren en verbeteren van beleid. Na enige tijd moet het huidige beleid geëvalueerd worden en moet geleerd worden van de opgedane ervaringen.
 6. Transparant proces. Vooraf moet het voor de telecom operators duidelijk zijn hoe de procesgang in de structurele aanpak zal zijn. Welke stappen worden doorlopen, wie heeft welke rol en verantwoordelijkheid en hoe ziet de besluitvorming eruit?
 7. Voorspelbaar proces. Naast dat het proces van de structurele aanpak transparant moet zijn, moet het ook zo veel mogelijk voorspelbaar zijn. Het vooraf kunnen inschatten van risico's is essentieel voor telecom operators. Objectiveerbaarheid is een centraal element. Ook het op basis van een kader kunnen inschatten van het recht op nadeelcompensatie kan bijdragen aan een voorspelbaar proces.
 8. Non-discriminatoire proces. Er mag geen onnodig onderscheid worden gemaakt tussen partijen.
 9. Begrijpelijk proces. Telecom operators moeten begrijpen waarom de analyses en besluitvorming op een bepaalde manier zijn ingericht.
 10. Proces met voldoende rechtsbescherming. De mogelijkheid om bezwaar te maken tegen besluiten van de overheid door deze te laten toetsen door een rechter, is voor telecomoperators een cruciaal recht. Hiertoe willen telecomoperators gerubriceerde informatie kunnen delen met hun advocaten.

- Er moet transparantie komen over hoe de structurele aanpak zich verhoudt tot bestaande gremia en structuren. De structurele aanpak wordt ontwikkeld binnen een context van bestaande institutionele kaders met gedefinieerde rollen en verantwoordelijkheden en gremia waar publiekprivaat informatie wordt uitgewisseld. Wat wordt waar behandeld en wat betekent dit voor de verantwoordelijkheden en rollen van de diverse betrokken partijen?

Bij het verder vormgeven van de structurele aanpak wordt aanbevolen aan de bovenstaande tien voorwaarden tegemoet te komen via heldere procesafspraken tussen overheid en telecomoperators. Dit draagt bij aan transparantie, voorspelbaarheid en een omgeving van vertrouwen. Dit is extra van belang omdat overheid en telecomoperators van elkaar afhankelijk zijn in de structurele aanpak om zinvolle uitkomsten te verkrijgen. Er zijn verschillende manieren om de aanpak vorm te geven. Aansluitend bij bestaande plannen lijkt de onderstaande afbeelding logisch.



In deze aanpak zijn er vijf stappen. Voor elk van deze stappen moet een aantal aspecten worden uitgewerkt:

1. Wat is het afwegingskader waarop getoetst wordt? Voor elke stap moet een inhoudelijk afwegingskader worden gemaakt. Zo wordt duidelijk op basis waarvan besluiten genomen worden. Centraal staat een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid.
2. Welke partijen zijn (in welke rol) betrokken bij deze stap? Voor elke stap zal moeten worden bepaald welke partijen in welke rol betrokken zijn.
3. Hoe worden besluiten genomen en hoe kan bezwaar worden gemaakt? Voor elke stap moet duidelijk zijn op welke wijze besluitvorming plaatsvindt. Dit is essentieel voor een transparant proces. Vooraf moet bepaald worden wat de routes zijn als er geen consensus is. Zowel een onafhankelijke toetsing als een formeel juridisch traject zijn opties.
4. Hoe wordt omgegaan met geheimhouding? Het is evident dat bepaalde informatie over dreigingen, kwetsbaarheden van netwerken en concurrentiegevoelige gegevens niet openbaar wordt. Aan de andere kant is de beschikbaarheid van bepaalde

informatie noodzakelijk voor een objectieve toetsing, de uitvoering van besluiten, het maken van bezwaar en onderling vertrouwen tussen partijen. Er moet een evenwicht worden gezocht, maar er moet vooral duidelijkheid zijn.

5. Wat is de doorlooptijd van een stap? Afspraken over de doorlooptijd per processtap zijn centraal voor een voorspelbare procesgang. Korte doorlooptijden zorgen ervoor dat telecomoperators niet onnodig lang in onzekerheid verkeren, maar dit kan ook ten koste gaan van de zorgvuldigheid.
6. (Hoe) kunnen deze bovenstaande afspraken veranderen? Goed beleid past zich aan aan de ontwikkelingen in de maatschappij. Echter, beleid dat wijzigt zorgt ook voor onzekerheid. Vooraf kan worden afgesproken wanneer het beleid geëvalueerd en aangepast kan worden.

Naast -of wellicht binnen- de structurele aanpak zijn er nog andere beleidsinstrumenten die te overwegen zijn. Het voorkomen van ongewenste investeringen is hierin een belangrijk element. Hieronder wordt een aantal opties genoemd. Echter voor alle opties geldt dat er geen absolute zekerheid door de overheid kan worden geboden. Mochten er over enkele jaren nieuwe grote dreigingen ontstaan, dan zal toch opgetreden moeten worden.

- Er kan bij het inkoopproces een toets van de investeringen plaatsvinden.
- Er kan vooraf worden aangegeven welke onderdelen van het netwerk zo gevoelig zijn dat verwijdering van systemen kan spelen.
- Er kan worden aangegeven welke leveranciers (niet) toegestaan zijn.
- Er kan een integrale visie op ICT worden ontwikkeld zodat telecomoperators zelf een kader hebben om investeringen aan te toetsen.

Een ander spoor voor beleid draait op het verbeteren van de marktdynamiek. De ontwikkeling van open standaarden voor netwerkapparatuur kan zorgen voor meer keuze in leveranciers. Er kan overwogen worden om dit te steunen. Ook het stimuleren van een strategie waarbij operators meer dan één leverancier per netwerkonderdeel gebruiken (multi-vendor) kan interessant zijn om kwetsbaarheden te verminderen. De vraag is echter of de beperkte schaal in Nederland geen te grote beperking is.

1 Introductie

1.1 Achtergrond

De afgelopen jaren is er een discussie ontstaan over de veiligheid en integriteit van telecommunicatiesystemen¹. Bij deze discussie ligt de focus op het gebruik van systemen van leveranciers uit landen met een naar Nederland mogelijk offensief cyberprogramma, en de risico's hiervan voor (1) de beschikbaarheid van de netwerken en (2) de confidentialiteit van de data die over deze netwerken gaat. In Nederland heeft dit er onder meer toe geleid dat telecomoperators kunnen worden verplicht bepaalde apparatuur en diensten van bepaalde leveranciers uit bepaalde delen van het netwerk te verwijderen. Daarnaast kunnen ook technische en organisatorische maatregelen worden opgelegd.

In het huidige tijdsgewricht zijn de dreigingen van gisteren niet altijd gelijk aan de dreigingen van vandaag. Daarom is er in het Besluit Veiligheid en Integriteit Telecommunicatie [1] (hierna: *Besluit*) het onderstaande opgenomen:

Artikel 2-lid 2: Indien dat naar het oordeel van Onze Minister noodzakelijk is om risico's voor de veiligheid en integriteit van diens netwerk of dienst die de nationale veiligheid of de openbare orde raken te beheersen, legt Onze Minister, in overleg met Onze Minister van Justitie en Veiligheid, een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst een verplichting op om in de daarbij aangewezen onderdelen van diens netwerk of bijbehorende faciliteiten, uitsluitend gebruik te maken van producten of diensten van anderen dan de daarbij door Onze Minister genoemde partij die:

a. een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft een in Nederland aangeboden elektronisch communicatienetwerk of -dienst te misbruiken of uit te laten vallen, of

b. nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld onder a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

Artikel 2-lid 3: Indien een verplichting op grond van het tweede lid betrekking heeft op reeds in gebruik zijnde producten en diensten ten behoeve van de daarbij aangewezen onderdelen, stelt Onze Minister in het belang van de continuïteit van dienstverlening een termijn vast voor het vervangen respectievelijk beëindigen van de betreffende producten en diensten.

Feitelijk betekent bovenstaande voor operators² dat er een onzekerheid ontstaat over (1) *wanneer* (2) *welke onderdelen*³ van de bedrijfsvoering, producten en diensten van (3) *welke*

¹ Onder (telecommunicatie)systemen vallen hardware, software en aanpalende dienstverlening.

² In dit stuk hanteren we de term (*telecom*) *operator* voor aanbieders van openbare elektronische communicatienetwerken.

³ Hierbij is het logisch om te denken in bepaalde "netwerkschillen". Immers, bepaalde delen van netwerken zijn veel gevoeliger voor dit vraagstuk dan andere delen.

*leverancier*⁴ verwijderd moeten zijn. Er zijn dus drie vormen van onzekerheid. Voor een investeerder in de telecommunicatiesector betekent deze onzekerheid een flinke uitdaging, want hoe kun je verantwoorden dat de overheid te allen tijde je miljoeneninvesteringen in systemen uit de markt kan nemen?

Op zijn beurt kan de onzekerheid ook voor Nederland een bredere impact hebben. Wij hebben behoefte aan de meest moderne, hoogwaardige telecomnetwerken die kunnen bijdragen aan het oplossen van economische en maatschappelijke uitdagingen. Hiervoor zijn aanzienlijke investeringen vereist door marktpartijen. Naast de continue investeringen in vaste netwerken, zal ook de uitrol van 5G flinke investeringen vergen. Er is echter enige mate van spanning tussen aan de ene kant investeringszekerheid en aan de andere kant de volledige flexibiliteit nemen die het Besluit biedt. Enerzijds zijn investeerders gebaat bij zoveel mogelijk zekerheid. Hoe lager de investeringszekerheid, hoe lager de investeringen. (of: hoe lager de investeringszekerheid, hoe hoger de opbrengsten moeten zijn voor een positieve business case). Anderzijds is vanuit een veiligheidsperspectief juist zoveel mogelijk flexibiliteit gewenst.

De besluitvorming rond eventuele nieuwe maatregelen zal door de Taskforce Economische Veiligheid worden uitgevoerd. Zij zullen hiertoe een "structurele aanpak" gaan vormgeven.

We kunnen ons voorstellen dat sommige lezers een link leggen tussen het besluit en de Wet ongewenste zeggenschap telecommunicatie (WOZ-T). Het Besluit heeft betrekking op de systemen die een telecom operator gebruikt, de WOZ-T heeft betrekking op buitenlandse investeerders die "overwegende zeggenschap" in een Nederlands telecombedrijf kunnen krijgen. In dit rapport gaat het echter alleen om het Besluit.

1.2 Onderzoeksvraag

De onderzoeksvraag die centraal staat is de volgende:

Hoe kan aan Nederlandse telecomoperators meer investeringszekerheid worden geboden in de vormgeving van de structurele aanpak?

Het doel van de structurele aanpak zoals verwoord door de Task Force Economische Veiligheid is: *een structurele aanpak tussen overheid en telecomaanbieders om de nationale veiligheid te beschermen tegen risico's die volgen uit de digitale dreiging vanuit geavanceerde (statelijke) actoren via misbruik van de telecomsector*. Bij het beantwoorden van de onderzoeksvraag moet worden gekeken naar verschillende opties en worden bepaald wat de voor- en nadelen hiervan zijn. Eén specifieke optie hiervoor is nadeelcompensatie. Het vormgeven van de nadeelcompensatie valt echter buiten de scope van deze opdracht.

1.3 Uitvoering

Om de onderzoeksvraag te beantwoorden is de volgende methodiek gehanteerd:

- Er is een literatuurstudie uitgevoerd. Onder meer naar de trade-off tussen investeringszekerheid en flexibiliteit in andere domeinen, maar ook naar de marktdynamiek in Nederland en de inrichting van publiek-private processen.
- Er zijn gesprekken met de drie mobiele operators gevoerd.

⁴ In dit stuk hanteren we de term *leverancier* voor partijen die systemen aan telecom operators leveren. Indien het niet anders kan, gebruiken we de Engelse term *vendor*. Dit doen wij bijvoorbeeld in Engelse stukken of in termen ("multi-vendor")

- Er zijn casestudies naar de wijze waarop andere landen met dit vraagstuk binnen de telecommunicatiesector omgaan uitgevoerd. Hiervoor zijn gesprekken geweest met buitenlandse beleidsmakers.

Op basis van deze input is een analyse gemaakt van het vraagstuk. De uitkomsten hiervan zijn zowel voorgelegd aan de mobiele operators als de betrokken departementen. Op basis van deze feedback zijn nuanceringen op bestaande analyses aangebracht en aspecten toegevoegd. De inhoud van dit rapport is echter geheel de verantwoordelijkheid van de auteurs. Niet alle organisaties en personen hebben aan alle hoofdstukken input geleverd of hebben expliciet aangegeven dat zij zich kunnen vinden in de inhoud.

Gezien de aard van het onderwerp komt in de dit stuk niet naar voren welke persoon -of welke organisatie welke uitspraak heeft gedaan of welke data heeft aangeleverd. Indien er verwezen kan worden naar openbare bronnen dan is dit uiteraard wel gedaan.

1.4 Leeswijzer

Dit rapport kent de volgende opbouw: in hoofdstuk 2 gaan we in op de relevantie van investeringszekerheid. Centraal staat de vraag hoe relevant het vraagstuk van investeringszekerheid is. Hierbij wordt niet specifiek gekeken naar de telecommunicatiesector, maar wordt een breed beeld geschetst. In hoofdstuk 3 gaan we in op de wijze waarop de nieuwe maatregelen de telecomoperators beïnvloedt. Hierbij ligt de focus uiteraard op investeringszekerheid, maar wij proberen ook een breder perspectief te hanteren. In hoofdstuk 4 gaan we in op verschillende manieren waarop binnen de structurele aanpak de investeringszekerheid kan worden vergroot. We presenteren onderscheidende opties en bespreken de merites hiervan. In het slothoofdstuk 5 komen we tot conclusies en aanbevelingen.

2 De relevantie van investeringszekerheid voor economische ontwikkeling

In dit hoofdstuk geven we een algemene introductie op het begrip investeringszekerheid. We leggen hierbij de relatie tussen investeringen en economische groei, om vervolgens aan te geven wat ervoor zorgt dat bedrijven juist minder gaan investeren. Deze bredere inzichten bieden handvatten voor het ontwerpen van een aanpak om een gewenste balans te vinden tussen bescherming en economische groei.

Wanneer de investeringszekerheid laag is, zal alleen worden geïnvesteerd in hoogrendementsinvesteringen, of in investeringen met laag rendement met kleiner risico. Investeringszekerheid is sterk afhankelijk van (1) de kosten van kapitaal en (2) de risico-opslag die aan een investering/project wordt toegekend. Een overheid kan investeringszekerheid beïnvloeden door beleid te voeren op deze twee aspecten. Onzekerheid over toekomstig beleid leidt echter ook tot een hogere risico-opslag. Zo draagt onzekerheid over eigendomsrechten op kapitaalgoederen bij aan een hogere risico-opslag en daarmee lagere investeringszekerheid.

In de volgende paragrafen werken we bovenstaande uit. Allereerst gaan we in op de relatie tussen investeringen en economische groei (§2.1), vervolgens op de rol van onzekerheid hierin (§2.2) en tot slot op strategieën om de investeringszekerheid te vergroten (§2.3).

2.1 Investerings leiden tot economische groei

Op de lange termijn zorgen investeringen voor economische groei. De voorbeelden hiervan zijn talloos. Investerings in wegen hebben ervoor gezorgd dat mensen zich veel sneller en goedkoper konden verplaatsen. Investerings in spoorwegen zorgden ervoor dat bepaalde gebieden zich economische konden ontwikkelen omdat zij eindelijk hun goederen goedkoop en snel konden verplaatsen. De komst van infrastructuur zorgt daarbij niet alleen voor economische groei, maar ook voor uitwisseling van kennis, vaardigheden en cultuur. Een meer recent voorbeeld, namelijk investeringen in ICT, zorg(d)en ervoor dat bedrijven productiever worden [2], zich nieuwe diensten en sectoren ontwikkel(d)en [3] en een groot deel van de Nederlandse bevolking op dit moment de mogelijkheid heeft om tijdens de Coronacrisis thuis door te werken. De afgelopen decennia was ICT verantwoordelijk voor ruim 1/3 van de economische groei in Nederland.[3] Kortom, een goed investeringsklimaat is essentieel voor Nederlandse internationale concurrentiepositie.




Met name infrastructuurprojecten zijn erg kapitaalintensief (zo kost de aanleg van een snelweg gemiddeld ± 1 miljoen euro per strekkende meter) en kennen een erg lange aanloop- en terugverdientijd (beiden tientallen jaren in het geval van weginfrastructuur). Zonder een stabiel investeringsklimaat komen deze (her)investeringen simpelweg niet tot stand, aangezien de risico's in verhouding moeten staan tot de potentiële inkomsten. Merk hierbij op dat dit geldt voor zowel de aanleg van *nieuwe* infrastructuren in gebieden of (opkomende) landen waar dit nog niet aanwezig is, als voor herinvesteringen in *bestaande* infrastructuur. Beide typen investeringen zijn nodig om economische groei mogelijk te (blijven) maken. De OECD schatte in 2006 al in dat er mondiaal tussen 2010 en 2030 een kleine \$50 triljoen (!) in weg-, spoor-, telecom-, elektriciteit- en waterinfrastructuur

geïnvesteed moest worden om deze toekomstbestendig te houden en economische groei te kunnen blijven borgen. [4]

Wat zijn nu de drijfveren die zorgen voor een gezond investeringsklimaat? Welke factoren op macro- (systeem), meso- (omgeving) of micro- (individueel) niveau zorgen er voor dat bepaalde investeringen meer en andere minder aantrekkelijk zijn? Deze factoren en hun onderlinge samenhang werken wij in de volgende sub-paragrafen (§2.1.1 en §2.1.2) nader uit. In §2.2 gaan we aansluitend in op de doorwerking hiervan op de daadwerkelijke investeringsbereidheid.

2.1.1 Pilaren van investeringszekerheid

Wat maakt een land of regio nu echt interessant om in te investeren? De Europese Commissie beschrijft de bouwblokken van een goed investeringsklimaat aan de hand van drie pilaren, op macro(-economisch) niveau, meso-economisch niveau (omgevingsfactoren) en het micro-economisch niveau (*human centered*). Daarnaast speelt duurzaamheid als factor die van invloed is op het beleid op alle niveaus. Wij hebben deze pilaren en bouwblokken samengevat in Figuur 1. [5]

 Macro-economisch	Macro-economische stabiliteit	Politieke stabiliteit	Openbaar bestuur, anti-corruptie en rechtsstaat
	Gemak van bedrijfsvoering	Wetgeving & sociale zekerheid	Investeringsbeleid
	Eigendomsrechten	Handelsbeleid	Toegang tot kapitaal
	Infrastructuur beleid en wetgeving	Beslechting zakelijke geschillen	Energiebeleid
 Meso-economisch: Omgeving			
 Micro-economisch: individueel	Human development	Innovatie (beleid)	

Figuur 1. Pilaren van investeringszekerheid (op basis van [5], visualisatie Dialogic)

Macro-economisch niveau

Om private partijen te verleiden om tot grootschalige investeringen over te gaan, moet er in een land ten eerste sprake zijn van een stabiele macro-economische politiek, waarbij de rijksuitgaven, belastinginning, staatsschuld, externe betrekkingen en kredietrating op orde zijn. Een gedegen staatsschuldbeleid en een gezonde ratio tussen de staatsschuld en het BBP zorgen voor een betere positie op de kapitaalmarkt. Publieke investeringen en *asset management* (oftewel integraal beleid op investeringen, beheer en vervanging van infrastructuur en gebouwen) kunnen de investeringsbereidheid van private partijen doen toenemen. Ook kan internationale samenwerking bijdragen aan het voorkomen van belastingontwijking en -fraude door uitholling van de grondslag (*base erosion*)

en winstverschuiving (*profit shifting*). Dit zorgt op haar beurt ook voor meer transparantie van geldstromen.

Ten tweede heeft een verhoogde kans op politieke instabiliteit en/of politiekgemotiveerd geweld (inclusief terrorisme) een sterke negatieve impact op investeringen. Dit geldt ook voor het afhandig maken of nationaliseren van eigendommen (hierover meer in §2.3) sociale onrust, gebrek aan oplossend vermogen bij natuurrampen, et cetera.

Goed openbaar bestuur wordt gekenmerkt door respect voor wet en regelgeving om rechten en plichten te waarborgen en vertrouwen te creëren. Onafhankelijke, onpartijdige en efficiënte rechtspraak zorgt op haar beurt voor meer kredietverlening, betrouwbaardere contracten, minder opportunistisch gedrag, lagere transactiekosten en minder corruptie (wat tot lagere productiviteit, investeringen, winstgevendheid en groei leidt).

De verschillende onderdelen van de macro-economische situatie leiden gezamenlijk tot een bepaalde mate van (in)stabiliteit en (on)aantrekkelijkheid voor partijen om in die context te investeren. Zoals wij in § 2.2 nader zullen uitleggen, zoeken investeerders niet zo zeer naar investeringskansen zonder risico's, maar wel naar situaties waarin deze risico's voorspelbaar zijn (en dus meegenomen kunnen worden in een businesscase).

Mesoniveau: omgevingsfactoren

Omgevingsfactoren zijn alle kenmerken van een economie en samenleving die direct (dus op een mesoniveau) invloed hebben op de bereidwilligheid van partijen om te investeren (het microniveau). Hier wordt worden een breed scala aan factoren onder geschaard, waaronder: [5]

- Eenvoud van bedrijfsvoering – hoeveel moeite kost het om een bedrijf administratief op te starten en operationeel te houden?⁵
- Belastingen en administratieve lasten – zijn de belastingregels stabiel, transparant en duidelijk?
- Investeringsbeleid – worden investeringen gepromoot, gefaciliteerd en krijgen alle partijen dezelfde kansen en mate van bescherming?
- (Intellectueel) eigendomsrecht – zijn de wetten en regels omtrent (intellectuele) eigendomsrechten transparant, duidelijk, stabiel en voor iedereen gelijk?
- Handelsregulering en -beleid – in hoeverre is er sprake van wetgeving, beleid, overeenkomsten en verdragen ter promotie en faciliteren van import, export en handel?
- Financiële markten – is er voldoende toegang tot kapitaal voor alle typen partijen?
- Ondersteuningsmogelijkheden bij juridisch problemen, geschillen of conflicten – is er sprake van een wettelijk kader en juridisch systeem voor effectieve gerechtsbescherming?
- Arbeidsrecht en sociale zekerheid – kent het land zekerheden en regels voor contractvorming, collectieve regelingen en professionele ontwikkeling (technisch, taal, etc.)
- Infrastructuurbeleid en -wetgeving. – is er sprake van coherent en doordracht infrastructuurbeleid met ruimte voor bijvoorbeeld PPP-constructies?
- Energiebeleid en -wetgeving – worden investeringen in (hernieuwbare) energiesystemen gefaciliteerd en wettelijk ingebed?

⁵ Zie in dit kader ook de jaarlijkse rapportage van de Wereldbank. [11] Hierin worden landen beoordeeld op de mate waarin er eenvoudig zaken gedaan kan worden. Ook in deze publicatie speelt de bescherming van eigendomsrechten (zie §2.2.1 verderop in dit hoofdstuk) een centrale rol.

Microniveau: Human-centered benadering

De laatste pilaar van investeringszekerheid rust op de human centered aspecten van een economie of samenleving. [6] Als er geen aandacht of kansen zijn voor persoonlijke ontwikkeling en innovatie, dan drukt dit op de korte of lange termijn op de kansen om tot succesvolle investeringen en (infrastructuur)projecten te komen.

Persoonlijke ontwikkeling begint bij een gezonde en veilige leefomgeving. Als dit ontbreekt, dan hoeven we niet eens te spreken over de mogelijkheden tot vergaring van kennis, kunde en persoonlijke en sociale vaardigheden. Innovatie zorgt op haar beurt voor groei in productiviteit en concurrentie, oftewel economische groei. Dit vraagt wel om juridische en institutionele kader waarin bedrijven (of andere adoptanten), industriële en innovatieve clusters en een hoge kwaliteit R&D kunnen ontstaan.

2.1.2 Samenhang tussen de factoren: wat is belangrijker?

Het spreekt voor zich dat de drie hiervoor genoemde pilaren en onderlinge factoren grote onderlinge afhankelijkheden kennen: het is som der delen die maakt dat het in sommige economieën eenvoudiger of aantrekkelijker is voor een investeerder (stabiel) rendement te maken dan andere.⁶ Ze bouwen als een piramide op (startend bij een veilige leefomgeving) en gezamenlijk zorgen ze voor de sterkte van het bouwwerk. Wij kunnen hierbij moeilijk uitspraken doen over omvang van het belang van individuele factoren: in welke mate is de toegang tot kapitaal belangrijker dan de ondersteuningsmogelijkheden bij geschillen? Of nog concreter: hoeveel extra investeringen worden gedaan als er een duidelijke roadmap of strategie ligt ten aanzien van de (telecom)infrastructuur?

In de verkenningen die wij eerder op dit vraagstuk hebben gedaan kwamen wij tot de conclusie dat een dergelijke inschatting moeilijk te maken is. De investeringsbeslissing van multinationals (bijvoorbeeld: waar plaats ik mijn hoofdkantoor, R&D-locatie of datacenter?) gebeurt, zo leren de voorbeelden ons, in eerste instantie aan de hand van een longlist waarop locaties op basis van een lange lijst eigenschappen worden vergeleken (in de geest van de factoren uit §2.1.1). Op basis van deze lijst en scoring komt men vervolgens tot een shortlist. De definitieve keuze blijkt in de praktijk meer een kwestie van persoonlijke voorkeur, bedrijfsstrategie (risicobereidheid), historie of, in sommige gevallen, minder bonafide processen (omkoping).[7]

2.2 Onzekerheid leidt tot lagere investeringen

Nu het in voorgaande paragraaf duidelijk is geworden welke factoren de basis vormen voor een goed investeringsklimaat en daarmee economische groei, is het nu de vraag hoe deze factoren neerslaan op de handelingsperspectieven van een ondernemer of investering. Oftewel: gegeven dat alle beschreven factoren 'op orde' zijn, wat kan er dan toch voor zorgen dat een investering of bedrijf minder rendabel is dan vooraf gedacht?

⁶ Later in dit stuk zullen we zien dat ook bij telecomoperators dit perspectief van investeerders van toepassing is. Voorbeeld: Twee van de drie grote partijen in Nederland zijn onderdeel van een internationaal opererend moederbedrijf. Dit moederbedrijf zal haar investeringscapaciteit moeten verdelen tussen dochterbedrijven in verschillende landen actief zijn.

De crux zit in de termen transparantie, begrijpelijkheid, (non)discriminatie en -wellicht de belangrijkste- voorspelbaarheid. Hieronder verstaan wij (kortgezegd) het volgende:

- **Transparantie:** zijn de probleemanalyse, besluitvorming en uitkomsten omtrent een beleidsmaatregel voor iedereen inzichtelijk?
- **Begrijpelijkheid:** snappen de stakeholders waarom een bepaalde maatregel wordt genomen?
- **Non-discriminatie:** geldt de beleidsmaatregel voor alle partijen (in dezelfde mate)?
- **Voorspelbaarheid:** in hoeverre was de getroffen beleidsmaatregel vooraf al bekend? Konden partijen er al rekening mee houden tijdens hun investeringsbeslissing?

Gezamenlijk dragen deze aspecten bij aan het objectief en coherent houden van het beleid. Zolang de condities waaronder een investering gemaakt wordt duidelijk gecommuniceerd worden, goed te begrijpen zijn en voor iedereen hetzelfde, dan ontstaat speelveld waar voor alle potentiële investeerders ruimte is om binnen te acteren. De spanning ontstaat als deze elementen niet bestaan, maar misschien nog wel belangrijker: veranderen over de tijd. Wij zullen hierna vanuit het macro- (2.2.1) en micro-perspectief (2.2.2) uitleggen wat hiervan de uitdaging is. We sorteren hierbij al enigszins voor op de discussies omtrent de veiligheidsmaatregelen (wat we vertalen als een vorm van onteigening), maar het argument van onzekerheid geldt in feite voor elke vorm van beleidsinterventie: positieve of negatieve prikkels zijn vooraf in te calculeren, plotselinge schokvormige veranderingen in beleid zijn het probleem.

2.2.1 Macro-economisch perspectief

Bij het zoeken van een juiste balans tussen de veiligheidsmaatregelen en economische groei spelen eigendomsrechten een belangrijke rol. Eigendomsrechten impliceren het recht om een goed naar eigen inzicht te gebruiken, het recht op de opbrengsten en het recht om het te vervreemden. Zonder dit recht heeft een investeerder geen zekerheid over of deze in de toekomst (exclusief) toegang behoudt tot het goed (denk aan land, machines, gebouwen en intellectueel eigendom), en daarmee de investering kan terugverdienen. Bij recht op bezit horen ook juridische kaders rondom *onteigening*: een overheid kan (meestal onder voorwaarde van het bestaan van een groot maatschappelijk belang daarbij en passende compensatie) bezit afnemen.

Het is de bescherming van eigendomsrechten die aan het einde van de Middeleeuwen in Europa de basis hebben gelegd voor de Industriële Revolutie en alle economische groei die hieruit is voortgekomen. Waar het bezitten en exploiteren van land en middelen voorheen alleen besteed was aan adel en grootgrondbezitters, bieden wettelijk en institutioneel geaccepteerde eigendomsrechten voor veel meer land- en kapitaaleigenaren een prikkel om deel te nemen in economische activiteiten, zoals investeringen, innovatie en handel.

Box: Onteigening van (bedrijfs)eigendommen

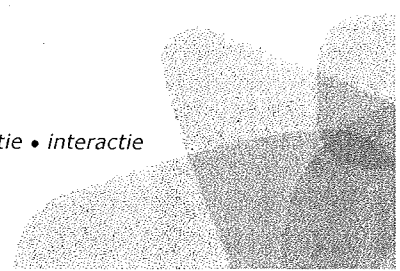
Het onteigenen van privaat bezit is een beperking van eigendomsrechten dat vele verschillende vormen kan aannemen. Zo kwamen de leden van het WHO onder het TRIPS-verdrag tot een verlicht regime voor medische octrooien in ontwikkelingslanden, waarbij de nationale overheden gemakkelijker verplichte (gratis/redelijke) licenties af kunnen dwingen om zo de productie en verkoop van betaalbare medicijnen mogelijk te maken. Hierdoor konden er op grote schaal goedkope hiv-medicijnen op de Afrikaanse markten beschikbaar komen.[8]

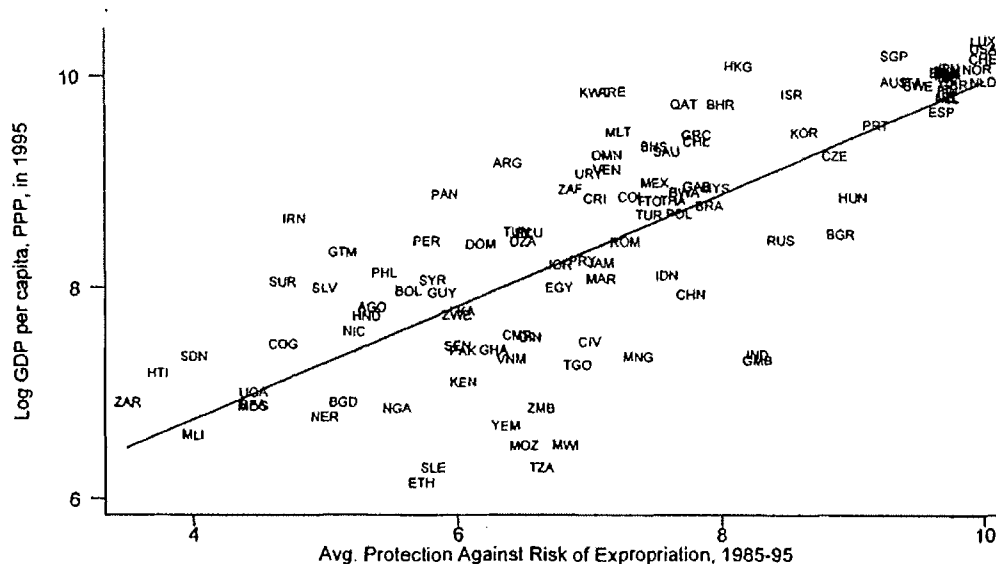
Het spreekt voor zichzelf dat het onteigenen van bedrijfseigendom een grote impact heeft op de bedrijfsvoering van de eigenaar. Het opzetten van een dergelijk instrument vraagt daarom om een weloverwogen kader, om zo de grenzen, impact en compensatie van het onteigeningsregime voor alle partijen acceptabel te houden. Centraal hierbij staan de volgende vragen:

1. In hoeverre is de overheid gebonden aan expliciete en afgebakende grenzen voor het onteigenen in de wet en praktijk?
2. Welke constitutionele of wettelijke kaders borgen dat de onteigening alleen kan plaatsvinden als deze niet-discriminerend is, een publiek belang dient, onder goede juridische procesgang gebeurt en er een redelijke compensatie tegenover staat?
3. Welke wettelijke en administratieve mechanismes bestaan er om tegen de onteigening of de compensatie in beroep te gaan?
4. Hoe verhoudt de nationale wettelijke bescherming tegen onteigening zich tot de bescherming uit investeringsverdragen?

Deze vragen kunnen als startpunt dienen bij het vormgeven van het onteigeningskader. Een verdere uitwerking is beschikbaar in de bijlage van het Investment Framework in de vorm van 32 vragen/criteria, waarbij met name wordt ingegaan op de reikwijdte/zeggenschap van het overheidshandelen bij onteigening, het compensatieregime, de wettelijke borging (incl. referentiecasses/jurisprudentie) en het betrekken of opzetten van onafhankelijke partijen voor review, bezwaar en beroep.

De crux van de relatie tussen eigendomsrechten en economische groei is gelegen in het feit dat eigendomsrechten garanties bieden op het toe-eigenen van het rendement dat gehaald kan worden uit de investeringen. Het geeft de eigenaar mogelijkheden om te investeren in land, *human capital* of technologie, bijvoorbeeld door een fabriek te bouwen, het land te bewerken of unieke kennis te ontwikkelen, zonder de onzekerheid dat deze fabriek wordt onteigend, de oogst afgedragen moet worden of de ideeën om niet beschikbaar gesteld moeten worden aan de samenleving. Daarbij zorgen eigendomsrechten voor lagere transactiekosten in een economie, aangezien het veel duidelijk wie de eigenaar is van een bepaald schaars goed (zoals een stuk land of onroerend goed). Figuur 2 toont dat er een directe relatie lijkt te zijn tussen zekerheid over eigendom (bescherming tegen onteigening) en het BBP in een economie.





Figuur 2 De mate van bescherming tegen onteigening in relatie tot het BBP van een land.[9]

Het wegvallen of inperken van deze eigendomsrechten zorgt direct voor een beperking in het economische verkeer, aangezien dit voor onzekerheid zorgt in de mate waarin de geprojecteerde rendementen daadwerkelijk aan de eigenaar toe zullen komen. Om nog preciezer te zijn: het is de *verandering* in de rechten die voor spanning zorgt, met name als het een onvoorspelbare verandering is. Het is namelijk heel normaal dat een bepaald deel van het rendement uit een investering door de Staat wordt afgeroomd in de vorm van belastingen. Een plotsklapse verdubbeling van deze belasting kan er echter bijvoorbeeld voor zorgen dat een investering niet in vijf, maar in tien jaar rendabel is. Dit geldt dus niet alleen voor belastingen, maar voor alle vormen van beperkingen van bezit (en in feite voor elke vorm van beleid): zolang het transparant, begrijpelijk, niet-discriminerend en voorspelbaar is, dan kan een rationele actor hier rekening mee houden bij zijn gedragskeuze.

Hoe deze onzekerheid voor een ondernemer of investeerder doorwerkt in zijn investeringsgedrag, werken wij in de volgende paragraaf nader uit.

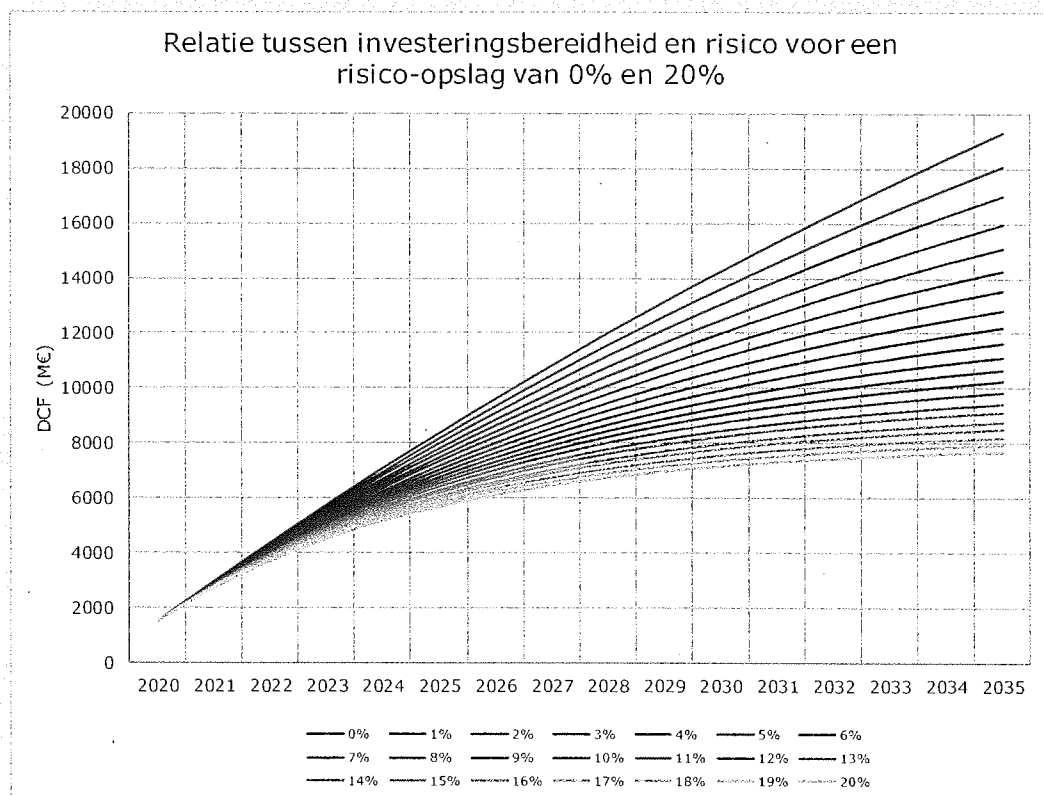
2.2.2 Micro-economisch perspectief

Bij het maken van investeringsbeslissing moet een bedrijf een inschatting maken van het risico dat met het project gemoeid gaat: de zogenoemde risico-opslag. In feite maakt men een inschatting van de kans dat er geen rendement (of zelfs verlies) gemaakt gaat worden als gevolg van de risico's die met het project gemoeid gaan. Hieronder leggen wij de werking hiervan nader uit.

Box: risico-opslag en investeringsbereidheid

Vanuit een klassiek bedrijfseconomisch perspectief is de waarde van een investeringsproject gelijk aan de som van de verdisconteerde kasstromen over de tijd (de netto contante waarde (NCW of NPV)). Hiermee wordt berekend hoeveel de gezamenlijke toekomstige kasstromen op dit moment waard zijn. De discontovoet wordt hierbij bepaald op basis van (1) de risk-free rate, (2) het reguliere rendement dat een bedrijf moet halen en (3) een project specifieke risico-opslag. Een hogere risico-opslag leidt tot een veel lagere investeringsbereidheid, zeker voor investeringen met een lange looptijd. Figuur 3 toont hoe groot de impact is van de risico-opslag. Het zou een afbeelding kunnen zijn dit

een operator gebruikt om in te schatten hoe groot zijn investeringen in een nieuw netwerk mogen zijn, wil dit rendabel zijn. Een operator die een project specifieke risico-opslag van 0% ziet en dus alleen de risico's ziet die gebruikelijk zijn voor de sector -zoals klanten die komen en gaan- is bereid om €19 miljard te investeren (de bedragen zijn uiteraard fictief). Echter, als de operator een extra risico-opslag van 20% hanteert, bijvoorbeeld als gevolg van een onvoorspelbare overheid, dan daalt zijn investeringsbereidheid tot minder van €8 miljard. De sterke relatie tussen investeringszekerheid en beleidsonzekerheid blijkt ook uit empirisch onderzoek.[10]



Figuur 3. Bedrijfseconomische waarde (en hiermee de investeringsbereidheid) van een investering die vijftien jaar lang 1500M€ kasstromen genereert op basis van een risico-opslag van 0%-20% bovenop de reguliere gewogen gemiddelde kapitaalkosten (WACC) van een operator.

Een hoge risico-opslag leidt ertoe dat alleen projecten die heel erg winstgevend zijn een netto constante waarde opleveren die goed genoeg is om ook bij een hoge kapitaalkosten⁷ tot een positief investeringsbesluit te komen. Het probleem van *onzekerheid* is echter dat de hoogte van de risico-opslag over de tijd kan veranderen. Een substantiële wijziging in het uitstaande risico van de investering zorgt voor onzekerheid of de benodigde inkomsten behaald kunnen worden over de looptijd van het traject. Zo kunnen (aanzienlijke) belastinghervormingen de netto-inkomsten (sterk) drukken en zorgt een verzwakking in het regime van eigendomsrechten voor een grotere kans dat de eigenaar van een idee, stuk land

⁷ Oftewel de kosten die een investeerder moet maken om het benodigde kapitaal beschikbaar te krijgen (*weighted average cost of capital* - WACC), hieronder vallen bijvoorbeeld de kosten/rentelasten die men maakt om het kapitaal aan de kapitaalmarkt te onttrekken of de rendementsverwachtingen die de aandeelhouders hebben ten aanzien van de investeringen.

of fabriek niet meer over zijn productie-assets kan beschikken om een bedrijf draaiend te houden.⁸

In de praktijk zien we overigens steeds vaker dat bedrijven en investeerders verschillende scenario's uitwerken. Ze maken hierbij bijvoorbeeld een afweging om nu te investeren in een project of technologie, de investering uit te stellen tot een fase waarin minder onzekerheid is, of helemaal af te zien van de investering en over te stappen op een andere bedrijfsstrategie (door bijvoorbeeld niet meer als koploper, maar als prijsvechter in te markt te stappen). In het geval van houders van grotere investeringsportefeuilles of multinationals wordt ook het totale uitstaande risico in acht genomen: men zoekt naar een aantrekkelijke balans tussen veilige (lage WACC, lage risico-opslag) en risicovollere (hoge WACC, hoge risico-opslag) investeringen en alles hier tussenin.

2.2.3 Onzekerheid in de Nederlandse context

Geredeneerd vanuit de Nederlandse context kunnen we stellen dat veel van de macro-economische en omgevingsfactoren uit §2.1.1 op een goed niveau zitten, of in ieder geval bekend en uitgekristalliseerd zijn voor alle partijen. De daadwerkelijke aantrekkelijkheid is uiteindelijk een kwestie van relativiteit: ten opzichte van Zuid-Soedan zijn de Nederlandse voorwaarden uitstekend, maar hoe vergelijken we ons tot Duitsland en Zweden? Of meer specifiek: hoe ervaart en waardeert een transcontinentaal logistiek bedrijf de Rotterdamse haven economie ten opzichte van die van Hamburg bij de investeringskeuze voor haar nieuwe hoofdkantoor?

Ook hier is het weer de vraag: blijven alle factoren hetzelfde en is de risico-opslag dus goed voorspelbaar? In de praktijk blijkt dit in Nederland ook een dynamisch speelveld te zijn, ten goede en ten kwade (in investeringstermen gesproken). Zo wijzigen de bijtellingsvoorwaarden van leaseauto's met (enige) regelmaat nog tijdens de grofweg vierjarige looptijd van een leasecontract (kostenverhogend) en worden de regels voor arbeidscontracten aangepast ten faveure van de werkgever (flexibeler = kostenverlagend) en werknemer (meer zekerheden = kostenverhogend). Ook het regime en de publieke attitude ten aanzien van belastingontwijking is in de afgelopen jaren aan verandering onderhevig (kostenverhogend). Dergelijke veranderingen maken dat de kosten voor bedrijfsvoering over de tijd kunnen veranderen.

2.3 Strategieën om de investeringszekerheid te vergroten

In feite bieden alle genoemde factoren van investeringszekerheid een aangrijppunt voor beleidsinterventies die kunnen bijdragen aan een verbetering van het investeringsklimaat. De factoren grijpen ofwel in op de *risico*-opslag ofwel op de *kosten* van kapitaal. Enkele voorbeelden zijn:

- Overheidsgaranties kunnen de *toegang tot kapitaal* vergroten, daarmee de WACC verlagen en dus de investeringsbereidheid verhogen (beter gezegd: de investeerder kan een hogere risico-opslag aan).
- Hetzelfde geldt voor alle maatregelen die worden getroffen om de *administratieve lasten* van de bedrijfsvoering te vereenvoudigen (regeldruk verlagen) en te

⁸ Of, bij intellectuele eigendomsrechten: niet meer over het *exclusief* recht tot gebruik beschikken. Een dergelijke discussie speelt op dit moment rondom tests voor het Coronavirus: fabrikant Roche kan er niet genoeg produceren, maar moet zij nu het recept vrijgeven, vanwege maatschappelijk belang? [businessinsider.nl]

digitaliseren (makkelijker belastingaangifte doen). Des te lager te lasten, des te meer van de investering ten goede kan komen aan het creëren van toegevoegde waarde aan een grondstof, idee of proces.

- Op het thema *innovatie* is een vaak gekozen strategie het creëren van een regelluwe experimenteerruimte. Hierin krijgen partijen de ruimte om te experimenteren met een bepaalde technologie of idee, zonder dat hier de gebruikelijke wetten en regels beperkingen op kunnen leggen. Denk hierbij aan het regelvrij vliegen met drones (zie Unmanned Valley Valkenburg waar men nieuwe dronetechniek kan testen), experimenten met de participatiewet (om te bezien of de uitvoering effectiever en efficiënter kan met minder verplichten of sancties) of de verschillende 5G field labs (waar met tijdelijke vergunningen in de 3,5 GHz-band gewerkt kan worden aan nieuwe diensten).
- Tot slot zien we een brede mix aan beleidsmaatregelen en instrumenten die erop gericht zijn om de *eenvoud van bedrijfsvoering* te vergroten en de van toepassing zijnde overheidsregelgeving inzichtelijk, begrijpelijk en breed bekend te maken. Denk hierbij aan voorlichtingscampagnes, websites, overlegtafels, informatieloketten, inzet van omgevingsmanagers, et cetera.

Investeerders zetten uiteindelijk de verwachte revenuen uit tegen de kosten en vergelijken dit met andere investeringsmogelijkheden. Het is aan een overheid gelegen om de voorwaarden zo goed mogelijk te stroomlijnen. De OECD vat dit als volgt samen in haar Policy Framework for Investment⁹:

- Een effectief investeringsbeleid is verankerd in sterke instituties en effectief openbaar bestuur.
- Investeringsbeleid wordt gefaciliteerd door een omgeving van vertrouwen.
- Overheidsbrede benadering van investeringsbeleid verbeteren de uitkomsten en vergroten het gebruik van publieke middelen.
- Interdepartementale coördinatie
- Transparantie en betrokkenheid kunnen leiden tot beter beleid met een hogere mate van steun van belanghebbenden.
- Innovatie en verbetering in beleidsontwerp en -uitvoering.
- Internationale samenwerking kan binnenlandse inspanningen ter verbetering van het zakelijk klimaat aanvullen en zelfs versterken.

De OECD heeft hiervoor een investeringsbeleidskader ontwikkeld, waarbij beleidsmakers aan de hand van een groot aantal vragen kunnen vaststellen in hoeverre de randvoorwaarden hun land of regio op orde zijn. Gegeven het onderwerp van deze studie, gaan wij hierna uitgebreider in op de zekerheden die geboden kunnen worden op het thema van eigendomsrechten.¹⁰ Met name het onderwerp onteigening toont aan zekerheid die een houder van het eigendomsrecht op bijvoorbeeld een stuk land, onroerend goed, (telecom)infrastructuur of idee heeft.

⁹ Zie [\[oecd.org\]](https://oecd.org)

¹⁰ Onderkend wordt dat de structurele aanpak veelal zal kunnen leiden tot het alleen treffen van technische en organisatorische maatregelen om risico's afdoende te mitigeren. Het zeker niet in alle gevallen leiden tot het moeten verwijderen van apparatuur. Toch focust dit rapport met name op dit laatste omdat de onzekerheid hieromtrent de grootste impact heeft op het investeringsvraagstuk van telecom operators.

3 De impact van het Besluit op investeringen in de telecomsector

In dit hoofdstuk lichten we nader toe hoe het Besluit Veiligheid en Integriteit Telecommunicatie investeringen in de telecomsector beïnvloedt. We bekijken allereerst de reikwijdte van het Besluit (§3.1). Vervolgens gaan we in op de huidige marktdynamiek en de wijze waarop wordt geïnvesteerd in de telecomsector (§3.2). Vervolgens gaan we in op investeringsbeslissingen en de impact die het Besluit daarop heeft (§3.3). Deze impact leidt tot veranderingen in de marktdynamiek (§3.4). De veranderde marktdynamiek kan tot slot effect hebben op andere delen van het telecom-ecosysteem buiten de eerder geïdentificeerde reikwijdte (§3.5).

3.1 Reikwijdte van de impact

Het Besluit Veiligheid en Integriteit Telecommunicatie richt zich op alle aanbieders van een openbaar elektronisch communicatienetwerk of -dienst en in potentie op alle onderdelen van diens netwerken en leveranciers. Een groot deel van de Nederlandse telecomsector valt onder deze afbakening. In onze visie is de impact op de korte en middellange termijn in potentie relatief groot voor een specifiek deel van de markt: toekomstige investeringen in mobiele netwerken. Hiervoor zijn twee redenen: (1) de hoogte van de investeringen en (2) de marktdynamiek aan de kant van leveranciers. Dat de impact op de mobiele netwerken naar verwachting relatief groot is, betekent uiteraard niet er geen impact op de andere aspecten zal zijn. Ook op het vaste netwerk zal er een substantiële impact zijn.

Ten eerste liggen bij mobiele netwerken doorlopend aanzienlijke investeringen in apparatuur en diensten in het verschiet. De bestaande mobiele netwerken zullen de komende jaren de transitie naar 5G gaan doormaken. De realisatie van 5G in Nederland is veel meer een doorontwikkeling van bestaande (4G)netwerken, dan het bouwen van een *nieuw* 5G netwerk. Een groot deel van de investeringen bestaan uit upgrades van bestaande systemen, bijvoorbeeld in de vorm van softwarelicenties. Daarnaast zal ook nieuwe apparatuur en diensten moeten worden ingekocht door telecomoperators. Hierbij ligt het zwaartepunt op het radiotoegangsdeel (RAN), aangezien het hier gaat om een groot aantal antennes die in nieuwe en bestaande opstelpunten moeten worden gerealiseerd. De drie mobiele telecom operators hebben nu samen circa 18.000 antenne-installaties. Uiteraard zien wij onder meer ook bij vaste netwerken flinke investeringen in het aansluitnetwerk; denk vooral aan de uitrol van glasvezel. Hierbij ligt het zwaartepunt van de kosten op civieltechnische aspecten ("de schep") en minder op actieve apparatuur ("het kastje").

Ten tweede zien wij vooral bij het RAN-deel van de mobiele netwerken een marktdynamiek waarbij leveranciers uit landen met een naar Nederland offensief cyberprogramma een grote rol spelen. Er is sprake van een oligopolistische markt waarin Nokia, Ericsson en Huawei de belangrijkste leveranciers zijn. De positie van Huawei groeit de laatste jaren sterk ten koste van de Europese leveranciers. [12] Haar sterke positie op haar thuismarkt draagt hieraan bij: recent hebben zij een opdracht verkregen om meer dan 200.000 5G basisstations in China uit te rollen.[13] Daarnaast vernemen wij uit de markt en uit onderzoeken [14] dat apparatuur en diensten van Huawei van hoge kwaliteit zijn, en tegen aantrekkelijke voorwaarden worden aangeboden. Op dit moment zijn er mondiaal slechts vier bedrijven (Amazon, Alphabet, Microsoft en Samsung) die meer per jaar uitgeven aan R&D dan Huawei.[15] Tot slot zien wij dat Huawei op dit moment de meeste patentaanvragen heeft

uitstaan op het gebied van 5G. [16] Nokia en Ericsson staan vierde en vijfde op deze lijst [16], maar er zijn goede argumenten dat zij relatief veel belangrijke *standard essential* patenten hebben.

Buiten toekomstige investeringen in mobiele netwerken zal er ook een impact zijn op investeringen in delen van de telecommunicatienetwerken waar mobiele netwerken geen rol spelen. Deze impact zal echter beperkter zijn. Dit komt doordat in veel marktsegmenten er veel minder sprake is van een sterke positie van leveranciers uit landen met een naar Nederland offensief cyberprogramma. De voornaamste uitzondering ligt waarschijnlijk op het gebied van eindgebruikersapparatuur zoals modems en set-top-boxes (*customer premises equipment*, CPE's) bij vaste netwerken. Een groot deel van de markt voor set-top boxen en meegeleverde modems komt van leveranciers uit risicolanden.

Ten derde stellen wij vast dat het besluit alleen impact heeft op aanbieders van openbare elektronische communicatienetwerken of -diensten. Dit blijkt duidelijk uit de wettekst. ACM registreert welke partijen daar onder vallen. [18] In dit kader is het woord *openbaar* zeer relevant. Niet-openbare netwerken vallen niet onder het besluit. Er zijn in Nederland verschillende grote organisaties die een eigen niet-openbaar telecomnetwerk hebben. Denk aan grote onderwijsinstellingen en gemeenten maar ook beheerders van andere netwerken zoals spoor, weg, water, gas en elektriciteit.

De impact van het Besluit op bestaande investeringen is relatief complex. Aan de ene kant kan beargumenteerd worden dat de impact beperkt is omdat de investeringen in het verleden liggen en de telecomoperator zijn gedrag uit het verleden (het doen van bepaalde investeringen) niet meer kan aanpassen. Maar aan de andere kant kan het invloed hebben wanneer door besluiten van de overheid bepaalde investeringen sneller moeten worden afgeschreven of waar onzekerheid bestaat over toekomstige investeringen. Ook het feit dat systemen op elkaar voortbouwen en er enige sprake is van vendor lock-in kan deze impact versterken.

3.2 Bestaande marktdynamiek

In de bovenstaande paragraaf hebben we aangegeven dat het Besluit de hele telecomsector beïnvloedt, maar in potentie een relatief grote impact kent bij (toekomstige) investeringen in mobiele netwerken. Feitelijk betekent dit dat de relevante markt in dit kader bestaat uit KPN, T-Mobile Nederland en VodafoneZiggo. In deze paragraaf beschrijven wij hoe het concurrentiespeelveld van deze partijen er uitziet. Dit is essentieel om later in dit hoofdstuk een inschatting te maken van de impact op investeringsbeslissingen. De structuur van een markt, bepaalt het gedrag van de actoren op de markt en dat bepaalt de uitkomsten van de markt.[17]

KPN, T-Mobile én VodafoneZiggo zijn de enige drie partijen met een mobiel netwerk in Nederland. Tele2 had een eigen netwerk, maar is overgenomen door T-Mobile. Er zijn in Nederland tientallen andere aanbieders van mobiele *diensten*, denk aan Simyo, Robin Mobile, Youfone en Simpel. Deze partijen gebruiken echter de achterliggende netwerken van de drie partijen en zijn Mobile Virtual Network operators (MVNO's). Alle drie partijen hebben een flink deel van de markt in handen.

Als wij kijken naar de telecommunicatiemarkt in brede zin dan zien wij dat er in Nederland bijna 800 partijen zijn die als aanbieder van een openbaar elektronisch communicatienetwerk zijn ingeschreven bij de ACM.[18] Toch hebben de drie partijen KPN, T-Mobile en VodafoneZiggo samen veruit het grootste deel van de telecommunicatiemarkt in handen. Naast alle grootschalige mobiele netwerken bedienen ook de vaste aansluitnetwerken van

deze partijen meer dan 99% van huishoudens en bedrijven in Nederland. De andere partijen opereren veelal in (zakelijke) niches.

Over het algemeen concurreren de drie partijen sterk met elkaar. Met name de mobiele markt wordt gezien als competitief. Er is weinig ruimte voor partijen om *niet* te investeren en achter te gaan lopen op concurrenten.

Op dit moment heeft Nederland een van de beste mobiele netwerkinfrastructuren ter wereld. Alle drie de netwerken krijgen uitstekende scores als het gaat om de dekking en capaciteit van de netwerken. [19] Mede dankzij deze hoge dekkingsgraad van snel internet en de beperkte schaalgrootte wordt Nederland internationaal (h)erkend als proeftuin voor ontwikkeling van digitale diensten. De prijzen van de diensten zijn in Nederland, voor West-Europese standaarden, gemiddeld. Voor mondiale begrippen zijn de prijzen in Nederland uiteraard relatief hoog. [20]

De grote drie aanbieders van openbare telecommunicatienetwerken in Nederland hebben enigszins verschillende uitgangspunten die in dit kader relevant zijn:

- Positionering en omvang: Op de consumentenmarkt hebben VodafoneZiggo, T-Mobile en KPN allen een substantieel deel van de markt in handen. Ten opzichte van veel andere landen ervaart de incumbent in Nederland (KPN) veel concurrentie van andere partijen. Doordat KPN en VodafoneZiggo grootschalige vaste aansluitnetwerken voor huishoudens hebben, hebben zij hier een sterkere positie dan T-Mobile. In veel zakelijke marktsegmenten heeft KPN een sterke positie. KPN is in Nederland de grootste speler met een omzet van €5,5 miljard.[21] De omzet van VodafoneZiggo is circa €3,9 miljard [22], T-Mobile komt op grofweg €2 miljard. [23]
- Aandeelhoudersstructuur: Hoewel KPN in Nederland een grote speler is, is zij op internationaal niveau een kleine speler. VodafoneZiggo is een joint venture van Vodafone en Liberty Global. De omzet van de Vodafone Group ligt op circa €50 Miljard [24] en die van Liberty Global op circa €11 miljard.[25] Deutsche Telecom, het moederbedrijf van T-Mobile, heeft een omzet van circa €80 miljard. Het feit dat twee partijen een buitenlandse moeder hebben, betekent ook dat investeringsbeslissingen deels op internationaal niveau worden bepaald.

Op dit moment is de markt in Nederland, maar ook daarbuiten- bezig met grote investeringen in de uitrol van 5G. Hierbij gaat het niet alleen om het investeren in apparatuur maar bijvoorbeeld ook om het bemachtigen van frequenties in veilingen, en uitrol van innovatieve nieuwe diensten. Hierbij is het belangrijk te beseffen dat de uitrol van 5G vooral een doorontwikkeling is van bestaande 4G-netwerken. 5G zal vaak juist vanuit een bestaand LTE-netwerk geleidelijk aan ingevoegd worden, vaak met software-updates op bestaande apparatuur. De meeste huidige 5G-netwerken wereldwijd zijn van het 5G Non Stand-Alone (NSA) type. Op hoofdlijnen betekent dit dat de bestaande LTE-laag zorgt voor de signalering en de 5G-laag alleen als een extra capaciteitslaag toegevoegd wordt. Ook in het bestaande RAN kan 5G geïntroduceerd worden, hetzij door *spectrum refarming* of binnenkort ook middels *Dynamic Spectrum Sharing* (DSS). Die link tussen bestaande infrastructuur en hoe een operator 5G introduceert is zeer relevant. Wereldwijd bouwt bijna geen enkele operator een 5G SA (Stand-Alone) netwerk vanaf de grond op. De recente aankondiging van VodafoneZiggo dat zij starten met 5G ondersteunt het beeld dat het incrementele doorontwikkeling is van bestaande systemen.[26]

Op een latere termijn zullen nieuwe opstelpunten ook voor een extra kostenpost gaan zorgen. In Nederland geldt dat operators na verkrijging van een licentie vanaf 1 september 2022 de 3,5 GHz band kunnen inzetten voor 5G. In Frankrijk anticipeert de Senaat dat

telecomoperators vanaf 2022 zullen investeren in eerste 5G-standalone netwerkimplementaties (zoals nieuwe opstelpunten). [27]

3.3 Impact op investeringsbeslissingen

In het vorige hoofdstuk is aangegeven dat investeerders een risico-opslag gebruiken om de waarde van investeringen te bepalen. Een additioneel risico zorgt voor een hogere risico-opslag, wat zorgt voor een hogere discontovoet en voor lagere investeringsbereidheid. Dit model verklaart in generieke zin hoe marktpartijen zich gedragen, maar in het kader van de structurele aanpak zien we ook drie specifieke effecten:

1. De impact op investeringsbeslissingen is onvoorspelbaar omdat het risico nauwelijks in te schatten is.
2. Er kan een situatie van "zelfcensuur" ontstaan.
3. De marktdynamiek dempt de impact op investeringsbeslissingen

De onderstaande punten werken we hieronder nader uit.

Hoge mate van onvoorspelbaarheid bij investeringsbeslissingen

In dit geval hebben we te maken met een situatie waarin het heel lastig is om te bepalen *wat* het risico is. Het besluit zorgt voor een dermate grote mate van onzekerheid, dat er onzekerheid *over de onzekerheid* is. Een deel van de risico's zijn voor partijen heel goed in te schatten en kunnen worden meegenomen in de business case. Denk aan de verschuivingen in marktaandelen, inflatie en ontwikkeling van de klantvraag. Echter, voor een deel van de risico's is er simpelweg geen inschatting mogelijk omdat er geen referentiepunten zijn.

Het is lastig om goede voorbeelden van *unknown unknowns* met een flinke omvang te vinden in de telecomsector. Het volgende voorbeeld toont echter goed aan dat telecomoperators goed om kunnen gaan met voorspelbare risico's ("known unknowns"), zelfs al zijn ze zeer groot. Echter, onvoorspelbare risico's kunnen catastrofaal zijn. Uit onze praktijk kennen wij het voorbeeld van telecomoperators in Afghanistan. Zij weten uit ervaring dat de Taliban jaarlijks een deel van hun masten opblaast. [29] Dit gebeurt echter al een decennium lang, en de operators kunnen vrij goed inschatten hoe veel masten zij per jaar moeten repareren: "*Replacing towers, which cost roughly \$100,000 each, is considered a normal (!) business operation.*" [30] Deze parameter nemen zij mee in hun investeringsbeslissingen. Wat voor hen echter niet te modelleren is, is het feit dat de overheid deze sector de afgelopen jaren zeer zwaar is gaan belasten, omdat het een van de weinig succesvolle manieren is belasting te heffen in dit land. In het afgelopen decennium is de bijdrage van de telecomindustrie aan de totale belastinginkomsten gegroeid tot meer dan 25%(!). [30] Hun investeringszekerheid wordt veel sterker aangetast door het niet te modelleren risico van een overheid die sterk ingrijpt, dan door de Taliban die masten opblaast.

Zelfcensuur

Een effect dat mogelijk eveneens kan ontstaan is zelfcensuur. Investeerders gaan op basis van hun interpretatie van (de impact van) het Besluit voor bepaalde leveranciers een risico-opslag hanteren. Concreet kan dit betekenen dat bij een inkooptraject enkele leveranciers een malus krijgen omdat de inschatting is dat de kans groter is dat hun apparatuur in de toekomst uit netwerken en systemen moeten worden gehaald.

Op zijn beurt kan deze zelfcensuur ertoe leiden dat de apparatuur van de overgebleven leveranciers duurder wordt aangeboden. In delen van de markt -vooral als het gaat om de RAN- is zoals aangegeven nu al sprake van een oligopolie. Het wegnemen of op achterstand

zetten van één partij zal er zeer waarschijnlijk voor zorgen dat de andere partijen de mogelijkheid hebben om prijzen te verhogen. Op de iets langere termijn kan dit ook de dynamische efficiëntie van deze markt, dat wil zeggen de mate van innovatie- aantasten.

Dempend of versterkend effect van de marktdynamiek

In het algemeen kan gesteld worden dat een hogere risico-opslag leidt tot lagere investeringen. De vraag is echter in welke mate dit door de bestaande marktdynamiek hier een effect op heeft. Hier spelen onzes inziens drie effecten.

Ten eerste is de vraag in welke mate noodzakelijke investeringen kunnen worden uitgesteld. Uit empirisch onderzoek [10] blijkt namelijk dat het effect van onzekerheid op investeringen over de tijd afneemt. Concreet voor de telecomsector komt de vraag naar voren *hoe lang je nog doorwerkt met een systeem dat niet meer (optimaal) werkt*. Indien er echt sprake is van systemen die niet meer functioneren, dan zal je deze hoe dan ook moeten vervangen: een telecomoperator kan niet anders. Indien er sprake is van de systemen die niet meer optimaal werken kan deze beslissingen wellicht worden uitgesteld, maar ook dat is slechts een tijdelijke optie.

Ten tweede speelt de vraag wat de kosten zijn van niet investeren. Met andere woorden: wat is als telecomoperator je alternatief? De onzekerheid zorgt ervoor dat investeren minder aantrekkelijk wordt, maar verandert wellicht weinig aan de optie niet investeren. Wellicht is het goed om dit concreter te maken. In welke mate hebben KPN, T-Mobile en VodafoneZiggo de optie om niet grootschalig in nieuwe netwerken te investeren? Niet investeren betekent voor hen dat zij op de langere termijn marktaandeel gaan verliezen. Indien één van de drie partijen er niet voor gekozen had om zijn 3G-netwerk door te ontwikkelen naar 4G, dan zou deze op dit moment veel minder klanten gehad hebben. Dit kan betekenen dat zij de langere termijn hun activiteiten moeten staken. De drempel om de markt te verlaten is echter zeer substantieel omdat hun bestaande investeringen weinig restwaarde hebben. Met andere woorden: de *exit barrier* op de markt is zeer hoog.¹¹ Dit laatste geldt in extreme mate voor KPN. Voor hen betekent uitstappen op de Nederlandse mobiele markt feitelijk dat zij direct hun omzet uit mobiel (circa €1,7 miljard van €5,5 miljard in totaal) verliezen. [21] Daarbij is het verder nog maar de vraag in welke mate de rest van hun omzet gerealiseerd kan worden zonder mobiele dienstverlening.

Ten derde bestaat er de vraag of investeringen elders een lagere risk risico-opslag kennen, het fenomeen *opportunity costs*. Voor internationaal opererende telecomoperators, in dit geval Vodafone/LibertyGlobal en Deutsche Telekom, speelt dit in sterke mate mee: investeringen in Nederland moeten 'intern' verkocht worden. Hierbij geldt dat wanneer de businesscase in Nederland relatief moeilijk rond is te krijgen er een kans bestaat dat Nederland laat aan de beurt komt bij de 5G-uitrol. Een eventuele vertraging in 5G uitrol kan ertoe leiden dat Nederland niet voorop zal lopen als het gaat om ontwikkeling en implementatie van 5G-gebaseerde diensten. Uiteraard geldt dit niet alleen voor mobiele netwerken maar ook voor vaste netwerken.

De impact kan ook gezien worden vanuit het perspectief dat een telecomoperator schaarse capaciteit heeft om activiteiten uit te voeren. Dit is niet alleen kapitaal in de klassieke zin

¹¹ Een goed recent voorbeeld van hoge exit barriers komt van de Amerikaanse producenten van (schalie)olie. Onder meer door de Coronacrisis viel de vraag naar olie sterk terug en de prijzen daalden sterk. De olieprijs ligt onder de productieprijs van veel Amerikaanse schalieolie. Echter, deze producenten van schalieolie hebben geen andere optie dan tegen lagere kosten blijven doorleveren en verlies blijven nemen. De verkoop van de systemen die zij hebben zal slechts een fractie opleveren dan waarvoor ze zijn aangeschaft.

van het woord, maar juist ook menselijk kapitaal. Als een telecomoperator veel van deze capaciteit moet inzetten om systemen te wijzigingen in het kader van het Besluit, dan kan deze capaciteit niet worden gebruikt voor andere (innovatieve) projecten.

3.4 Impact op marktdynamiek

Zoals eerder aangegeven in dit stuk (1) hebben ICT-voorzieningen een belangrijke impact op de economische groei voor de hele maatschappij, (2) hebben we in Nederland zeer goede mobiele netwerken tegen acceptabele kosten en (3) is een goede marktdynamiek een belangrijke randvoorwaarde om dit te realiseren en handhaven. Een interessant vraagstuk is dan ook in welke mate het Besluit de marktdynamiek in Nederland kan beïnvloeden. Op basis van onze analyse komen we tot de conclusie dat de marktdynamiek niet positief beïnvloed zal worden. Veel belangrijker is echter dat wij verwachten dat een negatieve ontwikkeling van de marktdynamiek vooral in grote schokken kan gaan en geen continu proces is. Met andere woorden: het bestaande (markt)evenwicht kan tegen een stootje, maar een te harde klap zorgt ervoor dat we op een ander, minder positief evenwicht terecht gaan komen. Hieronder gaan we hier nader op in.

Op dit moment hebben we in Nederland drie mobiele telecomoperators. De kans dat er een vierde bijkomt lijkt zeer klein. Recent is de vierde partij (Tele2) overgenomen door de toenmalige nummer drie (T-Mobile). De telecommunicatiemarkt is een markt van schaal en grotere partijen kunnen simpelweg tegen lagere kosten per klant leveren dan kleine partijen. In veel andere Europese landen (Duitsland, België, Oostenrijk, Ierland, Noorwegen, Portugal en Zwitserland [32]) zien wij ook drie grote operators in de markt. Binnenkort zullen er nieuwe veilingen plaatsvinden en dan wordt duidelijk of er in Nederland een vierde partij zich zal melden. Zonder frequenties is de markt feitelijk dicht voor nieuwe partijen. Aan de andere kant is de kans dat één partij zich uit de markt terugtrekt ook vrij gering: zoals eerder aangegeven zijn de exit barriers hoog. De condities moeten sterk verslechteren wil dit gebeuren.

De drie partijen in Nederland hebben *op hoofdlijnen* dezelfde strategie voor hun mobiele netwerken. Ze kiezen er alle drie voor om flink te investeren in hun netwerken en te zorgen voor hoogwaardige, innovatieve proposities voor klanten. Dit lijkt wellicht triviaal, maar dat is het zeker niet. In andere markten zien wij ook marktpartijen die kiezen voor het aanbieden van producten of diensten die vooral op prijs concurreren. Bij mobiele netwerken hebben we geen Ryanair of Easyjet; we hebben de equivalenten van KLM, Lufthansa en British Airways.

In ons perspectief ligt het grootste risico van het Besluit erin dat één mobiele telecomoperator ervoor kiest om zijn bestaande strategie te veranderen. Grootchalige investeringen worden als te risicovol gezien als gevolg van het besluit. Het meest waarschijnlijk is het dat deze partij ervoor kiest om de investeringen in zijn netwerk terug te schroeven, bestaande assets maximaal uit te nutten en te gaan concurreren op prijs. Naar ons beeld zal dit de marktdynamiek niet ten goede komen, zeker op de langere termijn. Het zal er naar alle waarschijnlijkheid voor zorgen dat de mate van innovatie in de markt in den brede omlaaggaat. Daarnaast zien wij een risico bestaan dat dit een voorbode kan zijn van het verlaten van de markt door deze partij. Dit kan de marktdynamiek in Nederland een flinke klap geven. Echter, voordat de markt zal worden verlaten moet er het nodige gebeuren. De exit barriers zijn zeer hoog.

Tot slot geldt er ook een internationaal perspectief. De telecommunicatiemarkt is een markt die zich bij uitstek kenmerkt door schaalvoordelen. Internationaal opererende telecomoperators zullen naar alle waarschijnlijkheid niet graag per land differentiëren in aanpak voor de keuze van typen/versies van hardware en software en al helemaal niet in leveranciers. Ook zullen bij telecomoperators met een buitenlandse moeder

investeringsbeslissingen op internationaal niveau worden bepaald. Vanuit deze redenering bedraagt de netto impact ten gevolge van onzekerheid n.a.v. het besluit de *additionele* onzekerheid die Nederland wordt opgeworpen ten opzichte van andere landen. Wanneer Nederland minder of evenveel onzekerheid opwerpt dan elders (bijv. niet strikter dan EU-maatregelen), dan kunnen telecomoperators die internationaal opereren dezelfde schaalvoordelen blijven nastreven. Nu zijn andere landen zeker niet eensgezind in hun pakket aan maatregelen, maar als Nederland sterk afwijkend beleid gaat voeren, dan gaan schaalvoordelen niet op en kan het zo zijn dat er in andere landen eerder wordt geïnvesteerd, waardoor uitrol in Nederland beperkt of vertraagd zal plaatsvinden. Dit onderstreept het belang van Europees samenwerking.

3.5 Impact op andere delen van het telecom-ecosysteem

Naast de impact op de marktdynamiek, kunnen we ons ook voorstellen dat andere delen van het telecom-ecosysteem beïnvloed worden door de intransparantie die nu wordt ervaren. Immers, ondanks het Besluit is vanuit de overheid in publiekelijk geen volledige transparantie geboden over de inhoud van de maatregelen. Hierdoor blijft de discussie over het pakket aan maatregelen voortduren. Uit de gesprekken komen drie vormen naar voren:

- Het Besluit leidt tot speculatie in de media en bij Kamerleden dat de Minister strenger beleid moet gaan voeren. Dit kan ertoe leiden dat (media)incidenten een grote impact hebben op investeringszekerheid waar het telecomaandieners niet duidelijk is hoe de overheid met eventuele druk vanuit politiek en media om extra maatregelen te nemen om gaat.
- Het Besluit -en hiervan afgeleide de exposure in de media die we hierboven noemden- leidt ertoe dat sommige lokale overheden additionele eisen willen gaan stellen aan het afgeven van vergunningen voor opstelpunten.
- Het Besluit leidt ertoe dat sommige grootzakelijke klanten zich afvragen of de netwerken die zij gebruiken wel veilig zijn. Zij nemen in de specificaties bij hun inkoop op -of overwegen dit- dat zij geen apparatuur van leveranciers uit risicolanden in de netwerken willen zien. Dit kan ertoe leiden dat ook onderdelen van het netwerk die weinig veiligheidsrisico's kennen aangepast moeten worden.

Voor alle drie aspecten geldt dat het zorgt voor een extra, lastig te voorspellen risico voor telecomoperators, hetzij op het gebied van *regulatory*, *operations* of *sales*.

4 Vormgeving van de structurele aanpak

In dit hoofdstuk gaan we in op de wijze waarop de (investerings)zekerheid voor telecomoperators kan worden vergroot. In §4.1 vatten we de lessen samen die we uit de vorige hoofdstukken kunnen halen. Dit geeft ons kaders voor de structurele aanpak. We stellen voor de bestaande vormgeving van de structurele aanpak uit te breiden met en/of meer uitwerking te geven aan elementen die zorgen voor meer investeringszekerheid. Echter, binnen deze kaders is veel vrijheid voor verschillende invullingen. Omdat een discussie beter verloopt als er concrete suggesties zijn, stellen wij in §4.2 een manier voor om procesafspraken vorm te geven. In §4.3 schetsen we op basis hiervan mogelijkheid om (mogelijk) ongewenste investeringen te voorkomen. Ten slotte wordt in §4.4 beschreven hoe op een meer fundamentele manier risico's kunnen worden aangepakt door de marktdynamiek bij leveranciers te beïnvloeden.

4.1 Kaders van de structurele aanpak

Het doel van de structurele aanpak zoals verwoord door de Task Force Economische Veiligheid is: *een structurele aanpak tussen overheid en telecomeaanbieders om de nationale veiligheid te beschermen tegen risico's die volgen uit de digitale dreiging vanuit geavanceerde (statelijke) actoren via misbruik van de telecomsector. Om ook het belang van investeringszekerheid voor telecomoperators als samenwerkingspartner een plek te geven in de structurele aanpak, wordt voorgesteld deze doelstelling te verbreden door investeringszekerheid op te nemen in de doelstelling.*

Uit de analyses in de vorige hoofdstukken en de input uit de gesprekken stellen we voor in de uitwerking van de structurele aanpak nadere uitwerking te geven aan de volgende punten:

1. De structurele aanpak moet een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid bieden.
2. Er zijn tien concrete randvoorwaarden voor meer investeringszekerheid in de structurele aanpak.
3. Transparantie over hoe de structurele aanpak zich verhoudt tot bestaande gremia en structuren.

Deze aspecten worden in de volgende paragrafen nader toegelicht.

4.1.1 Een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid

Er moet gestreefd worden naar een structurele aanpak waarin zowel de flexibiliteit van beleid als de investeringszekerheid zo veel mogelijk gewaarborgd blijven. Flexibiliteit van beleid en investeringszekerheid zijn (1) beide essentieel voor de Nederlandse maatschappij, (2) kunnen elkaar versterken, maar (3) kunnen elkaar ook negatief beïnvloeden. Er moet gezocht worden naar modellen waarbij die beide aspecten in optimaal evenwicht zijn, aangezien zowel markt als overheid gebaat zijn bij een model waarbij beide aspecten goed tot hun recht komen. Dit betekent dat marktpartijen moeten accepteren dat de overheid tot op zekere hoogte flexibel beleid moet kunnen voeren. De overheid moet accepteren dat investeringszekerheid voor marktpartijen een voorwaarde is voor het aanbieden van hoogwaardige dienstverlening in Nederland.

In dit stuk staat het perspectief van investeringszekerheid versus flexibiliteit van beleid centraal. Waarbij het rapport focust op het perspectief van investeringszekerheid gezien de opdracht.

Flexibel beleid is essentieel voor de Nederlandse maatschappij

De wijze waarop het Besluit geformuleerd is, houdt te allen tijde de mogelijkheid open tot het beslissen tot verwijdering van bepaalde systemen uit telecomnetwerken. Op basis van het Besluit blijft dan ook altijd de mogelijkheid bestaan dat systemen achteraf moeten worden verwijderd: een operator kan nauwelijks anticiperen. Er is immers sprake van een zeer dynamische wereld en hoge mate van onvoorspelbaarheid als het gaat om geopolitiek. Overheden die hiermee worden geconfronteerd willen altijd *kunnen* handelen wanneer het gaat om de nationale veiligheid, en de structurele aanpak mag dat niet te veel belemmeren. Zoals in een van de gesprekken werd gezegd: *"Je kunt vooraf alles afspreken en bedenken, maar als we over vijf jaar een fundamentele, niet oplosbare en voor de nationale veiligheid zeer relevante kwetsbaarheid in apparatuur van een bepaalde leverancier vinden, dan moet deze apparatuur er gewoon uit."*

Investeringszekerheid is essentieel voor de Nederlandse maatschappij

Telecomoperators bevinden zich in een zeer kapitaalintensieve industrie en investeren elk jaar grote bedragen in de Nederlandse markt. Dit heeft ervoor gezorgd dat Nederland een uitstekende digitale infrastructuur heeft. Deze infrastructuur draagt substantieel bij aan de welvaart en het welzijn in Nederland. [3] De investeringen worden echter alleen gedaan als de investeerders enige zekerheid hebben dat zij dit terug kunnen verdienen. Indien dit niet (of in veel mindere mate het geval is) dan zullen deze investeringen sterk teruglopen. Op de korte termijn heeft dit weinig impact, maar op de langere termijn zal de kwaliteit van de digitale infrastructuur afnemen. Hierdoor zijn we als Nederland minder goed in staat om onze internationale concurrentiepositie te handhaven. Maar er zijn ook talloze negatieve neveneffecten op maatschappelijk niveau aangezien de telecomindustrie ook hier een toeleverancier is. Een hoogwaardige digitale infrastructuur is essentieel voor innovaties in talloze sectoren. Denk aan zorg, onderwijs, veiligheid, logistiek, et cetera. Zonder onze uitstekende digitale infrastructuur was bijvoorbeeld ook de maatschappelijke en economische impact van de Coronacrisis een veelvoud geweest. Voor onze toekomstige welvaart en welzijn hebben we uitstekende digitale infrastructuren nodig.

Soms tegenpolen, soms versterkende effecten

De vrijheid van de overheid om beleid elke moment te kunnen wijzigen en de investeringszekerheid van marktpartijen staan in sommige gevallen op gespannen voet met elkaar. In extremis zijn deze twee concepten tegenpolen van elkaar. Als er geen enkel compromis gesteld mag worden aan de uitvoering van het Besluit veiligheid en integriteit telecommunicatie, dan is er nauwelijks investeringszekerheid. En omgekeerd: als investeringszekerheid voor alles gaat, dan zal het Besluit veiligheid en integriteit telecommunicatie elke vorm van flexibiliteit ontberen.

Beide extremen zijn onrealistische scenario's. In een wereld waarin de overheid geen enkele rekening houdt met de belangen van de markt, daar zal de markt al haar prikkels om te investeren verliezen. Zeker als het gaat om investeringen met een relatief hoog risicoprofiel. Hierboven maakten we duidelijk dat dit een negatieve impact op de Nederlandse maatschappij zal hebben. Het zou er bovendien aan kunnen bijdragen dat marktpartijen een prikkel verliezen om substantieel te investeren in veiligheid. De "netto-veiligheid" van netwerken zou dus wel eens kunnen afnemen. Daarnaast zal de bereidheid van marktpartijen om met de overheid samen te werken -in een breed scala aan dossiers in verschillende maatschappelijke sectoren- sterk afnemen. Omgekeerd zal in een wereld waarin de overheid

geen enkele vrijheid heeft om te handelen, de markt mogelijk investeringen doen die achteraf risico voor de Nationale veiligheid blijken te zijn. Het is duidelijk dat ook dit kan leiden tot zeer grote maatschappelijke kosten (uitval van netwerken, cyberaanvallen op kritieke infrastructuren, etc.).

Er moet gezocht worden naar een structurele aanpak die bestaat uit een samenwerking waarin markt en overheid elkaar versterken. Zeker niet in alle gevallen betekent een vergroting van de investeringszekerheid een beperking van de flexibiliteit van beleid. Omgekeerd kan een kleine beperking van de investeringszekerheid in sommige gevallen er voor zorgen dat de overheid veel meer slagkracht krijgt om te handelen. Daarnaast moet er gezocht worden naar manieren waarin de overheid en de markt elkaar versterken. Een goede mogelijkheid ligt op het gebied van het uitwisselen van kennis en expertise. Het belang hiervan is ook onderkend in het huidige plan van aanpak voor de structurele samenwerking. De kennis en expertise die de markt heeft op dit domein kan de positie van de overheid versterken en vice versa.

Verwijderen van systemen alleen als het echt niet anders kan

Het verwijderen van systemen is een essentieel beleidsinstrument om de nationale veiligheid te beschermen, naast het treffen van technische en organisatorische beveiligingsmaatregelen. De behoefte aan beide instrumenten wordt reeds onderkend binnen de aanpak van de Task Force Economische Veiligheid. In de structurele aanpak zou waar mogelijk moeten worden ingezet op mitigerende maatregelen, zoals het aanpassen van systemen of processen. Immers, het achteraf verwijderen van systemen kent hoge maatschappelijke kosten. Het betalen van nadeelcompensatie door de overheid aan een marktpartij is per definitie een maatschappelijk inefficiënte investering: er is een substantiële schade die de maatschappij linksom of rechtsom gaat dragen. Waar de kosten (in welke mate) neervallen maakt voor dit argument weinig uit. Stel dat er €100 miljoen schade is als gevolg van het verwijderen van apparatuur, dan komt deze terecht bij de overheid (door het uitbetalen van nadeelcompensatie) en/of de aandeelhouders van het telecombedrijf (doordat de nadeelcompensatie niet volledig is) en/of bij de afnemers (door hogere prijzen). Eén stap verder zijn dit allemaal (veelal Nederlandse) burgers: belastingbetalers, beleggers en klanten. Zij hebben er meer aan als deze 100 miljoen op andere manieren wordt ingezet.

4.1.2 Tien concrete voorwaarden voor een succesvolle invulling van de structurele aanpak

Op basis van de generieke theorie over investeringszekerheid (hoofdstuk 2), de impact van het Besluit op investeringen in de telecomsector in Nederland (hoofdstuk 3), de internationale studie en input uit de gesprekken met telecomoperators komen we tot tien concrete voorwaarden voor een invulling van de structurele aanpak die meer investeringszekerheid realiseert:

1. *Omgeving van vertrouwen tussen samenwerkende partijen.* De overheid moet de telecomoperators vertrouwen en vice versa. Informatie tussen telecomoperators en overheid moet (tot op zekere hoogte) worden uitgewisseld. Dit betreft zowel informatie die verband houdt met concrete risicoanalyses als met de vormgeving van de structurele aanpak. Dit vertrouwen is hier extra relevant omdat het vaak gaat om gerubriceerde informatie. Een omgeving van vertrouwen is ondersteunend aan andere hier genoemde punten.
2. *Overheidsbrede, interdepartementale insteek.* Het is evident dat overheid een veelkoppige entiteit is waarin verschillende perspectieven en belangen spelen. Richting de telecomoperators is het van belang dat de overheid met één mond spreekt, waarbij de verschillende perspectieven van de overheid vooraf afgestemd

en geharmoniseerd zijn. De Task Force Economische Veiligheid is een voorbeeld van deze interdepartementale afstemming en besluitvorming.

3. *Passend binnen internationale context.* De Nederlandse telecommarkt is slechts een klein deel van de mondiale markt, maar toch zijn alle leveranciers en twee van de drie telecombedrijven (onderdelen van) mondiale spelers. Internationale samenwerking kan het binnenlandse investeringsklimaat versterken. Beleid in Nederland zou niet te veel (negatief) moeten afwijken van beleid in het buitenland. Als wij dit in Nederland toch doen, dan zullen investeerders de voorrang geven aan investeringen in andere landen. Vooral Europese afstemming lijkt voor de hand te liggen.
4. *Stimuleren van een competitief concurrentiespeelveld.* Nederland kent uitstekende telecomnetwerken tegen acceptabele kosten die van groot belang zijn voor economische groei en maatschappij. Behoud van een goede marktdynamiek is een belangrijke randvoorwaarde voor investeringen door telecomoperators om deze goede uitgangspositie te behouden. De structurele aanpak moet rekening houden met het belang van het behoud van de marktdynamiek.
5. *Leren en verbeteren van beleid.* We kunnen in deze fase de structurele aanpak tot op zekere hoogte vormgeven, maar er moet op enig moment een evaluatiemoment zijn waardoor er geleerd wordt van de ervaringen. Zo blijft beleid zichzelf verbeteren.
6. *Transparant proces.* Het moet vooraf voor telecomoperators duidelijk zijn hoe de procesgang zal zijn. Welke stappen worden doorlopen? Hoe (vaak) wordt een risicoanalyse uitgevoerd? Hoe ziet de besluitvorming eruit? Welke rol hebben zij hierin? In het algemeen moet het proces meer concreet worden gemaakt zodat telecomoperators deze kennis kunnen meenemen bij het maken van (investerings)beslissingen.
7. *Voorspelbaar proces.* Naast dat het proces transparant moet zijn, zou het ook zo veel mogelijk voorspelbaar moeten zijn. Investeerders kunnen prima omgaan met risico's, mits het risico voorspelbaar is.¹² Er moet antwoord gegeven kunnen worden op vragen als: wat is het risico dat systemen moeten worden verwijderd? Welk kader voor nadeelcompensatie wordt gehanteerd? Zijn uit de structurele aanpak voortvloeiende beleidsmaatregelen vooraf in te schatten? In welke mate kunnen telecomoperators hier rekening mee houden? Zijn er objectieve eisen waaraan systemen moeten voldoen? Objectiviteit is een centraal element hierbinnen. Bij voorspelbaarheid hoort ook de wijze waarop regels veranderd kunnen worden in een later stadium (zie stap 5).
8. *Non-discriminair proces.* Er mag geen onnodig onderscheid worden gemaakt tussen partijen.
9. *Begrijpelijk proces.* Begrijpen telecomoperators waarom de risicoanalyse en de besluitvorming op een bepaalde wijze uitgevoerd worden? Begrijpen overheid en markt van elkaar dat zij een ander *risk appetite* hebben en waarop dit gebaseerd is?
10. *Proces met voldoende rechtsbescherming.* De mogelijkheid om bezwaar te maken tegen (de gevolgen van) besluiten die door de overheid worden genomen door deze te laten toetsen door een rechter, is (voor telecomoperators) een cruciaal recht.¹³ Het moet duidelijk zijn hoe beroep aangetekend kan worden, vooral als het gaat om

¹² Het opvallende voorbeeld van telecomoperators in Afghanistan dat wij eerder benoemden illustreert dit wellicht best: De Taliban die elk jaar een paar honderd masten opblaast is niet zo een probleem. Zowel de kosten als de frequentie zijn voorspelbaar. Maar de overheid die de belastingdruk op deze sector explosief laat toenemen is een groot probleem door de onvoorspelbaarheid ervan.

¹³ In paragraaf 2.2.1 staat de Box: Onteigening van (bedrijfs)eigendommen waarin dit verder wordt toegelicht.

het verwijderen van systemen.¹⁴ Voor een afdoende niveau van rechtsbescherming willen telecomoperators informatie, ook gerubriceerde, kunnen delen met hun advocaten.

Vanuit het perspectief van meer investeringszekerheid zal moeten worden gezien hoe bovenstaande elementen in de verdere vormgeving van de structurele aanpak kunnen worden meegenomen. Sommigen zitten er al in, zoals de interdepartementale coördinatie via de Task Force Economische Veiligheid en hoe gerubriceerde informatie tussen overheid en telecomoperators kan worden gedeeld. Voor veel andere punten geldt dit nog niet of beperkt.

4.1.3 Transparantie over aansluiten bij bestaande gremia en structuren

De structurele aanpak wordt ontwikkeld binnen een context van bestaande institutionele kaders met gedefinieerde rollen en verantwoordelijkheden en gremia waar publiekprivaat informatie wordt uitgewisseld tussen overheid en telecomoperators. Hierbij gaat het ook om informatie over veiligheid en continuïteit van telecommunicatie. Helder moet zijn hoe de structurele aanpak zich verhoudt tot deze bestaande context. Wat wordt waar behandeld en wat betekent dit voor de verantwoordelijkheden en rollen van diverse betrokken partijen?

In de basis zijn de telecommunicatieoperators op operationeel gebied zelf verantwoordelijk voor de veiligheid van hun netwerken. Het uitgangspunt is dat een telecomoperator een eigen verantwoordelijkheid heeft hoe zij de continuïteit en integriteit van de netwerken realiseert, passend bij hun specifieke situatie. Die verplichting hebben zij vanuit de Telecommunicatiewet. Het Agentschap Telecom is de partij die verantwoordelijk is voor toezicht hierop.

Er bestaan diverse publiek-private structuren die zich richten op informatie-uitwisseling en het vergroten van de veiligheid van netwerken. Zo wordt via de ISAC-Telecom tussen overheid (NCSC en I&V diensten) en telecomoperators informatie gedeeld over dreigingen, kwetsbaarheden, incidenten en maatregelen op cybersecuritygebied. Verder bestaat het Nationaal Continuïteits Overleg Telecom waarin het Ministerie van EZK met de telecomoperators onder andere business continuity vraagstukken bespreekt.

De structurele aanpak moet goed aansluiten bij de bestaande gremia en structuren. De verwachting is dat veel van de dreigingen via deze bestaande gremia en structuren kunnen worden afgehandeld. Maar specifiek voor de situaties waarvan het vermoeden bestaat dat op basis van nieuwe informatie over dreiging of techniek het weerbaarheidsniveau van de telecomnetwerken onvoldoende om de nationale veiligheidsbelangen te beschermen, de structurele aanpak in scope komt. Daar zijn de afspraken over verantwoordelijkheden en rollen nog diffuus, hetgeen onzekerheid met zich meebrengt voor telecomoperators.

4.2 Inrichten van een proces hoe met nieuwe dreigingen wordt omgegaan

In paragraaf 4.1.2 schetsten wij belangrijke voorwaarden voor de structurele aanpak vanuit het perspectief van investeringszekerheid. Voor het vervolgproces is het ons inziens van belang om aan die voorwaarden tegemoet te komen via op te stellen procesafspraken tussen overheid en telecomoperators. Omdat een discussie beter verloopt als er concrete suggesties

¹⁴ Een goed voorbeeld is de Ontheeningswet uit 1851(!) die de overheid kan inzetten om grond te onteigenen voor de bouw van wegen of bedrijventerreinen. Ontheening kan alleen onder strikte wettelijke voorwaarden en er is uitvoering beschreven hoe het juridisch proces loopt.[34]

zijn, wordt in deze paragraaf een voorzet daartoe gedaan. Het betreft een voorstel voor de wijze waarop de structurele aanpak nader *kan* worden vormgegeven. Er zijn in de praktijk uiteraard ook andere manieren mogelijk. Het is daarom mogelijk dat uitwerkingen in dit document niet overeenkomen met andere voorstellen op het gebied van de structurele aanpak. Deze paragraaf moet dan ook gezien worden als een eerste voorzet die aan het begin staat van een discussie tussen stakeholders en niet als de uitkomst van de discussie.

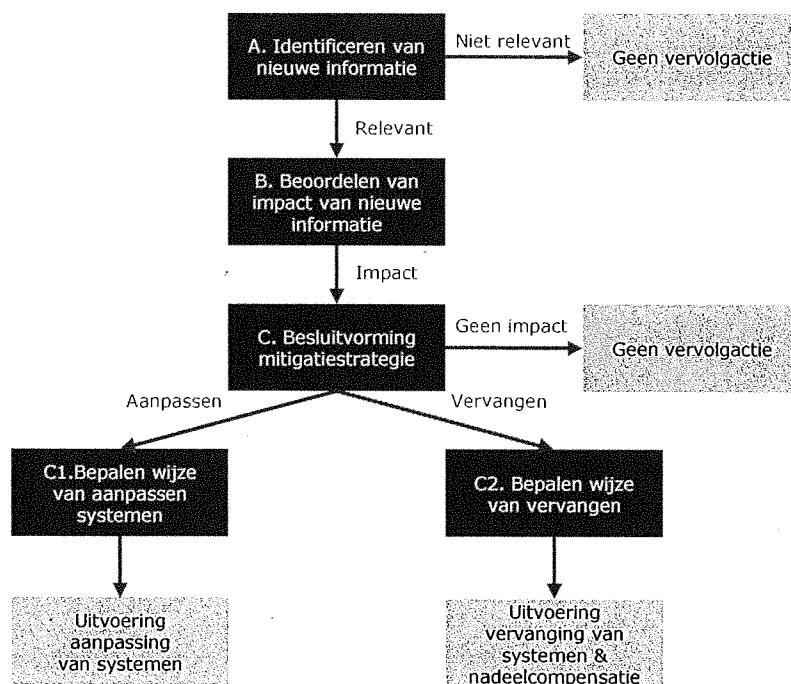
4.2.1 Doelstelling van procesafspraken

Heldere procesafspraken tussen overheid en telecomoperators over de structurele aanpak dragen bij aan een betere *transparantie, begrijpelijkheid* (en daarmee voorspelbaarheid) van die structurele aanpak en een *omgeving van vertrouwen*. Dit is extra van belang omdat overheid en telecomoperators van elkaar afhankelijk zijn in de structurele aanpak om zinvolle uitkomsten te verkrijgen. Tevens zullen zij elkaar regelmatig tegen komen in de structurele aanpak wat een relatie gericht op samenwerking met aandacht en begrip voor elkaars belangen essentieel maakt. Zowel overheid als telecomoperators hebben baat bij een goede en heldere procesgang. Samenwerking zal moeten worden gevoerd op verschillende niveaus: uitvoerend, beleidsmatig en besluitvormend. Partijen (verschillende onderdelen van de overheid en de telecomoperators) zijn van elkaar afhankelijk bij zowel het uitvoeren van een goede risicoanalyse (ieder brengt een deel van de benodigde kennis in) als voor het adequaat vormgeven van de maatregelen. Draagvlak voor die maatregelen en de achterliggende analyse is van belang omdat (1) verschillende partijen invulling moeten geven aan die maatregelen, (2) het risico op slepende bezwaar- en beroepsprocedures wordt verkleind en (3) men in volgende risicoanalyses weer met elkaar moet samenwerken en van elkaar afhankelijk is.

Bij de procesafspraken moeten marktpartijen en overheid begrip hebben voor elkaars uitgangspunten. Partijen bekijken de problematiek vanuit hun eigen perspectief en kernwaarden en er kan sprake zijn van tegenstrijdige belangen. Zo kunnen partijen verschillende opvattingen hebben over de gewenste relatie tussen de markt en overheid, een andere bereidheid hebben ten aanzien van het lopen van risico's ("risk appetite"), et cetera. Er kan verschil van inzicht zijn over de uitgangspunten, maar niet over de feitelijke situatie. De partijen zouden elkaar moeten gebruiken om beter inzicht te krijgen in hoe de feitelijke situatie werkelijk in elkaar steekt. Hierin kan het procesontwerp een belangrijke rol spelen.

4.2.2 Procesontwerp

Er is een ruime literatuur over procesontwerp in dit soort complexe omgeving, zie De Bruijn & Ten Heuvelhof [42]. Met dit, en het bovenstaande als achtergrond, zijn er uiteraard talloze goede manieren om het proces in te vullen. Ter illustratie hebben wij aansluitend bij bestaande plannen een voorbeeld van een proces gemaakt dat gebaseerd is op bestaande plannen voor de structurele aanpak: Figuur 4.



Figuur 4. Verschillende stappen in het proces van deze waarop nieuwe dreigingen impact hebben

De verschillende stappen behelzen het volgende:

- In de eerst stap (stap A) worden nieuwe dreigingen geïdentificeerd. Vanuit verschillende bronnen kan nieuwe informatie betrokken worden. Door deze informatie te analyseren worden nieuwe dreigingen geïdentificeerd. Er kunnen ook nieuwe dreigingen ontstaan doordat telecom operators veranderingen aan hun netwerk doorvoeren. Op basis van een eerste inschatting kan worden bepaald of verder onderzoek nodig is. Zo ja, dan wordt overgegaan naar stap B.
- In stap B wordt diepgaander onderzocht of het huidige niveau van weerbaarheid van de telecomnetwerken voldoende is afgezet tegen de dreiging. En wordt op basis daarvan een advies gemaakt van wat nodig wordt geacht voor de weerbaarheid. In deze stap wordt ook de impact van eventuele maatregelen in kaart gebracht op economische, diplomatieke en juridische belangen.
- In stap C wordt op basis van de verkregen informatie uit stap B besloten welke vervolgactie wordt genomen ten aanzien van een goede mitigatiestrategie. Hier moet een goede balans worden gevonden tussen verschillende publieke belangen: economische belangen en veiligheid. In sommige gevallen zullen deze belangen overeenkomen, maar in een aantal gevallen zal er ook enige mate van tegenstelling zijn: De mitigatiestrategie die het best is vanuit het perspectief van veiligheid, is dan niet optimaal zijn vanuit bedrijfseconomisch perspectief (en vice versa).
- De oplossing kan liggen in het oordeel dat geen vervolgactie nodig is, het aanpassen van systemen (C1), of in het vervangen van systemen (C2). Hoewel vervangen in dit rapport een grote rol heeft gekregen, zullen in de praktijk waarschijnlijk veel dreigingen kunnen worden opgelost door technische (zoals het aanpassen van de instellingen, het uitvoeren van software-updates) en niet-technische maatregelen.

Voor alle stappen moeten de volgende aspecten worden uitgewerkt om tot succesvolle besluitvorming te kunnen komen:

1. Wat is het afwegingskader waarop getoetst wordt?

2. Welke partijen zijn (in welke rol en verantwoordelijkheid) betrokken bij deze stap?
3. Hoe worden besluiten genomen en hoe kan bezwaar worden gemaakt?
4. Hoe wordt omgegaan met geheimhouding?
5. Wat is de doorlooptijd van een stap?
6. (Hoe) kunnen deze bovenstaande afspraken veranderen?

Deze stappen worden hieronder nader uitgewerkt. Wij geven nadrukkelijk onze visie op de invulling en wij kunnen ons goed voorstellen dat alternatieve implementaties ook hun waarde hebben. In het begin van dit hoofdstuk hebben wij een aantal voorwaarden gegeven waaraan beleid zou moeten voldoen. Dit gebruiken wij hier bij op het opstellen van een mogelijk proces.

4.2.3 Afwegingskader

Voor alle processtappen zal vooraf een inhoudelijk afwegingskader moeten worden gemaakt zodat duidelijk is op basis waarvan de besluiten genomen worden. Bij het opstellen van deze kaders staat centraal dat er een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid moet zijn. Het kader geeft aan marktpartijen zekerheid hoe vaak dit gehele proces doorlopen gaat worden. Het zorgt voor een objectieve toetsing en biedt duidelijkheid aan alle partijen over de criteria waarop beoordeeld wordt. Ook sluit het aan bij de beginselen van non-discriminatie. De transparantie leidt tot vertrouwen tussen de betrokken partijen.

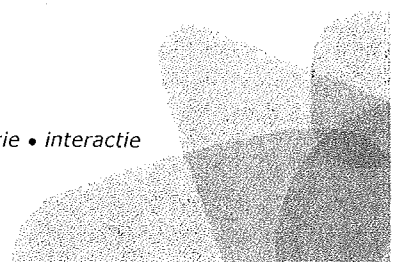
Bij het opstellen van de afwegingskaders zal in veel gevallen kunnen worden aangesloten bij bestaande kaders, zoals het Integraal Afwegingskader (IAK). Daarnaast is het aan te bevelen om juist hier te kijken naar de wijze waarop andere (Europese) landen hun beleid vormgeven.

In de vorige paragraaf toonden we een afbeelding met hierin de stappen in het proces. Voor elke stap zou moeten worden bepaald welke vragen moeten worden beantwoord in deze stap. Ook zou vooraf duidelijk moeten zijn hoe op basis van de antwoorden op deze vragen wordt besloten wat de vervolgstap is. Merk op dat een afwegingskader nooit volledige zekerheid zal bieden: elk kader biedt ruimte voor interpretatie en (dus) discussie. Het beantwoorden van de vragen wordt mogelijk vergemakkelijkt wanneer er een visie bestaat waartegen de afweging kan worden gemaakt. In de paragraaf 4.3.4 gaan we hier nader op in.

4.2.4 Betrokken partijen

Voor elke stap zal moeten worden bepaald welke partijen in welke rol betrokken zijn. Zoals eerder aangegeven is een brede, interdepartementale vertegenwoordiging van de overheid een pré. Als de juiste stakeholders aan tafel zitten dan, wordt de benodigde kennis ingebracht, zijn belangen vertegenwoordigd en wordt gekomen tot "*negotiated knowledge*". Dit zorgt voor een evenwichtige besluitvorming vanuit de overheid. Voor telecomoperators is het wel essentieel dat de overheid eenduidig communiceert richting hen. Ze hebben immers te maken met verschillende departementen en verschillende onderdelen hiervan die alleen een bepaalde rol nemen.

Aan de kant van de marktpartijen zal zorgvuldig moeten worden bepaald in welke stappen alle telecompartijen aan tafel zitten en wanneer sprake is van afzonderlijke trajecten met de individuele marktpartijen. Alleen zo kan een omgeving van vertrouwen gerealiseerd worden en de marktdynamiek niet negatief beïnvloed worden. Aan de ene kant leidt samenwerking tot een hoger niveau van veiligheid, maar aan de andere kant willen we niet het concurrentieverhoudingen verstoren.



Tot slot kan er ook nog worden overwogen om onafhankelijke experts te betrekken bij specifieke processtappen. Zij kunnen vanuit hun onafhankelijke expertise een brug vormen tussen overheid en markt. Dit kan zorgen voor een hogere mate van objectiviteit en vertrouwen.

4.2.5 Besluitvorming en bezwaar

Voor elke stap moet vooraf duidelijk zijn op welke wijze de besluitvorming plaatsvindt. Dit is een essentiële voorwaarde voor een transparant proces. Het zorgt tevens voor enige mate van voorspelbaarheid en vertrouwen tussen partijen. Hierbij spelen verschillende vraagstukken: hoe zorgen we dat alle relevante informatie in het besluit is meegenomen? Wie is betrokken bij de besluitvorming? Wat is het proces als er geen consensus is over het besluit? Tot slot: hoe loopt de mogelijkheid tot bezwaar?

De meest interessante vraag is uiteraard wat er gebeurt als er geen consensus is tussen overheid en een marktpartij over besluiten. Juist dit zou vooraf goed moeten vastgelegd. Het kunnen aantekenen van beroep is een essentieel aspect in dit proces. Grofweg zien wij twee escalatieroutes:

1. Er kan een onafhankelijke partij worden betrokken die een oordeel velt over het vraagstuk. Overheid en markt kunnen overeenkomen om samen een vooraf aangewezen expert te betrekken, welke partij dat is en wat de status van dit advies is: bindend of adviserend. Dit kan gezien worden als een vorm van arbitrage. Dit leidt tot een kortere doorlooptijd en meer flexibiliteit.
2. Er kan een formeel juridisch traject worden gestart waarin bezwaar wordt aangetekend door een marktpartij tegen een beslissing van de overheid. Hierbij is vooraf duidelijk hoe dit bezwaarproces eruitziet. Hiervoor geldt grofweg hetzelfde als voor de nadeelcompensatie (en veel andere juridische trajecten): het zijn instrumenten die noodzakelijk zijn in het proces, maar waarvan je eigenlijk wilt voorkomen dat je ze gebruikt.

4.2.6 Geheimhouding

Er zullen in dit proces -voor de verschillende stappen afzonderlijk- duidelijke afspraken moeten worden gemaakt over geheimhouding. Dit is wellicht het meest complexe vraagstuk in dit geheel. Aan de ene kant is het evident dat bepaalde informatie over dreigingen, de kwetsbaarheden van netwerken en concurrentiegevoelige gegevens niet openbaar worden. Aan de andere kant is de beschikbaarheid van bepaalde informatie noodzakelijk voor een objectieve toetsing, het maken van bezwaar, onderling vertrouwen tussen partijen. Er moet dus zorgvuldig worden afgewogen welke informatie in welke fase tussen welke partijen op welke wijze gedeeld gaat worden. Hierbij moet oog zijn voor zowel het overheidsperspectief vanuit nationale veiligheid om informatie zoveel mogelijk geheim te houden als het perspectief van telecomoperators om informatie breder te kunnen delen.

Dat het maken van afspraken hiervoor relevant is, blijkt uit de gesprekken die gevoerd zijn. Bij de telecomoperators is nu onvoldoende duidelijk welke informatie met welke personen mag worden gedeeld. Wat mag wel en niet openbaar of met bepaalde stakeholders besproken worden? Hoe gaan we om met het feit dat een beursgenoteerd bedrijf koersgevoelige informatie openbaar moet maken? Hoe kunnen telecomoperators hun recht op bezwaar en beroep goed uitoefenen als zij hiervoor bepaalde informatie niet mogen delen met hun advocaat? Leveranciers doen veel meer dan het aanleveren van systemen, het zijn eerder partners waarmee informatie gedeeld moeten worden om systemen optimaal te laten functioneren. Bij het maken van afspraken over geheimhouding is het van belang om naast

het perspectief van nationale veiligheid ook het perspectief van de telecomoperators mee te nemen.

4.2.7 Doorlooptijd

Afspraken over een (maximale en minimale) doorlooptijd per processtap zijn centraal voor een voorspelbare procesgang. Korte doorlooptijden zorgen ervoor dat telecomoperators niet onnodig lang in onzekerheid verkeren. Aan de andere kant kan het ten koste gaan van de zorgvuldigheid. Concreet zouden afspraken over doorlooptijd kunnen betekenen dat als er een nieuwe dreiging uit stap A naar voren is gekomen, de beoordeling van de relevantie maximaal een bepaalde periode (X werkdagen) mag duren. De onderstaande box geeft een voorbeeld van de situatie in Denemarken.

Box 1. Planning van ad-hoc informatieverzoeken in Denemarken

Het is evident dat bij acute, nieuwe dreigingen er direct maatregelen getroffen dienen te worden. Als het gaat om ad-hoc screening zien we dat hier weinig duidelijkheid geschept kan worden over de frequentie van informatieverzoeken. Wel kan er op andere wijzen worden getracht meer duidelijkheid te scheppen. Zo is in Denemarken bekend om welke informatie het mogelijk zou gaan, en is bij wet vastgelegd dat operators minimaal 4 weken de tijd hebben om de gevraagde informatie op te leveren.

Deens Centrum voor Cyberveiligheid

Het Deense Center for Cyber Security (CFCS) kan een bevel uitvaardigen aan operators om schriftelijk informatie te verstrekken over essentiële onderdelen van de netwerken en diensten van de aanbieders of de werking daarvan. Mogelijk gevraagde informatie betreft: hardware, firmware en software, configuratie, typeaanduiding, serienummer, nummer en equivalent, informatie over netwerkarchitectuur en -ontwerp, eventuele leveranciers, inclusief serviceproviders, evenals de geografische locatie van providers en de hardware van relevante leveranciers, en exploitatie- en ondersteuningscentra.

Het CFCS is eveneens gemachtigd om een uiterste datum vast te stellen waarvoor de informatie dient te zijn aangeleverd, waarbij geldt dat operators minimaal vier weken de tijd moeten hebben om aan het verzoek te kunnen voldoen.

Naast de doorlooptijd van de processtappen, zou er ook aandacht moeten zijn voor de doorlooptijd voor het geval telecomoperators aanpassingen moeten doorvoeren. De termijn waarbinnen een systeem verwijderd moet worden heeft een doorslaggevend effect op de impact voor een telecomoperator. In het algemeen geldt dat kortere termijnen zullen leiden tot hogere risico's en hogere kosten: de telecomoperator heeft immers minder tijd en onderhandelingsmacht bij het aanschaffen van nieuwe systemen, of bijvoorbeeld om aan te sluiten op 'logische' vervangingsmomenten, bijvoorbeeld door te wachten op een nieuwe serie hardware met betere specificaties. De voorkeursoptie betreft het vooraf scheppen van duidelijkheid over de termijn waarop besluiten dienen te worden uitgevoerd. Gezien de grote verschillen tussen systemen, bedrijven en mogelijke dreigingen is het echter niet realistisch om hier vooraf zekerheid over te geven. Een meer realistische invulling is maatwerk: het inrichten van een proces waarbij gestreefd wordt naar een goede afweging tussen continuïteit en veiligheid. Er moet een realistische termijn worden bepaald die beide belangen dient. Gezien de complexiteit van dit vraagstuk moeten telecomoperators nauw betrokken worden bij het bepalen van de termijn en de gelegenheid krijgen om hun visie hierop te geven.

Frankrijk kiest voor de genoemde maatwerk aanpak, waarin per casus wordt beoordeeld binnen welke termijn aan voorwaarden dient te worden voldaan.

Box 2. Frankrijk kiest voor een case-by-case aanpak

Frankrijk zet sinds augustus 2019 in op een **autorisatiesysteem** waarbij toestemming van de premier vereist is **voorafgaand** aan implementatie van nieuwe hardware, software of diensten voor 5G-netwerken (of opvolgende generaties). In het geval van een afwijzing wordt er per casus bekeken binnen welke termijn aan de voorwaarden dient te worden voldaan. Op deze manier bestaat er de flexibiliteit voor de regering om op korte termijn resultaat te vereisen wanneer er een ernstig risico bestaat voor de nationale veiligheid of defensie. Anderzijds bestaat er ook de ruimte om de operator langer de tijd te geven, om zo te voorkomen dat de beschikbaarheid van het netwerk in het geding komt. Daar is ook nog een clause over opgenomen in de wet: *Wanneer een eventuele afwijzing de beschikbaarheid van het netwerk in gevaar brengt, dient de operator de Secretaris-Generaal van Defensie en Nationale Veiligheid hiervan onmiddellijk op de hoogte te stellen.* [35]

Een best practice uit het buitenland betreft het uitwerken van scenario's waarin de gevolgen van impactvolle beslissingen wordt benaderd. Per scenario (bijvoorbeeld direct apparatuur verwijderen, na vijf jaar apparatuur verwijderen, uitfasen tot einde levensduur) onderbouwen telecomoperators wat de consequenties zullen zijn in bedrijfseconomische termen alsmede voor de beschikbaarheid van het netwerk. Op basis van deze scenario's kan worden besloten welke termijn de voorkeur verdient, waarbij een afweging wordt gemaakt tussen (1) het risico voor de nationale veiligheid (2) de beschikbaarheid van de communicatie-infrastructuur en (3) de bedrijfseconomische impact voor de telecomoperators. Hiermee wordt niet alleen de absolute impact voor operators inzichtelijk, maar ook de verschillen in de mate waarin spelers gevolgen ondervinden van de maatregel.

4.2.8 Aanpassingen

Goed beleid is beleid dat zich kan aanpassen aan de ontwikkelingen in de maatschappij. Alleen zo kan duurzaam worden geanticipeerd op de toekomst. Aan de andere kant zorgt dit ook voor een spanning: Bij de voorgaande vijf stappen is immers zojuist beargumenteerd dat er juist zoveel mogelijk afspraken moeten worden vastgelegd, om zo te zorgen voor vertrouwen en voorspelbaarheid. De beste manier om deze tegengestelde belangen te verenigen is om bepaalde uitgangspunten vast te leggen waaronder het proces kan worden bijgesteld. Dit kan bijvoorbeeld gebonden zijn aan externe omgeving ("we passen het aan als de dreigingen sterk toenemen"), onderlinge consensus ("we passen het aan als iedereen het ermee eens is"), een bepaalde periode ("we gaan over vijf jaar evalueren") of een combinatie van deze aspecten.

4.3 Voorkomen van ongewenste investeringen

In de vorige paragraaf stond centraal hoe kan worden omgegaan met nieuwe dreigingen. Met het de §4.2 voorgestelde procesgang hebben wij in feite een kader geïntroduceerd om de ex-post maatregelen ordentelijk te organiseren. Er is uiteraard ook een andere, meer op de lange termijn gerichte, manier om te voorkomen dat systemen later moeten worden verwijderd: Het voorkomen van ongewenste investeringen. Dit betekent dat de overheid vooraf (ex-ante) aan de markt zou moeten communiceren wat de kaders van investeringen zijn.

In deze paragraaf gaan we in op vier manieren waarop hier vorm aan gegeven kan worden. We beginnen in §4.3.1 met de meest concrete variant waarbij de overheid nieuwe investeringen toetst. Daarna schetsen we kaders hoe de overheid meer concreet kan maken welke netwerkonderdelen (§4.3.2) en leveranciers (§4.3.3) (mogelijk) onderwerp van discussie zijn. Tot slot kijken we in §4.3.4 naar model waarin de overheid een meer holistische visie presenteert.

Een inherent nadeel van alle opties die genoemd worden is dat het dreigingsbeeld over de tijd kan veranderen. We kunnen nu wel investeringen (in)direct goedkeuren, maar er bestaat een reëel kans dat we hier over enkele jaren anders over denken. Dat moet er gekozen worden tussen twee kwaden: (1) De systemen in de netwerken laten en accepteren dat er een groot risico is of (2) de systemen uit de netwerken verwijderen.

4.3.1 Ex-ante toetsing van investeringen

Om te voorkomen dat een marktpartij de foute investeringen doet, zou de overheid bij het inkoopproces de investeringen kunnen toetsten. Dit kan bijvoorbeeld vorm krijgen doordat een marktpartij het aanbod van de leverancier bij een overheidsinstantie voorlegt. Deze partij kijkt of het aanbod voldoet aan de eisen en communiceert of deze investering toegestaan is. We zien dat dit model in een aantal landen wordt gehanteerd. In deze paragraaf kijken we dan ook sterk naar de ervaringen uit anderen landen.

We zien dat o.a. Denemarken, Estland, Frankrijk en Nieuw-Zeeland inzetten op een *ex ante* toetsings- of adviesprocedure, waarin hardware, software en diensten voorafgaand aan implementatie worden getoetst aan nationale veiligheidskaders. Hoewel operators bij een dergelijke aanpak wellicht minder vaak miljoeneninvesteringen hoeven terug te draaien, kent deze aanpak wel een belangrijk nadeel: in elk inkoopproces komt een administratieve last die voor vertraging zorgt in het inkoopproces. Daarbij geldt dat een dergelijke procedure niet op zichzelf staat:

- Ten eerste dient er altijd een mogelijkheid te bestaan voor ad-hoc besluitvorming om acute nieuwe dreigingen te kunnen mitigeren. De vraag is dus hoeveel zekerheid deze toetsing daadwerkelijk geeft.
- Ten tweede gaat een dergelijke aanpak in werking in een bestaande situatie, waar reeds is (voor)geïnvesteed in verschillende generaties apparatuur, leveranciersrelaties, waar reeds contracten gelden of onderhandelingen lopen. We zien dan ook dat een aantal landen worstelt met een overgangperiode, waarin de huidige invulling van het netwerk mogelijk door dezelfde toetsingsprocedure gaat (eventueel met minder zware condities) als de te implementeren wijzigingen.

In zowel Denemarken, Estland, Frankrijk als Nieuw-Zeeland wordt ingezet op het *vooraf* toetsen van (of in het geval van Denemarken adviseren over) investeringen van operators. In het geval van Denemarken vindt de advisering plaats zodra er een contract ligt met een leverancier. De beoordeling daarvan zou binnen tien dagen gereed moeten zijn. In een dergelijke korte tijd zal in de praktijk vooral worden gekeken naar contractvoorwaarden (denk aan: geen beheer uit risicolanden) en whitelists/blacklists (van leveranciers of landen per systeemtype). In Nieuw-Zeeland dient reeds in het beginstadium van onderhandelingen contact gezocht te worden met het Government Communications Security Bureau. In Estland en Frankrijk legt men de keuze van het moment waarop de voorgenomen investering getoetst wordt neer bij de operator zelf, zolang dit maar voorafgaand aan implementatie in het netwerk gebeurt. In Frankrijk wordt bovendien een zeer duidelijke frequentie aangeduid: elementen dienen bij introductie en hierna elke 8 jaar te worden gescreend.

Frankrijk verleent toestemming voor 8 jaar

Frankrijk zet sinds augustus 2019 in op een **autorisatiesysteem** toestemming van de premier vereist is **voorafgaand** aan implementatie van nieuwe hardware, software of diensten voor 5G-netwerken (of opvolgende generaties). Hier geldt dat er sprake is van een case-by-case aanpak operators doen een autorisatie-aanvraag, en per aanvraag wordt een dossier opgesteld waarin wel of geen toestemming wordt gegeven voor een periode van **acht jaar**. Daarna kan worden verlengd middels een verlengingsaanvraag die minimaal 2 maanden voor het verstrijken van de geldende toestemming moet worden ingediend.

In de tabel hieronder geven we een beknopt overzicht van de aanpak in de genoemde vier landen.

Tabel 1. Ex ante toetsing per land

Land	Moment van toetsing	Tijdpad	Conditie	Betrokken instantie(s)
Denemarken	Voorafgaand aan sluiten overeenkomst	Maximaal 10 werkdagen	Maatschappelijk belang	Centrum voor Cybersecurity
Estland	Voorafgaand aan implementatie	Maximaal 60 dagen (best case) of 120 dagen (bij negatief advies)	Nationale veiligheid	Consumentenbescherming en de Technische Toezichtautoriteit (coördinatie) Veiligheidsautoriteiten (besluit), CERT (besluit) Evt. interdepartementale raad Cybersecurity Council (besluit)
Frankrijk	Voorafgaand aan implementatie	Maximaal 2 maanden	Beveiligingsniveau van de apparaten, hun inzet en bedieningsmethoden die de exploitant voor ogen heeft en het feit dat de exploitant of zijn dienstverleners, onder meer door uitbesteding, onder controle staat of onderhevig is aan inmenging van een staat die geen lid is van de Europese Unie	Secretaris-generaal van Defensie en Nationale veiligheid (coördinatie) Premier (besluit)
Nieuw-Zeeland	Voorafgaan aan uitvraag in de markt	Intake veelal binnen drie werkdagen, maximaal 20 werkdagen	Netwerkbeveiligingsrisico's: waarschijnlijkheid dat het voorstel (of een deel ervan) zal leiden tot een compromis of aantasting van het openbare telecommunicatienetwerk en de aantasting van de vertrouwelijkheid, beschikbaarheid of integriteit van telecommunicatie via het netwerk en het potentiële effect daarvan op de levering van belangrijke diensten.	Government Communications Security Bureau

We zien vrij veel scepsis over de ex-ante optie. Primair raken argumenten aan de volgende drie aspecten, die een sterke samenhang kennen:

1. **Doorlooptijd van de toets:** Om een werkbaar proces te houden, moet de toets snel worden uitgevoerd. Het is echter niet realistisch om te veronderstellen dat de overheid binnen deze periode deze toets kan uitvoeren. Hier bovenop komt de vraag of het überhaupt mogelijk is om deze toets uit te voeren. Een deel van de kwetsbaarheden komt voort uit de wijze waarop systemen worden ingezet in organisaties en zijn geen inherente eigenschap van het systeem.
2. **Transparantie over gehanteerde condities.** In veel gevallen zijn condities waarop het besluit wordt gebaseerd apparatuur toe te staan (dan wel af te keuren) zeer summier benoemd. Deze 'nationale black box' is een bewuste keuze, zo kunnen dynamische condities worden gehanteerd, gebaseerd op de laatste inzichten rondom beveiliging en integriteit van netwerken. Bovendien wordt onderbouwing niet gedeeld wanneer deze betrekking heeft op geheime informatie. Desondanks is een gefundeerde onderbouwing noodzakelijk, met het oog op eventuele rechtszaken waarin het besluit wordt aangevochten.
3. **Administratieve impact.** De administratieve impact aan de kant van de operator en betrokken overheidsinstantie(s) is afhankelijk van de scope van de regelgeving (worden alle investeringsbeslissingen onder de loep genomen of zijn er uitzonderingen?), mate van detail in de informatieplicht aan de kant van de operator, de grondigheid van de analyse van deze informatie en het aantal betrokken instanties in de toetsing hiervan. De informatieplicht verschilt per land maar kent vaak een hoge mate van detail. De volgende tabel geeft hiervan een overzicht weer.

Tabel 2. *Gevraagde informatie over diensten en apparatuur in het telecommunicatienetwerk per land op hoofdlijnen*

Land	Gevraagde informatie ¹⁵
Frankrijk[35]	<ul style="list-style-type: none"> • Het object, de naam, versie of versies en technische kenmerken van het apparaat, vergezeld van de technische documentatie van het apparaat geleverd door de fabrikant; • Het beoogde gebruik van het apparaat binnen het radionetwerk van de aanvrager; • De gebruiksvoorwaarden van het apparaat, met vermelding van de activering of niet-activering van optionele functies ervan, de beschermingsvoorwaarden die zijn aangenomen voor de onderlinge verbindingen met andere netwerkelementen en niet-gespecialiseerde computersoftware, besturingssystemen en mogelijke virtualisatieoplossingen waarop de computerhosting van het apparaat en zijn gegevens is gebaseerd, de methoden om deze software te beveiligen, evenals de mogelijke hosting van het apparaat met andere apparaten op dezelfde IT-infrastructuur; • De bedrijfsomstandigheden van het apparaat, met specificatie van de configuratie-, supervisie- en onderhoudswerkzaamheden die kunnen worden uitgevoerd tijdens de werking of op de IT-hosting, evenals de onderaannemers die configuratie, supervisie of onderhoud aan het apparaat;
Estland [36]	<ul style="list-style-type: none"> • de naam van de hardware en software;

¹⁵ Gefragmenteerde informatie op basis van vertalingen van wetteksten. De genoemde informatieplicht is voorwaardelijk op basis van condities genoemd in diezelfde wet waaraan gerefereerd wordt. Mogelijk betreft dit overzicht een onderschatting omdat er - naast de genoemde wettelijke bepalingen - aanvullende informatieplichten bestaan die niet in deze wet staan vastgelegd.

Land	Gevraagde informatie ¹⁵
	<ul style="list-style-type: none"> • een bedrijf dat hardware en software heeft geproduceerd; • de functie van hardware en software in het communicatienetwerk; • de plaats van gebruik van hardware en software in het communicatienetwerk; • de datum van het begin en het einde van het gebruik van de hardware en software.
Denemarken	<p>Kennisgeving over essentiële onderdelen van de netwerken en diensten van de aanbieders of de werking daarvan.</p> <ol style="list-style-type: none"> 1) Welke kritieke netwerkcomponenten, systemen en tools, inclusief de werking daarvan, die de overeenkomst beoogt op te nemen. 2) De beoogde reikwijdte van de overeenkomst. 3) Mogelijke plaatsing van taken buiten Denemarken. 4) Alle leveranciers die naar verwachting bij de contractonderhandelingen zullen worden betrokken. 5) Algemeen tijdschema voor de onderhandelingen over de overeenkomst. 6) Beoogde duur van de overeenkomst.

Tot slot geldt dat ook bij ex-ante toetsen maatregelen kunnen doorwerken op investeringen in het bestaande netwerk, bijvoorbeeld omdat door besluiten de interoperabiliteit van generaties technologie in het netwerk wordt bemoeilijkt. In het volgend kader illustreren we dit.

Box 3. Interoperabiliteitsissues in Nieuw-Zeeland

Operators *Spark* en *2degrees* gebruiken beiden apparatuur van Huawei in het 3- en 4-G RAN netwerk. Het Nieuw-Zeelandse *Government Communications Security Bureau* blokkeerde in 2018 op grond van veiligheidsoverwegingen een voorstel van telecomoperator *Spark* om Huawei-apparatuur in het 5G-netwerk te gebruiken.[38]

Als de bezwaren van de GCSB standhouden, zullen beide bedrijven waarschijnlijk toegangsapparatuur van een andere leverancier moeten kopen wanneer ze hun RAN upgraden om 5G te leveren. *2degrees* moet mogelijk eveneens een deel van het core-netwerk vervangen: *CTO Mike Davies acknowledges that 2degrees might have had the option of reusing what could be described as the "core of the core" of its existing network – its Huawei-supplied packet-switching network – in the upgrade to 5G, but that may now also become impossible depending on the GCSB's stance.*[39]

In de VS is sprake van een situatie waarin bestaande apparatuur uit netwerken moet worden verwijderd. De onderstaande box illustreert hoe sterk onderdelen van het netwerk met elkaar samenhangen.

Box 4. Onzekerheid over de omvang van de nadeelcompensatie in de VS

De omvang van nadeelcompensatie is een centraal aspect in deze discussie, maar is niet eenvoudig om te bepalen. Dit komt vooral omdat systemen sterk verankerd zitten in allerlei delen van de organisatie en allerlei andere systemen. Daarnaast zijn er verborgen kosten bij vervanging van systemen. In de VS speelt op dit moment het vervangen van apparatuur van Huawei en ZTE in netwerken van kleine operators. Een vertegenwoordiger van een telecomoperator stelt dat: *"Despite having just \$500,000 of Huawei equipment, [I] estimate that buying new parts and hiring a contractor to replace the equipment could cost between \$1.2 million and \$1.5 million.* [33].

Ondanks bovengenoemde bezwaren biedt ex-ante toetsing duidelijkheid over het moment waarop elementen van netwerken worden getoetst, hoe lang deze toets gaat duren, en wie de toets uit zal voeren. Besluiten worden expliciet gemaakt, naast afkeuring is er ook goedkeuring, hetgeen perspectief biedt voor andere operators. Hoewel er weinig duidelijkheid bestaat over de condities waarover wordt besloten trachten landen dit af te vangen door frequent afstemming te zoeken met telecomoperators. Op deze manier is op voorhand op hoofdlijnen duidelijk welke elementen (leveranciers) mogelijk discussie opwerpen.

4.3.2 Realiseren van duidelijkheid over welke onderdelen in aanmerking kunnen komen om verwijderd te moeten worden

Om telecomoperators meer duidelijkheid te geven, is het een optie om aan te geven welke delen van het netwerk in aanmerking kunnen komen om verwijderd te moeten worden. Immers, niet elk deel van het netwerk van een telecomoperator is even gevoelig voor dreigingen. Indien duidelijk is welke onderdelen "*niet onder een vergrootglas liggen*", dan heeft de telecomoperator meer investeringszekerheid op deze gebieden. Wederom kijken we naar de ervaringen van verschillende andere landen op dit gebied.

We zien dat landen verschillend beleid voeren als het gaat om de scope van de risicoanalyses. In Denemarken zijn zowel vaste als mobiele netwerken in de scope van de analyse. In Frankrijk gaat het expliciet om mobiele netwerken: 5G en volgende generaties. Estland moet nog besluiten wat de scope gaat worden, de regering pleit voor een brede scope die zowel mobiele als vaste netwerken omvat, de telecomoperators lobbyen voor een smallere scope enkel mobiele 5G netwerken zouden wat hen betreft moeten worden getoetst. In het Verenigd Koninkrijk geeft het National Cyber Security Centre een advies toegespitst op het type netwerk (alle netwerken, 5G-netwerken, 4G-netwerken). In de Europese risicoanalyse wordt voor verschillende netwerkonderdelen aangegeven hoe kritiek ze zijn.[60]

Naast de afbakening naar type netwerken, kan ook vooraf duidelijkheid worden verschaft over de onderdelen waarop analyse betrekking heeft. Frankrijk en het Verenigd Koninkrijk gaan hier erg ver in en benoemen in detail de functionele onderdelen van het netwerk. Frankrijk duidt nadrukkelijk aan op welke onderdelen de analyse geen betrekking heeft, zoals passieve elementen in het netwerk en corrigerende software-updates. Ook Nieuw-Zeeland benoemt een aantal uitzonderingen.

Box 5. Uitzonderingen notificatiesysteem Nieuw-Zeeland

In Nieuw-Zeeland is een notificatiesysteem al sinds 2013 operationeel. Dit systeem, vastgelegd in de **Telecommunications Interception Capability and Security Act (TICSA)**, stelt dat operators het GCSB op de hoogte stellen van bepaalde voorgestelde besluiten, maatregelen of wijzigingen in hun netwerk. Omdat het systeem al een aantal jaren meedraait, zijn bepaalde wijzigingen structureel bevonden geen significante netwerkbeveiligingsrisico's met zich mee te brengen. Dit betreffen de volgende wijzigingen:

Exemption I. Routine changes to networks

A routine decision, course of action, or change is a decision, course of action, or change that will not: (a) alter the architecture of the network; or change the effective ownership, control, oversight, or supervision of any equipment, system, or service within an area of specified security interest; or change the overall

capabilities or functions of the equipment, systems or services, or introduce new functionality.

Exemption 2. Standard builds and bulk changes

Exemption 3. Emergency changes.¹⁶

Een te nauwe scope van netwerkonderdelen heeft als probleem dat er veiligheidsrisico's kunnen bestaan die de analyse over het hoofd ziet. Een te brede scope leidt ertoe dat de markt onnodig of misschien wel onevenredig belast wordt ten aanzien van spelers in aanpalende markten. Dit lichten we toe aan de hand van een voorbeeld in Denemarken.

Box 6. De wait-and-see strategy in Denemarken

De strategie van Denemarken wordt ook wel aangemerkt als een wait-and-see strategy. De wetgeving borgt interactie tussen telecomoperators en overheid om zo risico's te beoordelen en wanneer het maatschappelijk belang dit rechtvaardigt, maatregelen te nemen. Volgens de wet zijn telecommunicatiebedrijven in Denemarken verplicht, alvorens met een leverancier een contract te sluiten, met het Centre for Cyber Security te bespreken welke risico's ontstaan door een specifieke technologie en leverancier en wat er kan worden gedaan om met deze risico's om te gaan. CFCS kan hier wijzen op eventuele veiligheidsproblemen die de telecomoperator moet betrekken bij de onderhandelingen en contracten met de potentiële apparatuur en/of operationele leverancier.

De genoemde verplichting geldt voor **Critical network components, systems and tools:** *operationele ondersteuningssystemen, netwerkbeheersystemen en bedrijfsondersteunende systemen die kunnen worden gebruikt voor het lezen, wijzigen van inhoud of directe gegevens met betrekking tot eindgebruikers, evenals gebruikte hardware, firmware en software in of in verband met core netwerken in mobiele netwerken, vaste lijnen en internet, of in centrale routers en servers in de backbone-netwerken of in controle-eenheden die worden gebruikt voor de besturing van de radionetwerken van de mobiele netwerken.*

De industrie is van mening dat deze laatste definitie zo breed is geschreven dat deze in de praktijk slaat op alle delen van de netwerken, systemen en diensten van providers, terwijl zou graag zouden zien dat deze verplichting alleen betrekking zou hebben op kritieke netwerkcomponenten, systemen en tools die rechtstreeks worden gebruikt voor de netwerkwerving van elektronische communicatienetwerken of -diensten.[37] Dit omdat er eisen worden gesteld aan diensten (zoals spraaktelefonie, lineaire tv, sms / mms) die concurreren met aanbieders als Google, Facebook en Microsoft die niet vallen onder de 'essential business provider' definitie.

Hoewel de definitie niet is aangepast is er wel een conditie ingebouwd in het notificatieproces in Denemarken, die ertoe leidt dat niet alle conceptovereenkomsten met leveranciers onder besluitvorming onderhevig staan (en dus mogelijk kunnen worden afgekeurd). Operators moeten alle voornemens notificeren, maar alleen op basis van een concreet bevel van de CFCS zijn besluiten aan adviesvorming onderhevig.

Bij het geven van duidelijkheid vooraf, in dit geval over de onderdelen van het netwerk, moet er gewaakt worden dat dit geen schijnzekerheid biedt. Er is immers sprake van een dynamisch speelveld. Als morgen toch een ander deel van de systemen een risico blijken te bevatten dan staan we voor een dilemma. We kunnen het lastig simpelweg negeren en het

¹⁶ Volledige beschrijving is te vinden op de website van de Nationale NCSC

risico accepteren. Maar als wij gaan schuiven met de afbakening dan hebben we markt alleen maar meer onduidelijkheid gegeven. Want de kaders die gegeven worden, worden direct losgelaten bij een probleem.

4.3.3 Realiseren van duidelijkheid over welke leveranciers (niet) toegestaan zijn

Om telecomoperators meer duidelijkheid te geven, is het een optie om vooraf aan te geven welke leveranciers niet toegestaan zijn. Er zou vooraf lijst kunnen worden aangedragen met leveranciers die als ongeschikt worden gezien. Uiteraard kan dit gecombineerd worden met de beleidsoptie uit de vorige paragraaf: bepaalde leveranciers die ongeschikt zijn voor bepaalde delen van het netwerk. Wederom kijken we naar de ervaringen van verschillende andere landen op dit gebied.

Het Verenigd Koninkrijk is één van de landen die expliciet de keuze heeft gemaakt om een leverancier (namelijk Huawei) aan te duiden als risicovolle leverancier. Omdat op voorhand duidelijk is welke mogelijke impact deze beslissing heeft, kan een concrete termijn worden bepaald waarbinnen apparatuur redelijkerwijs kan worden verwijderd. In het geval van het Verenigd Koninkrijk wordt ingezet op drie jaar om de inzet van Huawei te verminderen tot aanbevolen richtlijnen.

Box 7. Verenigd Koninkrijk zet in op drie jaar om inzet Huawei te verminderen

Primaire inzet UK is het vooraf vastleggen van eisen in een **veiligheidskader**: de Telecom Security Requirements (TSR). Het kader wordt momenteel nog opgesteld. De markt bevindt zich echter momenteel in een cruciale fase (o.a. uitrol 5G) en heeft behoefte aan advies. Daarom heeft het (Britse) National Cyber Security Centre (NCSC) ter overbrugging van de periode een niet-bindend technisch advies gepubliceerd als het gaat om de het gebruik van apparatuur van risicovolle leveranciers (high risk vendors **HRVs**). [40] De netwerkelementen waarvoor geen High Risk Vendors (HRV) gebruikt mogen worden, worden expliciet benoemd.

De Britse Overheid heeft ingestemd om Huawei aan te duiden als risicovolle leverancier. Het NCSC adviseert om het gebruik diensten en apparatuur van Huawei te verminderen tot de aanbevolen richtlijnen, zo snel als praktisch mogelijk is. Er wordt ervan uit gegaan dat operators dit binnen **drie jaar** kunnen realiseren.

De netwerkelementen waarvoor geen High Risk Vendors (HRV) gebruikt mogen worden, worden expliciet benoemd. Hierbij wordt onderscheid gemaakt naar alle netwerken, 4G en 5G netwerken. Voor access networks geldt het advies om het gebruik van een HRV te limiteren, hierbij wordt een harde bovengrens afgegeven voor effectief risicomanagement van cyberveiligheid: maximaal 35% van de netwerkapparatuur zou in handen mogen zijn van HRVs en deze apparatuur mag niet gebruikt worden in de buurt van gebieden die relevant zijn voor de nationale veiligheid. Er zijn echter discussies of deze 35% toch niet terug moet naar 0%. [45] Daarmee wordt het heel snel praktisch onmogelijk om een HRV te gebruiken in RAN. Dit omdat er in de praktijk de voorkeur bestaat om één leverancier in te zetten per regio omdat er problemen optreden bij transitie tussen leveranciers.¹⁷

¹⁷ LTE-5G tussen verschillende leveranciers werkt lang niet altijd of slechts met beperkte functionaliteit; over tijd zal dat wel beter worden maar traditioneel waren er in RAN altijd functionele beperkingen in wat mogelijk is op grenzen.

Met het geheel of deels uitsluiten van bepaalde leveranciers wordt direct duidelijk welke leveranciers niet gewenst zijn. Het is hiermee een heel krachtig instrument. Een nadeel van deze methode is dat het een grof instrument is. Ook komt de vraag naar voren in welke mate systemen van deze leveranciers wel in andere delen van de markt gebruikt mogen worden. Daarnaast is het vraag in welke mate dit een statische lijst kan zijn. Zo speelt op dit moment de mogelijkheid dat Nokia wordt overgenomen door een andere partij. [46] Het argument over schijnzekerheid waar we de vorige paragraaf mee afsloten, is ook hier relevant. Tot slot kan het uitsluiten van bepaalde leveranciers flinke politieke en diplomatieke problemen veroorzaken. Hiermee wordt immers heel duidelijk naar één land gewezen waarmee Nederland relaties onderhoudt.

4.3.4 Ontwikkelen van integrale visie zodat telecomoperators zelf een kader hebben

Bij dit laatste onderdeel ligt de focus op het ontwikkelen van een Rijksbrede visie op digitalisering in het algemeen en telecommunicatie in het bijzonder. Dit biedt telecomoperators kaders bij het maken van investeringsbeslissingen, maar kan ook bij andere vraagstukken worden gehanteerd. Op dit moment lijkt de Rijksoverheid beperkt een visie over digitalisering in 2030 te communiceren. Waar moet Nederland in 2030 staan op het gebied van digitalisering? Wat zijn onze kernwaarden? Er spelen vragen als:

- Welk kennis willen we als Nederland wel en niet in huis hebben? In hoeverre is afhankelijkheid van kennis uit het buitenland gewenst?
- Hoe gaan we om met het gegeven dat wij niet autonoom kunnen zijn als het gaat om (telecom)systemen?
- Hoe wegen we privacy, veiligheid en economische belangen af?
- Gaan we inzetten op een open (source) ecosysteem of juist op een markt met sterke concurrerende gesloten ecosystemen?
- Hoe trekken we samen in Europees verband op?

De afgelopen jaren is er in Nederland steeds meer een Rijksbrede visie ontwikkeld op digitalisering. De Nederlandse Digitaliseringsstrategie uit 2018 is hier wellicht het beste voorbeeld van. Hier wordt een breed scala aan onderwerpen behandeld van economische kansen, onderzoek, marktwerking tot weerbaarheid en ethiek. Hiermee worden er kaders geboden voor allerlei andere vormen van beleid. We zien dan ook dat op een groot aantal andere specifieke onderwerpen ook digitale agenda's worden ontworpen.

Vanuit de gesprekken is naar voren gekomen dat er wellicht behoefte is aan een publiek-privaat kennisinstituut dat gericht is op de ontwikkeling van een visie op digitalisering. Deze partij kan een *sparring partner* zijn voor zowel publieke als private partijen. Daardoor kan er breder beleid worden gevoerd. Dit kan bijvoorbeeld ook betrekking hebben op inkoopprocessen van de overheid. Er bestaat een kans dat er vanuit verschillende departementen vraag is naar een dergelijk orgaan. Een vraagstuk is echter in welke mate een dergelijk kennisinstituut niet al bestaat of in welke mate de verschillende onderdelen hiervan al elders belegd zijn. Er is in Nederland een breed scala aan (publieke en/of private) organisaties die zich met deze vraagstukken bezighouden, denk aan TNO, ECP.nl, Rathenau, NLdigital, Waag Society, en verschillende onderdelen van Ministeries, uitvoeringsorganen en decentrale overheden.

Een andere discussie die meer aan deze specifieke problematiek raakt heeft betrekking op het achterliggende doel van het Besluit. Is het gericht op nationale veiligheid of liggen er geopolitieke overwegingen aan ten grondslag? Of spelen beide aspecten een rol? En zo ja: in welke mate? Voor de partijen die investeringen doen is het relevant om te weten vanuit welk perspectief het Besluit zal worden ingezet. Hoewel beide aspecten tot op zekere hoogte leiden tot dezelfde uitkomsten, zullen er ook verschillen zijn in de concrete impact.

4.4 Ontwikkelen van instrumenten om marktdynamiek te verbeteren

In de gesprekken die wij over dit onderwerp voerden en in de beschikbare literatuur zijn ook andere voorbeelden naar voren gekomen die de kwetsbaarheden in de netwerken kunnen verminderen. Hierbij ligt focus veel meer op het wijzingen van onderliggende structuren in de markt (zowel technisch als niet-technisch) waardoor de dreigingen zich minder snel voordoen of een kleinere impact hebben: niet de spelers, maar het spel wordt aanpakt. Een dergelijke aanpak valt buiten de primaire scope van dit onderzoek waarbij de focus ligt op de structurele aanpak. Toch zullen wij deze elementen ter inspiratie kort bespreken.

4.4.1 Open standaarden

De laatste jaren wordt steeds meer ingezet op open oplossingen voor het RAN en de Core (Open EPC en Open 5G Core) waarbij hard- en software ontkoppeld worden. Voor Open RAN zijn op dit moment drie organisaties actief: OpenRAN Alliance, Telecom Infra Project en Open RAN Policy Coalition. Met open standaarden kunnen twee vliegen in een klap worden geslagen. Ten eerste wordt het breed mogelijk om inzicht te krijgen in de software die gebruikt wordt in telecommunicatienetwerken. Er ontstaat ontkoppeling tussen hardware en software - de 'black boxes' veranderen in systemen gebaseerd op 'white box' (generieke en daardoor uitwisselbare) hardware, waarop open software draait. Ten tweede zorgt het ervoor dat er veel minder afhankelijkheid komt van een handvol leveranciers. In dit model is het mogelijk om verschillende soorten hard- en software te combineren. Hierdoor wordt de marktdynamiek verbeterd.

Er wordt steeds meer ingezet op dit ontwikkelpad. Vodafone heeft reeds aangegeven dat zij OpenRAN in Europa gaan uitrollen op 100.000 opstelpunten. [48] Rakuten, een Japanse e-commerce partij, heeft een volledig netwerk uitgerold in Japan op basis van virtualisatie.[49] Recent hebben Rakuten en NEC aangegeven OpenRAN 5G apparatuur te zullen gaan produceren.[50] The Economist argumenteert tot slot dat :*"Open standards, not sanctions, are America's best weapon against Huawei"*. [51]

Het voornaamste nadeel van deze ontwikkeling is dat de performance van de systemen nog niet op het niveau is van de traditionele leveranciers. Dit wordt deels bepaald doordat een afstemming van specifieke hardware en software tot een betere performance kunnen leiden.

In een aantal gevallen heeft *open* niet alleen betrekking op de ontkoppeling van hard- en software maar ook op de broncode (open source). Een belangrijk argument dat spreekt voor inzet van open source is dat de broncode kan worden geanalyseerd op veiligheidsrisico's alvorens deze in gebruik wordt genomen. In een ideaal scenario zou dat betekenen dat er geen enkel risico meer aanwezig is in de code, en de systemen perfect veilig zijn: *"given enough eyeballs, all bugs are shallow"* is een bekend adagium in de open sourcewereld.[52] De realiteit is echter dat zelfs in veelgebruikte en geanalyseerde open sourcecode, zoals bijvoorbeeld de Linuxkernel of de OpenSSL-bibliotheek die wordt gebruikt voor beveiliging, nog regelmatig nieuwe zwakheden worden gevonden. Daarnaast zijn er aanwijzingen dat er in open sourcecode achterdeurtjes worden gebouwd, en is het niet zonder meer aan te nemen dat deze altijd zullen worden opgemerkt, zie ter illustratie het "Underhanded C Contest"[53].

Een vraagteken is tot slot in hoeverre Nederland in staat is om deze ontwikkelingen aan te jagen. Ook hier geldt dat samenwerking (op Europees niveau of breder) wenselijk is.

4.4.2 Multi-vendorstrategie

Een ander alternatief dat ook in de Europese Toolbox genoemd is, is het inzetten op een multi-vendor strategie. Hierbij neemt de operator dezelfde systemen van meerdere leveranciers af. Indien een multi-vendorstrategie goed wordt ingezet kan deze ertoe leiden dat een netwerk minder kwetsbaar is: bij een vervanging hoeft slechts een deel van de systemen te worden vervangen. Bovendien zijn migraties tussen leveranciers eenvoudiger: deze is al aanwezig in het netwerk, en zou bij het wegvallen van de systemen van de andere leverancier eenvoudiger moeten kunnen worden opgeschaald.

Aan de andere kant is het de vraag in welke mate de kleine marktomvang in Nederland er niet toe gaat leiden dat er te veel inefficiënties in het netwerk komen. In het licht van de ontwikkeling van open standaarden en systemen is een multi-vendorstrategie waarschijnlijk makkelijker te implementeren, omdat onderdelen meer uitwisselbaar worden. In Nederland nemen de operators op dit moment van meerdere leveranciers systemen af (in veel gevallen vanwege legacy; zo draaien bijvoorbeeld oude 2G-systemen van een leverancier nog door terwijl er op enig moment 3G- en 4G- systemen zijn bijgeplaatst van andere leveranciers). In grotere landen (zoals Duitsland) zien we dat operators met name in het RAN kiezen voor multi-vendor. Vanwege de standaardisatie (in 3GPP) van de interfaces tussen RAN en core is dit relatief eenvoudig te realiseren. Onder de landen waar een multi-vendorstrategie wordt verplicht zien we het Verenigd Koninkrijk en Qatar.

4.4.3 Niet-technologische mitigatiestrategieën

De hiervoor gepresenteerde structurele aanpak en procesgang kent een sterk technologische focus als het op de mitigatiestrategieën aankomt: het weren van bepaalde technologieleveranciers, het vervangen van ongewenste technologiecomponenten, de selectiestrategie van technologiecomponenten, et cetera. Als wij de aanpak van andere landen bestuderen, dan zien wij hier ook ruimte voor niet-technologische mitigatiestrategieën (m.n. aan de kant van de operators). Denk hierbij aan de verplichte aanwezigheid van en rapportage over werkprocessen veiligheidsrisico's (*risk monitoring & control*). Ook striktere security clauses in de contracten met leveranciers vallen onder deze categorie van oplossingen. Dergelijke organisatorische maatregelen kunnen goed (en in sommige gevallen zelfs beter) bijdragen aan de beheersing van het (gepercipieerde) veiligheidsrisico.

5 Conclusies

De onderzoeksvraag van dit rapport luidde: *"Hoe kan aan Nederlandse telecomoperators meer investeringszekerheid worden geboden in de vormgeving van de structurele aanpak?"*

De structurele aanpak kan Nederlandse telecomoperators meer investeringszekerheid bieden. Drie pijlers zijn hiervoor van belang:

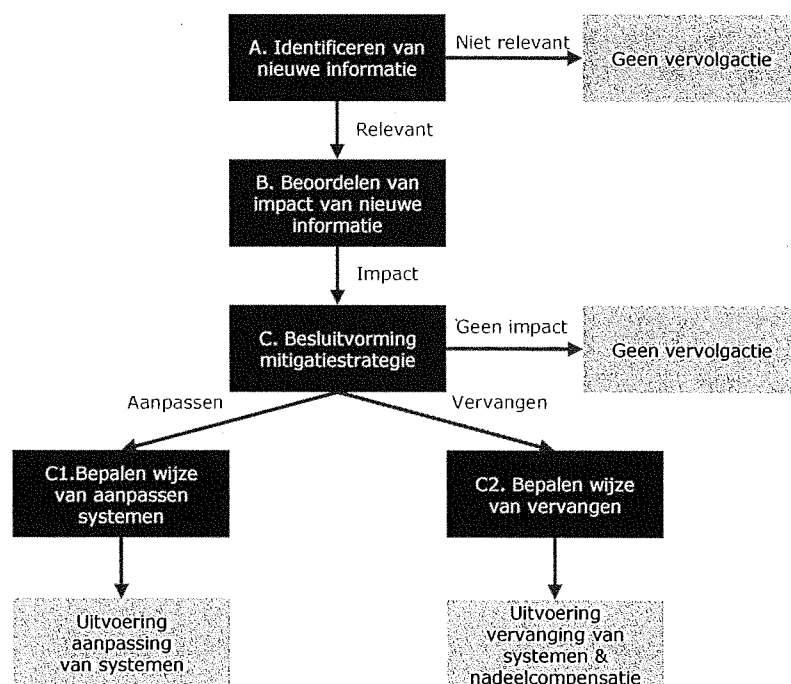
- Er moet een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid worden gevonden. Beide aspecten zijn essentieel voor onze maatschappij. Overheden moeten accepteren dat volledige flexibiliteit niet mogelijk is en dat bedrijven investeringszekerheid nodig hebben. Bedrijven moeten accepteren dat volledige investeringszekerheid niet mogelijk is om digitale dreigingen het hoofd te bieden. Om het belang van investeringszekerheid een plek te geven in de structurele aanpak, wordt voorgesteld de huidige doelstelling te verbreden door naast nationale veiligheid ook investeringszekerheid daar in op te nemen.
- Vanuit het perspectief van meer investeringszekerheid zal moeten worden gezien hoe onderstaande tien voorwaarden in de verdere invulling van de structurele aanpak kunnen worden meegenomen:
 1. Omgeving van vertrouwen tussen samenwerkende partijen. Er moet zeer vertrouwelijke informatie tussen telecomoperators en overheid worden uitgewisseld en partijen gaan een langdurige samenwerkingsrelatie aan. Het kunnen werken in een omgeving waarin partijen elkaar vertrouwen, is daartoe essentieel.
 2. Overheidsbrede, interdepartementale insteek. De overheid is een veelkoppige entiteit met verschillende belangen. Voor eenduidige communicatie richting telecomoperators is interne afstemming en met één mond spreken door de overheid van belang.
 3. Passend binnen internationale context. Twee van de drie grote telecomoperators zijn (onderdeel van) mondiale spelers. Ons beleid zou niet te veel moeten afwijken van beleid in andere (EU)landen om te voorkomen dat ons investeringsklimaat zwak wordt.
 4. Stimuleren van een competitief concurrentiespeelveld. Concurrentie tussen telecomoperators zorgt voor uitstekende netwerken tegen acceptabele kosten. Een goede marktdynamiek waarin telecomoperators durven te investeren moet behouden blijven.
 5. Leren en verbeteren van beleid. Na enige tijd moet het huidige beleid geëvalueerd worden en geleerd worden van de opgedane ervaringen.
 6. Transparant proces. Vooraf moet het voor de telecom operators duidelijk zijn hoe de procesgang in de structurele aanpak zal zijn. Welke stappen worden doorlopen, wie heeft welke rol en verantwoordelijkheid en hoe ziet de besluitvorming eruit?
 7. Voorspelbaar proces. Naast dat het proces van de structurele aanpak transparant moet zijn, moet het ook zo veel mogelijk voorspelbaar zijn. Het vooraf kunnen inschatten van risico's is essentieel voor telecom operators. Objectieverbaarheid is een centraal element. Ook het op basis van een kader kunnen inschatten van het recht op nadeelcompensatie kan bijdragen aan een voorspelbaar proces.
 8. Non-discriminatoire proces. Er mag geen onnodig onderscheid worden gemaakt tussen partijen.

9. Begrijpelijk proces. Telecom operators moeten begrijpen waarom de analyses en besluitvorming op een bepaalde manier zijn ingericht.

10. Proces met voldoende rechtsbescherming. De mogelijkheid om bezwaar te maken tegen besluiten van de overheid door deze te laten toetsen door een rechter, is voor telecomoperators een cruciaal recht. Hiertoe willen telecomoperators gerubriceerde informatie kunnen delen met hun advocaten.

- Er moet transparantie komen over hoe de structurele aanpak zich verhoudt tot bestaande gremia en structuren. De structurele aanpak wordt ontwikkeld binnen een context van bestaande institutionele kaders met gedefinieerde rollen en verantwoordelijkheden en gremia waar publiekprivaat informatie wordt uitgewisseld. Wat wordt waar behandeld en wat betekent dit voor de verantwoordelijkheden en rollen van de diverse betrokken partijen?

Bij het verder vormgeven van de structurele aanpak vorm wordt aanbevolen aan de bovenstaande tien voorwaarden tegemoet te komen via heldere procesafspraken tussen overheid en telecomoperators. Dit draagt bij aan transparantie, voorspelbaarheid en een omgeving van vertrouwen. Dit is extra van belang omdat overheid en telecomoperators van elkaar afhankelijk zijn in de structurele aanpak om zinvolle uitkomsten te verkrijgen. Er zijn verschillende manieren om de aanpak vorm te geven. Aansluitend bij bestaande plannen lijkt de onderstaande afbeelding logisch.



In deze aanpak zijn er vijf stappen. Voor elk van deze stappen moet een aantal aspecten worden uitgewerkt:

1. Wat is het afwegingskader waarop getoetst wordt? Voor elke stap moet een inhoudelijk afwegingskader worden gemaakt. Zo wordt duidelijk op basis waarvan besluiten genomen worden. Centraal staat een gezond evenwicht tussen flexibiliteit van beleid en investeringszekerheid.
2. Welke partijen zijn (in welke rol) betrokken bij deze stap? Voor elke stap zal moeten worden bepaald welke partijen in welke rol betrokken zijn.

3. Hoe worden besluiten genomen en hoe kan bezwaar worden gemaakt? Voor elke stap moet duidelijk zijn op welke wijze besluitvorming plaatsvindt. Dit is essentieel voor een transparant proces. Vooraf moet bepaald worden wat de routes zijn als er geen consensus is. Zowel een onafhankelijke toetsing als een formeel juridisch traject zijn opties.
4. Hoe wordt omgegaan met geheimhouding? Het is evident dat bepaalde informatie over dreigingen, de kwetsbaarheden van netwerken en concurrentiegevoelige gegevens niet openbaar worden. Aan de andere kant is de beschikbaarheid van bepaalde informatie noodzakelijk voor een objectieve toetsing, de uitvoering van besluiten, het maken van bezwaar en onderling vertrouwen tussen partijen. Er moet een evenwicht worden gezocht, maar er moet vooral duidelijkheid zijn.
5. Wat is de doorlooptijd van een stap? Afspraken over de doorlooptijd per processtap zijn centraal voor een voorspelbare procesgang. Korte doorlooptijden zorgen ervoor dat telecomoperators niet onnodig lang in onzekerheid verkeren, maar dit kan ook ten koste gaan van de zorgvuldigheid.
6. (Hoe) kunnen deze bovenstaande afspraken veranderen? Goed beleid past zich aan aan de ontwikkelingen in de maatschappij. Echter, beleid dat wijzigt zorgt ook voor onzekerheid. Vooraf kan worden afgesproken wanneer het beleid geëvalueerd en aangepast kan worden.

Naast -of wellicht binnen- de structurele aanpak zijn er nog andere beleidsinstrumenten die te overwegen zijn. Het voorkomen van ongewenste investeringen is hierin een belangrijk element. Hieronder wordt een aantal opties genoemd. Echter voor alle opties geldt dat er geen absolute zekerheid door de overheid kan worden geboden. Mochten er over enkele jaren nieuwe grote dreigingen ontstaan, dan zal toch opgetreden moeten worden.

- Er kan bij het inkoopproces een toets van de investeringen plaatsvinden.
- Er kan vooraf worden aangegeven welke onderdelen van het netwerk zo gevoelig zijn dat verwijdering van systemen kan spelen.
- Er kan worden aangegeven welke leveranciers (niet) toegestaan zijn.
- Er kan een integrale visie op ICT worden ontwikkeld zodat telecomoperators zelf een kader hebben om investeringen aan te toetsen.

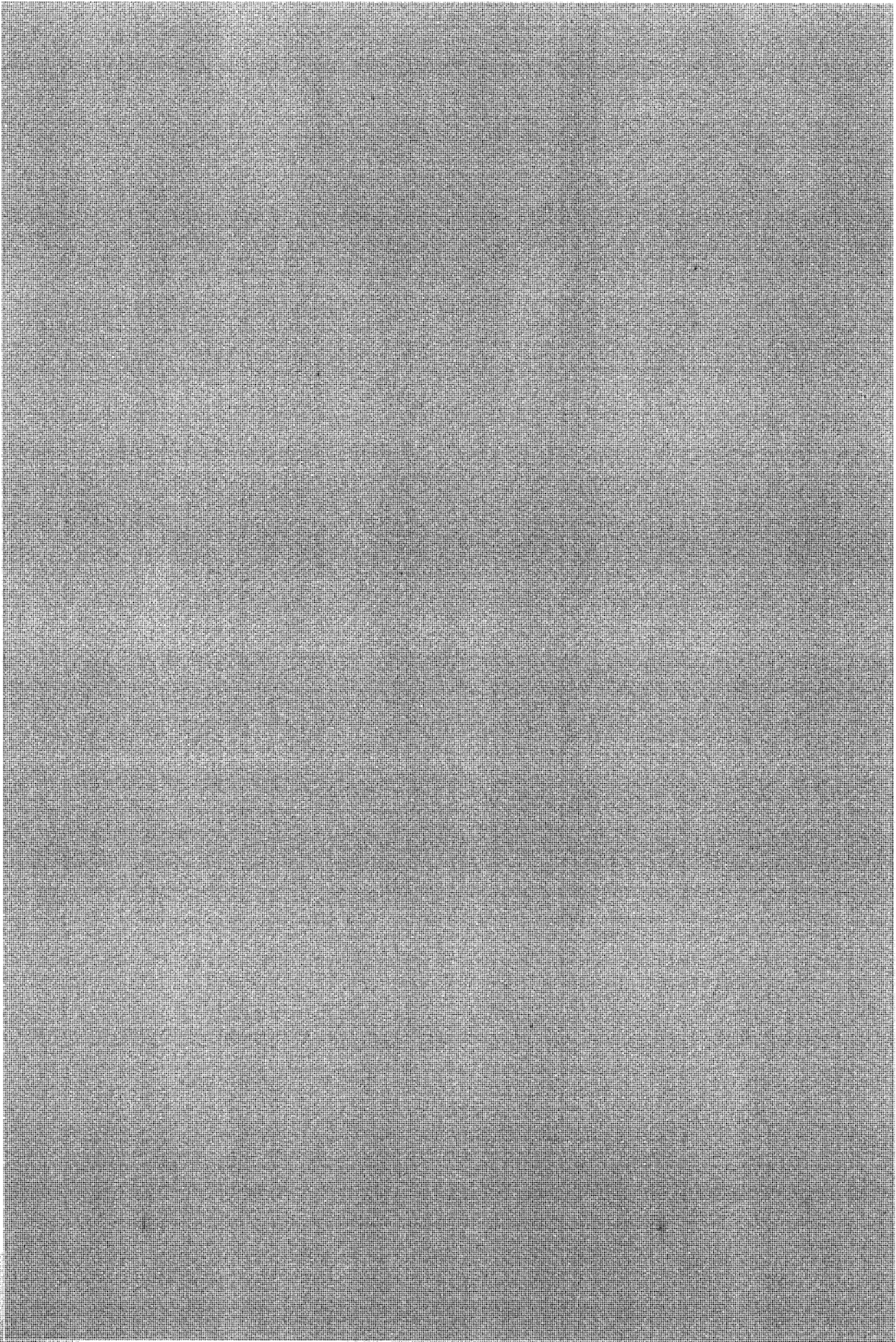
Een ander spoor voor beleid draait op het verbeteren van de marktdynamiek. De ontwikkeling van open standaarden voor netwerkkapparatuur kan zorgen voor meer keuze in leveranciers. Er kan overwogen worden om dit te steunen. Ook het stimuleren van een strategie waarbij operators meer dan één leverancier per netwerkonderdeel gebruiken (multi-vendor) kan interessant zijn om kwetsbaarheden te verminderen. De vraag is echter of de beperkte schaal in Nederland geen te grote beperking is.

Referenties

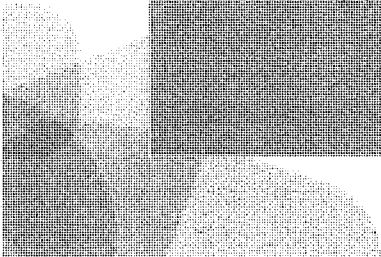
- [1] *Besluit veiligheid en integriteit telecommunicatie*. Zie wetten.overheid.nl
- [2] CBS (2015) *ICT and Economic growth*. Zie CBS.nl
- [3] Dialogic (2016). *De impact van ICT op de Nederlandse economie*. Zie dialogic.nl
- [4] OECD (2011) *Strategic Transport Infrastructure Needs to 2030 – Main Findings* [oecd.org]. Hierin wordt verwezen naar de niet-publieke OECD (2006) *Infrastructure to 2030 - telecom, land transport, water and electricity* [oecd.org]
- [5] EC (2019). *Handbook on improving the Investment Climate through EU action. Implementation of Pillar 3 in the integrated approach of the External Investment Plan* [ec.europa.eu]
- [6] De Soto (2003). *The Mystery of Capital. Why Capitalism Triumphs in the West and Fails Everywhere Else*. ISBN 9780465016150.
- [7] Dagblad van het Noorden voor Google bij datacenter in Eemshaven; rechter legt straffen op. Zie [dvh.nl]
- [8] WHO (2003) TRIPS, Pharmaceutical Patents and Access to Essential Medicines: Seattle, Doha and Beyond. Zie [who.int]
- [9] Acemoglu, Johnson & Robinson (2005). *Institutions as a fundamental cause of long-run growth*. In: *Handbook of Economic Growth, Volume 1A*. Edited by Philippe Aghion and Steven N. Durlauf. Zie: economics.mit.edu
- [10] Gulen, Huseyin & Ion Mihai (2015) *Policy Uncertainty and Corporate Investment*. The Review of Financial Studies, Volume 29, Issue 3, March 2016, Pages 523–564. Zie DOI.
- [11] World Bank Group (2020). *Doing business 2020. Comparing Business Regulation in 190 Economies*. [worldbank.org]
- [12] Dell'Oro Group (2019). *The Telecom Equipment Market 2019*. Zie delloro.com
- [13] Financial Times (2020). China Mobile picks Huawei and ZTE to build its 5G network. Zie ft.com
- [14] Global Data (2019). *Competitive Landscape Assessment (CLA) of the 5G Radio Access Network (RAN) infrastructure*. Zie globaldata.com
- [15] The Wall Street Journal (2020) *Huawei Workers Return After Coronavirus, But CEO Sees Financial Hit*. zie wsj.com
- [16] Technical University of Berlin & IPLytics GmbH (2020) *5G patent study 2020*. Zie iplytics.com.
- [17] Ferguson P.R. (1988) *The Structure-Conduct-Performance Paradigm*. In: *Industrial Economics: Issues and Perspectives*. Palgrave, London. Zie springer.com
- [18] ACM (2020) *Geregistreerde telecom- en postbedrijven*. Zie ACM.nl
- [19] AD (2019). *Nederlandse mobiele netwerken beste en snelste van de wereld*. Zie AD.nl.
- [20] Cable.co.uk (2018). *Worldwide mobile data pricing: The cost of 1GB of mobile data in 230 countries*. Zie: Cable.co.uk.
- [21] KPN (2020) *KPN Integrated Annual Report 2019* Zie KPN.com
- [22] VodafoneZiggo (2020). *VodafoneZiggo boekt goede resultaten in 2019*. Zie vodafoneziggo.nl
- [23] T-Mobile (2019) *T-Mobile nummer twee in mobiele markt*. Zie T-Mobile.nl
- [24] Vodafone Group Plc (2020) *Annual Report 2019* Vodafone.com
- [25] Liberty Global (2020). *Investor relations*. Zie LibertyGlobal.com

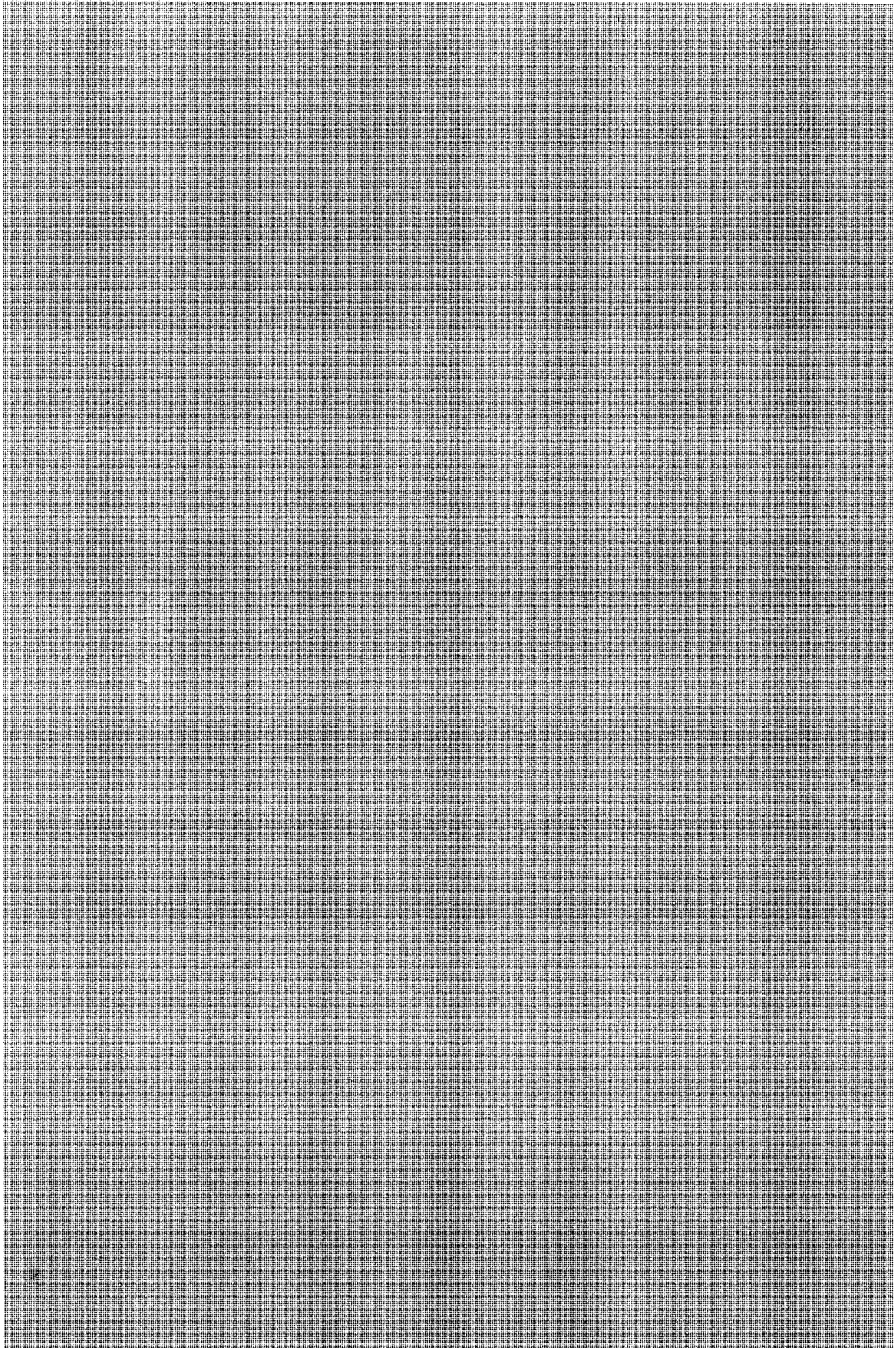
- [26] VodafoneZiggo (2020) Vodafone start met 5G in Nederland. Zie vodafoneziggo.nl
- [27] Sénat (2020). *Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles*. Zie senat.fr
- [28] Deutsche Telekom (2020). *Full year results 2019*. Zie telekom.com
- [29] Salaam Times (2019). *Millions of Afghans lose telecom services as Taliban destroy over 200 towers*. Zie afghanistan.asia-news.com.
- [30] The New York Time (2016) *Once a Bright Spot, Afghan Telecoms Face Unsustainable Losses*. Zie [NYTimes.com](https://nytimes.com)
- [31] IWPR (2015). *Afghans Alarmed by New Telecoms Tax*. Zie [IWPR.net](https://iwpr.net).
- [32] Wikipedia (2020). *List of mobile network operators of Europe*. Zie wikipedia.org
- [33] The Verge (2020) *Ripping Huawei out of US networks could be a nightmare for rural providers*. Zie: theverge.com
- [34] *Onteigeningswet*. Zie wetten.overheid.nl
- [35] Conseil d'État (2019). Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications électroniques. Zie legifrance.gouv.fr
- [36] Riigikogu (2020) *Elektroonilise side seaduse muutmise seadus 138 SE*. Zie riigikogu.ee
- [37] *Radet for Digital Sikkerhed (2016) Bemærkninger til udkast til bekendtgørelser vedrørende net- og informationssikkerhed*. Zie squarespace.com
- [38] Tom Pullar-Strecker (2020) *Spark and 2degrees expected to test waters with GCSB after UK clears Huawei for 5G*. Zie stuff.co.nz
- [39] Tom Pullar-Strecker (2018) *2degrees could face 'significant' costs if Huawei banned from 5G*. Zie stuff.co.nz
- [40] NSCS (2020) *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks*. Zie ncsc.gov.uk
- [41] Barkan, Biham & Keller (2003). *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*" Zie cs.technion.ac.il
- [42] De Bruijn & Ten Heuvelhof (2012) *Policy analysis and decision making in a network: how to improve the quality of analysis and the impact on decision making*. Zie tandfonline.com
- [43] Ministerie van Economische Zaken en Klimaat (2018). *Nederlandse Digitaliseringsstrategie*. Zie [Rijksoverheid.nl](https://rijksoverheid.nl)
- [44] HSCES (2018) *Huawei Cyber Security Evaluation Centre Oversight Board - Annual Report 2018. A report to the National Security Adviser of the United Kingdom*. Zie assets.publishing.service.gov.uk
- [45] CNBC (2020) *Why Huawei's role in Britain's 5G networks is under scrutiny once again*. zie cnbc.com
- [46] Business Insider (2020) *How a potential Nokia takeover would impact the network equipment market*. Zie [BusinessInsider.com](https://businessinsider.com)
- [47] NIS Cooperation group (2019) *EU Coordinated risk assessment of the cybersecurity of 5G networks*. Zie ec.europa.eu
- [48] Mobile World Live (2019) *Vodafone offers Europe up to OpenRAN*. Zie mobileworldlive.com

- [49]Rakuten (2019) *Rakuten Launches First Real-World End-to-End Tests in a Fully Virtualized Cloud-Native Mobile Network*. Zie [Rakuten.com](https://rakuten.com)
- [50]NEC (2020) *Rakuten Mobile and NEC Begin Production of Open RAN 5G Radio Equipment*. Zie [NEC.com](https://nec.com)
- [51]The Economist (2020) *Open standards, not sanctions, are America's best weapon against Huawei*. Zie economist.com
- [52]E. Raymond (1999) *The Cathedral and the Bazaar*. Zie o.a. [Wikipedia.org](https://wikipedia.org)
- [53]Sue Gee (2013) *Underhanded C Contest Revived*. Zie i-programmer.info

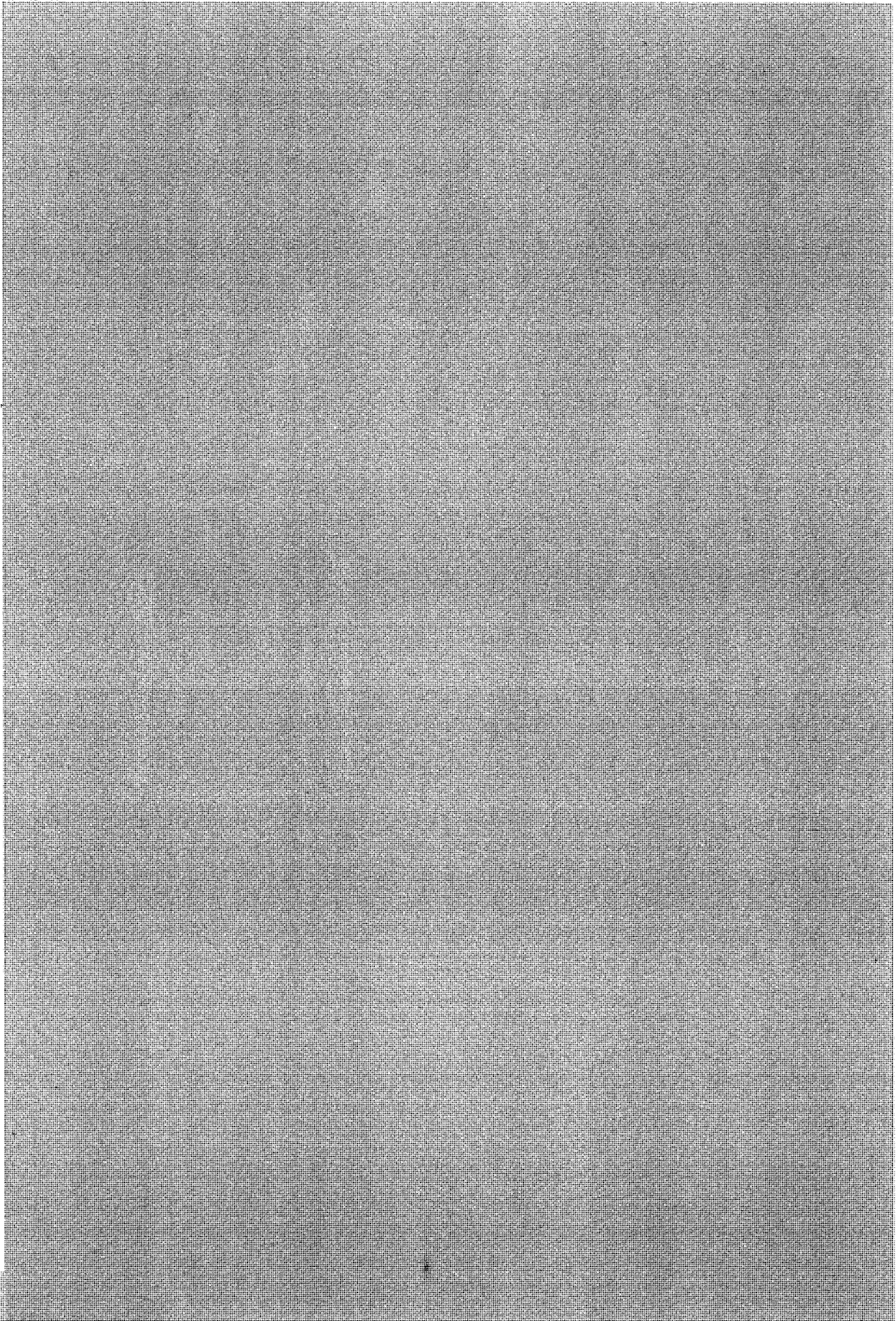


5.1.2a



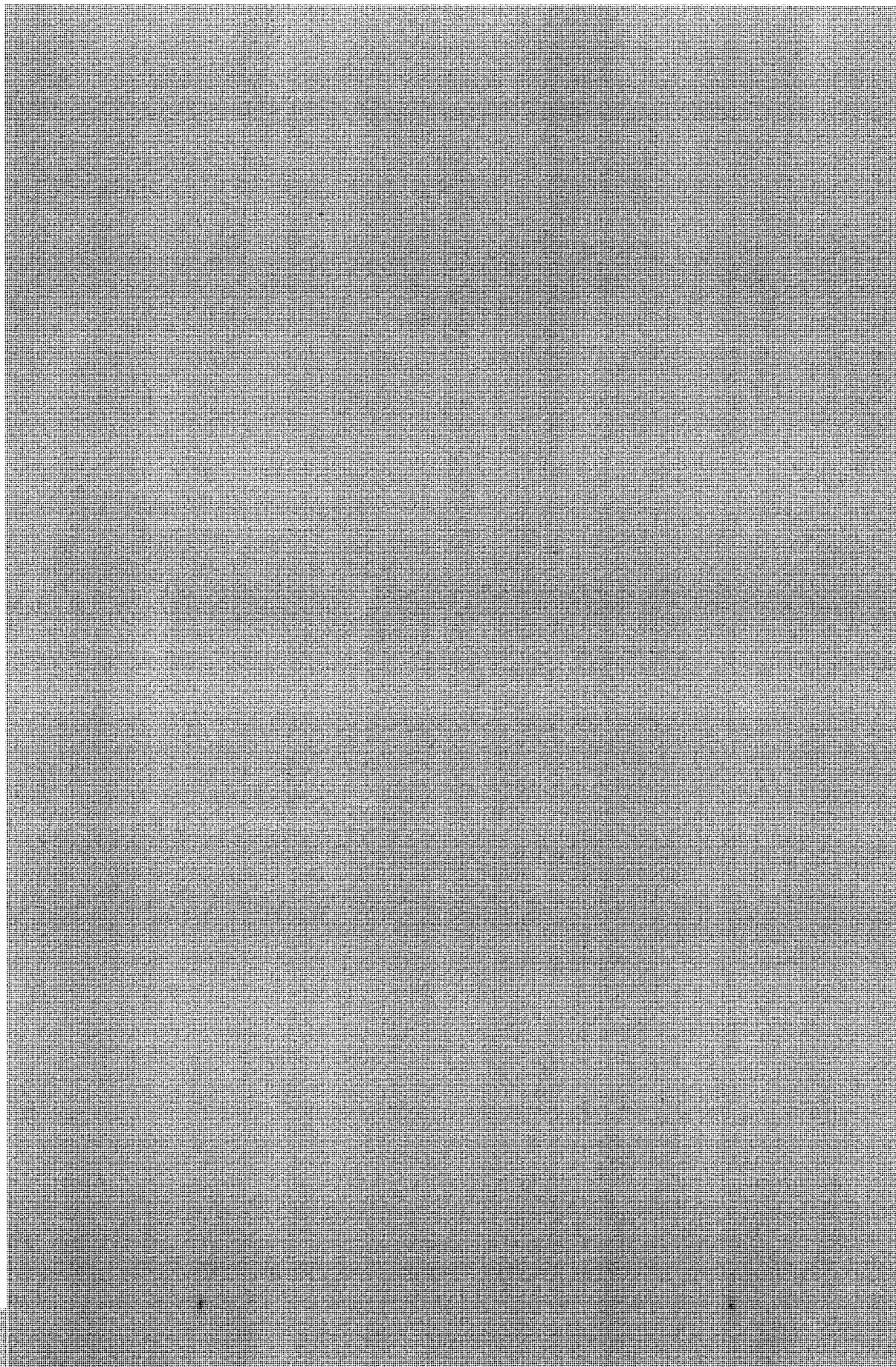


5.1.2a

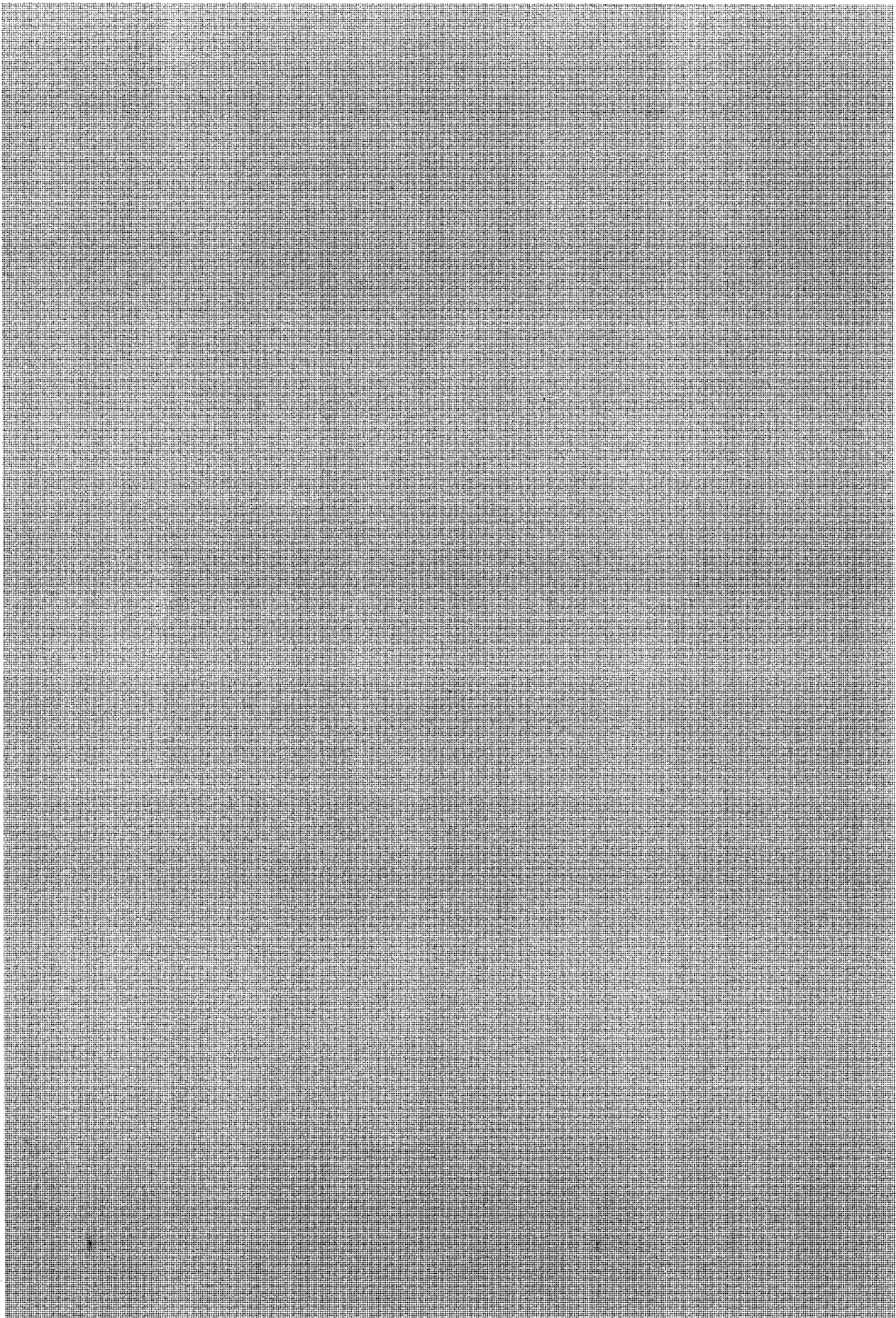


5.1.2a

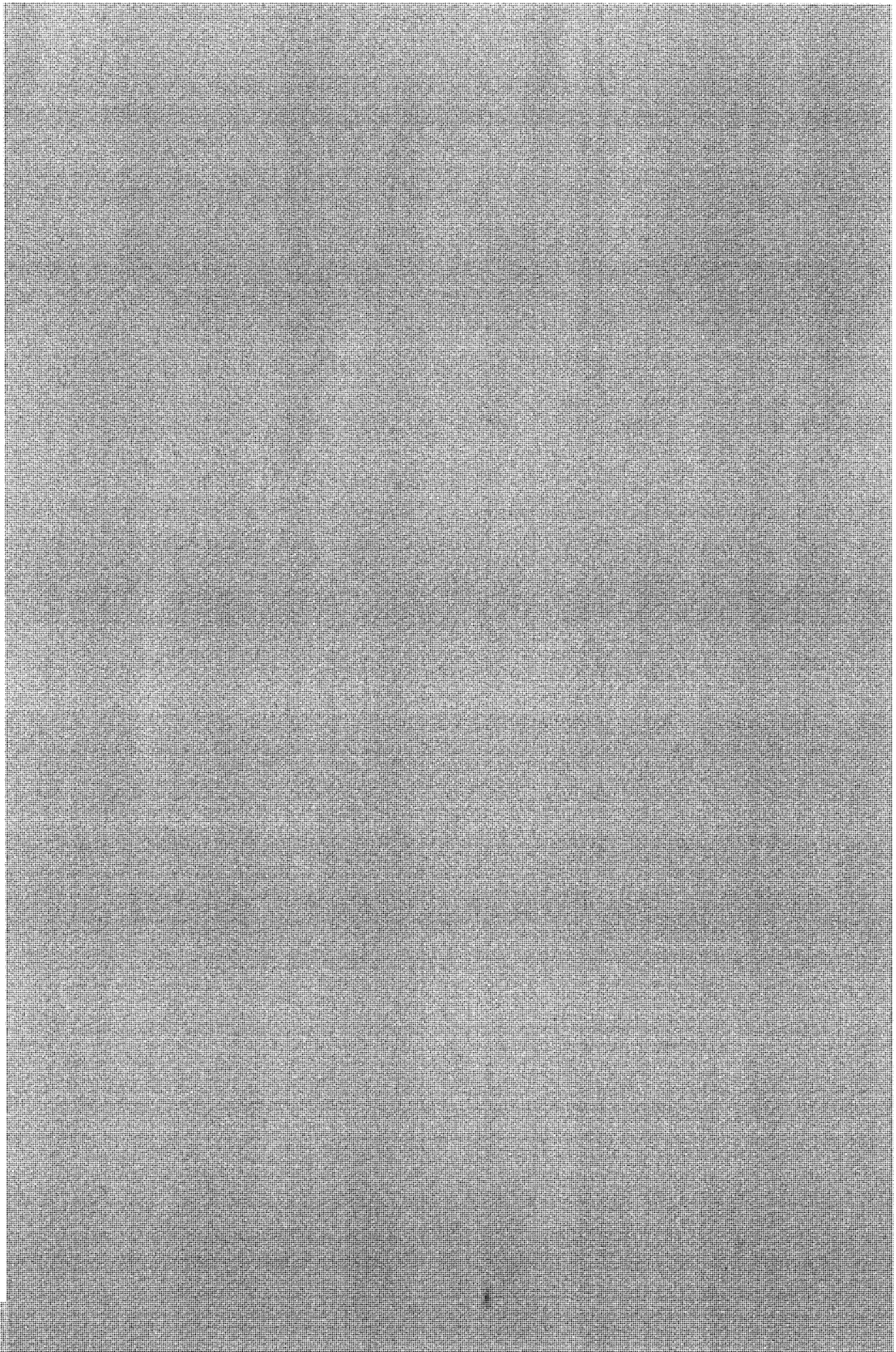
5.1.2a



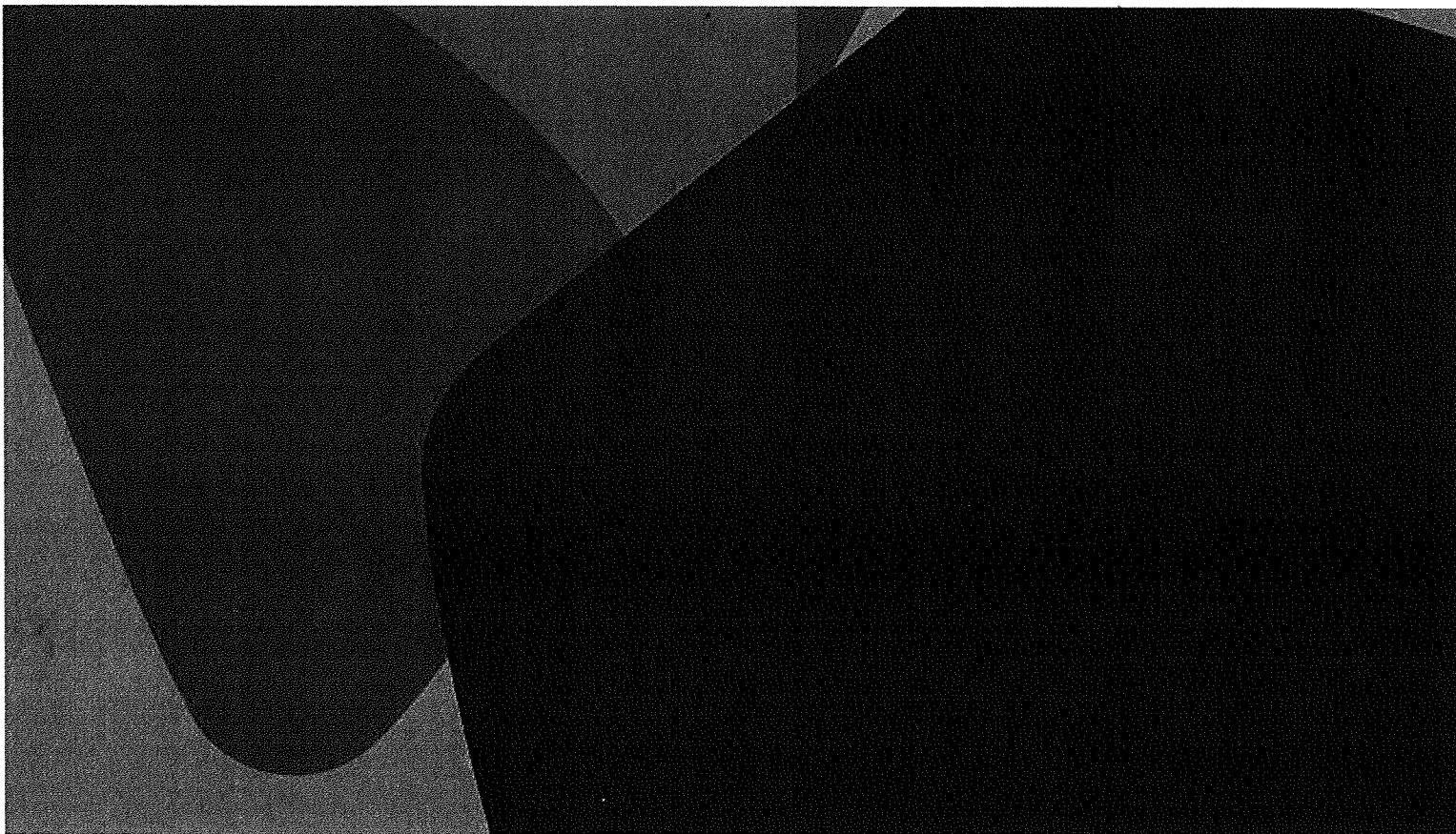
5.1.2a



5.1.2a

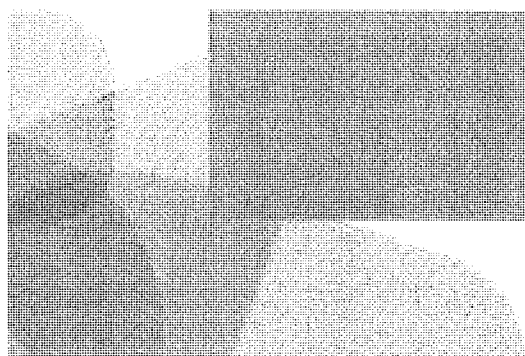


5.1.2a



Contact:

Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl



Aanleiding

- Naar aanleiding van gesprekken met internationale contacten en actuele complexe casussen is door de TFEV opgemerkt dat het dienstig zou zijn als er een gedeelde basispositie op het thema economische veiligheid komt. Het gaat hier om een set uitgangspunten die tevens als beknopte lijn kan dienen voor het uitdragen en duiden van de Nederlandse economische veiligheidsaanpak. BZ is verzocht met EZK en NCTV hiertoe een concept te ontwikkelen.

Kernpunten

- In de voorliggende basispositie economische veiligheid wordt toegelicht uit welke elementen de Nederlandse economische veiligheidsaanpak bestaat en wat de uitgangspunten zijn. Kern is dat veiligheidsbelangen en economische belangen in samenhang worden gezien. Dit stuk ligt voor ter discussie tijdens de TFEV op 26 juni a.s.
- Voorstel is om deze positie te gebruiken als basis voor verdere beleidsontwikkeling, evenals ten behoeve van spreeklijnen (politiek en hoog ambtelijk) over het thema economische veiligheid.
- De basispositie in bijlage 1 is zodanig opgesteld dat deze kan worden aangepast op specifieke instrumenten en beleidsverantwoordelijkheden.
- De basispositie is opgesteld door BZ, EZK en NCTV en wordt namens deze departementen ingebracht als discussiestuk.

Discussievragen

- Onderschrijven de leden van de TFEV de inhoud van de Basispositie Economische Veiligheid?
- Geeft de basispositie voldoende handvatten om teksten en spreeklijnen op te baseren, al naar gelang de context van het gesprek?
- Kunnen we de punten in deze basispositie beschouwen als basisprincipes om toekomstig beleid op economische veiligheid op te baseren.

Toelichting

- Economische veiligheidsvraagstukken staan ook in het licht van de Covid-19 uitbraak toenemend in de belangstelling.
- Een gezamenlijke basispositie draagt ertoe bij dat beleid op economische veiligheid het *case-by-case* karakter, en het risico op divergerende benaderingen, ontstijgt. De basispositie is daarmee een stap naar een meer strategische en samenhangende benadering van de gerelateerde thema's.
- Er lopen verschillende trajecten in ambtelijk/politiek Den Haag rondom economische veiligheid. De uitgangspunten in de basispositie kunnen deze trajecten een gemeenschappelijk kader bieden.
- Zo werken EZK, BZ en NCTV aan een eerste aanzet voor een breder afwegingskader cq. werkwijze voor economische veiligheid (werktitel). Dit afwegingskader (werktitel) zal worden uitgewerkt met de overige TFEV leden en eventuele overige relevante departementen en biedt een mogelijkheid om de uitgangspunten van de basispositie te operationaliseren.
- Bij verdere beleidsontwikkeling is het van belang om onderscheid te maken tussen maatregelen in reactie op een crisis (zoals corona) enerzijds en anderzijds maatregelen die blijvend van toepassing zijn, ook buiten crisissituaties.

Bijlage 1 – Basispositie Economische Veiligheid

1. Uitgangspunt [position]

- Nederland wil open en veilig zijn.
- Open markten en sterke verwevenheid van landen in mondiale waardeketens zorgen voor meer welvaart, toegang tot de beste productiefactoren en belangrijke bronnen van kennis die van groot belang zijn voor ons welzijn.
- Wederzijdse afhankelijkheid in mondiale waardeketens in een op regels gebaseerde wereldorde verlaagt kans op conflicten.
- Een doorslaggevende positie in waardeketens kan echter ook leiden tot eenzijdige strategische afhankelijkheden. Eenzijdige afhankelijkheden mogen niet ten koste gaan van het adequaat borgen van publieke belangen in Nederland en Europa.
- Daarbij is het ook een gegeven dat eenzijdige (strategische) afhankelijkheden van een bondgenoot of een democratische rechtsstaat minder bezwaarlijk zijn dan afhankelijkheden van autoritaire staten cq staten die wij als systeem-concurrent zien.
- De Nederlandse inzet is daarom enerzijds gericht op het voorkomen van nodeloze ontvechting van waardeketens. Anderzijds moeten die waardeketens binnen de grenzen blijven van onze kernbelangen. Als die kernbelangen in het geding zijn, is interventie nodig (denk aan: diversificatie van aanbod; nationale productie of productie in de interne markt etc).

2. NL is zich bewust [context]

- Tegelijkertijd zorgt de combinatie van snelle en diepe technologische ontwikkelingen en veranderende politieke trends, voor het ontstaan van risico's die mogelijk gevolgen hebben voor de economie en de nationale veiligheid.
- Risico's die men (h)erkent zijn situaties die ons kwetsbaar maken voor o.a. (cyber) spionage en sabotage, manipulatie en beïnvloeding als ook ongewenste buitenlandse inmenging in het NLse bedrijfsleven.
- We geven ons er rekenschap van dat sommige landen hun preponderante positie in de waardeketens aanwenden om (geo)politieke invloed uit te oefenen, en ook niet aarzelen om te dreigen om derde landen (tijdelijk) uit de ketens uit te sluiten als zij vinden dat deze landen een hen onwelgevallige politiek voeren.
- Gevolgen voltrekken zich zowel op economisch gebied als op het gebied van veiligheid van Nederland en Nederlanders.

3. Nederland handelt bewust [call for action]

- De huidige situatie vraagt om waakzaamheid en daaraan verbonden proportionele maatregelen om risico's voor de economie en nationale veiligheid beheersbaar te houden.
- Er is nieuw - of effectiever bestaand - beleid nodig om nieuwe of toegenomen bestaande negatieve gevolgen te ondervangen, zonder de baten van een open economie te verliezen.
- Nederland heeft een governance structuur ingericht om deze beleidsontwikkeling in goede banen te leiden (ACEV en MCEV).

4. Daarom: strategie [essence of action]

- De NLse strategie op economische veiligheid:
 - Is adaptief. Zodat gepast ingespeeld kan worden op veranderende omstandigheden, zonder afbreuk te doen aan maatschappelijke zekerheden omtrent openheid en veiligheid.
 - Is subsidiair en proportioneel, er worden geen zware maatregel genomen als een lichtere maatregel volstaat om een risico te adresseren en de genomen maatregel is in proportie met het risico.
 - Bezielt economische- en veiligheidsbelangen in samenhang. In de context van economische veiligheid zijn deze belangen geen losstaande pijlers en daarnaast niet per definitie tegengesteld aan elkaar.
 - Handelt offensief en defensief, zowel unilateraal, bilateraal, multilateraal zijn complementair.
 - Offensief = beleid om te zorgen voor een concurrerende, weerbare, innovatieve en hoog technologische samenleving
 - Defensief = beleid gericht op het beheersbaar houden van nationale veiligheidsrisico's.
- NL streeft ernaar risico's op diplomatieke consequenties die impact (kunnen) hebben op Nederlandse belangen zoveel mogelijk te mitigeren.

5. Europees Unie en derde landen [action with whom]

- NL streeft naar zo breed mogelijke multilaterale oplossingen, wat bilaterale oplossingen niet uitsluit. Bilateraal en multilateraal overleg kunnen complementair zijn aan elkaar en elkaar versterken.
- De EU heeft door haar omvang de benodigde slagkracht. Door als één blok op te trekken met de 27 EU-landen worden de lidstaten inclusief NL weerbaarder tegen druk van buiten de EU. Ongewenste politieke invloed via financieel-economische positionering van derde landen binnen de EU vermindert de slagkracht van de EU als geheel
- Coördineren van maatregelen op EU niveau, zodat lidstaten de economische- en veiligheidsbelangen in samenhang bezien.
- Ontwikkeling van maatregelen op EU niveau.
- Het uitgangspunt is dat handelingen rondom economische veiligheid subsidiair van aard zijn.
- NL erkent dat zich kwetsbaarheden op het gebied van economische veiligheid kunnen voordoen die te urgent zijn om af te wachten tot er een gecoördineerde EU aanpak is.
- Dialoog met derde landen, in het bijzonder ook met bondgenoten, is noodzakelijk om de economische veiligheidsbelangen van NL te waarborgen. Van bijzonder belang is de trans-Atlantische dialoog over dit onderwerp. Wel is het van belang om ook hierbij zoveel mogelijk op te trekken met gelijkgezinde EU-partners.



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

oplegnota

Rapport implementatie toolbox 5G

Datum
22 juni 2020

Bijlagen
1

Gevraagde beslissing/doel

Akkoord gaan met het versturen van de definitieve versie van het rapport met begeleidende brief aan de Kamer.

Samenvatting

Bijgaand vindt u een eerste conceptrapport van de Cooperation Group over de implementatie van de Toolbox 5G. Het rapport geeft een overzicht van de maatregelen uit de eerder gepubliceerde Toolbox die verschillende lidstaten nemen. De Nederlandse inbreng op het rapport wordt gecoördineerd vanuit de NCTV via de interdepartementale werkgroep EU 5G.

U wordt gevraagd om akkoord te gaan met het versturen van de definitieve versie van het rapport met een begeleidende brief aan de Kamer. Dit is eerder ook gedaan bij de publicatie van het Europees Risk Assessment en de Toolbox.



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

[Redacted]

[Redacted]

5.1.2e

Datum

22 juni 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Reactie IenW op gevraagde besluiten Taskforce Economische Veiligheid
Vergaderdatum en -tijd	26 juni 2020, 08.30-10.00 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Beschikkingen 5G (EZK)

Bijlage 1. Beschikkingen 5G

3. Begrotingsvoorstel economische veiligheid: inzet 2020 en 2021 (NCTV)

Bijlage 2. Begrotingsvoorstel economische veiligheid: inzet 2020 en 2021

Gevraagd besluiten: Prioritaire onderwerpen 2020 -2021 en middelen

1. Bepalen prioritaire onderwerpen voor 2020 en 2021;

- Voor wat betreft prioriteiten 1, 2 en 4 wil IenW tijdig worden betrokken als eventuele vervolgotrajecten consequenties voor het beleidsdomein van IenW krijgen;
- Prioriteit 3 'uitvoering stelsel van investeringstoetsing' is een maatregel die niet voorkwam in bijlage 3 (claim VJN 2020);
- Er lijkt verband te bestaan tussen prioriteit 3 en de maatregel onder 15 in het begrotingsvoorstel 'in kaart brengen strategische afhankelijkheden'. Ook is er een verband met het versterkingsprogramma vitaal (ketenafhankelijkheden);
- De Minister van IenW moet nog worden geïnformeerd en geadviseerd over de uitgangspunten en invulling van het stelsel van investeringstoetsen, voordat er formeel kan worden ingestemd met de prioritering en uitwerking van deze maatregel.

2. Instemmen (door desbetreffende organisaties) met het vrijmaken van middelen voor prioritaire onderwerpen.

IenW kan niet instemmen met een financiële bijdrage voor prioriteit 3 (investeringstoets), omdat:

- het concept wetsvoorstel en concept AMvB (lijst van vitale sectoren en toeleveranciers op basis van analyse strategische afhankelijkheden) nog niet zijn gedeeld;
- IenW nog niet is betrokken bij de voorbereiding van dit wetsvoorstel
- er nog geen overeenstemming is over de uitgangspunten voor de bevoegdheden en verantwoordelijkheden (en de consistentie van het voorgestelde beleid hierin);
- IenW heeft hiervoor geen bedragen in de begroting opgenomen;
- er geen kostenverdeelsleutel ligt;
- M IenW formeel nog een principiële besluit over de uitgangspunten moet nemen over deze prioriteit.

Gevraagde besluit: Structurele middelen t.b.v. kabinetsformatie

Structurele middelen voor alle onderwerpen uit het begrotingsvoorstel vanaf 2022 meenemen in de inzet richting komende regeerperiode;

- Het TFEV gaat over het begrotingsvoorstel voor het onderwerp economische veiligheid. Alleen voor dit onderwerp vormt het begrotingsvoorstel een 1^e aanzet.
- Er moet bekeken worden waar besluitvorming over cyber en aanverwante onderwerpen het beste kan plaatsvinden waarbij ook gekeken wordt naar de bestaande gremia op dit terrein.
- Tabel in bijlage 2 (en 3) is onvolledig/gedateerd, bij punt 5 ontbreekt bijv. de ANVS en de intensivering van het toezicht door de ILT als gevolg van de wijziging van de Wbni (WRR-kabinetsreactie). Ook moet er nog een discussie worden gevoerd over het meenemen van additionele kosten van Rijkswaterstaat om vanaf 2021 en verder te voldoen aan de Wbni).

Bijlage 3. Begrotingsvoorstel EV voorjaarsnota 2020

4. Inzet voor de komende regeerperiode (NCTV)

Bijlage 4. Inzet voor de komende regeerperiode

- Besluitvorming over dit agendapunt heeft in dit stadium geen zin, bijlage 4 is te vaag en moet eerst goed worden uitgewerkt.

Gevraagde besluit 1: Scope

Akkoord gaan met de hierboven omschreven scope: economische veiligheid, inclusief maatregelen die nodig zijn voor structurele samenwerking vitale processen.

- IenW is voorstander van een nauwe scope van het TFEV welke zich alleen richt op economische veiligheid.
- Cyber security en vitaal zijn geen bijzaken van economische veiligheid, maar separate hoofddossiers (uiteraard is afstemming gewenst).
- Structurele samenwerking bij statelijke dreigingen op vitale processen is vooral onderdeel van vitaal (IWV/DOCB/nieuw gremium), niet de scope van het TFEV.

Gevraagde besluit 2: Ambitie

Richting geven voor de inzet richting nieuwe regeerperiode:

1. *Huidige ambitie waarmaken*
2. *Huidige ambitie uitbreiden*
3. *Nieuwe ambitie opstellen/'next level'*

- [REDACTED]

5.2.1

Gevraagd besluit 3: Besluitvorming

Akkoord gaan met voorstel om besluitvorming in ACEV en MCEV plaats te laten vinden.

Akkoord mits:

- cyber security via het DOCS gaat en vitaal via het DOCB of nieuw gremium (re: versterkingsprogramma vitaal);
- vakdepartementen verantwoordelijk voor vitale sectoren van IenW tijdig, transparant en volledig worden geïnformeerd en betrokken als er relevante stukken in het TFEV, ACEV en het MCEV worden geagendeerd en verstuurd;
- de vertegenwoordiger in het ACEV ook het mandaat heeft om namens het vakdepartement besluiten te nemen;
- vakdepartementen rechtstreeks worden betrokken bij het voorbereiden van wetgevingsvoorstellen die hun verantwoordelijkheden raken (bijv. prioriteit 3 'de investeringstoets');
- M IenW wordt uitgenodigd voor het MCEV als er besluiten worden genomen die haar bevoegdheden en verantwoordelijkheden raken.

Gevraagd besluit 4: Tijdspad

Akkoord gaan met bovenstaand tijdspad.

- Besluitvorming is pas zinvol na probleemanalyse en groslijst (juli), dus na de zomervakantie.

5. Structurele samenwerking: verzoek regie en sturing (NCTV)

Verzoek regie en sturing: Mondelinge toelichting NCTV

Ter info: Bijlage 5. Oplegnota Rapport Dialogic, Bijlage 6. Rapport Dialogic Investeringszekerheid Telecommunicatiesector

6. Basispositie Economische Veiligheid (BZ)

Bijlage 7. Basispositie Economische Veiligheid

Discussievragen:

Onderschrijven de leden van de TFEV de inhoud van de Basispositie Economische Veiligheid?

Geeft de basispositie voldoende handvatten om teksten en spreeklijnen op te baseren, al naar gelang de context van het gesprek?

Kunnen we de punten in deze basispositie beschouwen als basisprincipes om toekomstig beleid op economische veiligheid op te baseren.

- Goed kernachtig stuk, deze basispositie biedt voldoende houvast. Economische veiligheid valt en staat bij de zwakste (economische) schakel, als bondgenoten elkaar niet economisch steunen, maken 'concurrenten' daar misbruik van;
- Wat ontbreekt is de beveiliging van hoogwaardige technologie in Nederland, waar bij diefstal/spionage van die technologie de internationale rechtsorde in het gedrang komt. Dus dat gaat verder dan het niveau van enkel Nederland/Europa. De problematiek is mondiaal.

7. Internationaal/Europees

Bijlage 8. Oplegnota Rapport implementatie toolbox 5G

Bijlage 9. Rapport implementatie toolbox 5G

8. Parlementair

9. Rondvraag en afsluiting

Van:**Aan:**

BD/ minezk.nl"; @minbzk.nl"; @minbzk.nl";
 @minbzk.nl"; @minbzk.nl"; @minbzk.nl";
 @mindef.nl"; @mindef.nl"; @mindef.nl"; @mindef.nl";
 @minaz.nl"; @minbuza.nl"; @minbuza.nl"; @minbuza.nl";
 @minbuza.nl"; @minbuza.nl"; politie.nl"; @minfin.nl";
 @minienw.nl"; BD/NCIV; @minocw.nl"
 @minbzk.nl"; @minbzk.nl"; @minbzk.nl";
 @minezk.nl"; @minezk.nl"; @minfin.nl";
 @minfin.nl"; @minbuza.nl"; @minbuza.nl";
 minbuza.nl"; @minaz.nl"; @minaz.nl"; @minaz.nl";
 @mindef.nl"; @mindef.nl"; @mindef.nl"; politie.nl";
 @politie.nl"; @politie.nl"; @politie.nl";
 @minienw.nl"; @minienw.nl"; @minocw.nl";
 @minocw.nl"

5.1.2e

Cc:

5.1.2e

Onderwerp:

Verslag TFEV 26/6 en bijlage

Datum:

dinsdag 7 juli 2020 10:27:47

Bijlagen:

5.1.2a

Geachte leden van de TFEV,

Zojuist is via [REDACTED] het verslag van 26 juni naar u toegestuurd. Voor degene die niet aangesloten zijn op [REDACTED] wordt apart een afspraak gemaakt om het verslag hardcopy te bezorgen. Daarnaast op verzoek van BZ in de bijlage een document [REDACTED]

5.1.2i

5.1.2i

5.1.2a

Zoals besproken vindt de eerstvolgende TFEV na het reces plaats. U ontvangt hiervoor binnenkort een uitnodiging.

Vriendelijke groet,

5.1.2e

Ministerie van Justitie en Veiligheid

Turfmarkt 147 | 2511 DP | Den Haag

Postbus 20301 | 2500 EH | Den Haag

[REDACTED]
 [REDACTED]

5.1.2e



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK

Contactpersoon

[REDACTED]

5.1.2e

[REDACTED]

Datum

24 augustus 2020

agenda

Taskforce Economische Veiligheid

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	26 augustus 2020, 08.30-10.00 uur
Vergaderplaats	ICCb/MCCb-zaal (3e etage)

1. Opening en mededelingen

2. [REDACTED]

5.1.2a

3. Expertmeeting [REDACTED]

5.1.2a

4. Parlementair

5. Rondvraag en afsluiting

Dep. VERTROUWELIJK

Proposal for a [REDACTED] / Dutch expert-meeting

5.1.2a

Introduction and motivation for the meeting

Both the Netherlands and [REDACTED] benefit from open, fair and sustainable markets. Open markets and interconnectedness between countries via global value chains have enabled global access to technologies, ideas and production factors, and contribute to our wellbeing. Moreover, mutual dependencies via global value chains in a rules-based global order reduce the risk of conflict. Recently, however, parties have been using dominant economic positions to achieve political goals. Of particular concern are strategic dependencies. These could undermine the safeguarding of public interests, including national security, of open economies. [REDACTED]

5.1.2a

5.1.2a

The Netherlands and [REDACTED] acknowledge that a European approach based on equality, reciprocity and reduced unilateral strategic dependence is needed to safeguard public interests while maintaining open, fair, and sustainable markets. Since the EU as a whole has far more leverage towards others than its individual member states, EU-cohesion remains of utmost importance. A European approach should be based on analysis and it should combine both defensive and offensive policy measures to safeguard public interests and bolster Europe's position in the world. As these are multifaceted challenges any approach should take into account, economic, security and foreign policy aspects.

5.1.2a

Goal and result of the meeting:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2a
+ 5.2.1

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

We stand ready to consider other suggestions for the next step and way forward from the [REDACTED] side.

5.1.2a

Date:

15 or 16 September in The Hague

The [REDACTED] delegation proposes to arrive on the evening ahead of the consultations in order to dedicate a full day to [REDACTED].

5.1.2a
5.1.2a**Proposed participants:**

Polymakers from relevant departments and security services.

[REDACTED]:

- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]

5.1.2a

Netherlands- representatives from the Dutch economic policy, foreign policy and national security policy departments:

- [REDACTED]
- BZ, tbc

5.1.2e

- BHOS, [REDACTED]
- EZK, [REDACTED]

5.1.2e

Proposed structure of the meeting:

[REDACTED]

5.2.1

[REDACTED]

5.2.1

[REDACTED]

5.2.1

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

5.2.1

- [REDACTED]
- [REDACTED]

Draft Agenda [REDACTED] **wishes:**

5.1.2a

A) [REDACTED]

5.1.2a
+5.2.1

[REDACTED]

B) [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

5.1.2a
+5.2.1

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

C) Deliverables and way forward

[Redacted text block]

- [Redacted text]
- [Redacted text]
- [Redacted text]
- [Redacted text]
- [Redacted text]
- [Redacted text]

5.1.2a
+5.2.1

[Redacted text block]

- [Redacted text]
- [Redacted text]
- [Redacted text]
- [Redacted text]

Appendix – Netherlands' Position on economic security policy

1. Key principles (position)

- The Netherlands wants to be open and secure.
- Open markets and close connections between countries in global value chains boost prosperity and facilitate access to the best production factors and important sources of knowledge, and therefore have a major positive impact on our wellbeing.
- Mutual dependency in global value chains in a rules-based global order reduces the risk of conflict.
- However, dominant positions in value chains can also lead to unilateral strategic dependencies. Unilateral dependencies must not undermine the safeguarding of public interests in the Netherlands and Europe as a whole.
- It also goes without saying that unilateral strategic dependency on an ally or a democratic state governed by the rule of law is less objectionable than dependency on authoritarian states or states that we regard as systemic rivals.
- The Dutch approach therefore focuses, on the one hand, on preventing unnecessary decoupling of value chains. At the same time, those value chains must remain compatible with our core interests. If these core interests are threatened, intervention is required (diversification of supply, national production, production in the single market, etc.).

2. The Netherlands is aware (context)

- At the same time, the combination of rapid and profound technological advances and changing political trends is creating risks that may affect the Netherlands' economy and national security.
- Recognised risks include situations that make us vulnerable to cyber espionage and sabotage, manipulation and influencing, and also undesired foreign intervention in Dutch businesses, knowledge institutions and local authorities.
- We are aware that some countries use their dominant position in value chains to exert geopolitical influence, and do not hesitate to threaten third countries with exclusion from those value chains, even if only temporarily, if they feel that those countries are pursuing policies they disapprove of.
- This impacts the Netherlands and its inhabitants both economically and in terms of security.

3. The Netherlands acts consciously (call for action)

- The current situation calls for vigilance and proportionate measures to keep the risks to the economy and national security under control.
- New – or existing but more effective – policies are needed to deal with new negative effects or an increase in existing ones, without losing the benefits of an open economy.
- The Netherlands has created a governance structure to guide policy development, in the form of the Official Committee on Economy and Security (ACEV) and the Ministerial Committee on Economy and Security (MCEV).

4. Therefore: strategy (essence of action)

- The Dutch strategy on economic security:
 - is adaptive, allowing an appropriate response to changing circumstances, without undermining public goods like openness and security;
 - is subsidiary and proportionate. A drastic measure is never taken if a milder measure is sufficient to address a risk and is proportionate;
 - views economic and security interests as two sides of the same coin. In the context of economic security, they are not separate pillars and they are not by definition opposing interests;
 - involves both offensive and defensive action, whether unilateral, bilateral or multilateral, with all three levels being complementary.
 - Offensive action aims to ensure a competitive, resilient, innovative and high-tech society.
 - Defensive action aims to keep national security risks under control.
- The Netherlands seeks to minimise the risk of diplomatic effects that could impact Dutch interests.

5. European Union and third countries (action with whom)

- The Netherlands seeks the broadest possible multilateral solutions, but does not rule out bilateral solutions. Bilateral and multilateral consultations can complement and reinforce one another.

- Given its size, the EU has the necessary strength. By acting as a united bloc, the 27 member states, including the Netherlands, are better able to withstand pressure from outside the EU. Undesirable political influence arising from the financial and economic positioning of third countries within the EU reduces the effectiveness of the EU as a whole.
- Measures should be coordinated at EU level so that member states view economic and security interests as two sides of the same coin.
- EU-level measures should be developed.
- As a rule, action on economic security should be of a subsidiary nature.
- The Netherlands recognises that economic security vulnerabilities can occur that are too urgent to wait for a coordinated EU approach.
- Dialogue with third countries, especially allies, is necessary to safeguard the Netherlands' economic security interests. The transatlantic dialogue on this subject is particularly important. But here, too, it is important to act with like-minded EU partners wherever possible.



TFEV

NCTV/PSD

Contactpersoon

5.1.2e

Datum

25 augustus 2020

Ons kenmerk

xxx

nota

Artikel in FD 25 augustus

Aanleiding

Op 25 augustus publiceerde het FD het artikel 'Amsterdamse universiteiten gaan samenwerken met Huawei'. Dit artikel is als bijlage toegevoegd. In dit artikel wordt verwezen naar een gesprek tussen de VU en overheidspartijen. In deze nota wordt een toelichting gegeven op het gesprek dat heeft plaatsgevonden.

Toelichting gesprek

- Het gesprek heeft plaatsgevonden op 30 januari 2019 op verzoek van de VU. Het gesprek is gefaciliteerd door OCW.
- Aanwezig bij het gesprek waren : OCW, NCTV , AIVD, UvA, VU, IXA VU-VUmc ().
- De AIVD heeft een algemene presentatie gehouden over de risico's van samenwerking.
- Tijdens dit gesprek heeft de VU aanvullende informatie gegeven over de samenwerking. In reactie hierop zijn ten aanzien van de casus enkele aandachtspunten geschetst.
- De AIVD en de NCTV hebben het aanbod gedaan om nader contact te hebben.
- Na het gesprek heeft een mailwisseling plaatsgevonden tussen VU en de NCTV. Hierin is door de NCTV aangegeven dat op basis van ontvangen informatie er geen directe NV risico's te zien zijn, maar dat er wel een aantal aandachtspunten zijn die in het gesprek onder de aandacht zijn gebracht. Ook is nogmaals het aanbod gedaan om hierover mee te denken.
- De NCTV en de AIVD hebben na dit gesprek geen verzoeken om nadere informatie/duiding ontvangen.

5.1.2e

Bijlage 1: artikel in Het Financieele Dagblad 'Amsterdamse universiteiten gaan samenwerken met Huawei'

NCTV/PSD

Korte beschrijving: Terwijl steeds meer Europese landen de omstreden Chinese telecomgigant weren, sluiten de UvA en de VU er juist een overeenkomst mee

Datum
25 augustus 2020

Ons kenmerk
xxx

Publicatiedatum: 25 Aug 2020 03:15

Rubriek:OVERZICHT, p.1

Terwijl steeds meer Europese landende omstreden Chinese telecomgigant weren, sluiten de UvA en de VU er juist een overeenkomst mee

Jan Fred van Wijnen

Amsterdam

Binnen de samenwerking met de universiteiten investeren de Chinezen €3,5 mln in een 'lab' voor deontwikkeling van kunstmatige intelligentie (AI).

De opmerkelijke overeenkomst heeft de goedkeuring van de AIVD en de ministeries van Economische Zaken en Onderwijs, ondanks scherpewaarschuwingen van het kabinet voor Chinese partners.

De samenwerking draait om nieuwe zoektechnologie. In het lab wordt AI ontwikkeld voor zoekmachines die in gesprek gaan met de gebruiker. Ook moet de technologie 'beledigende' en andere 'ongepaste' teksten weg kunnen filteren, zo meldt een wervingsadvertentie voor promovendi. Huawei werkt al enige tijd aan eigen zoektechnologie. Door een Amerikaanse boycot kan het geen GoogleSearch meer op zijn mobieltjes zetten.

Huawei ligt zwaar onder vuur. De Verenigde Staten verdenken het bedrijf, dat wereldwijd mobieltjes, telecomnetwerken en datacenters verkoopt, van spionage voor de Chinese overheid. In de VS mag het geen zaken meer doen. Ook de Europese Commissie waarschuwt voor Huawei bij aanbesteding van 5G-telecomnetwerken.

De campagne tegen Huawei maakt deel uit van de slepende handelsoorlog tussen de Verenigde Staten en China. De regering-Trump wil de opmars van de Chinese techsector afremmen, en dwingt ook bondgenoten in het gelid. De Nederlandse regering werd vorig jaar onder druk gezet om te voorkomen dat chipmachinefabrikant ASML - een spil in de mondiale chipindustrie - zijn meest geavanceerde machines exporteert naar China.

Zelf waarschuwde Den Haag Nederlandse universiteiten eind vorig jaar uitdrukkelijk voor de 'geopolitieke powerplay' van China. De supermacht jaagt actief op buitenlandse kennis en technologie, zo stelde het kabinet in de Beleidsnota China. Samenwerking met Chinese bedrijven en universiteiten kan leiden tot 'ongewilde kennisoverdracht', onder meer in kunstmatige intelligentie. Dat raakt zowel de nationale veiligheid als de economische belangen.

Chinese wetenschappers snappen beter dan de Nederlandse wat ze uitsamenwerking willen halen, aldus het kabinet. Uit gesprekken zou blijken dat Nederlandse universiteiten 'relatief snel tegemoetkomen' aan Chinese wensen.

NCTV/PSD

Datum

25 augustus 2020

Ons kenmerk

xxx

Toch maken de Nederlandse veiligheidsdiensten geen bezwaartegen de komst van het Huawei-lab, zo blijkt uit navraag door het FD.

Begin dit jaar hebben de VU en de UvA hun plan toegelicht tegenover vier medewerkers van inlichtingendienst AIVD en de coördinatorterrorismebeveiliging NCTV. De bijeenkomst werd gehouden op het ministerie van Onderwijs, bij de plaatsvervangend directeur Wetenschap.

De AIVD spreekt desgevraagd van een 'bewustwordingspresentatie', en wil verder niet reageren. Volgens de twee universiteiten waren de veiligheidsdiensten tevreden met de garanties tegen mogelijke kennisdiefstal.

Ook de ministeries van Economische Zaken (EZ) en Onderwijs, Cultuur en Wetenschap (OCW) steunen de samenwerking, blijkt desgevraagd.

Bijlage 2

'Vervolg Amsterdamse universiteiten gaan samenwerken met Huawei'

Het Financieele Dagblad (Van onze redacteur) | 25 aug 2020 03:15 (published: 25 aug 2020 03:15) | 278 woorden

Rubriek: p.3

Lengte: 278 woorden

Van onze redacteur

'De verantwoordelijkheid voor de samenwerking en het beheersen van die risico's ligt bij de universiteiten', aldus OCW. Het ministerie bevestigt dat het op 30 januari een gesprek heeft 'gefaciliteerd' tussen de twee universiteiten en de veiligheidsdiensten.

Het ministerie van Economische Zaken stelt dat het in een apart gesprek met de UvA 'nadrukkelijk' heeft gewezen op de 'mogelijk grote risico's' van de deal. De twee Amsterdamse universiteitsbesturen zijn tevreden met de overeenkomst. Volgens een gezamenlijke woordvoerder heeft het onderzoek voor Huawei 'niets te maken met netwerkkapparatuur waarover veel publieke discussie is'. De universiteiten hebben 'zeer grondig onderzocht' of de wetenschappers onafhankelijk kunnen publiceren, en of gevoelige kennis in de juiste handen blijft. Het Rathenau Instituut, onafhankelijk techadviseur van kabinet en parlement, waarschuwt dat bij onderzoek naar kunstmatige intelligentie de grens vervaagt tussen militaire en civiele technologie.

Daarom roept het adviesorgaan de politiek op duidelijkheid te geven aan universiteiten, in het bijzonder over de vraag of samenwerking 'met een bedrijf als Huawei' nog mag.

De Britse universiteit van Oxford staakte vorig jaar na publieke ophef de samenwerking met Huawei.

Hoogleraar kunstmatige intelligentie Frank van Harmelen (VU), een van de oprichters van het lab, verwacht dat het lab uitgroeit tot een zelfstandig onderzoekscentrum met honderd medewerkers. Huawei zegt in een reactie dat de beslissing hierover later wordt genomen.

Het contract tussen de Amsterdamse universiteiten en Huawei is op 15 mei getekend. De eerste vacatures voor promovendi staan open.

Netherlands' Position on Economic Security

1. Key principles (position)

- The Netherlands wants to be open and secure.
- Open markets and close connections between countries in global value chains boost prosperity and facilitate access to the best production factors and important sources of knowledge, and therefore have a major positive impact on our wellbeing.
- Mutual dependency in global value chains in a rules-based global order reduces the risk of conflict.
- However, dominant positions in value chains can also lead to unilateral strategic dependencies. Unilateral dependencies must not undermine the safeguarding of public interests in the Netherlands and Europe as a whole.
- It also goes without saying that unilateral strategic dependency on an ally or a democratic state governed by the rule of law is less objectionable than dependency on authoritarian states or states that we regard as systemic rivals.
- The Dutch approach therefore focuses, on the one hand, on preventing unnecessary decoupling of value chains. At the same time, those value chains must remain compatible with our core interests. If these core interests are threatened, intervention is required (diversification of supply, national production, production in the single market, etc.).

2. The Netherlands is aware (context)

- At the same time, the combination of rapid and profound technological advances and changing political trends is creating risks that may affect the Netherlands' economy and national security.
- Recognised risks include situations that make us vulnerable to cyber espionage and sabotage, manipulation and influencing, and also undesired foreign intervention in Dutch businesses, knowledge institutions and local authorities.
- We are aware that some countries use their dominant position in value chains to exert geopolitical influence, and do not hesitate to threaten third countries with exclusion from those value chains, even if only temporarily, if they feel that those countries are pursuing policies they disapprove of.
- This impacts the Netherlands and its inhabitants both economically and in terms of security.

3. The Netherlands acts consciously (call for action)

- The current situation calls for vigilance and proportionate measures to keep the risks to the economy and national security under control.
- New – or existing but more effective – policies are needed to deal with new negative effects or an increase in existing ones, without losing the benefits of an open economy.
- The Netherlands has created a governance structure to guide policy development, in the form of the Official Committee on Economy and Security (ACEV) and the Ministerial Committee on Economy and Security (MCEV).

4. Therefore: strategy (essence of action)

- The Dutch strategy on economic security:
 - is adaptive, allowing an appropriate response to changing circumstances, without undermining public goods like openness and security;
 - is subsidiary and proportionate. A drastic measure is never taken if a milder measure is sufficient to address a risk and is proportionate;
 - views economic and security interests as two sides of the same coin. In the context of economic security, they are not separate pillars and they are not by definition opposing interests;
 - involves both offensive and defensive action, whether unilateral, bilateral or multilateral, with all three levels being complementary.
 - Offensive action aims to ensure a competitive, resilient, innovative and high-tech society.
 - Defensive action aims to keep national security risks under control.
- The Netherlands seeks to minimise the risk of diplomatic effects that could impact Dutch interests.

5. European Union and third countries (action with whom)

- The Netherlands seeks the broadest possible multilateral solutions, but does not rule out bilateral solutions. Bilateral and multilateral consultations can complement and reinforce one another.

- Given its size, the EU has the necessary strength. By acting as a united bloc, the 27 member states, including the Netherlands, are better able to withstand pressure from outside the EU. Undesirable political influence arising from the financial and economic positioning of third countries within the EU reduces the effectiveness of the EU as a whole.
- Measures should be coordinated at EU level so that member states view economic and security interests as two sides of the same coin.
- EU-level measures should be developed.
- As a rule, action on economic security should be of a subsidiary nature.
- The Netherlands recognises that economic security vulnerabilities can occur that are too urgent to wait for a coordinated EU approach.
- Dialogue with third countries, especially allies, is necessary to safeguard the Netherlands' economic security interests. The transatlantic dialogue on this subject is particularly important. But here, too, it is important to act with like-minded EU partners wherever possible.



L1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep.-VERTROUWELIJK

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

6 oktober 2020

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	14 oktober 2020, 09:00-10:30 uur
Vergaderplaats	NCTV, ICCb/MCCb zaal (3e etage)

1. Opening en mededelingen

2. Beschikkingen 5G (EZK)

- a. Bijlage 1. Oplegnota beschikkingen 5G
- b. Bijlage 2. Conceptbeschikking

3. Ministeriele regeling (EZK)

- a. Bijlage 3. Oplegnota ministeriele regeling
- b. Bijlage 4. Concept regeling veiligheid en integriteit telecommunicatie

4. [REDACTED]

5.1.1b + 5.1.2a +
5.1.2i

5. Structurele samenwerking (NCTV)

- a. Bijlage 5. Oplegnota voortgang structurele samenwerking
- b. Bijlage 6. Procesbeschrijving structurele samenwerking

6. Inzet formatie EV en cybersecurity (NCTV)

- a. Bijlage 7. Oplegnota inzet formatie EV en cybersecurity
- b. Bijlage 8. Probleemanalyse EV

7. Internationaal/Europees

- [REDACTED]

5.1.2a

8. Parlementair

9. Rondvraag en sluiting

Dep.-VERTROUWELIJK

NOTA TFEV 14 oktober 2020

5G Beschikkingen

7 oktober 2020

Penvoerder: EZK

Aanleiding

In de bijlage vindt u de concept beschikking aan de mobiele netwerk operators (hierna: MNO's of telco's) die wij voor een zienswijze aan hen willen voorleggen. Deze beschikking heeft het Besluit veiligheid en integriteit telecommunicatie als grondslag en geeft uitvoering aan een eerder besluit van de TFEV omtrent het niet toestaan van bepaalde leveranciers in kritieke onderdelen van het mobiele netwerk. In deze nota wordt een aantal in deze concept beschikking gemaakte keuzes toegelicht.

Verzoek

U wordt gevraagd akkoord te gaan met deze concept beschikking.

Kernpunten

- In deze beschikking wordt aan de telco's de verplichting opgelegd om in de kritieke onderdelen van hun telecomnetwerken voor verschillende producten en diensten geen gebruik te maken van enkele specifieke leveranciers. De beschikking benoemt welke kritieke onderdelen het betreft (gebaseerd op eerdere risicoanalyse van TFEV), van welke leveranciers daarbinnen geen producten of diensten kunnen worden gebruikt, motiveert waarom de verplichting met het oog op de risico's voor de nationale veiligheid noodzakelijk is, en geeft de termijn binnen welke de te weren leveranciers uit de kritieke onderdelen moeten worden verwijderd.
- EZK en NCTV hebben in overleg met BZ, de inlichtingen- en veiligheidsdiensten en Agentschap Telecom de beschikking voorbereid. Fin heeft op de beschikking meegelezen. De concept beschikking is tevens voorgelegd aan de Landsadvocaat.
- Het is van belang dat deze concept beschikking op korte termijn wordt verstuurd aan de telco's, gezien de doorlooptijd en het belang dat de bewindspersonen en de Kamer hechten aan dat we de definitieve beschikking in Q1 kunnen versturen.
- In deze nota wordt toegelicht hoe om is gegaan met bepaalde daarin gemaakte keuzes: motivering toetsing aan criteria voor aanmerken van partijen als niet-vertrouwde partij, [redacted], motivering van de noodzakelijkheid van de verplichting, [redacted], de vervangingstermijn, en vertrouwelijkheid van de bijlage met kritieke onderdelen. Daarnaast wordt een voorzet gedaan voor de communicatie rondom de beschikkingen om een zachte landing te bewerkstelligen, de budgettaire consequenties, alsmede een korte vooruitblik op het vervolgproces en de nadeelcompensatie.

5.1.2i
5.1.1b

Toelichting

Motivering toetsing aan criteria voor aanmerken partijen als niet vertrouwde partij (paragraaf 6 en 7)

- [redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

5.1.2i

[REDACTED]

5.1.2i

[REDACTED]

5.1.2i

[REDACTED]

[REDACTED]

5.1.2i

[REDACTED]

[REDACTED]

[REDACTED]

5.1.2i

[REDACTED]

[REDACTED]

5.1.2i

[REDACTED]

5.1.2i

[REDACTED]

[REDACTED]	[REDACTED]	5.1.2i
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
[REDACTED]	[REDACTED]	5.1.2i
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
[REDACTED]	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	

Noodzakelijkheid van de verplichting

- Voor het opleggen van de verplichting is vereist dat het opleggen daarvan noodzakelijk is. Daartoe zal meer in het bijzonder moeten kunnen worden geconcludeerd dat er geen andere beheersmaatregelen mogelijk en realiseerbaar zijn om de nationale veiligheid voldoende te beschermen.
- In de beschikking is toegelicht dat die noodzaak er is, omdat uit het [REDACTED]-rapport blijkt dat zelfs met het treffen van aanvullende beveiligingsmaatregelen (die krachtens ministeriële regeling komen te gelden), bij het gebruik maken van [REDACTED] in de kritieke onderdelen van het netwerk, het in onvoldoende mate mogelijk is om spionage te voorkomen of tijdig te detecteren.

5.1.2i

5.1.2i

- [REDACTED]

5.1.2i

[REDACTED]

- [REDACTED]

5.1.1b

Category	5.1.1b (%)	5.1.1b (%)	5.1.1b (%)
1.1.1.1	100	100	100
1.1.1.2	100	100	100
1.1.1.3	100	100	100
1.1.1.4	100	100	100
1.1.1.5	100	100	100
1.1.1.6	100	100	100
1.1.1.7	100	100	100
1.1.1.8	100	100	100
1.1.1.9	100	100	100
1.1.1.10	100	100	100
1.1.1.11	100	100	100
1.1.1.12	100	100	100
1.1.1.13	100	100	100
1.1.1.14	100	100	100
1.1.1.15	100	100	100
1.1.1.16	100	100	100
1.1.1.17	100	100	100
1.1.1.18	100	100	100
1.1.1.19	100	100	100
1.1.1.20	100	100	100
1.1.1.21	100	100	100
1.1.1.22	100	100	100
1.1.1.23	100	100	100
1.1.1.24	100	100	100
1.1.1.25	100	100	100
1.1.1.26	100	100	100
1.1.1.27	100	100	100
1.1.1.28	100	100	100
1.1.1.29	100	100	100
1.1.1.30	100	100	100
1.1.1.31	100	100	100
1.1.1.32	100	100	100
1.1.1.33	100	100	100
1.1.1.34	100	100	100
1.1.1.35	100	100	100
1.1.1.36	100	100	100
1.1.1.37	100	100	100
1.1.1.38	100	100	100
1.1.1.39	100	100	100
1.1.1.40	100	100	100
1.1.1.41	100	100	100
1.1.1.42	100	100	100
1.1.1.43	100	100	100
1.1.1.44	100	100	100
1.1.1.45	100	100	100
1.1.1.46	100	100	100
1.1.1.47	100	100	100
1.1.1.48	100	100	100
1.1.1.49	100	100	100
1.1.1.50	100	100	100
1.1.1.51	100	100	100
1.1.1.52	100	100	100
1.1.1.53	100	100	100
1.1.1.54	100	100	100
1.1.1.55	100	100	100
1.1.1.56	100	100	100
1.1.1.57	100	100	100
1.1.1.58	100	100	100
1.1.1.59	100	100	100
1.1.1.60	100	100	100
1.1.1.61	100	100	100
1.1.1.62	100	100	100
1.1.1.63	100	100	100
1.1.1.64	100	100	100
1.1.1.65	100	100	100
1.1.1.66	100	100	100
1.1.1.67	100	100	100
1.1.1.68	100	100	100
1.1.1.69	100	100	100
1.1.1.70	100	100	100
1.1.1.71	100	100	100
1.1.1.72	100	100	100
1.1.1.73	100	100	100
1.1.1.74	100	100	100
1.1.1.75	100	100	100
1.1.1.76	100	100	100
1.1.1.77	100	100	100
1.1.1.78	100	100	100
1.1.1.79	100	100	100
1.1.1.80	100	100	100
1.1.1.81	100	100	100



Vervangingstermijn

- In de concept beschikking is de door AT opgestelde concept paragraaf voor de vervangingstermijn opgenomen, om een indicatie te geven van de termijn en de daarbij behorende motivering. Hierbij is als voorbeeld gekozen voor de beschikking [REDACTED]. 5.1.2i
- Dit is nadrukkelijk een concept formulering, waar nog een redactionele slag op kan plaatsvinden.
- [REDACTED] Dialogic en AT hebben de voorstellen van de telco's beoordeeld, achten deze redelijk, en stellen voor om deze termijnen in de beschikking over te nemen, rekening houdend met de continuïteit van het netwerk en de noodzaak van vervanging. [REDACTED] 5.1.2i
- [REDACTED] 5.1.1c
- Indien zou worden afgeweken van dit voorstel, en bijvoorbeeld worden gekozen voor een kortere vervangingstermijn, dan zou dit goed gemotiveerd moeten worden. Omdat nu wordt voorgesteld om aan te sluiten bij het voorstel van de telco's, kan de motivering beknopter.

Proces

- [REDACTED] 5.1.2f
- [REDACTED] en Dialogic hebben de telco's een aantal verduidelijkingsvragen gesteld, [REDACTED] 5.1.2i
- De plannen zijn door [REDACTED] en Dialogic beoordeeld op volledigheid ten aanzien van de te beschermen belangen en noodzakelijke doorlooptijd in verband met de continuïteit. 5.1.2i

Bevindingen

-  5.1.1c
- De bevindingen van Dialogic en  zijn: 5.1.2i
 - dat de werkwijze in de plannen niet onlogisch of onrealistisch is, 5.1.1c
 - dat in de plannen een (voor de telecomsector) gangbare fasering /termijnen wordt gehanteerd,
 - dat alle kritieke onderdelen worden geadresseerd, en

- o dat met de plannen invulling gegeven wordt aan de van overheidswege gestelde verplichting.
- Gezien bovenstaande adviseren [REDACTED] en Dialogic en AT om de termijnen [REDACTED] over te nemen.

5.1.2i
5.1.1c

- [REDACTED]
[REDACTED]
[REDACTED]

5.1.1c
en
5.1.2i

Rubricering van de bijlage met kritieke onderdelen

- In de concept beschikking wordt voorgesteld om de bijlage bij de beschikking, met daarin de opsomming van kritieke onderdelen, net zoals gedaan is voor de huidige lijst met kritieke onderdelen, op Dep-V te rubriceren.
- Mede op basis van afstemming met en binnen de centrale juridische directies van EZK en JenV kan worden geconcludeerd dat dit mogelijk is. In de beschikking zal nog een korte motivering, om welke redenen die rubricering aangewezen is, worden toegevoegd.
- In de begeleidende brief die meegestuurd wordt met de beschikking aan de telco's, zullen de telco's nogmaals worden gewezen op de vertrouwelijkheid van de lijst met kritieke onderdelen en de manier waarop zijn daarmee om moeten gaan.

Communicatie rondom beschikkingen/zachte landing

- [REDACTED]
[REDACTED]
[REDACTED] Om dit tegen te gaan is het noodzakelijk dat de beschikkingen zoveel mogelijk vertrouwelijk behandeld worden.
- Uitgangspunten voor communicatie richting markt en maatschappij zijn:
 - o Geen actieve communicatie/publicatie vanuit de overheid
 - o Herbevestiging van uitgangspunten communicatie richting land en bedrijf (zie eerder verspreide stukken communicatielijn, bezien of deze t.z.t. nog actueel zijn)
 - o Telco's verzoeken om de beschikkingen vertrouwelijk te behandelen, ook al worden ze niet voorzien van rubricering.

5.1.2i

- Verder zal de Kamer middels een vertrouwelijke technische briefing worden geïnformeerd.

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2a

Budgettaire consequenties

- De keuze van de vervangingstermijn heeft direct gevolgen voor de hoogte van de nadeelcompensatie. [REDACTED]
[REDACTED]
[REDACTED]
- Bij grotere financiële gevolgen dan gereserveerd moet EZK dit z.s.m. in kaart brengen en een dekkingsvoorstel met FIN afstemmen via het reguliere budgettaire proces.
- Vanuit financieel perspectief is naast het oogpunt van de nadeelcompensatie voor de telco's ook mogelijke schadeclaims van derdebelaagden, zoals de leveranciers, van belang. Hier zijn op dit moment nog geen middelen voor gereserveerd, omdat wordt aangenomen dat het besluit rechtmatig is, en de rechter geen schadeclaim zal toewijzen.

5.1.2f

Vervolgproces en nadeelcompensatie

- Zie hieronder een planning op hoofdlijnen. Belangrijkste is dat het proces bestaat uit eerst een voornemen dat aan partijen wordt verstuurd, welke vervolgens kunnen reageren met een zienswijze, en die punten worden dan meegenomen in de definitieve beschikking (feb 2021). Vervolgens kunnen belanghebbenden hier bezwaar en beroep tegen instellen.
- Als het definitieve besluit (het schadeveroorzakende besluit) is genomen, dan kunnen de telco's vervolgens nadeelcompensatie aanvragen, waarop wederom hetzelfde proces volgt met een voornemen, zienswijze, en besluit.
- De telco's hebben reeds de gelegenheid gehad om te reageren op een concept nadeelcompensatiekader. Deze reactie wordt momenteel verwerkt tot een definitief nadeelcompensatiekader door de landsadvocaat en twee gerenommeerde economen. Dit kader zal worden afgestemd met Financiën gezien de budgettaire consequenties. Het kader wordt samen met de beschikking vastgesteld in de MR in februari.

Planning op hoofdlijnen

	Beschikking	Nadeelcompensatie
Aanvraag	-	Mrt 2021
Voornemen	Okt 2020	Mei 2021
Zienswijze	Nov 2020	Jul 2021
Afstemming interdepartementaal (incl MR)	Feb 2021	Sep 2021
Besluit	Feb 2021	Sep 2021



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep.-VERTROUWELIJK
TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon
T 070 751 50 50

Datum
6 oktober 2020

Ons kenmerk
-

Bijlagen

nota

Voortgang structurele samenwerking

Gevraagd

- Akkoord gaan met de procesbeschrijving van de structurele samenwerking (bijlage 6) en kennisnemen van de voortgang.

Toelichting

In bijlage 6 vindt u een procesbeschrijving van de structurele samenwerking; een samenwerking waarin overheids- en telecompartijen op structurele basis informatie delen over te beschermen belangen, dreigingen, technologische ontwikkelingen en weerbaarheid. Indien nodig worden hier gezamenlijke risicoanalyses uitgevoerd en aanvullende maatregelen voorgesteld om telecomnetwerken te beschermen tegen dreigingen vanuit geavanceerde (statelijke) actoren.

5.1.2i

Voortgang algemeen

In het eerstvolgende overleg worden o.a. de sancties van de VS en de impact hiervan op de Nederlandse telecomnetwerken besproken. Agentschap Telecom heeft hier in een eerder stadium al onderzoek naar gedaan; op basis hiervan wordt besproken wat de vervolgstappen zijn.

5.1.2i

Voortgang technische werkgroep

In de volgende TFEV wordt u hier verder over geïnformeerd.

5.1.1b

Op korte termijn zal de technische werkgroep zich ook buigen over nieuwe beveiligingsmaatregelen.

5.1.1c

Dep.-**VERTROUWELIJK**

Datum
6 oktober 2020

Ons kenmerk

5.1.1c

[REDACTED]

Deelprojecten

Een aantal elementen binnen de structurele samenwerking worden verder uitgewerkt in deelprojecten. Dit betreft de informatiedeling tussen partijen (o.a. vertrouwensfuncties en faciliteiten om informatie uit te wisselen), investeringszekerheid (n.a.v. rapport Dialogic) en [REDACTED]. Hierover wordt u op een later moment geïnformeerd.

5.1.2i



Dep. **VERTROUWELIJK**
TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

5.1.2e

Datum
30 september 2020
Ons kenmerk

nota

Inzet formatie economische veiligheid en cybersecurity

Gevraagd

- Kennisnemen van de uitkomsten van de probleemanalyse, de thema's van de fiches en de vervolgstappen.

Toelichting

In de TFEV van 26 juni 2020 is gesproken over de gewenste inzet op economische veiligheid en cybersecurity bij een nieuw kabinet. Om te komen tot een gezamenlijk beeld van deze inzet is afgesproken een probleemanalyse uit te voeren op het gebied van economische veiligheid. Voor cybersecurity was deze analyse niet nodig omdat dit al door het schrijven van de kabinetsreactie op het WRR-rapport 'Voorbereiden op digitale ontwrichting' is gebeurd. De probleemanalyse voor economische veiligheid vindt u in de bijlage.

Thema's

Op basis van de probleemanalyse zijn een aantal thema's gedestilleerd. Voor ieder thema wordt een fiche geschreven, waarbij er drie varianten in ambitieniveaus worden uitgewerkt: huidige ambitie, uitbreiding van de huidige ambitie en 'next level' ambitie. De fiches die vallen onder economische veiligheid worden binnen de werkgroep van de Taskforce Economische Veiligheid opgesteld en afgestemd. Voor de fiches vallend onder cybersecurity geldt dat deze worden opgesteld en afgestemd binnen het IOCS en DOCS. De fiches voor de overkoepelende thema's worden in beide werkgroepen uitgewerkt.

Economische veiligheid

1. Vergroten eigen kracht (EZK)
2. Beschermen technologie en kennis (OCW)
3. Voorkomen ongewenste zeggenschap (EZK)
4. Informatiedeling, risicoanalyses en adviezen vitale processen (NCTV)
5. Veilige inkoop en aanbesteding rijksoverheid (en vitaal) (BZK en DEF)
6. Veilige communicatie rijksoverheid (encryptie) (BZK)

Cybersecurity

7. Vitaal (NCTV)
8. Overheid (BZK)
9. Niet-vitale organisaties en burgers (EZK)
10. Gemeenschappelijk fundament cyber: oefenen & testen, productontwikkeling en kennis (EZK en NCTV)
11. Kunnen leveren van slagkracht (DEF)

Dep.-VERTROUWELIJK

Overkoepelende thema's

- 12. Versterken inlichtingenpositie (BZK en DEF)
- 13. Versterken kennisbasis overheid gevoelige technologie en afhankelijkheden (EZK)
- 14. Strafbaarstelling spionage (NCTV)
- 15. Internationale samenwerking (BZ)

Datum

30 september 2020

Ons kenmerk

PSD

Vervolg

In de TFEV van 5 november worden de fiches inhoudelijk besproken en wordt bepaald welk ambitieniveau gewenst is. Voor het eind van het jaar vindt hierover besluitvorming plaats in de ACEV en MCEV.



M1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

28 oktober 2020

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	5 november 2020, 12:00-13:30 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Verslag TFEV 14 oktober 2020 [REDACTED] 5.1.2i

3. [REDACTED] 5.1.1b + 5.1.2a + 5.1.2i

4. Bijeenkomst [REDACTED] (stuk volgt nog) 5.1.2a

5. Internationaal/Europees

6. Parlementair

7. Rondvraag en sluiting

Dep. **VERTROUWELIJK**



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

M6

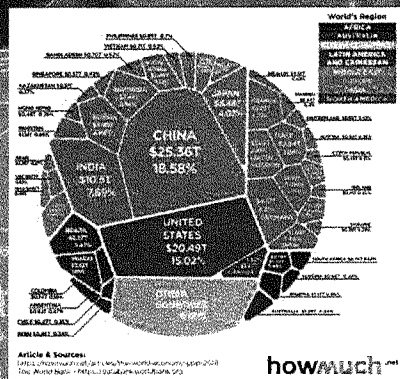
Case presentation 5G

Cybersecurity and supply chain
security in critical infrastructure

9 October 2020



5G Security: Main catalyst in forming a Dutch economic security policy



NATIONAL SECURITY
INTELLIGENCE
PEACE
Cyberwar
Strategy
Propaganda
Nuclear
Extremism
digital sovereignty
Information
Bioweapons
VERIFICATION

Before 5G case: National security (National competence) and economic policy (EU) were separate spheres

After 5G case: National security and economic policy have become irrevocably intertwined.

Result: Dutch economic security policy - balancing national security concerns with economic interests and broader geopolitical considerations

Current sense of urgency: Action is needed on national and EU level to address national security concerns and strategic economic challenges.



5G Security case (proces)

- **Start:** [REDACTED]
[REDACTED] 5.1.1b
- **Formation of Task Force Economic Security:** high level coördinating and advisory council on economic security. First task to adress 5G security but rapidly expanding agenda.
- **Three stages in proces:**
 1. Risk assessment (technical and security analysis)
 2. Impact assessment (security, economic, financial and geopolitical)
 3. Recommendations to the Council of Ministers and letter to parliament: balance between national security and economical interests

• [REDACTED]

5.1.2a

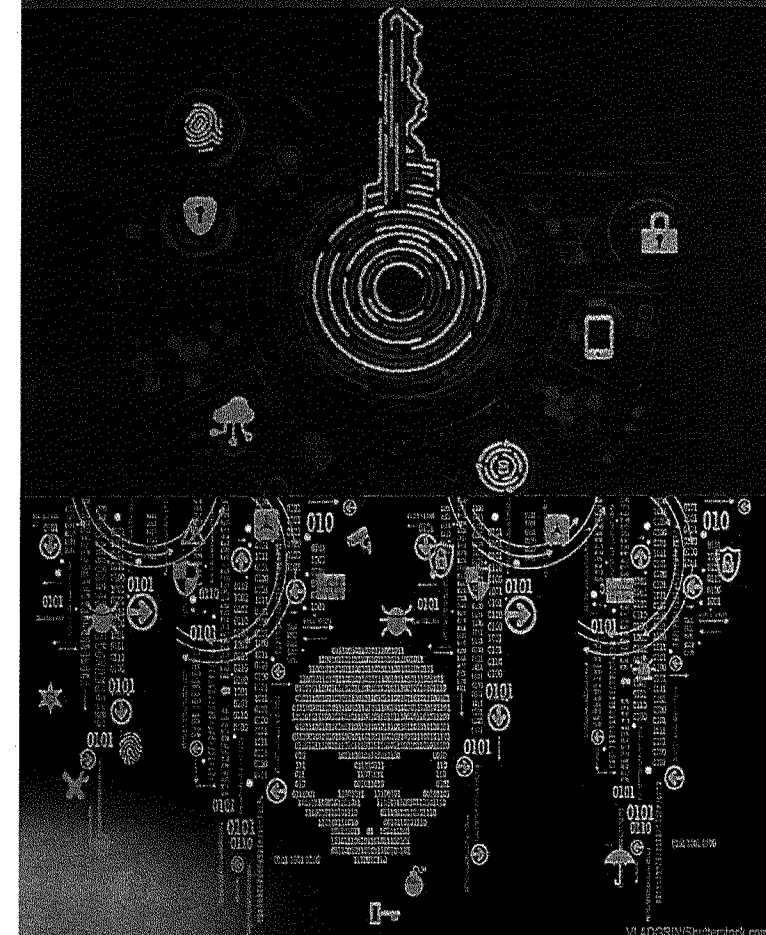


Findings Risk Analysis: the keys to the Kingdom in peril?

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

5.1.1b

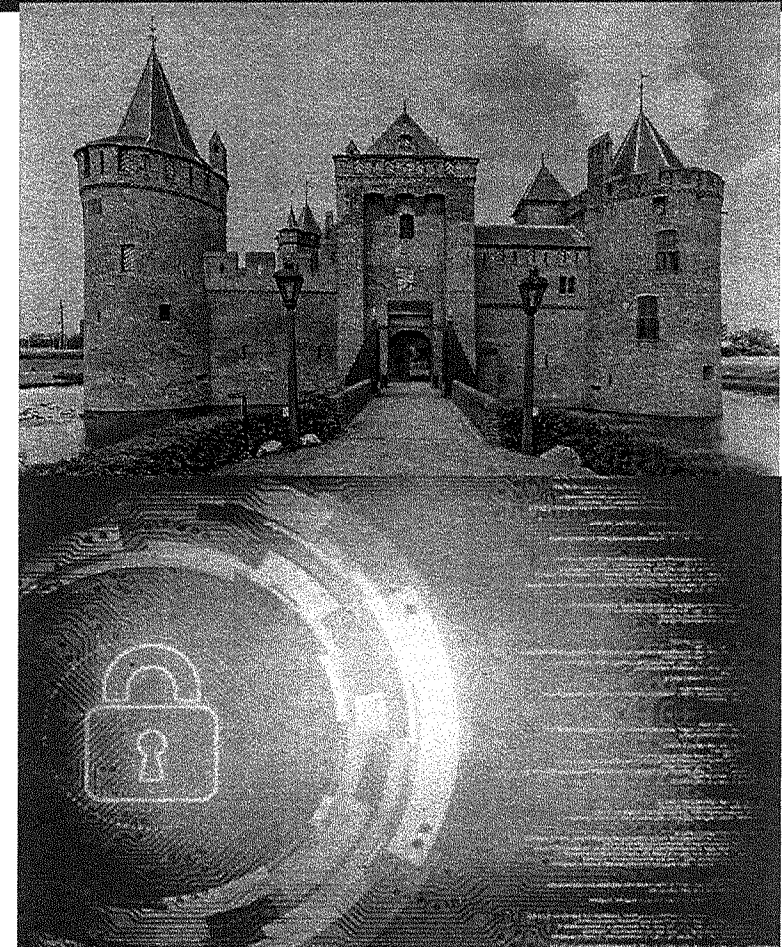
5.1.1b





5G security measures to manage and mitigate risks

- Telecom providers will be obliged to put additional security measures in place in order to increase existing resilience
- Extra stringent requirements for suppliers of products and services to critical components of the telecom network are set out.
- Structural and continuous approach to assess risks for 5G-networks in cooperation with telecom providers, whereby technical and threat-related developments will be considered in conjunction with one another.





Three strategic challenges

1. Limited knowledge and expertise on the national security impact of new and emerging technologies;
2. A limited number of suppliers with large price-quality disparities; A possible growing problem in other strategic areas as a result of industrial policy.

5.1.2a

3.

5.1.2a

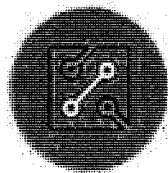




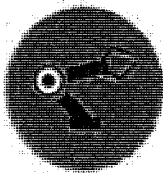
Proposal 1: Organise knowledge and expertise on technological developments for early warning

5.1.2a

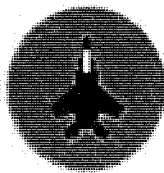
The 10 key sectors



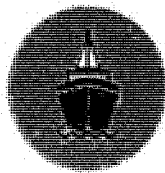
New information
technology



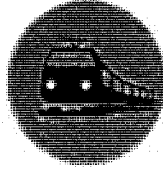
Numerical
control tools



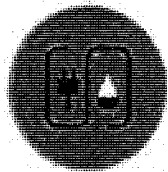
Aerospace
equipment



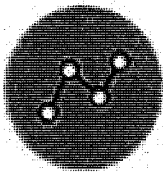
High-tech ships



Railway
equipment



Energy saving



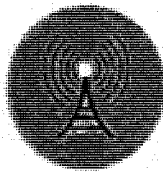
New
materials



Medical
devices



Agricultural
machinery



Power
equipment

- Establish an ongoing European research and monitoring project into the security risks and challenges for EU countries, posed by new and emerging technologies.
- Starting with European critical infrastructure (energy and telecommunications).
- The insights from this project must give EU countries the capability to pre-emptively determine ways to address these security risks.



Proposal 2: Reduce and prevent unwanted strategic dependencies

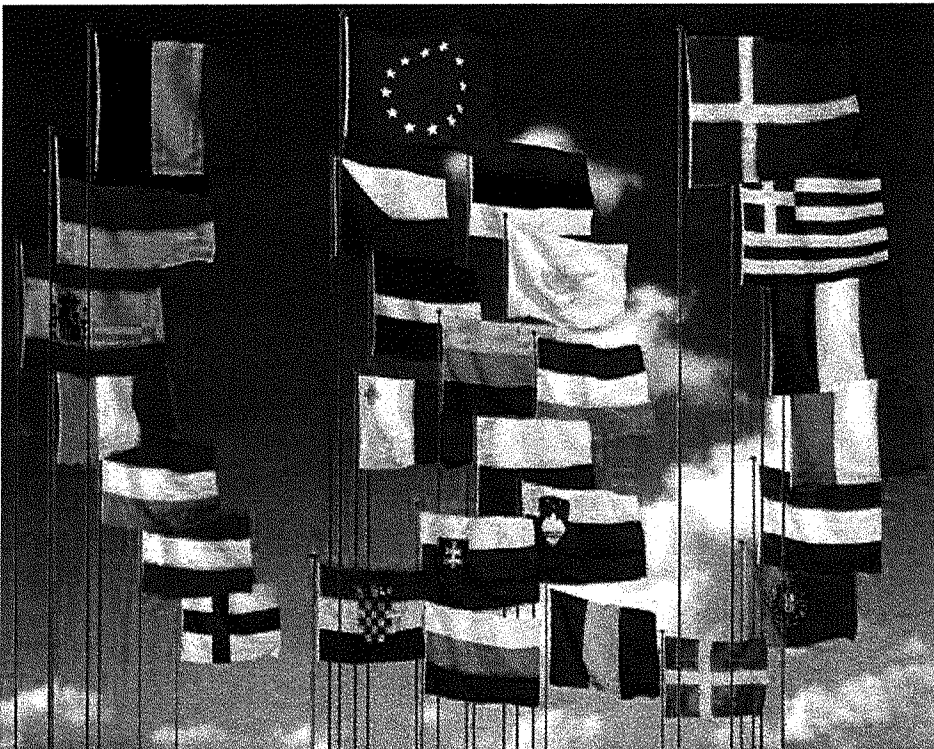
- Determine from a European and national security perspective which industrial products and/or which know how should be protected or unrestricted access guaranteed for EU members to prevent unwanted strategic dependencies.
- For this purpose an analytic framework for determining sensitive production and knowledge areas could be developed.





Proposal 3. Establish a high level EU coördinating mechanism to organise EU cohesion on sensitive security issues

- Establish a high level cooperation and coordination mechanism, specifically aimed at quickly organising EU cohesion and solidarity on sensitive security issues like 5G and Covid19
- In this regard we should also look at smaller coalitions within the EU as a start and, the possibility of cooperation of this group with non EU partners.





Ministerie van Economische Zaken
en Klimaat

M7

Case Study Integrated Photonics in the Netherlands

A state intervention to retain a key technology

5.1.2e

Directorate Innovation &
Knowledge – Ministry of Economic Affairs &
Climate Policy The Netherlands



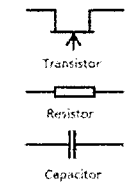
Introduction

- Integrated photonics is considered as an important, promising but fragile ecosystem in NL
- Government is committed to strengthen this ecosystem and supports the public private partnership PhotonDelta.
- The ecosystem builds on unique R&D from technical universities in Eindhoven and Twente with all parts of the chain represented in NL
- Key player is the chip maker, Eindhoven based scale up Smart Photonics, an assential part of the chain.
- When this company was about to be lured to Asia, the Dutch government decisively stepped in with 20 million euros



What is integrated photonics?

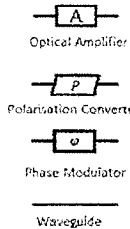
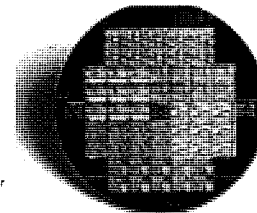
- The manipulation of light on a single chip
- Integration of **multiple** photonic **functions** on a Photonic Integrated Circuit (PIC), allowing these chips to become **smaller, lighter, faster, cheaper, and greener**, as transferring data by light costs less energy than by electrons.
- This technology is a key enabler for a wide range of applications and innovations in data transfer and sensor applications.
- The Netherlands is currently a technological leader in this field.



Electrical connector

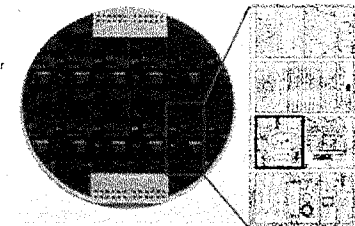
Electronic integration

Silicon ICs ~1979



Photonic integration

Photonic ICs ~2014



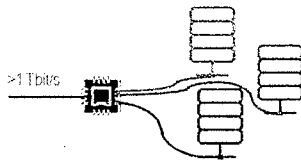


The benefits of integrated photonics: solve major societal challenges

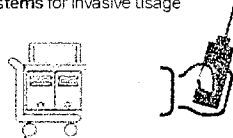
Scalability leads to cost reductions



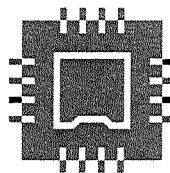
Processing fiber optic signals in a **fast, reliable and energy-efficient** way enables communication applications with high bandwidth to become cheaper



A compact method of **light manipulation** that can be used to reduce the size of **medical scanners and sensor systems** for invasive usage



INTEGRATED PHOTONICS



Small chips that process light signals with **speed, accuracy and reliability**



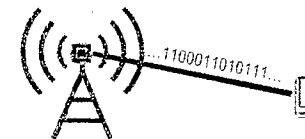
Selection of applications in which
The Netherlands has a strong position

...AND MANY MORE APPLICATIONS!

Unique properties lead to new technical possibilities



The processing of radio signals for **5G network** via beamforming technologies could be **sped up by a factor of 1,000 to 1 million** when performed with an integrated optical-wireless fabric



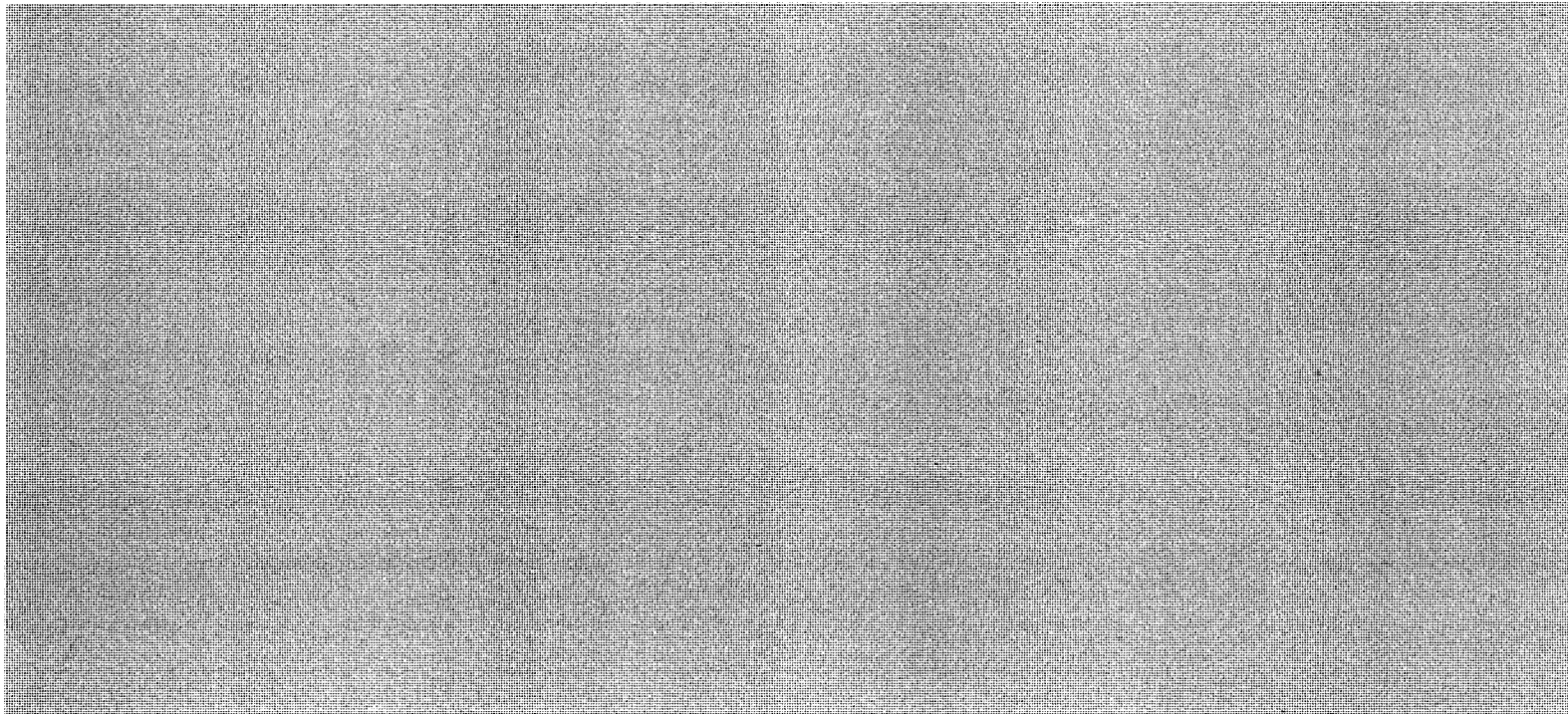
Fiber Optics Sensor systems for **real-time accurate distributed structural health monitoring** in large/high-duty objects and (composite) structures, like airplane wings



The impact is comparable to the impact that microelectronics had (semiconductors industry) on electronics in the last 40 years



Ecosystem operates in a wide context of national and international stakeholders – with all parts of value chain from design to module represented in NL



5.1.2a +

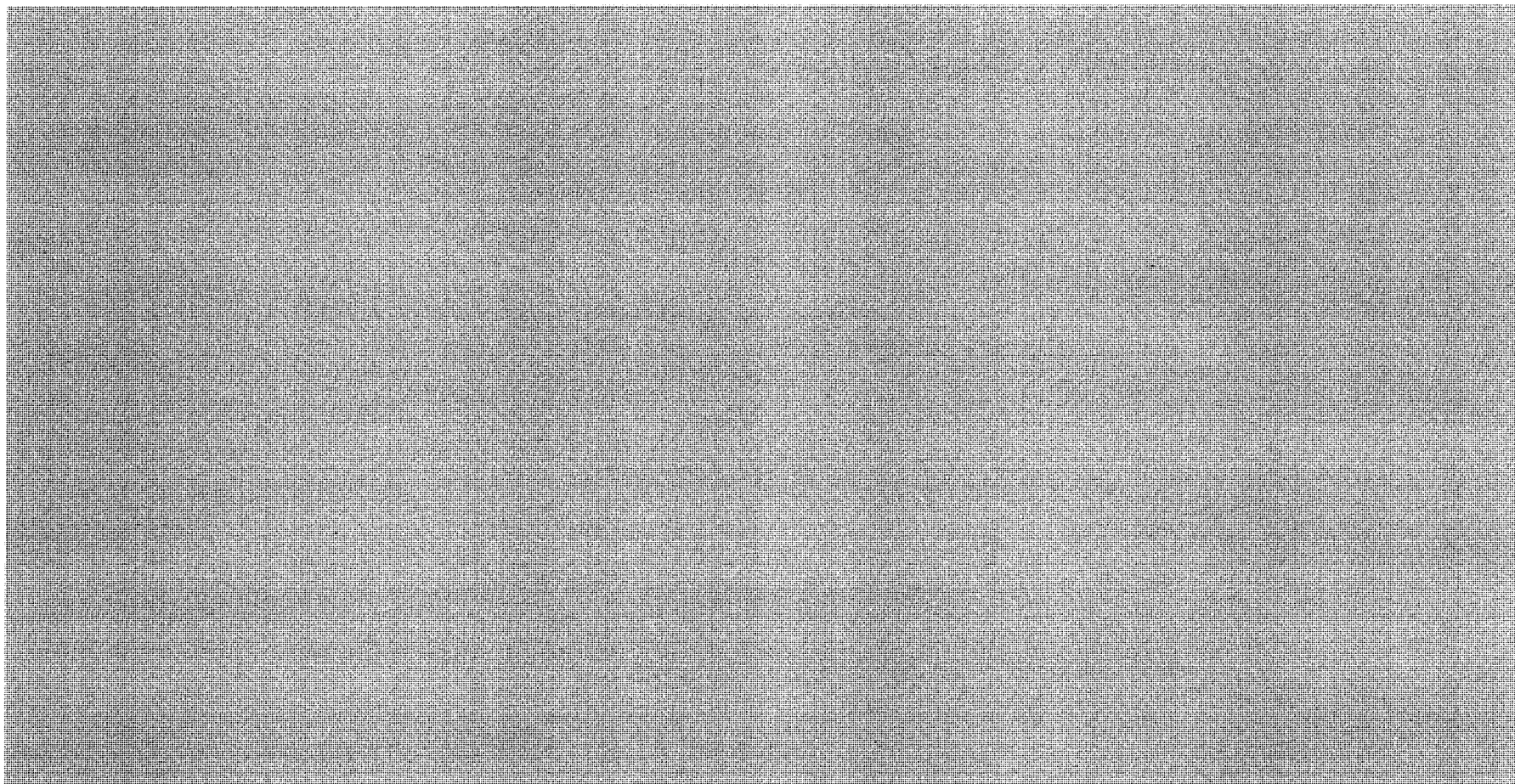
5.1.2i



AND CENTRALLY WITHIN EUROPEAN PHOTONIC ECOSYSTEM

5.1.2.a +

5.1.2i





SWOT Analysis: threat of takeover & relocation

STRENGTHS

- Companies with good global potential and market access
- Attractive ecosystem for end-users
- Strong knowledge base
- Available resources and supply chain
- Good European and global network

OPPORTUNITIES

- PIRC as development organization for innovations in PIC technology and system integration
- CIRC (packaging) for industrial packaging expertise
- Startup program, stimulating new entries
- Slow but stable growth in ecosystem, triggering interest of industrial parties

WEAKNESSES

- Not enough startups, new companies & spin-offs
- Knowledgebase is fragmented, no common research agenda
- Critical mass of the total ecosystem
- System integration function not at the required level
- Little involvement yet from corporate industries

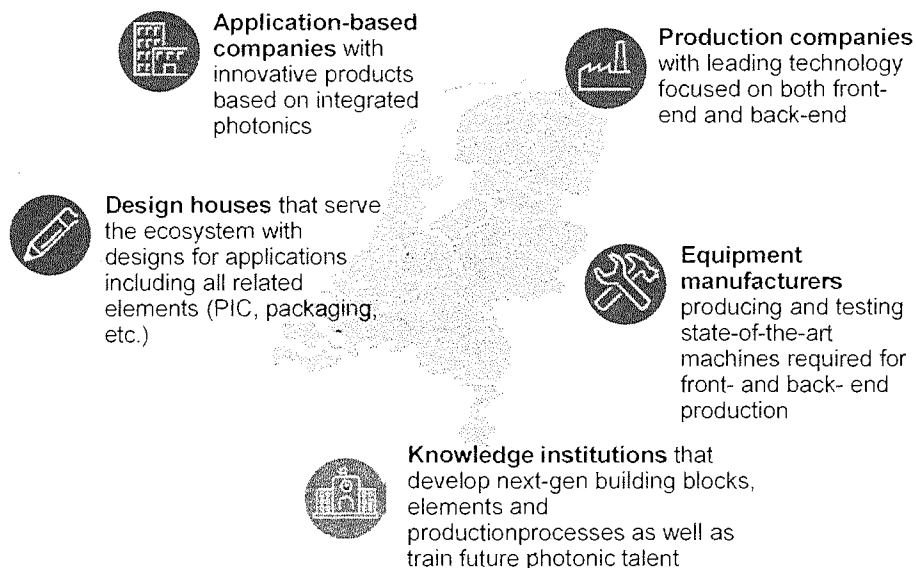
THREATS

- Speed of development to a mature supply chain (NB speed considered more important than IP protection)
- Upscaling requires large capital investments
- **Take-overs with relocation**





National ambition

Building an industrial ecosystem that includes all players from the integrated photonics value-chain



Targeted impact

-  **>25 companies** in integrated photonics generating an annual turnover of **EUR 1 mld**
-  Structural and direct employment opportunities for **4,000 fte** within those companies, with many more indirect opportunities outside
-  Business activity in the Netherlands for both **applied photonics** as well as **design, production, and production technology**
-  Applications must serve public interest, such as **reducing energy footprint**, reducing **healthcare costs**, and improving the **competitive position** of the Netherlands



Response by Dutch Government

- National ambition to develop industrial ecosystem that includes all players from the integrated photonics value chain – under threat
- Careful background check of Asian player.
- Threat of takeover considered undesirable for the continuity of the Dutch ecosystem and for national security in the longer term.
- National funding secured, state loan used as leverage for an additional investment by national consortium-partners
- Intervention fits in new proposed legislation on screening FDI.



A European approach

- By coordinating European R&D, funding and (manufacturing) expertise a mature and sustainable European industry for photonic chips can be built
- Upscaling of current production facilities preferable with commercial loans from European investors
- For future developments and testing of new processes with industry an imec model with public funding is needed.
- Make optimal use of Horizon Europe funding (Photonic partnership) and explore the use of RRF and of IPCEI
- Have defensive EU measures – both legislation on FDI screening and public funding - in place to prevent take overs & relocation



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. ~~VERTROUWELIJK~~

Contactpersoon

5.1.2e

Datum

19 november 2020

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	25 november 2020, 16:00-17:30 uur
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Verslag TFEV 5 november 2020

5.1.2i

3. Formatieclaim economische veiligheid, cybersecurity en vitaal

Stukken: Nota Formatieclaim economische veiligheid, cybersecurity en vitaal
en bijlagen 1-5

4.

5.1.1b + 5.1.2a
+ 5.1.2i

5. Structurele samenwerking

5.1.2i

6. Internationaal/Europees

7. Parlementair

8. Rondvraag en sluiting



de TFEV

Datum

19 november 2020

Ons kenmerk

NCTV

Bijlagen

1. Hoofdboodschap
2. Kapstok samenvoegen claims
3. Cybersecurity claim
4. Economische veiligheid claim
5. Economische analyse

nota

Formatieclaim economische veiligheid, cybersecurity en
vitaal

Aanleiding

In de TFEV van 26 juni 2020 is gesproken over de scope van de formatieclaim en is besloten deze breed te houden: economische veiligheid, cybersecurity en vitaal. Hierbij is afgesproken dat de eerste uitwerking van de twee claims in aparte trajecten zal plaatsvinden. Dit is afgerond. Er liggen nu twee losse concept claims en de volgende fase is het samenvoegen hiervan. In de TFEV ligt een voorstel hiertoe voor ter bespreking.

Gevraagd besluit

1. Gaat u akkoord met de bijgevoegde geïntegreerde boodschap en kapstok als basis voor verdere uitwerking van de boodschap?
2. Kunt u instemmen met het proces hiertoe zoals beschreven onder punt 1c.?
3. Gaat u akkoord met het verder aanscherpen van de financiële onderbouwing middels de werkwijze zoals beschreven onder punt 2b.?
4. Gaat u akkoord met het bespreken van de uitkomst van het vervolg in de ACEV van 12 januari in plaats van 3 december?

Toelichting

1. Proces samenvoegen claims

a. Huidige stand van zaken

- De EV claim is uitgewerkt door de leden van de voorbereidingsgroep TFEV en de cybersecurity claim door de leden van het interdepartementaal overleg cybersecurity (IOCS).
- De maatregelen in beide claims zijn concept en moeten op verschillende punten nog verder worden uitgewerkt maar de globale richting en scope is al duidelijk.
- Het directeurs overleg cybersecurity (DOCS) heeft aangegeven dat de hoofdboodschap nog onvoldoende de urgentie op cybersecurity schets. Dit kan in een volgende versie worden meegenomen.

b. Samenvoegen claims

- In bijlage 1. een eerste voorstel opgenomen voor de hoofdboodschap. Het uitgangspunt van de hoofdboodschap is dat we door veranderende geopolitieke verhoudingen, toenemende dreiging van statelijke actoren en vergaande digitale afhankelijkheid, maatregelen moeten nemen om Nederland ook in de toekomst stabiel en welvarend te houden.

- Op sommige onderwerpen hebben de twee claims veel overlap. O.a. de maatregelen voor vitale infrastructuur en operationele slagkracht. Bij andere onderwerpen zoals landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden en tegengaan van spionage is deze overlap minder aanwezig.
- De afgelopen periode is er veel aandacht geweest voor het tegengaan van versnippering. Het samenvoegen van de fiches draagt bij aan een geïntegreerd beleid op het terrein van cybersecurity, EV en vitaal. Dit is noodzakelijk voor een succesvolle centrale aanpak vanuit de eigen rollen en verantwoordelijkheden.
- In bijlage 2. is een eerste voorstel gedaan voor het samenvoegen van de claims.

Datum
19 november 2020
Ons kenmerk
NCTV

c. Proces

- Zowel de kapstok als de overkoepelende boodschap zijn eerste concepten.
- Het DOCS heeft de behoefte uitgesproken om de hoofdboodschap middels een ambtelijke schrijfgroep verder uit te werken.
- Om snel te kunnen werken wordt voorgesteld deze schrijfgroep te beperken tot één voldoende senior persoon per organisatie die zicht heeft op zowel cybersecurity als economische veiligheid. Zij zullen kritisch kijken naar de overkoepelende boodschap en de kapstok en dit verder aanvullen vanuit de verschillende departementen. De NCTV zal het voorzitterschap van de schrijfgroep op zich nemen.
- EZK heeft voor de hoofdboodschap een economische analyse (zie bijlage 5.) opgesteld waarmee de economische impact van het niet acteren om de geschetste risico's inzichtelijk wordt voor economische veiligheid. Het schrijfteam kan deze analyse betrekken bij het opstellen van de hoofdboodschap.
- Parallel aan het samenvoegen worden de verschillende maatregelen verder uitgediept en eventuele knelpunten besproken met de relevante partijen.
- De samengevoegde claim wordt in de ACEV van 12 januari besproken.

2. Aanscherpen financiële onderbouwing

a. Huidige stand van zaken

- Beide claims komen momenteel uit op ongeveer 400 miljoen. Een samengevoegde claim wordt daarmee ongeveer 800 miljoen. Enkele departementen hebben aangegeven punten nog nader te verkennen, dus het bedrag kan nog hoger worden. In het DOCS is de wens uitgesproken om de rationale achter de bedragen te verhelderen.
- Het doel is om de bedragen stevig te onderbouwen, scherp te krijgen of alle maatregelen bijdragen aan de doelstellingen van de claim en om handvatten te bieden voor een mogelijke prioritering. Dat vergt een ordeningsprincipe. Hiertoe wordt onderstaand beoordelingskader voorgesteld. In de TFEV kan besproken worden welke punten nog meer meegenomen moeten worden in het beoordelingskader.

b. Voorgestelde werkwijze: beoordelingskader claims formatiefiche

Verzoek is aan de departementen om nadat de cybersecurity en EV claims zijn samengevoegd, de eigen onderdelen van de claim te verhelderen langs de onderstaande lijn.

Fase 1: Langs lopen ingediende claims op de volgende punten:

Wat is de effectiviteit van de claim?

Een beoordeling van de effectiviteit gaat in op de mate waarin het doel van een claim bij uitvoering gerealiseerd wordt. Bekeken kan worden in hoeverre

claims concreet bijdragen aan de realisatie van het doel van de verschillende deelonderwerpen.

Wat is de doelmatigheid van de claim?

Een beoordeling van de doelmatigheid gaat over de vraag of het verwachte effect in verhouding staat tot de kosten die hiervoor gemaakt gaan worden. Een goede 'p x q' onderbouwing is daarbij belangrijk. Met deze onderbouwing kun je een inschatting maken in hoeverre, bijvoorbeeld, het aantal gevraagde fte in een claim realistisch is in relatie tot het beoogde doel. Onder doelmatigheid kan ook worden beoordeeld of binnen een claim voldoende wordt samengewerkt, omdat betere samenwerking door grotere efficiëntie leidt tot minder inzet van middelen.

Draagt de claim bij aan een heldere rolverdeling en het tegengaan van versnippering?

De roep om regie en het tegen gaan van versnippering in het cyber- en EV-domein tegen te gaan is een luide. De voorgestelde maatregelen in de fiches en de claims zouden gehoor moeten geven aan die roep door bij te dragen aan integratie en gezamenlijkheid in werkwijze.

Komt de claim voort uit een harde toezegging of niet?

Hiermee wordt een onderscheid gemaakt tussen de claims die voortkomen uit een harde toezegging aan de Kamer/samenhangen met ingezet beleid waar nog onvoldoende/geen dekking voor is en de claims op basis van nieuw beleid.

Wat gebeurt er als de claim niet gehonoreerd wordt?

Een beoordeling op dit punt helpt om de risico's in kaart te brengen en daarmee de urgentie van de claims te benadrukken. EZK heeft bij de economische analyse een format opgesteld die fichehouders kunnen gebruiken om deze urgentie nader inzichtelijk te maken.

Datum

19 november 2020

Ons kenmerk

NCTV

Fase 2: Na het aanscherpen van de financiële onderbouwing en bespreking hiervan in de ACEV in januari doen we een voorstel voor prioritering door middel van het uitwerken van verschillende scenario's. Hiermee kunnen we ons voorbereiden op een situatie waarin maar een deel van de geclaimde middelen wordt toegekend. Dit wordt besproken in de ACEV van februari.

Een veilige welvarende samenleving, klaar voor de toekomst

Voorstel hoofdboodschap Vitaal, Economische Veiligheid en Cyber

Onze samenleving en economie zijn sterk verweven met geopolitiek en veiligheid. Dreigingen zijn groter, complexer en veelomvattender dan voorheen. Onze traditionele openheid biedt kansen, maar de combinatie met verslechterde geopolitieke verhoudingen maken ons kwetsbaar en beperken onze huidige en toekomstige kansen. De afhankelijkheid van digitale systemen die we als samenleving hebben opgebouwd zorgt ervoor dat digitale onveiligheid ons harder dan ooit raakt en vergroot onze kwetsbaarheid. Door de impact van COVID-19 is dit alleen nog maar groter geworden.

Momenteel kan de overheid deze uitdaging onvoldoende het hoofd bieden. Dit vereist een aanpak waarin economie, digitalisering en veiligheid in samenhang gezien worden zodat de economie kan floreren en de veiligheid tegelijkertijd vergroot wordt. Dit vraagt om investeringen met als doel onze open en concurrerende samenleving toekomstbestendig te maken.

Weerbaarheid tegen dreigingen, veerkracht bij incidenten

De geopolitieke situatie leidt ertoe dat andere landen in hun handelen een dreiging vormen voor de nationale veiligheid, de democratische rechtsstaat, en daarmee voor de economie en de samenleving. De weerbaarheid tegen deze dreigingen moet op brede schaal versterkt worden. Dit vereist een veerkrachtige samenleving bij incidenten, maar nog belangrijker is het versterken van de weerbaarheid van onze economie, democratie, maatschappij en vitale infrastructuur. De dreiging uit zich onder meer in de inzet van economische middelen om kennis en informatie te bemachtigen of invloed te verkrijgen door te investeren in bedrijven in Nederland, en digitale aanvallen die een risico vormen op (economische) spionage, voorbereidingshandelingen voor sabotage en beïnvloedingscampagnes.

Autonomie om kennispositie te borgen, afhankelijkheden te beperken en concurrentiekracht te stimuleren

De vestiging van hightech-bedrijven en het goede academische klimaat zorgen ervoor dat Nederland een unieke kennispositie heeft. Om deze positie te behouden is inzicht noodzakelijk in welke kennisgebieden wij moeten beschermen en welke sensitieve technologieën wij moeten stimuleren. Vaak zijn er in deze gebieden afhankelijkheden van derde landen. Om onze unieke positie te behouden én onze autonomie te vergroten is inzicht in waardeketens essentieel, en actie om ongewenste strategische afhankelijkheden te beperken noodzakelijk.

Fundament van hoogwaardige kennis en betrouwbare infrastructuur

Topsectoren, onderscheidende kennis en een betrouwbare vitale infrastructuur vormen het fundament om de kracht van Nederland tot zijn recht te laten komen. Dit fundament heeft versterking nodig om de complexe dreigingen en het huidige tijdsvak door te komen. Dat vraagt om adaptiviteit en flexibiliteit in de aanpak. Dreigingen en geopolitieke verhoudingen zijn aan steeds snellere verandering onderhevig. Ook technologie ontwikkelt zich razendsnel. Onze aanpak moet in minimaal hetzelfde tempo meegaan om onze samenleving weerbaar en veerkrachtig te kunnen laten groeien, de economie toekomstbestendig te maken en de impact van dreigingen te beperken. Dit vereist assertiviteit in de aanpak, zowel op nationaal niveau als met Europese en internationale partners. Autonomie waar het moet, samenwerking waar het kan.

Voorstel opbouw formatie claim cybersecurity, economische veiligheid en vitaal

Voor een toekomstbestendig Nederland is het nodig om te investeren in:

1. Verbeteren inlichtingenpositie en vergroten handelingsperspectief t.a.v. digitale dreigingen en economische veiligheid

Om het Nederlandse handelingsperspectief in het digitale domein te vergroten, is gedegen en zorgvuldig onderzoek naar deze dreiging onontbeerlijk. Daarnaast is deze kennis nodig om passend en effectief te kunnen interveniëren en reageren en daarmee de kosten van ongewenst gedrag aan de zijde van kwaadwillende actoren te verhogen. Toenemende casuïstiek illustreert daarnaast dat de omvang en diversiteit van de economische veiligheid (EV) dreiging toeneemt. De vraag naar EV-inlichtingen vanuit de publieke sector, bedrijven en kennisinstellingen neemt hierdoor toe.

Bouwblokken uit de huidige claims:

- Versterken inlichtingenpositie EV
- Vergoten slagkracht cyber
- Diplomatiek responskader
- Strafbaarstelling spionage

2. Een veerkrachtige vitale infrastructuur

De vitale aanbieders bieden essentiële diensten voor de continuïteit van de economie en maatschappij. Onderbreking of uitval van een dergelijke dienst kan leiden tot ernstige maatschappelijke ontwrichting in Nederland. De dreiging vanuit statelijke actoren, digitalisering en toenemende ketenafhankelijkheden vragen om diepgaande sectorale expertise om de juiste maatregelen te kunnen treffen om de beveiliging van de vitale infrastructuur naar een nog hoger niveau te tillen.

Bouwblokken uit de huidige claims:

- Expertise Teams en Expertise eenheid Vitaal
- Vitaal cyber : toezicht, toekomst vitaal begrip, informatieplatform vitaal
- Testen cyber
- Ongewenste zeggenschap

3. De schokbestendige samenleving

Schokbestendigheid over de hele breedte van de samenleving draagt bij aan de weerbaarheid van vitaal. De overheid kan nooit 100% veiligheid garanderen maar moet wel een omgeving creëren waarin iedereen weet waar men terecht kan voor informatie over de dreiging en de te nemen maatregelen.

Bouwblokken uit de huidige claims:

- Niet-vitaal cyber: landelijk dekkend stelsel, zorg, ocw
- Oefen cyber

4. Een weerbare overheid

De gesignaleerde dreiging richt zich zeker ook tegen de overheid zelf op alle lagen. Aanvullende investeringen in informatiebeveiliging en continuïteit van de overheid is daarom noodzakelijk.

Bouwblokken uit de huidige claims:

- Een veilige digitale overheid cyber
- Inkoop en aanbesteding EV

5. Verstevigen en beschermen kennispositie t.b.v. onze strategische autonomie

De mogelijkheid voor Nederland om haar belangen te beschermen en te bevorderen (al dan niet in EU-verband) hangt in belangrijke mate af van de (innovatie)kracht van de technologiesector. Er zal daarom geïnvesteerd moeten worden in de eigen (Nederlandse en Europese) opbouw van kennis en innovatie en het beschermen hiervan tegen buitenlandse invloeden.

Bouwblokken uit de huidige claims:

- Versterken kennisbasis sensitieve technologie
- Veilige hard en software
- Versterken kennisbasis overheid gevoelige technologie en afhankelijkheden

Nederland digitaal veilig

Digitale incidenten hebben de potentie maatschappelijke ontwrichting en grote economische schade te veroorzaken. Onze samenleving en economie zijn in een hoog tempo gedigitaliseerd. We zien, op basis van zowel openbare als niet-openbare bronnen, een permanente digitale dreiging van statelijke actoren en criminelen. De afhankelijkheid van digitale processen is groot en is door COVID-19 nog verder toegenomen. Dit maakt digitale veiligheid essentieel voor de economie en maatschappij en daarmee een kerntaak van de overheid. De overheid is momenteel onvoldoende in staat om deze taak effectief in te vullen.

Iedereen- overheid, bedrijven en burgers – speelt een rol in het zorg dragen voor een digitaal veilig Nederland. De afgelopen kabinetsperiode zijn met de Nederlandse Cybersecurity Agenda (NCSA) als leidraad concrete stappen gezet om de digitale weerbaarheid van Nederland te verhogen. De ontwikkelingen op het gebied van digitalisering gaan echter snel en met de introductie van nieuwe technologieën zoals 5G en AI zal dit de komende jaren ook zo blijven. We moeten dan ook de volgende stap zetten in de samenwerking en integratie tussen overheidspartijen onderling maar ook tussen privaat-publiek en in internationaal verband. Hiervoor zijn forse overheidsinvesteringen nodig. In dit fiche zetten wij uiteen hoe we dat gezamenlijk kunnen bereiken en wat daar voor nodig is.

1. De schokbestendige samenleving: breed informeren en het bieden van handelingsperspectief

De overheid kan niet de gehele digitale ruimte voor 100% beschermen maar moet wel een omgeving creëren waarin iedereen weet wat te doen bij een digitaal incident en waar men terecht kan voor informatie over de dreiging en de te nemen maatregelen. Het delen van informatie ter bescherming van de cyberveiligheid moet snel en onbelemmerd gebeuren. Hiertoe is het belangrijk dat een volgend kabinet investeert in het versterken van het Nationaal Cybersecurity Centrum (NCSC) als nationale CERT en het Digital Trust Centre (DTC) als eerste aanspreekpunt voor het niet-vitale bedrijfsleven. Zij vormen de ruggengraat van het stelsel van cybersecurity samenwerkingsverbanden dat onder meer middels subsidies voor het oprichten van (sectorale) samenwerkingsverbanden zal worden uitgebreid en versterkt.

2. Kunnen leveren van de slagkracht

De overheid beschermt in het kader van de nationale veiligheid de samenleving en economie actief tegen digitale dreigingen vanuit (statelijke) actoren. Beter zicht op de dreiging, een passende incident response en doorvertaling van dreiging naar handelingsperspectief zijn noodzakelijk. Dit vergt meer investeringen en verregaande samenwerking tussen operationele partijen onderling en met de private sector.

3. Het beschermen van de vitale infrastructuur tegen complexe aanvallen

Daarbij moet in het bijzonder in publiek-privaat verband gewerkt worden aan het continu verhogen van de weerbaarheid van de vitale infrastructuur tegen complexe aanvallen. Er moet daarom onder andere geïnvesteerd worden in beter inzicht in dreigingen met als doel sneller en gericht te kunnen adviseren en acteren. Daarnaast wordt er op verschillende manieren in publiek-privaat verband geoefend met als doel de weerbaarheid te vergoten. Ook het versterken van de capaciteit en kennis van cybersecurity bij toezichthouders is noodzakelijk.

4. Een veilige digitale overheid

De gesignaleerde digitale dreiging richt zich zeker ook tegen de overheid zelf op alle lagen. Aanvullende investeringen in informatiebeveiliging en continuïteit van de overheid is daarom noodzakelijk als integraal onderdeel van de doorontwikkeling van de digitale overheid. Hiermee kan

men erop vertrouwen op de veiligheid en continuïteit van overheidsfunctioneren en – dienstverlening. Hiertoe moet onder andere geïnvesteerd worden in de CIO en CISO-rijk, de aanpak van risico's ter voorkoming van lokale ontwrichting, meer aandacht voor ketenafhankelijkheden, het vergroten van operationele capaciteit ten behoeve van de overheid en het bieden van een stevig wettelijk fundament voor cybersecurity in de openbare sector.

5. Het fundament; versterking kennis en innovatiepositie

Het fundament onder de Nederlandse aanpak voor cybersecurity wordt voor een belangrijk deel bepaald door de mate van strategische digitale autonomie die Nederland en de EU bezitten. De mogelijkheid voor Nederland om haar belangen te beschermen en te bevorderen (al dan niet in EU-verband) hangt in belangrijke mate af van de (innovatie)kracht van de technologiesector en de digitale weerbaarheid van de samenleving. Er zal daarom geïnvesteerd moeten worden in de eigen (Nederlandse en Europese) opbouw van kennis en innovatie. Ook wordt de komende periode met extra investeringen de ontwikkeling van veilige hard- en software verder gestimuleerd. Dit gebeurt vooral voor de ontwikkeling en implementatie van nieuwe Europese wet- en regelgeving met een publiek-private inzet.

6. Effectieve internationale inzet

De internationale herkomst van de digitale dreiging vereist ook robuuste internationale inzet. Nederland wil daarom met nationale en internationale partners voorop blijven lopen bij effectieve diplomatieke en politieke respons tegen ongewenste statelijke cyberoperaties. Hiertoe zal worden gewerkt dient te worden aan effectieve koppeling tussen het nationale en internationale domein op diplomatiek vlak, operationeel vlak (civiel en militair) en economisch. Hierdoor kan Nederland op alle lagen nieuwe cyberpartnerschappen vormgeven om de nationale veiligheidsbelangen effectiever te beschermen. Een bijzondere uitdaging daarbij is het waarborgen van de normen en waarden van onze internationale rechtsorde bij het gebruik van nieuwe technologieën.

1. De schokbestendige samenleving: breed informeren en het bieden van handelingsperspectief

Digitale dreigingen en weerbaarheid gaan verder dan alleen de Rijksoverheid en de vitale infrastructuur en raken alle doelgroepen in de samenleving en economie. Hierbij valt te denken aan incidenten als NotPetya Citrix en gijzelsoftware waaruit blijkt dat juist dat de hele samenleving potentieel kwetsbaar is. Het is daarom van belang om ook de weerbaarheid te vergroten bij burgers, het niet-vitale bedrijfsleven en organisaties en blijvend te investeren in bewust veilig digitaal gedrag door middel van het bieden van handelingsperspectief, en waar aan de orde het verscherpen van o.a. toezicht en handhaving op de geldende wet- en regelgeving. Covid-19 benadrukt de afhankelijkheid van ICT nog eens met het meer werken en leren vanuit huis.

Specifiek in de zorg- en onderwijssector neemt de digitalisering door onder andere Covid-19 enorm toe. Het verhogen van de cybersecurity is voor deze sectoren een essentiële randvoorwaarde en de huidige situatie benadrukt het belang om verder te investeren in de versteviging van het informatiebeveiligingsbeleid en het verhogen weerbaarheid van deze sectoren.

Tabel versterken digitale weerbaarheid niet-vitale organisaties en burgers (€ miljoen)

	2022	2023	2024	2025	2026	Struc.
EZK.BZK.JenV ¹						
EZK						
OCW						
JenV/DGRR						
VWS						
NCTV/NCSC						
Totaal						

5.1.2i

Landelijk Dekkend Stelsel

Om de weerbaarheid te kunnen verhogen is het snel kunnen uitwisselen van informatie essentieel. Versterken van het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden (LDS) moet ervoor zorgen dat rollen en verantwoordelijkheden helder zijn, zodat dreigingsinformatie en handelingsperspectieven binnen Nederland als geheel zo snel mogelijk de juiste organisaties bereiken en zodoende de juiste maatregelen tijdig kunnen worden genomen. We zetten in op:

- Versterken operationele rol en juridische basis NCSC om (urgente) informatie over dreigingen, incidenten en kwetsbaarheden breder, effectiever en efficiënter te delen en daarmee de digitale weerbaarheid van Nederland te vergroten,
- Het wettelijk verankeren van het DTC en het verder uitbouwen en versterken van het DTC qua capaciteit, expertise en informatie-uitwisseling met bedrijven.
- Het in kaart brengen van blinde vlekken binnen een landelijk dekkend stelsel en het vrijmaken van subsidiegelden voor het gericht stimuleren van nieuwe regionale of sectorale cybersecurity-samenwerkingsverbanden door EZK en JenV.
- Inrichten van een onderwijs CERT (of ISAC) voor het funderend onderwijs.
- Ondersteunen en verder versterken van Z-CERT als expertisecentrum cybersecurity voor de zorg om doorgroei te realiseren om meer zorgsectoren aan te kunnen laten sluiten.

Versteviging informatiebeveiligingsbeleid en verhogen weerbaarheid van de sectoren zorg en onderwijs

Digitale dienstverlening is, zeker nu door COVID-19, essentieel voor en een snelgroeiend onderdeel van zowel de zorg als het onderwijs. De primaire verantwoordelijkheid voor

¹ De genoemde bedragen en onderbouwing van JenV (in samenwerking met EZK en BZK) en JenV/DGRR betreffen een gedeeltelijke kopie van de bedragen en onderbouwing die door JenV in het fiche 'Effectieve opsporing en preventie in het digitale domein' (DGRR/DRC) zijn genoemd. Deze zijn dus dubbel opgenomen, en betreffen geen aanvulling op elkaar.

informatiebeveiliging blijft bij de organisaties zelf liggen, maar de overheid pakt hierin een sterkere stimulerende, faciliterende en controlerende rol.

Voor de zorg zetten we daarom in op:

- Doorontwikkelen van het informatieveiligheidsbeleid met concrete uitwerking van het 4B model (bewustwording, beveiligen, bewaken en blussen)
- Doorontwikkelen, versterken en verscherpen van toezicht en controle op de geldende informatiebeveiligingsnormen in de zorg

Bovenstaande voornemens zijn niet gekoppeld aan de lopende vitaliteitsbeoordeling van (delen van) de zorg maar zijn bedoeld om de zorg veiliger en weerbaarder te maken.

Voor het onderwijs zetten we in op:

Vanuit de verantwoordelijkheid voor het stelsel wil OCW stimuleren en faciliteren dat onderwijsinstellingen cybersecurity risico's beter managen:

- Zorgen dat de sectoren adequaat kunnen acteren wanneer zich een incident voordoet. Dus naast de ontwikkeling naar een CERT/ISAC voor het funderend onderwijs ook inzet op het doorontwikkelen van de SOC's voor het mbo en hoger onderwijs.
- Zorgen dat de sectoren (en de betreffende instellingen) hun verantwoordelijkheid kunnen nemen door ze te ondersteunen bij het ontwikkelen/formuleren van specifieke normen, het afdwingen hiervan bij leveranciers, en het uitvoeren van audits/DPIA's (zowel intern als op externe partijen/leveranciers).

Burgers

Nederlanders zijn steeds meer afhankelijk van het internet voor hun werk en levensbehoeften, terwijl online dreiging stijgt en de digitale weerbaarheid achter lijkt te blijven. Door structurele voorlichting over simpele handelingen wordt de weerbaarheid van Nederlanders verhoogd. Naast brede publiekscampagnes gaat speciale aandacht uit naar kwetsbaardere groepen: senioren, jongeren, laaggeletterden, en MKB-ondernemingen. Dit doel is in het algemeen belang, en versnippering van communicatie en effectiviteitsverlies moeten worden voorkomen. Daarom willen in ieder geval BZK, EZK en JenV – gelet op de overlap in doelgroepen – zich inzetten voor een gezamenlijke campagneprogrammering gedrag opzetten waar middelen aan gekoppeld zijn.

Verder wordt ingezet op:

- Gemeenten, regionale veiligheidsallianties en regionale platforms veilig ondernemen spelen een belangrijke rol bij het weerbaar maken van burgers en ondernemers. Zij worden gesubsidieerd om lokaal hun aanpak te versterken.
- Monitoring digitale criminaliteit
- Wetenschappelijk onderzoek naar slachtofferschap
- Doorontwikkelen van het Actieplan Informatieveilig gedrag in de zorg

2. Kunnen leveren van slagkracht

Om het Nederlandse handelingsperspectief in het digitale domein te vergroten, is gedegen en zorgvuldig onderzoek naar deze dreiging onontbeerlijk. Daarnaast is deze kennis nodig om passend en effectief te kunnen interveniëren en reageren en daarmee de kosten van ongewenst gedrag aan de zijde van kwaadwillende actoren te verhogen. Hierbij kan bijvoorbeeld gedacht worden aan opsporing, verstoring, slachtoffernotificatie, voorkomen van (verdere) schade en preventie, diplomatieke en politieke attributie als ook een militaire respons. Er is een stevige investering nodig in al deze onderdelen om Nederland veilig te maken en te houden. Al deze investeringen hebben bovendien een afschrikkende werking: criminele en statelijke acteren zullen minder geneigd zijn kwaadaardige acties te organiseren als ze weten dat de kans dat ze gezien, gepakt en in de schijnwerpers worden gezet groot is. Dit maakt een investering in de operationele partijen voorwaardelijk voor de rest van het investeringsprogramma.

Tabel Kunnen leveren van slagkracht (€ miljoen)

	2022	2023	2024	2025	2026	Struc.
NCSC						
AIVD						
MIVD						
OM						
Politie						
Defensie						
Totaal						

5.1.2i

Versterken informatie- & inlichtingenpositie

Een investering in de Nederlandse informatie- en inlichtingenpositie vormt de basisvoorwaarde voor de overige onderdelen van het investeringsprogramma. Zonder de resultaten uit deze onderzoeken kan de overheid de maatschappij als geheel nauwelijks extra handelingsperspectief bieden. Deze kennis is een randvoorwaarde voor het kunnen weren van aanvallen van statelijke actoren, het blootleggen van cybercriminele netwerken en is noodzakelijk bij het opschonen van systemen na een hack in het geval er toch een incident heeft plaatsgevonden. Op basis hiervan kan bovendien worden besloten of, en zo ja, welke interventiemogelijkheden het meest effectief zijn.

- Investeren in de capaciteit voor technisch onderzoek bij (doelgroep)organisaties (NCSC);
- Vergroten van de operationele slagkracht door het uitwerken en realiseren van een publiek/privaat samenwerkingsplatform onder coördinatie van het NCSC (NCSC);
- Onderhoud, continuïteit en innovatie van het Nationaal Detectie Netwerk (I&V-diensten en NCSC);
- Bestendigen en verder uitbouwen versterkte operationele samenwerking CIIC (I&V-diensten);
- Uitbreiden capaciteiten voor inlichtingenmatig diepteonderzoek (I&V-diensten);
- Doorvertalen van dreiging naar handelingsperspectief en maatregelen (I&V-diensten);
- Uitbreiden capaciteiten om partijen bij te staan bij aanvallen door statelijke actoren (I&V-diensten);
- Verbeteren inzet technologie voor de politietaak om zo te komen tot data-gedreven intelligence (NP);
- Verhogen van de cyber security van de IT-infrastructuur van Politie en OM (NP en OM).

Interventie

Een zorgvuldige en integrale afweging van Nederlandse (veiligheids)belangen staat centraal bij het bepalen van respons en interventie opties. Voor politie en OM betreft het hier opsporing en

vervolg, verstoring, slachtoffernotificatie, voorkomen van schade en/of preventie. Het NCSC verricht door middel van technisch onderzoek slachtoffernotificatie en voorkomt schade middels verstoring en/of preventie. De I&V-diensten kunnen een dreiging verstoren voordat deze zich manifesteert verstoren. Defensie kan militaire middelen inzetten om anderen te ondersteunen of zelfstandige militaire doelen te bereiken. Optreden tegen ongewenste statelijke cyberoperaties, bij voorkeur internationaal gecoördineerd of in coalitieverband met gelijkgezinde landen, is bovendien effectief ter bestendiging van de internationale rechtsorde en (inter)nationale veiligheidsbelangen.

- Uitbreiden van de wettelijke mogelijkheden voor het NCSC voor het verrichten van technisch onderzoek bij doelgroeporganisaties, waardoor potentiële kwetsbaarheden sneller kunnen worden geconstateerd en schade kan worden voorkomen (NCSC);
- Equiperen van I&V-diensten opdat ze volwaardig ondersteuning kunnen leveren aan het interdepartementale responsbeleid waaronder attributie (I&V-diensten, zie ook onderdeel 6);
- Versterken opsporingsteams en capaciteiten van Politie en digitaal vaardig maken organisatie door tooling en opleiding (NP);
- Versterking van de kwantitatieve en kwalitatieve capaciteit van het OM om de groei en diversificatie van cybercrime bij te houden (OM);
- Verhogen van de digitale capaciteiten van de KMar voor zowel de politietaak als Defensietaak (J&V/DEF);
- Vergroten van de robuustheid van o.a. het Defensie Cyber Security Centrum zodat Defensie haar rol in de *last line of defence* kan borgen (DEF);
- Uitbreiden slagkracht Defensie Cyber Commando door het aantrekken en behouden van meer cyberpersoneel (DEF).

3. Het beschermen van de vitale infrastructuur

De vitale aanbieders bieden essentiële diensten voor de continuïteit van de economie en maatschappij. Deze vitale aanbieders en hun supply chain, van toeleveranciers naar eindgebruikers digitaliseren in toenemende mate. Onderbreking of uitval van een dergelijke dienst kan leiden tot ernstige maatschappelijke ontwrichting in Nederland. De vitale processen vallen onder de verantwoordelijkheid van de vakministers. Hierdoor is sectorale expertise geborgd, tegelijkertijd vraagt de complexiteit van de dreiging en benodigde maatregelen in combinatie met het risico op spillover effecten om een stevige centrale basis. De afgelopen periode zijn daarom al gezamenlijk stappen gezet om de digitale beveiliging van de vitale infrastructuur naar een hoger niveau te tillen o.a. door de implementatie van de Wbni. In de volgende kabinetsperiode moet in samenwerking met de vitale aanbieders verder worden gewerkt aan het snel en doelmatig uitwisselen van dreigingsinformatie, het inzichtelijk krijgen van potentiële kwetsbaarheden en het nemen van passende maatregelen. Dit wordt o.a. gedaan door de oprichting van sectorale expertise teams.

	2022	2023	2024	2025	2026	Struc.
EZK						
JenV						
Totaal						

5.1.2i

Informatie-uitwisseling vitale aanbieders

Om een digitale verstoring te voorkomen of te herstellen is het cruciaal dat informatie over dreigingen, kwetsbaarheden en mitigerende maatregelen snel gedeeld wordt met elke organisatie die daar belang bij heeft. Zowel in de warme als koude fase moet de informatie-uitwisseling tussen vitale aanbieders en overheidspartijen zoals het NCSC, veiligheidsdiensten en toezichthouders verbeterd worden. Vitale aanbieders krijgen nog niet alle informatie die zij nodig hebben om geïnformeerde besluiten te nemen. Het NCSC en de veiligheidsdiensten hebben op hun beurt beperkt zicht op welke systemen vitale aanbieders in gebruik hebben en kunnen bij incidenten lastig inschatten of vitale aanbieders potentieel kwetsbaar zijn.

Daarom zetten we in op:

- Het opzetten van kanalen voor vertrouwelijke informatie-uitwisseling van en naar vitale aanbieders en andere ketenpartners. Door het inrichten van een digitaal portaal waarmee vitale aanbieders en toezichthouders informatie over de organisatie kunnen delen en kunnen aangeven welke informatie voor hen relevant is en over welke vraagstukken zij geïnformeerd willen blijven. Zo ontstaat nauwkeuriger inzicht in de informatiebehoeften en vraagstukken bij vitale aanbieders en sectorale toezichthouders. Hiermee kan het NCSC efficiënter en gericht informatie verzamelen over relevante kwetsbaarheden en dreigingen monitoren en een op de doelgroep afgestemd handelingsperspectief bieden.
- Daarnaast ontwikkelt het NCSC zijn beveiligingsadviezen voor risicovolle kwetsbaarheden verder door, zodat doelgroep organisaties nog beter in staat worden gesteld om op dreiging en kwetsbaarheden te acteren. Dit doet het NCSC door kwetsbaarheden met potentiële hoge impact te verrijken en van gerichte duiding te voorzien.
- De complexiteit van de digitale infrastructuur, de digitale afhankelijkheden van de vitale infrastructuur en de permanente dreiging vereisen een actueel nationaal en internationaal cybersecuritybeeld. Door het uitbreiden van het aantal triage officers en duidingsspecialisten bij het NCSC wordt de impact van adviezen kwalitatief en kwantitatief versterkt.

Kennis operationele techniek

De digitalisering van productieprocessen neemt de komende jaren verder toe en daarmee groeit de afhankelijkheid van Industrial Automation & Control Systems (IACS) in onze samenleving. Naast ICT moeten ook vitale processen met operationele techniek (IACS) goed worden beschermd, omdat zij van cruciaal belang zijn voor het functioneren van de vitale infrastructuur. Om doelgroeporganisaties met actuele kennis van zaken over IACS te kunnen adviseren, is een

stevige kennispositie van het NCSC noodzakelijk. Het NCSC wil in dit kader onder andere inzetten op:

- Cybersecurity advies geven in het in/aankoopproces van IACS;
- Opstellen van controle raamwerken voor IACS;
- Opbouwen kennissteunpunt IACS voor bedrijven (i.s.m. EZK);
- Opzetten Publiek Private Samenwerking IACS;
- Uitbreiden oefencapaciteit.

Toekomstbestendige vitale infrastructuur

Door technologische ontwikkelingen en digitalisering verandert de werking van vitale processen en systemen. Steeds meer organisaties en systemen raken hierin met elkaar verweven en er ontstaan sterke ketenafhankelijkheden. We richten ons op de bescherming van deze processen als geheel door het:

- Voorbereiden van nieuwe wetgeving. De huidige herziening van de NIB-richtlijn door de Europese Commissie zal leiden tot een wijziging van de Wbni.
- Uitbreiden van juridische en beleids capaciteit bij departementen.
- Het inrichten van structurele dekking voor het CSIRT voor digitale dienstverleners (CSIRT DSP). Dit is een verplichting uit de NIB-richtlijn waar nu onvoldoende capaciteit voor beschikbaar is gesteld.
- De toenemende aandacht voor de supply chain in de vitale processen betekent dat er een link moet komen tussen de informatievoorziening tussen vitaal en niet-vitaal en dus de informatie-uitwisseling tussen NCSC en DTC, NCSC en CSIRT-DSP's en CSIRT-DSP's en AT.
- In het kader van het versterkingsprogramma vitaal wordt gewerkt aan het vormgeven van de bescherming van vitale infrastructuur dat aansluit op de huidige stand van de techniek en ontwikkelingen in het (actuele) dreigingsbeeld. We zetten daarom in op:
 - Het integreren van op vitaal gerichte governance structuren, beleidslijnen en wetgevingstrajecten (zoals de Wbni) in één gecoördineerde aanpak vitale infrastructuur, waarbinnen ketenafhankelijkheden, digitale en fysieke veiligheid, en supply chain security in samenhang worden geadresseerd.
 - Herijking van de scope van vitale infrastructuur, door op basis van de nationale veiligheidsbelangen uit de NVS 2019 in kaart te brengen wat we willen beschermen.
 - (Technische) kennis en kunde versterken ten behoeve van de bescherming van vitale infrastructuur, zodat de bescherming van vitale infrastructuur aansluit op de technologische ontwikkelingen en digitalisering.

Toezicht

Toezichthouders sturen en controleren bij vitale bedrijven op het nemen van passende maatregelen om digitaal weerbaar te zijn en kunnen in het uiterste geval handhavend optreden. Omdat digitale processen een steeds grotere rol krijgen binnen de vitale infrastructuur wordt cybersecurity ook een steeds omvangrijker onderdeel van het werk van toezichthouders, zowel in de vitale als de niet-vitale sectoren. Met de huidige mensen en middelen zijn de toezichthouders onvoldoende in staat om mee te groeien in de digitalisering van hun toezichtdomein en hun eigen methodieken. We zetten daarom in op:

- Opbouw en uitwisseling van kennis en expertise bij sectorale toezichthouders
- Coördineren en verder uitbreiden van nationale en internationale samenwerking tussen toezichthouders, onder meer ten behoeve van gezamenlijke onderzoeken en samenhangende inspectiebeelden alsmede Europese afstemming tussen toezichthouders.
- Verbeteren van uitwisselen en combineren van informatie, zodat het toezicht informatie gestuurd en risicogericht kan opereren. Zowel in onderling verband als met andere partijen, zoals het NCSC
- Ontwikkeling van toezichtmethodieken die passen bij digitalisering en ketenafhankelijkheden en daarbij passende middelen, zoals specifieke tooling voor complexe risicoanalyses ter ondersteuning van de toezichtprogrammering.

4. Een veilige digitale overheid

Investeren in digitale weerbaarheid is noodzakelijk om te waarborgen dat de overheid haar taken betrouwbaar en veilig kan blijven uitvoeren en effectief kan reageren op digitale ontwrichting. Ook de overheid wordt steeds afhankelijker van informatie en ICT en onze werkprocessen zijn steeds meer data-gedreven. Dit vraagt om een samenhangende en gecoördineerde aanpak op lokaal, regionaal en nationaal niveau. Deze kabinetsperiode zijn stappen gezet, maar extra investeringen zijn noodzakelijk om een volwaardig stelsel van coördinatie, beheersing en verantwoording op te zetten.

	2022	2023	2024	2025	2026	Struc.
Kaderstelling						
Monitoring						
Nationale cryptostrategie						
Crisisrespons						
Kennis en kunde						
Toezicht en handhaving						
Totaal Overheid (enkel BZK)						

5.1.2i

Kaderstelling

Momenteel ontbreekt een generiek wettelijk kader voor informatieveiligheid, waardoor een complexe waaier aan overlappende sectorale informatieveiligheidswet- en regelgeving is ontstaan. We zetten daarom in op het creëren van duidelijkheid en het maken heldere afspraken d.m.v. één generiek wettelijk kader voor de overheid met uniforme regels over verantwoordelijkheid, verantwoording, risicomanagement en toezicht voor verschillende beveiligingsniveaus tot en met vitaal, waarin recht wordt gedaan aan het proportionaliteitsbeginsel. Bij deze aanpak zal relevante expertise van de overheidskennispartijen worden betrokken.

- Als onderdeel van het generieke wettelijke kader opstellen van bestuurlijke afspraken, beleidskaders en wet- en regelgeving voor alle overheidssectoren uit het Besluit BNI (vitale digitale overheid, ook niet-AED)² en niet-vitale overheidssectoren.
- Adoptie van normenkaders gericht op beveiliging van procesautomatisering of industriële automatisering (IA) voor vitale en niet vitale infrastructuur overheid (in aanvulling op de BIO).
- Uitrol, beheer en stimuleren van gebruik van cybersecurity inkooppeisen voor alle overheidslagen (Inkooppeisen Cybersecurity Overheid) na 2021.
- Investeren in het opzetten van een beleidsvisie en de implementatie daarvan voor het provinciaal domein;
- Investeren in het gezamenlijk opzetten van nieuwe informatiebeveiligingskaders voor de (rijks)overheid en toeleveranciers (AIVD/NBV, MIVD/BIV, NCSC en CIO Rijk), voortbouwend op de reeds opgedane kennis en ervaring met het ABDO.

Monitoring en risicobeheersing

Op dit moment hebben we te weinig zicht op de kwetsbaarheden en afhankelijkheden van de netwerk- en informatiesystemen van de overheid, en op de risico's die daardoor gelopen worden. Ook is meer inzicht in de effectiviteit van beveiligingsmaatregelen noodzakelijk, zodat snel en doelmatig de juiste interventies kunnen worden gepleegd. We gaan daarom:

- Een monitoringsinstrument ontwikkelen, gebaseerd een transparant volwassenheidsmodel, om de effectiviteit van maatregelen in kaart te brengen.
- Het verstevigen van de informatiepositie binnen de gehele overheid door beter zicht op netwerk en informatiesystemen, kwetsbaarheden en afhankelijkheden (gericht op kantoor- en procesautomatisering), zodat risico's sneller worden geadresseerd en interventies mogelijk zijn.

² Dit omvat zowel de rijksoverheid als de medeoverheden

- Investeren in voorzieningen om risico's te identificeren en op te kunnen lossen zoals kwetsbaarheidscans, aanpak ketenanalyse (inzicht in ketenafhankelijkheden), Nationaal Detectie Netwerk (NDN) en inzet van ethische hackers. Ook zetten in op een "keurmerk" van overheidsberichten en een validatieregister van overheidswebsite. Burgers en ondernemers kunnen zo websites valideren en melding doen van verdachte websites. Dit doen we samen met private partners.
- Versterken van de rol van de inlichtingendiensten ten aanzien van het vertalen van dreiging van statelijke actoren naar handelingsperspectief en weerbaarheid verhogende maatregelen.

Nationale Cryptostrategie (NCS)

Uitvoering van de NCS voorziet in de behoefte aan uniforme beveiliging en optimalisering van de Rijksbrede digitale informatiebeveiligingsmiddelen. De opbouw en het behoud van kennis en ontwikkelcapaciteit binnen Nederlandse bedrijven, kennisinstellingen en overheid is daarbij een belangrijk uitgangspunt.

- Het verder ontwikkelen en implementeren van de Nationale Cryptostrategie (NCS) met als doel te zorgen dat de Rijksoverheid zich kan verzekeren van bestendige beschikbaarheid van goede (cryptografische) beveiligingsmiddelen en behoud van digitale soevereiniteit.
- In het kader van de Nationale Cryptostrategie zal worden geïnvesteerd in (aanschaf van) cryptografische (informatie)beveiligingsproducten.

Cyber incident response overheid

Een computer emergency response team (CERT) is essentieel om een cyberincident te voorkomen en de gevolgen te bestrijden. CERTs adviseren doelgroepen over cybersecurity en leveren bijstand tijdens een incident. Elk overheidsorgaan moet toegang hebben tot een CERT (in de eigen bestuurslaag) en de CERTs die er zijn moeten voldoende middelen en capaciteit krijgen om hun taak adequaat uit te kunnen voeren.

- Ondersteuning Gemeenten bij realisatie van Gemeentelijk programma Digitale Veiligheid waaronder, versterking IBD t.b.v. gemeenten en gemeenschappelijke regelingen, Investeren in samenwerkingsafspraken om de effecten van digitale inbreuken in de samenleving te onderkennen en de gevolgen daarvan te minimaliseren en investeringen in ontwikkeling van initiatieven en samenwerkingsafspraken rond het voorkomen van cybercriminaliteit door burgers en ondernemers daartegen beter weerbaar te maken.
- Versterken cyberweerbaarheid veiligheidsregio's o.m. in relatie tot SOC/ CERT functionaliteit.
- Inregelen CERT-functie voor openbare lichamen (Caribisch deel NL).
- Versterken in oprichting zijnde provinciaal informatieknooppunt cybersecurity (potentieel nieuwe CERT/bestuurslaag).
- Uitbreiden CERT/ SOC watermanagement (naast RWS en Waterschappen ook versterken in de dienstverlening met IBD (gemeenten) en provincies).
- Investeren in cybergevolgbestrijding bij de gehele overheid, door implementatie van het NCP-D en de aansluiting van óók lokale overheden te waarborgen. Organiseren van (verplichte) oefeningen (zoals de Overheidsbrede Cyberoefening van BZK) en het verder uitwerken van oefen en test initiatieven per bestuurslaag in aansluiting op het overheidssbrede oefen- en testprogramma.

Kennis en kunde

Digitale veiligheid vergt niet alleen technische maatregelen, maar is ook mensenwerk.

- Investeren in veilige voorzieningen en veilig gedrag van medewerkers (awarenessprogramma).
- Het versterken van de samenwerking tussen specialistische organisaties die zich bezighouden met cybersecurity binnen de gehele overheid. Het identificeren van lacunes in de dienstverlening. Het inrichten van een kennis en expertisecentrum (kennisontwikkeling, innovaties) om deze te adresseren. Denk hierbij aan samenwerking tussen SOC's.
- Opzetten van een rijksbreed PhD-netwerk voor cyber security. Dit betreft van een programma voor het uitvoeren van promotieonderzoek. Een doelstelling van het rijksbreed doen van onderzoek met een groep PhD's is kennisverwerving.

Toezicht en handhaving

We versterken het risico gestuurd toezicht op digitale veiligheid en weerbaarheid. Hierdoor sturen we de overheid naar een hoger niveau van volwassenheid van risicomanagement.

- We zetten een escalatieladder op met bijhorende interventies. Bepaald moet worden in welke omstandigheden bij welke informatieprocessen (vitaal versus niet-vitaal) bij welk type organisaties (rijksdienst, mede-overheden, ZBO's en RWT's) het aan de orde is om (interbestuurlijk) te kunnen interveniëren, waaruit een dergelijke interventie bestaat en welk juridisch/bestuurlijk instrument daarvoor geëigend is.
- Organiseren van onafhankelijk toezicht binnen de overheid op informatie en processen van nationaal belang, zoals vitale processen en staatsgeheimen. Uitbreiding van taken van AIVD/NBV als nationale toezichthouder ten behoeve van de bescherming van de nationaal gerubriceerde informatie binnen de Rijksoverheid.

5. Gemeenschappelijk fundament cybersecurity: kennis en innovatie, veilige producten en diensten, oefenen & testen

Een effectieve bescherming tegen digitale dreigingen en een adequate voorbereiding op digitale incidenten is alleen mogelijk als belangrijke randvoorwaarden op orde zijn. Er zijn investeringen nodig in de onderliggende bouwstenen. Met meer mogelijkheden voor cybersecurityonderzoek, kennisopbouw en -innovatie op het gebied van onder andere Quantum, IoT en Artificial Intelligence zorgen we ervoor dat Nederland in de digitale kenniswedloop voorop kan blijven lopen. Ook investeren we in het opleiden van gekwalificeerd cybersecuritypersoneel. Door het implementeren van wettelijke afspraken en certificering van ICT-producten en diensten worden marktpartijen geprikkeld om digitaal veilige producten aan te bieden. We gaan meer investeren in kennis, procedures en vaardigheden om Nederland voor te bereiden op een (grootschalig) incident, onder andere door beter en gevarieerder te oefenen, en we testen de ICT-systemen van de overheid en vitale partijen op kwetsbaarheden. Tezamen vormt dit het fundament onder een cyberveilig Nederland.

Tabel gemeenschappelijk fundament (€ miljoen)

	2022	2023	2024	2025	2026	Struc.
EZK						
J&V						
AIVD						
MIVD						
Totaal						

5.1.2i

Kennis en innovatie cybersecurity

Cybersecurity en digitale veiligheid zijn onderwerp van een wereldwijde kenniswedloop. Nederlands onderzoek op dit terrein draait nu nog mee in de internationale top. Deze positie willen we vasthouden. Om de Nederlandse kennisniveau op peil te houden moet Nederland in staat blijven zelfstandig hoogwaardig cybersecurityonderzoek te doen en experts op te leiden. Het oprichten van een cybersecurityecosysteem bestaande uit kennisinstellingen, overheid en private partijen en voldoende financiering om onderzoek mogelijk te maken is daarbij essentieel. Vanuit die basis kan aansluiting worden gezocht bij internationale initiatieven en tegelijkertijd de Nederlandse digitale autonomie versterkt worden. We nemen de volgende acties:

- Het nieuwe samenwerkingsplatform cybersecurity, specifiek gericht op kennis en innovatie, krijgt een stevige programmering met aandacht voor onderwerpen als automated security, cryptocommunicatie en IoT.
- We sluiten door het oprichten van een nationaal centrum aan bij de ontwikkeling van een Europees netwerk van Nationale Cyber Competence Centers. Dit centrum zal als verbindend orgaan fungeren tussen de beschikbare Europese instrumenten en de Nederlandse initiatieven op het gebied van cybersecurity kennis en innovatie.
- Versterken van de Nederlandse digitale autonomie door het gericht investeren in samenhangende onderzoeksprogrammering van onderwijs- en kennisinstellingen. Dit voorkomt afhankelijkheid van buitenlandse expertise en oplossingen. Belangrijke onderwerpen in deze context zijn veilige digitale infrastructuur, secure cloud toepassingen, en up-to-date defensieve cyber technologie. We creëren een Human Capital Agenda Cybersecurity Personeel. Door structureel aandacht te geven aan en te investeren in cybersecurity in het onderwijs kan het huidige tekort aan capabele cybersecurity professionals worden tegengegaan.
- Defensie richt een Cyber Innovation Hub (CIH) op om in publiek-privaat verband innovatie te stimuleren en te benutten. Innovaties gaan razendsnel en continue aandacht is vereist om deze beschikbaar te maken voor Defensie, de Rijksoverheid in het algemeen en de vitale infrastructuur.
- De kennispositie van het NCSC wordt versterkt door de inzet van meer capaciteit om inzicht te verkrijgen in nieuwe technologieën (o.a. automated security, zero-trust

encryptie, containerisation). Daarnaast levert het NCSC een bijdrage aan het breed agenderen en programmeren van cybersecurityonderzoek (o.a. op het gebied van herstelvermogen, supply chain risico's, kwantificering van cyberrisico's), inclusief het zelf begeleiden van toegepast (wetenschappelijk) onderzoek.

Veilige ICT-producten en diensten en veilige internetstandaarden

Het cybersecurity-niveau van ICT-producten en diensten (waaronder *Internet of Things*-apparaten) is onvoldoende. De afgelopen kabinetsperiode is geïnvesteerd in verschillende trajecten vanuit onder andere de Roadmap Digitaal Veilige Hard- en Software. De komende periode wordt met extra investeringen deze lijn voortgezet en doorontwikkeld onder meer met de ontwikkeling en implementatie (incl inrichten uitvoering en toezicht) van nieuwe Europese wet- en regelgeving en een publiek-private inzet. Hierdoor worden onder meer onveilige slimme apparaten geweerd van de Europese markt, wordt ICT-producten en diensten gecertificeerd en krijgen consumenten (veiligheids-)updates voor een redelijke termijn. De implementatie van bestaande veilige internet- en emailstandaarden wordt bevorderd en de veiligheid van open source software wordt gestimuleerd.

Oefenen en testen

Om te weten hoe te handelen in een crisissituatie is het voor organisaties binnen de Rijksoverheid en vitale infrastructuur belangrijk om goed voorbereid te zijn op incidenten. Oefenen en testen is, als onderdeel van de crisispreparatiecyclus, daarom essentieel voor de digitale weerbaarheid van Nederland. Door het *oefenen* van fictieve cyberincidenten kunnen organisaties zich voorbereiden en zodoende bij een daadwerkelijk incident snel en adequaat handelen. Naast het oefenen van incidenten is het nodig om de systemen en processen van het rijk en de vitale infrastructuur op digitale veiligheid te *testen*. Door een test worden kwetsbaarheden gesignaleerd en kunnen deze preventief worden verholpen. Op dit moment zijn de huidige mogelijkheden binnen de bestaande middelen te beperkt, daarom kan een volgend kabinet inzetten op uitbreidingen binnen het oefenen testprogramma.

- Voor *oefenen* bouwen we verder binnen de bestaande sporen. Het eerste spoor bestaat uit het organiseren van grootschalige oefeningen in het kader van het Nationaal Crisisplan Digitaal. Het tweede spoor is de deelname van de overheid aan bestaande cyberoefeningen in verschillende sectoren. Het derde spoor is het ontwikkelen van initiatieven op oefeningen in publiek privaat verband om oefeningen in verschillende sectoren verder te stimuleren.
- Voor *testen* is het nodig om verschillende initiatieven te starten om het testen van systemen van de overheid, en het testen van systemen binnen de vitale infrastructuur, te bevorderen.

6. Effectieve internationale inzet

Wat in het buitenland gebeurt, raakt rechtstreeks aan de veiligheid van Nederland. Effectieve internationale inzet is daarom nodig in het Nederlands belang. Veiligheid is cruciaal voor het Nederlandse buitenlandbeleid. De internationale veiligheidssituatie is de afgelopen jaren verslechterd. Dit vraagt om extra inzet op het internationale veiligheidsterrein. Dit fiche richt zich op digitale veiligheid als belangrijk onderdeel daarvan.

Tabel internationale inzet (€ miljoen)

	2022	2023	2024	2025	2026	Struc.
BZ						
JenV						
EZK						
Totaal						

5.1.2i

Digitale veiligheid

Nederland bevindt zich door zijn actieve rol - die voortvloeit de noodzaak de hoogwaardige digitale infrastructuur te beschermen - in de voorhoede van internationale discussies op het cyberbeleid. Deze positie doet recht aan het belang voor Nederland van dit domein. Kwaadaardige cyberoperaties van statelijke actoren nemen sterk toe. Daarnaast worden nieuwe technologieën op grote schaal geïntroduceerd waarbij normen en waarden van de internationale rechtsorde niet voldoende zijn gewaarborgd. Deze ontwikkelingen hebben verstrekkende gevolgen voor onze fysieke en maatschappelijke veiligheid. Samen met nationale en internationale partners wil Nederland voorop blijven lopen bij effectieve diplomatieke en politieke respons tegen ongewenste statelijke cyberoperaties. Ook wil Nederland nieuwe cyberpartnerschappen vormgeven om de nationale veiligheidsbelangen effectiever te beschermen. Een bijzondere uitdaging daarbij is het waarborgen van de normen en waarden van onze internationale rechtsorde bij het gebruik van nieuwe technologieën. Om in de dynamische omgeving van het digitale domein een actieve rol in de voorhoede van de internationale discussies op het cyberbeleid te kunnen blijven spelen, is extra inzet nodig.

A. Effectieve diplomatieke respons (o.a. attributie) tegen ongewenste statelijke cyberoperaties

Terwijl de internationale discussie over de toepassing en de reikwijdte van het internationaal recht in het digitale domein voortduurt, blijven sommige staten schadelijke activiteiten ontplooiën. Diplomatiek optreden (o.a. attributie) tegen ongewenste statelijke operaties, bij voorkeur internationaal gecoördineerd of in coalitieverband met gelijkgezinde landen draagt bij aan de bevordering van de (inter)nationale veiligheid. Bij het bepalen van respons staat een zorgvuldige en integrale afweging van NL veiligheidsbelangen centraal. NL zet in op versterking van de capaciteit om ondermijnende cyberoperaties tegen te gaan door:

- Versterking van diplomatieke capaciteit om (inter)nationaal gecoördineerd in coalitieverband diplomatiek en politiek te kunnen reageren op ondermijnende cyberoperaties, o.m. door publieke attributie en andere maatregelen zoals het opleggen van sancties.
- Versterking van inlichtingencapaciteit en capaciteit voor technisch onderzoek om adequater in coalitieverband diplomatiek en politiek te kunnen reageren, o.a. met behulp van attributie en sancties, op ondermijnende cyberoperaties is weergegeven in onderdeel 5.

B. Versterking capaciteiten om nieuwe cyberpartnerschappen vorm te geven en effectiever de Nederlandse veiligheidsbelangen te beschermen

Vanwege het grensoverschrijdende karakter van digitale dreigingen is Europese en internationale samenwerking essentieel om de nationale veiligheidsbelangen adequaat te beschermen. Het is van belang om partnerschappen te bouwen om (inter)nationaal de weerbaarheid tegen digitale dreigingen door o.a. statelijke actoren te verhogen. Een bijzondere uitdaging hierbij vormt het waarborgen van normen en waarden van onze internationale rechtsorde bij het gebruik van nieuwe technologieën. NL zal extra inzetten op effectieve cyberpartnerschappen om het digitale

domein open, vrij en veilig te houden en de bescherming van zijn nationale veiligheidsbelangen te versterken door:

- Versterking van capaciteit om (inter)nationaal gecoördineerd in bilateraal, Europees en internationaal verband op te treden.

- Versterking van technologische (aan diplomatieke capaciteit te koppelen) expertise om binnen de EU en multilateraal (o.a. ISO en ITU) de veiligheid van nieuwe technologieën te kunnen waarborgen.

Fiche 1 EV. Versterken eigen kracht en soevereiniteit middels offensief industriebeleid**DOEL FICHE:**

1. Beleidsintensivering rond concurrentiekracht om publieke belangen beter te borgen,
2. Urgentie om tot extra maatregelen te komen om (toekomstige) strategische afhankelijkheden te verkleinen ten opzichte van 3e landen,
3. In staat zijn aan te sluiten bij Europese initiatieven bij doelen 1 en 2.

Probleemstelling

Door de handelsoorlog en (geopolitieke) concurrentie tussen de VS en China, hebben economisch nationalisme en protectionisme een veel centrale rol gekregen wereldwijd. Daarmee is duidelijk geworden dat in de nabije toekomst:

- a. Toegang tot kritische sleutel technologieën minder vanzelfsprekend zal zijn, dat
- b. Economische en technologische afhankelijkheden steeds geopolitiek worden, en het
- c. Borgen van de Nederlandse publieke belangen onder druk komt te staan.

Oplossingsrichtingen:

Bovenop bestaand beleid en middelen zien wij voor deze problemen drie oplossingsrichtingen:

Ad 1. Intensivering staand beleid op innovatie en valorisatie

Om in algemene zin op Europees- en nationaal niveau ons beter te kunnen verweren bij geopolitieke druk van buitenaf vraagt dit (naast een bredere beleidsinzet) onder meer om het vergroten van de Nederlandse en Europese technologische en economische capaciteiten en competenties op vlakken als onderwijs, kennismigratie, onderzoek en innovatie. Dit maakt de kans het grootst dat derde landen ook afhankelijk van ons blijven en borgt daarmee een wederzijdse afhankelijkheid. Dit vergroot de economische weerbaarheid.

Ad 2. Additioneel budget om kwetsbare economische afhankelijkheden te adresseren

Naast het breed versterken van onze technologische en economische capaciteiten en competenties, zullen wij kwetsbare afhankelijkheden bij sleutel technologieën moeten adresseren. Een goed beeld van kwetsbaarste afhankelijkheden kan om extra beleid vragen. Soms is dat defensief (strategische voorraden van mondkapjes bijvoorbeeld), andere keren offensief (extra investeringen in onderzoek, innovatie of productiecapaciteit). Hiermee worden kwetsbare afhankelijkheden voorkomen, vooral wanneer onze *economische veiligheid* in het geding is. Dit streven om strategisch autonoom te worden mag niet tot onnodige verstoring van de markt leiden, maar moet deze juist repareren.

Een offensieve beleidsinzet vraagt om additioneel budget om waar nodig gerichte investeringen te kunnen doen in onderzoek, ontwikkeling en het opschalen van technologie. In het bijzonder geldt dit waar ze raken aan: maatschappelijke missies; zij bijvoorbeeld economisch relevant brede toepassingsmogelijkheden hebben zoals general purpose technologies met belangrijke potentie tot volginnovaties; zij een winner-takes-all dynamiek raken; of anderszins kunnen leiden tot geopolitieke strijdpunten.

Ad 3. Budget voor het aansluiten bij EU-initiatieven

Bij maatschappelijke uitdagingen en kwetsbare afhankelijkheden is schaal vaak een vereiste. Vanuit de EU wordt dit verder in kaart gebracht (o.a. op medische middelen, grondstoffen, cybersecurity en sensitieve technologieën) en worden vergaande en zeer kapitaalintensieve Europese samenwerkingsprogramma's gestart. Nederland steunt deze ontwikkeling en bepaalt aan de hand van een afwegingskader op een case-to-case basis aan welke initiatieven zij deelneemt. Hiervoor zijn wel meer middelen nodig, voor a) cofinanciering bij EU programma's zoals Horizon Europe en b) budget om deel te nemen aan IPCEIs op terreinen waar Nederland dit met oog op maatschappelijke uitdagingen en de eerder beschreven uitdagingen van belang acht.

Beoogd extra budgetbehoefte

	Bedoeld voor:	Per jaar (bij benadering)
Fiche 1	Investeren in sleuteltechnologieën als AI, Semicon, Fotonica, Quantum en sectoren als Cyber en Defensie-industrie	130 miljoen
Fiche 2	Budget voor aanhaken bij Europese initiatieven als: - Industrie Allianties - IPCEI	Minimaal 50-100 miljoen per jaar

Fiche 1 – Gerichte investeringen in sleuteltechnologieën en sectoren

Omschrijving voorgestelde maatregelen

De grootste vragen die relateren aan het bevorderen concurrentiekracht en weerbaarheid liggen op het domein van technologieën waarvan we vermoeden dat ze in staat zijn aan toekomstige vitale processen te gaan raken, maar nog niet zeker weten in welke mate en hoe de precieze goederen en diensten waarin ze gebruikt gaan worden eruitzien. Momenteel vindt al onderzoek plaats naar welke technologieën als sensitief geduid kunnen worden. Toch moet je ondanks deze onzekerheid daar nu al strategieën maken welke rol je als overheid hier wil innemen. In lijn met beleidsoptie 15 uit de BMH 16 pleiten wij in dit fiche ook voor investeringen in sleuteltechnologie die mogelijk aan publieke- en veiligheidsbelangen raken. In dit BMH rapport is een afwegingskader gemaakt waarin zowel in het kader van concurrentiekracht als nationale veiligheid gemeten kan worden of sprake is van een publiek belang en hoe groot de impact van ongewenste interventies kan zijn.

Vanuit de sleuteltechnologieën aanpak, die bij het missie gedreven topsectoren en innovatiebeleid is gepresenteerd, zijn op basis van MJPs een aantal *technologieën* te identificeren die vanwege hun toepassing zowel maatschappelijk als economisch mogelijk impact hebben indien hier ongewenste interventies plaatsvinden. Deze ongewenste interventies door of grote afhankelijkheden van derde landen kunnen grote gevolgen hebben voor de economische veiligheid. Dit zijn met name sectoren die actief zijn op het gebied van digitalisering en robotisering, maar momenteel nog een lager TRL level hebben. Door gericht te investeren in innovatie kunnen de sectoren van morgen toekomstbestendiger worden, kan kennis meer gevaloriseerd worden en houden we het heft in eigen hand (oplossingsrichting 1 en 2).

De technologieën:

De halfgeleider (semiconductor, ook wel *semicon*) industrie en hieraan verwante technieken zijn door Nederland aangemerkt als een *sleuteltechnologie*. De waardeketen van de halfgeleider industrie bestaat uit verschillende hoog- technische segmenten, is complex, hoog innovatief en mondiaal sterk verweven. Nederland heeft binnen deze industrie een bijzondere positie. Wij zijn sterk in high- tech machinebouw en hebben op het gebied van de halfgeleider industrie een mondiale sterspeler met ASML die als enige op de wereld machines kan leveren voor de fabricage van de meest gespecialiseerde chips (5 nanometer). ASML opereert in een sterk ecosysteem van toeleveranciers en is daarmee in feite een groter ecosysteem van zeer gespecialiseerde bedrijven die Nederland hierin op de wereldkaart zetten. Ook het Nederlandse NXP heeft een belangrijke positie binnen de halfgeleider industrie en ook NXP leunt op het sterke Nederland cluster van toeleverende bedrijven en de kennisinstellingen.

De Nederlandse kracht licht dus onder anderen in de machinebouw voor de halfgeleider industrie (Semicon Equipment). Vanuit het TKI HTSM is specifiek voor de *Semicon Equipment* markt een roadmap opgesteld als onderdeel van het missie- gedreven innovatiebeleid. Ook speelt het Nederlandse ecosysteem rondom de Semicon Equipment een belangrijke rol in het themateam Sleuteltechnologieën. Binnen deze roadmaps is er ook met name ruimte voor het toeleverende ecosysteem in de machinebouw met veel MKB'ers. De bedragen zoals genoemd in dit fiche zijn dan ook afkomstig uit ramingen van deze roadmap. Voor geïntegreerde fotonica heeft Nederland met PhotonDelta een krachtige ecosysteem partij en een leidende rol in de ontwikkeling van chips gebruikmakend van lichttechnologie. Fonicachips zijn sneller, energie-efficiënter, en kunnen veel verder geminiaturiseerd worden t.o.v. reguliere elektronica-chips.

Op het gebied van AI is het Nederlandse onderzoek naar computerscience excellent en van wereldniveau. Momenteel is Nederland in de waardeketen echter vooral interessant als 'proeftuin'. Nederland moet de krachten op het gebied van cybersecurity, AI, cryptocommunicatie en kwantumtechnologie bundelen door middel van innovatieve ecosystemen. Deze ecosystemen moeten resulteren in samenwerkingsverbanden van bedrijven, overheden en kennisinstellingen gericht op het leveren van een belangrijke bijdrage aan maatschappelijke missies, het toekomstig verdienvermogen van Nederland en het behouden van onze welvaarts- en kennispositie. Een voorbeeld van een dergelijk ecosysteem is het samenwerkingsplatform voor cybersecurity kennis en innovatie. Er liggen grote economische kansen bij het door ontwikkelen van de

Nederlandse cybersecurity aanpak door betere uitwisseling tussen bedrijfsleven en wetenschap en investering en toegang tot (durf)kapitaal. Via het samenwerkingsplatform komen vraag, aanbod en middelen voor cybersecurity onderzoek, innovatie en onderwijs bij elkaar in een thematische en keten-georiënteerde aanpak.

Nederland staat wereldwijd in de top 10 landen waar de meeste kennis aanwezig is in toonaangevende kennisinstellingen over *kwantumtechnologie*. Nederland kan deze unieke voorsprong verder uitbouwen door meer te investeren in productie en levering van kwantumtechnologie. Door lange termijn investeringen en garanties van de overheid in deze sector krijgen bedrijven meer incentives zich in Nederland te vestigen en in Nederland te investeren. Ook hier liggen veel kansen op het gebied van Europese samenwerking en Nederland kan hier potentieel een van de leidende posities innemen. De Quantum Delta TK brief benoemt de ambitie om het gehele ecosysteem te versterken met uitgesproken nadruk op marktontwikkeling.

Ook binnen de Life Sciences & Health sector liggen kansen. Door de Brexit en de verplaatsing van EMA naar NL kan de LSH sector groeien. Door in Europees verband meer samen te werken in bijvoorbeeld een API alliantie, kan afhankelijkheid van bepalende grondstoffen voor medicijnen verkleind worden. Nederland is van oudsher een belangrijke speler op het terrein van vaccins- en infectieziektebestrijding. De sector kenmerkt zich door de behoefte aan veel risicovol kapitaal. Een mogelijkheid is het vergroten van overheidsuitgaven richting lifesciences R&D. Een dergelijke stimulatie kan werken als katalysator om de sector interessanter te maken voor private investeerders. Met het nationale medtech programma (MJP ST) wordt gewerkt aan het versterken van het verdienvermogen van Nederland. Het programma is gericht op het oplossen van maatschappelijke vraagstukken in de zorg, zoals geformuleerd in het MTIB.

De sectoren:

In de defensie gerelateerde industrie bestaat behoefte aan een grotere overheids-opdrachtgeversrol (launching customer). Voorfinanciering of cofinanciering van defensiematerieelprojecten met grote maatschappelijke/economische waarde en stimuleren van de overheidsrol als Launching Customer vergt een defensie brede voorziening, waaruit gerichte investeringen kunnen worden gedaan, zoals deelname aan internationaal samenwerkingsprogramma ontwikkeling, productie en instandhouding van de Joint Strike Fighter (F-35), voorfinancieringen van innovatieve logistieke proposities binnen het F-35 programma en investeren in de ontwikkeling van radarsystemen. Een andere innovatie betreft emissieloos varen, waarmee in 2030, 30 CO₂vrije schepen gerealiseerd moeten worden voor defensie gebruik. Defensie en I&W zullen optreden als launching customer. Dit steunt tevens de scheepsbouw. De gevraagde financiële reeks is gebaseerd op het *masterplan emissieloze maritieme sector* dat is opgesteld door de sector in samenwerking met I&W, Defensie en EZK.

De EU heeft daarnaast de ontwikkeling van eigen capaciteit op ruimtevaart als beleidsinzet. Dat betekent marktkansen. Nederland heeft een onderscheidende optische satcom technologie waar internationaal vraag naar is. Hoewel de vraag groeiend is, zou schaalgrootte waarop dit afgezet kan worden aanzienlijk verbeterd kunnen worden. Hier zou een investering in ESA kunnen helpen.

Effecten, voor- en nadelen

+ *Minder afhankelijkheid van derde landen en daarmee sterkere concurrentiepositie in waardeketens:* door het versterken van de eigen positie in waardeketens of te investeren in de potentie van strategische technologieën, verminderen wij ongewenste eenzijdige afhankelijkheden van derde landen. Hiermee verminderen wij de inzet van waardeketens/afhankelijkheden als geopolitiek instrument en kun autonoom handelen ondanks geopolitieke druk.

+ *Investeren in weerbaarheid en concurrentiekracht van waardeketens verbetert het vestigings- en investeringsklimaat.* Door een goede digitale en financiële infrastructuur te installeren, creëren we duurzame randvoorwaarden voor innovatie en investering. Door vanuit de overheid zekerheden mee te geven, creëren we vertrouwen bij bedrijven dat Nederland een duurzame plek is voor investeringen. Hiermee trekken we mogelijk investeringen uit het buitenland aan.

+ Gerichte samenwerking met landen binnen de EU versterkt de economische positie van de EU op het wereldtoneel. Landen om ons heen hanteren veel meer een systematiek van gerichte impulsen

in technologieën. Frankrijk en Duitsland investeren bijvoorbeeld intensief in hun semicon sectoren. Ook Finland en Zweden maken voor technologie subsidies beschikbaar. Samenwerking met deze landen kan Nederlandse sleuteltechnologieën en partners in het ecosysteem daaromheen, verder helpen en een grotere afzetmarkt creëren (marktontwikkeling, waardeketenversterking). Dat vergt grotere PPS-budgetten aan NL zijde die er nu vaak niet zijn.

+ *De maatregelen passen in de Nederlandse uitgangspunten.* Het beleid dient ten eerste geen bodem voor protectionisme te worden. De impulsen dienen als katalysator waarmee innovaties worden gerealiseerd die de economie verder helpen, maar die bedrijven zelf niet hadden kunnen realiseren. Tevens sluit het goed aan op de *basispositie economische veiligheid* die recent is gepubliceerd.

- Mogelijk gevaar dat investering in impulsen als staatssteun wordt bestempeld. Mogelijkheid dat straks veel investeringen in en risico's rondom R&D publiek zijn, maar de baten privaät.
- Impulsen in de eigen economie kan de indruk wekken dat we wegdraaien van andere internationale partners, zoals de VS, Japan en China. Daarom moeten ze zoveel mogelijk binnen internationale afspraken vallen (bijvoorbeeld de WTO staatssteunregels). Als de EU zich niet hieraan houdt dan is dat het failliet van het internationale *rules-based* systeem
- De inzet van de impulsen moet secuur en weloverwogen gebeuren ter voorkoming van overheidsfalen. Een gedegen analyse voor extra investeringen is van vitaal belang. Wanneer blijkt dat het potentiële marktaandeel klein is vanwege compartieue nadelen, er geen marktfalen aan ten grondslag ligt, of er geen ongewenste afhankelijkheid bestaat, dan is de publieke investering van minder groot belang, of zelfs onrechtmatig volgens de Interne Markt regels omtrent staatsteun

Uitvoering: Min EZK – B&I → directies I&K, Topsectoren en Industriebeleid, CMP; RVO; DEF; DEIZ

Budgettaire gevolgen in mln. euro's (+ = saldooverslechterend). Cijfers zijn gebaseerd op de begrotingen in de MJP/TKI:

	2022	2023	2024	2025	2026	Struc.
Sleuteltechnologieën						
Semicon equipment ¹						
Fotonica ²						
AI ³						
Kwantumtechnologie						
Cybersecurity						
Samenwerkingsplatform						
Sectoren						
Ruimtevaart						
Defensie						
Emissieloos varen						

5.1.2i

¹ https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/25%20MJP%20Halfgeleider%20Fabricage%20Apparatuur%20final%20_28Mei2019.pdf

² <https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/22%20MJP%20Photonics%20update%20gecombineerd.pdf>;
<https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/21%20MJP%20Photonics%20for%20Society.pdf>

³ <https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/44%20MJP%20Nationaal%20%20Artifici%C2%89le%20Intelligentie%20%28AI%29%20Onderzoekscentrum%20.pdf>; <https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/45%20MJP%20Nederland%20Werkt%20in%20Slimme%20Ketens%20aan%20Artifici%C2%89le%20Intelligentie%20%28AI%29.pdf>; <https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/48%20MJP%20AI%20enabled%20Electronic%20Components%20%26%20Systems%20addressing%20societal%20solutions%20%28v5b%29.pdf>

Fiche 2 Houd Nederland internationaal aangehaakt

Omschrijving maatregelen

Duurzame innovatierelaties kunnen op verschillende manieren worden opgericht om concurrentiekracht te bevorderen. Dit kan bijvoorbeeld bilateraal of Europees. Behoeftte bestaat aan een instrument voor bilaterale innovatiesamenwerking vanuit waarmee RVO.nl internationale projecten kan opzetten. Dit instrument kan dan ingezet worden voor duurzame innovatie betrekkingen. De kosten die hier mee gemoeid gaan zullen ongeveer 20 miljoen euro per jaar bedragen om met 17 zowel Europese als niet-Europese prioriteitslanden op gebied van R&D en innovatie structureel te kunnen samenwerken (VS, Japan, Zuid-Korea, India). Ook het breder opzetten van bilaterale economische betrekkingen met bijvoorbeeld, maar niet uitsluitend, Duitsland geeft innovatie en economische samenwerking een boost, door uitwisseling kennis, talent en ideeën. Duitsland heeft zelf ook vergaande interesse geuit deze betrekkingen op te bouwen.

De eerder genoemde Europese strategische industriële allianties rondom strategische ecosystemen en waardeketens bieden mooie kansen de handen in een te slaan met Europese partijen, als overheidsinstanties, bedrijven en kennisinstellingen. Nederland zal per alliantie de mate van inzet bepalen. Wij pleiten voor SMART ingerichte allianties die doeltreffend en efficiënt te werk gaan.

Echter, voor deelname aan initiatieven die uit deze allianties voortkomen, zoals mogelijke IPCEI-projecten, is geld nodig. Hoewel volgend jaar 255 miljoen aan cofinanciering zal binnenkomen, dient voor de lange termijn ook een faciliteit te worden ingebouwd.

Een budget speciaal voor (het faciliteren en warm begeleiden vanuit RVO.nl) voor deelname vanuit het industrie en innovatie-ecosysteem aan allianties en, in uitzonderlijke gevallen, aan IPCEI-projecten is noodzakelijk. Het lastige hieraan is dat een exact bedrag niet genoemd kan worden. Toch kan gesteld worden dat het rond de 50 tot 100 miljoen per jaar zou moeten bedragen om op Europees niveau niet buiten de alliantie boot te vallen. Een goed voorbeeld hiervan is de *IPCEI micro-elektronica 2*. Mocht hier vanuit de industrie commitment voor zijn en een noodzaak voor extra staatssteun bestaan, dan is het op dit moment lastig om aan te sluiten bij de door Duitsland voorgestelde IPCEI aangezien Nederland niet over budget beschikt om aan dit soort initiatieven deel te nemen. Gevolg: een sterke Europese waardeketen waar Nederland potentieel buiten valt en op haarzelf de concurrentie moet blijven voeren.

Nederland is van mening dat IPCEI projecten niet ingezet dienen te worden voor het creëren van zogenaamde 'Europese kampioenen' die vanwege een sterke lobby bescherming genieten. De inzet van IPCEI zijn met name bedoeld voor sectoren waarbinnen marktfalen gecorrigeerd dient te worden. Nederland vindt daarnaast dat IPCEI-projecten onderdeel moeten zijn van een bredere lange termijn strategie ter versterking van strategische waardeketens en ecosystemen. Ook moet er eerst een gegronde analyse zijn die aantoont dat staatssteun in de vorm van IPCEI-projecten nodig is om de Europese ambities vastgelegd in de strategie te bereiken.

Hiernaast is aandacht nodig voor risico's rondom leveringszekerheid van belangrijke grondstoffen, in het bijzonder kritieke grondstoffen en *active pharmaceutical ingredients* (API's).

Bij specifieke grondstoffen kan een verstoring in aanlevering, om welke reden dan ook, zorgen voor langdurige impact op productieketens, aangezien alternatieven niet of nauwelijks voor handen zijn. Dit kan leiden tot verstoringen tot wel 5 – 7 jaar. Waar dit gaat om toelevering tot economisch belangrijke en strategische industrieën (te denken valt aan de semiconsector, batterijen, defensie-gerelateerde industrie, farmaceutische bedrijven) kan dit een significant economisch en mogelijk ook veiligheidsrisico opleveren. Overheden en internationaal opererende bedrijven zijn risico-intoleranter geworden voor leveringszekerheidsrisico's en handelsrisico's. Europese afhankelijkheid van invoer uit derde landen als China en India zijn op dit moment groot en de projectie is dat deze nog sterk zal stijgen, mede onder invloed van de groeiende vraag naar grondstoffen voor de energietransitie.

Leveringszekerheid van grondstoffen staat al langer op de agenda in Nederland. Ook in de EU groeit de aandacht voor onderwerp. Dit blijkt onder andere uit de ER-conclusies van 1-2 oktober 2020 (waarin meerdere keren over grondstoffen worden gesproken), de maakindustriebrief en uit het feit dat prioriteit wordt gegeven aan een grondstoffen alliantie (EUCO 13/20). De Europese Unie volgt een zinvolle, brede aanpak gericht op veerkrachtige waardeketens voor de Europese industrie, afhankelijkheden verminderen o.a. door innovatie en circulair gebruik, stimuleren duurzame

Europese winning en verwerking, en diversificatie aan de importkant inclusief versterking van het regelgevend kader voor duurzame winning, verwerking en handel in grondstoffen.

Het zou voor Nederland strategisch zijn ook deel te nemen in de recent ingerichte industriële alliantie voor grondstoffen, de European Raw Materials Alliance (ERMA) en de eigen inspanningen te intensiveren parallel met deze brede Europese aanpak, met ook aandacht voor verduurzaming van waardeketens van (kritieke) grondstoffen om op deze manier bij te dragen aan leveringszekerheid, klimaatdoelstellingen en de SDGS. Bij EZK komen verschillende invalshoeken op dit dossier (politiek, concurrentiekracht, klimaat, strategische autonomie, circulaire economie, economische veiligheid) allemaal samen. Gelet op de enorme kwetsbaarheid op dit dossier voor Nederland en de EU, en de ontwikkelingen tot dusver, verzoekt EZK middelen om zijn positie als sleutelspeler op dit dossier te verstevigen. Er wordt gedacht aan een bedrag van €40.000.000 voor de komende coalitieperiode, te weten €10.000.000 per jaar, waarbij bezien zal worden of dit bedrag (naast EZK) deels toegekend moet/kan worden aan andere betrokken departementen. Deze intensivering wordt deels geïnvesteerd in het voor langere tijd aantrekken van personeel met kennis van zaken, en voor programmageld om als volwaardige partner deel te kunnen nemen aan (Europese) projecten. Focus hierbij zou, in lijn met en in aanvulling op Europese initiatieven, liggen op R&D gericht op substitutie van essentiële grondstoffen. In samenwerking met betrokken departementen kan ten slotte gekeken worden naar het instellen van een functionaris die de Nederlandse positie op het onderwerp grondstoffen kan vertegenwoordigen in het buitenland, kansen kan vertalen naar het Nederlands perspectief, partnerschappen kan opbouwen met gelijkgezinde landen om gezamenlijk afhankelijkheden te verminderen, en kan bijdragen aan meer ketenverduurzaming.

Effecten, voor- en nadelen

+ *Vergroting van de weerbaarheid van de Nederlandse economie.* Strategische autonomie is een mogelijk middel dat kan bijdragen aan een weerbare economie die publieke belangen kan blijven borgen. Strategische autonomie betekent niet dat de EU volledig zelfvoorzienend dient te worden. In plaats daarvan moeten ongewenste afhankelijkheden in kaart worden gebracht en proportioneel geadresseerd worden om leveringszekerheid van essentiële goederen en diensten te verzekeren en zo onze publieke belangen te kunnen borgen op de lange termijn.

+ *De kennis die bij de Innovatie Attachees aanwezig is.* De specialistische kennis van innovatie systemen vanuit deze netwerken is groot. Daarmee kunnen 'van dichtbij' structurele innovatiebetrekkingen worden opgebouwd met (derde) landen, kennis worden uitgewisseld en talent worden aangetrokken waar de Nederlandse markt in brede zin van profiteert. Investeren in bilaterale innovatiesamenwerking met NL priolanden: middelen voor R&D&I-samenwerking, versterking IA netwerk in priolanden, uitbreiding middelen voor bilaterale innovatiemissies en betere aansluiting internationaal handels- investerings- en innovatiebeleid.

+ Gerichte samenwerking binnen de EU vanuit marktdenken versterkt de economische positie van de EU op het wereldtoneel.

+ Cofinanciering vanuit de EU kan de toepassing van sleuteltechnologieën in Nederland verder helpen en een grotere afzetmarkt creëren. Door als EU brede lange termijn strategieën te creëren rondom missiegedreven ecosystemen, sleuteltechnologieën en strategische waardeketens, kan de EU voor betere marktcreatie, valorisatie en commercialisatiezorgen en de concurrentiekracht van de EU vergroten.

+ Deelname aan inzet IPCEI Micro-elektronica 2 heeft een tweeledig voordeel: enerzijds het versterken van de Nederlandse/Europese semicon markt, een markt die belangrijk is voor de Europese ambities op digitaal als mede op klimaatgebied (chips/datacenters nemen steeds groter deel van energievraag voor hun rekening). Anderzijds vermindert het eenzijdige afhankelijkheid van derde landen.

- Gewaakt moet worden voor een wildgroei aan IPCEI. Nederland is van mening dat het IPCEI instrument alleen gebruikt mag worden als uit gedegen onderzoek blijkt dat er markt- of systeemfalen optreedt. Meerdere lidstaten willen hun delen van het Recovery and Resilience Fund, nieuwe IPCEI initiatieven opzetten. Er moet gewaakt worden dat dit niet leidt tot

overheidsfalen en dat alleen geïnvesteerd wordt in projecten waar ook echt een rol van de overheid noodzakelijk is. Het creëren van Europese kampioenen is geenszins de bedoeling.

- Lidstaten kunnen het IPCEI instrument gebruiken om zgn. 'kampioenen' te creëren. Bij het gebruik van het IPCEI instrument moet, mede door de Europese Commissie, het gelijkspeelveld binnen de Interne Markt beschermd worden. Doordat grote landen grotere budgetten hebben om voor het IPCEI instrument te gebruiken, wordt er het gevaar gelopen dat er kampioenen gecreëerd worden, puur vanwege de financiële slagkracht van grotere lidstaten.
- De drempel voor deelname aan een ESIA lijkt laag, waardoor het gevaar dreigt dat er zeer veel worden opgericht en ze te groot en inefficiënt kunnen worden. Hiermee gaat het doel van de EIA, het bevorderen van samenwerking tussen overheden, bedrijven en kennisinstellingen, verloren.
- De focus mag niet alleen op de EU liggen, betrekkingen met landen als VS, Japan, India en China dienen ook warm te blijven. De EU doet er niet goed aan zich volledig autonoom te gaan onderscheiden in de wereld. Per definitie zijn afhankelijkheden niet slecht, alleen eenzijdige afhankelijkheden moeten zoveel mogelijk vermeden worden.

Uitvoering

- EZK – Directe TOP, I&K, DEIZ; IA netwerken, PV Brussel; BuZa.

Budgettaire gevolgen in mln. euro's (+ = saldoerslechterend)

	2022	2023	2024	2025	2026	Struc.
Grondstoffen						
<i>Grondstofscanner</i>						
Internationaal						
<i>Innovatiepact DUI</i>						
<i>IPCEI-Alliantie voorziening</i>						

5.1.2i

Fiche 3 – Vitale infrastructuur

Omschrijving voorgestelde maatregelen

Dit fiche neemt een ietwat vreemde plaats in ten opzichte van de voorgaande twee fiches, maar is opgenomen vanwege het grote maatschappelijke belang. Het uitvallen van vitale infrastructuur kan een maatschappelijk een ontwrichtend effect hebben, maar ook de reputatie van Nederland vestigingsland schaden. In dit fiche vragen wij in het algemeen brede aandacht voor goede vitale infrastructuur, maar focussen wij net iets meer op een goede cyberinfrastructuur.

Nederland heeft de ambitie en de kans om de (Europese)vestigingsplaats te zijn voor duurzame (basis)industrie (kabinetvisie duurzame basisindustrie, mei 2020). Daarbij moet worden ingezet op het beschikbaar komen van nieuwe technieken en op bijbehorende nieuwe infrastructuur. Nederland heeft een uitgebreid netwerk van buisleidingen, elektriciteit-, binnenvaart-, spoor- en weginfrastructuur en staat internationaal te boek als veilige vestigingsplaats vanwege haar multimodaliteit. Energieveiligheid is een belangrijk thema en een goede en betrouwbare infrastructuur hoort daar ook bij. Zoals gezegd: het vergroot niet alleen de veiligheid, maar ook de concurrentiepositie van Nederland als aantrekkelijk vestigingsland.

De fysieke infrastructuur dient op ICT-gebied een goede bescherming te genieten. Samenwerking binnen Topsectoren op het gebied van cybersecurity en de aansluiting van deze sectoren op het Landelijk Dekkend Stelsel wordt aangejaagd. Dit gebeurt onder andere door het in kaart brengen van witte vlekken en samenwerking in de vorm van *Information Sharing and Analysis Centers* (ISAC's) en zogenaamde OKTT's⁴ of sectorale computercrisisteams te stimuleren en faciliteren. Binnen deze verbanden kunnen bedrijven vertrouwelijk ervaringen uitwisselen met elkaar over *best practices* op het gebied van cyberveiligheid en kunnen organisaties via het Landelijk Dekkend Stelsel aangesloten worden op de informatievoorziening van het NCSC en DTC.

Effecten, voor- en nadelen

- + Door hier breder in te investeren kunnen zowel veiligheid als meer aantrekkingskracht bedrijven te vestigen worden bewerkstelligd.
- + Vitaal voor behalen klimaatdoelstellingen van de industrie en ook verdienkansen voor industrie (systeemintegratie) van clusters, maar ook voor export/import naar buurlanden (bv. op het gebied van waterstof of CCS).
- Maatregelen zijn duur en ingrijpend

Uitvoering

NCSC, DTC

Budgettaire gevolgen

Budgettaire gevolgen in mln. euro's (+ = saldooverslechterend)

	2022	2023	2024	2025	2026	Struc.
ISAC Aansluiting DTC						

5.1.2i

⁴ Een OKTT is een samenwerkingsverband dat 'Objectief Kenbaar Tot Taak' heeft om aangesloten organisaties te informeren over dreigingen, incidenten en kwetsbaarheden op het gebied van cybersecurity. OKTTs kunnen zich aansluiten op de informatievoorziening van het NCSC door middel van aanwijzing in het kader van Art. 3.2 Wbni.

Fiche 2 EV. Beschermen Technologie & Kennis

PM

CONCEPT

Fiche 3 EV. Voorkomen Ongewenste Zeggenschap**Huidig beleid**

Het kabinet werkt aan stelsel van investeringstoetsing op risico's voor de nationale veiligheid. Het wetsvoorstel Toetsing Economie en Nationale Veiligheid speelt hier een centrale rol in. De focus in dit wetsvoorstel ligt op wijzigingen van zeggenschap of significante invloed bij bedrijven die van wezenlijk belang zijn voor de vitale processen en bedrijven die hoogwaardige technologie ontwikkelen die raakt aan nationale veiligheid (hierna: sensitieve technologie). Het gehele stelsel bestaat, naast deze brede investeringstoets, uit bestaande en nieuw te introduceren investeringstoetsen die zijn ingebed in sectorale wetgeving, zoals onder andere in het energiedomein en de telecom (Wet Ongewenste Zeggenschap in de Telecommunicatie). Aan een sectorale toets voor de defensie-industrie wordt eveneens gewerkt. De brede investeringstoets zal als een vangnet werken voor investeringen die niet goed door middel van sectorspecifieke wetgeving kunnen worden afgedekt. Tijdens het toetsingsproces worden nationale veiligheidsrisico's als gevolg van wijzigingen van zeggenschap geanalyseerd en indien nodig gemitigeerd. In het uiterste geval bestaat de mogelijkheid om wijzigingen van zeggenschap te verbieden.

Daarnaast wordt er met de uitvoeringswet Wet FDI-screeningsverordening uitvoering gegeven aan de Europese verplichting om informatie uit te wisselen met andere lidstaten en de Europese Commissie over FDI die raakt aan veiligheid en/of openbare orde. Hiertoe wordt een contactpunt ingericht.

Omschrijving beleidsoptie

De brede investeringstoets ziet op risico's voor de nationale veiligheid, bij wijzigingen van zeggenschap of significante invloed bij bedrijven die van wezenlijk belang zijn voor de vitale processen en bij bedrijven met sensitieve technologie. Concreet gaat het om:

1. Het invoeren van een meldplicht voor wijzigingen van zeggenschap of significante invloed in bedrijven die van wezenlijk belang zijn voor de vitale processen of bedrijven actief met sensitieve technologie.
2. Het uitvoeren van analyses op risico's voor de nationale veiligheid.
3. Het in kaart brengen van de meest proportionele manier om evt. geconstateerde risico's te mitigeren dmv mitigerende maatregelen of (in het uiterste geval) het opleggen van een verbod;
4. Het nemen van een toetsingsbesluit.

Dit zorgt voor eerder en beter zicht op mogelijke nationale veiligheidsrisico's bij bijv. investeringen en overnames en biedt een wettelijk kader om deze te beoordelen, risico's te mitigeren en, in het uiterste geval, investeringen en overnames tegen te houden. De beleidsoptie voorziet in een structurele aanpak van risico' voor de nationale veiligheid die kunnen ontstaan als gevolg van (vaak) economische transacties zoals investeringen, overnames en fusies. Deze risico's ontstaan in veel gevallen in de context van een veranderende geopolitieke situatie waarbij economische belangen steeds meer een machtsmiddel worden.

Effecten, voor- en nadelen

- + Eerder en beter zicht op investeringen, fusies etc en bijbehorende risico's voor de nationale veiligheid.
- + Het beheersen van risico's voor de nationale veiligheid als gevolg van economische transacties.
- + Versterking van het wettelijke instrumentarium om risico's te mitigeren
- + De opbouw van strategische afhankelijkheden kan worden beperkt, de continuïteit van vitale processen wordt beter geborgd en gevoelige of vertrouwelijke informatie wordt beter beschermd.
- Verhoogt voor bedrijven die onder de reikwijdte van de toets vallen de administratieve last bij investeringen of overnames, doordat meldingen moeten worden gedaan en afgehandeld.

- Mogelijk diplomatieke consequenties wanneer een investering of overname tegengehouden wordt.
- Kan leiden tot een verslechtering van het investeringsklimaat, omdat het in specifieke gevallen de mogelijkheid kan beperken om nieuw kapitaal aan te trekken voor hoogtechnologische bedrijven die potentieel binnen de reikwijdte van de investeringstoets vallen. Onzekerheid over het investeringsklimaat schrikt potentiële investeerders af. Dit kan de concurrentiekracht verminderen.

Uitvoering

Het meldpunt voor de toetsing van investeringen en het contactpunt voor informatie-uitwisseling met EU-lidstaten over FDI wordt ingericht door EZK. De brede investeringstoets wordt toegepast door de minister van EZK, in overeenstemming met de minister van J&V en (indien van toepassing) de betrokken vakminister. Sectoraal ingebedde investeringstoetsen worden door de betreffende vakminister toegepast. De uitvoering van het stelsel van investeringstoetsing en opvolging betreft een groot aantal partijen, in ieder geval AIVD, BHOS, BZ, BZK, DEF, EZK, FIN, IenW, JenV/NCTV en MIVD. In het geval dat de casus zich verhoudt tot de nationale veiligheid en/of de gewichtige belangen van de staat wordt er door de relevante inlichtingen- en veiligheidsdienst naslag gedaan in door de door hen verwerkte gegevens.

Niveau van overheidsoptreden

Nationaal, aangezien het overnames van en investeringen in Nederlandse vitale infrastructuur en bedrijven die hoogwaardige technologie ontwikkelen die raakt aan de nationale veiligheid betreft.

Budgettaire gevolgen

Budgettaire gevolgen in mln. euro's (+ = saldoerslechterend)

	2021	2022	2023	2024	2025	Struc	Struc in
Meldpunt, contactpunt en infrastructuur							
Uitvoering investeringstoetsing ⁵							
Naslag door AIVD ⁶							
Naslag door MIVD ⁷							

5.1.2i

⁵ [Redacted text]

⁶ [Redacted text]

⁷ [Redacted text]

5.1.1b

Fiche 4 EV. Fiche Expertise Teams en Expertise eenheid Vitaal

Versie 2 – 19 november 2020

Door NCTV, NCSC, AIVD, DEF/MIVD, EZK, IenW

Aanleiding en maatregelen in het kort

De vitale aanbieders bieden essentiële diensten voor de continuïteit van de economie en maatschappij. Onderbreking of uitval van een dergelijke dienst kan leiden tot ernstige maatschappelijke ontwrichting in Nederland. De dreiging vanuit statelijke actoren, digitalisering en toenemende ketenafhankelijkheden vragen om diepgaande sectorale expertise om de juiste maatregelen te kunnen treffen om de beveiliging van de vitale infrastructuur naar een nog hoger niveau te tillen.⁸

De huidige sector-overstijgende aanpak op vitaal wordt versterkt met diepgaande expertise op specifieke vitale processen. Hierdoor wordt er enerzijds centraal kennis opgebouwd en kunnen tegelijkertijd vitale processen gericht getoetst worden vanuit nationale veiligheidsperspectief. Op die manier kunnen de vitale processen beter worden beschermd tegen risico's die volgen uit de dreiging vanuit geavanceerde (statelijke) actoren via zowel digitale route als op het gebied van economische veiligheid. Hierbij is samenwerking met de relevante publieke en private partijen essentieel.

Hiervoor wordt een adaptieve expertise eenheid vitaal opgericht. Deze eenheid richt zich op het bundelen van werkwijzen, initiatieven, kennis, expertise en deze levert mobiele capaciteit op vitaal waar nodig. De eenheid biedt actieve ondersteuning aan alle vitale processen, bijvoorbeeld bij de herbeoordeling van vitaal en verplichtingen voortkomend uit de Wbni. Daarnaast worden drie expertiseteams ingericht op de vitale processen Telecom, Elektriciteit en Keren en Beheren.⁹ Deze expertiseteams richten zich op:

- Het verdiepen van sectorale kennis over dreigingen en maatregelen;
- Het in kaart brengen van ketenafhankelijkheden binnen een sector;
- Het in kaart brengen van de afhankelijkheden en raakvlakken van sectoren onderling; en,
- Het vergroten van het inzicht in de strategische afhankelijkheden en de weerbaarheidsverhogende maatregelen (van organisaties binnen een sector.)

Maatregelen

1. Oprichting Expertise Eenheid Vitaal

- Voert de regie op de bescherming van de vitale infrastructuur in Nederland en let daarbij met en voor alle betrokkenen op samenhang, efficiëntie en effectiviteit van weerbaarheidsverhogende maatregelen. Bundelt bestaande werkwijzen, initiatieven en kennis, zodat deze breder toegankelijk worden voor meerdere vitale processen en bestaande structuren beter op elkaar aansluiten. Zorgt voor inzicht in dreigingen en keteneffecten en biedt handelingsperspectief.
- Ondersteunt expertise teams vitaal o.a. op het gebied van specialistische en generieke kennis en kunde, faciliteert bij het doen van risicoanalyses en het toepassen van de systematiek dreigingen, belangen, weerbaarheid en biedt een structuur voor het delen van (gerubriceerde en ongerubriceerde) informatie. Hierbij hoort ook het adviseren over de (sectorale) zorgplicht en drempelwaarden onder de Wbni op het gebied van integraliteit en nationale veiligheidsaspecten. Ondersteunt in onderlinge samenwerking de verschillende sectorale toezichthouders onder de Wbni met expertise producten.

⁸ Dit geeft invulling aan het besluit van het kabinet om een versterkte aanpak van de bescherming van vitale infrastructuur te ontwikkelen (Nationale Veiligheid Strategie 2019) en is onderdeel van de binnen de Nederlandse Cyber Security Agenda aangekondigde versterking van cybersecurity op vitaal.

⁹ Op basis van de dreiging, weerbaarheid, mogelijke cascade effecten en onderlinge afhankelijkheden op een vitaal proces wordt gekozen voor intensievere teams van hoogwaardige kwaliteit. In sommige expertise teams zal de nadruk vooral liggen op cyber security vraagstukken, terwijl op andere vitale processen een bredere inzet nodig is op het beheersen en voorkomen van risico's voor de continuïteit van het vitale proces, het weglekken van kennis en informatie en het ontstaan van strategische afhankelijkheden.

- Zorgt voor kennisopbouw en ontwikkeling van tools om strategische afhankelijkheden in de toeleveranciersketen van een vitaal proces in kaart te brengen, en voor het vergroten van het zicht op onderlinge afhankelijkheden en cascade effecten tussen de vitale processen.

2. Oprichten expertise teams op drie geprioriteerde vitale processen:

- Expertise team Telecom, Intensieve informatiedeling tussen publiek-private partijen waardoor dreiging en technologische ontwikkelingen in samenhang worden gezien. Uitvoeren van gezamenlijke risicoanalyses, op basis waarvan waar nodig aanvullende maatregelen kunnen worden genomen voor de telecomnetwerken.
- Expertise team Elektriciteit en duurzame energietransitie, Intensieve informatiedeling tussen publieke en private partijen (bv EZK, netbeheerders, energieproducenten en toezichthouders) en opbouw van gezamenlijke kennis en expertise. Hierdoor worden dreiging en technologische ontwikkelingen in samenhang gezien en kunnen risico's tijdig worden gesignaleerd en gemitigeerd. De partijen in de energiesector gebruiken deze informatie om hun weerbaarheid te verhogen tegen risico's voor de nationale veiligheid. De betrouwbaarheid en continuïteit van de energievoorziening hangt steeds meer af van veilige gegevensuitwisseling. Door ontwikkelingen op de energietransitie, steeds verder gaande digitalisering en intensievere (Europese) samenwerking ontstaan mogelijk nieuwe risico's voor de nationale veiligheid.
- Expertise team Watermanagement, Intensieve informatiedeling en bundelen van kennis tussen rijksoverheid en regionale overheden waardoor dreiging en technologische ontwikkelingen in samenhang worden gezien en de samenwerking in de keten verbetert. Inzet op opbouw van gezamenlijke kennis en expertise, zoals standaarden voor gezamenlijk inkoopbeleid en strategisch cyber personeelsbeleid.

3. Beleidsopvolging

Op basis van de uitkomsten van de risicoanalyses van de expertise teams en/of op basis van eigen beleidsanalyses kan beleidsintensivering nodig zijn om de nieuwe maatregelen uit te voeren. Ook kunnen er extra financiële middelen nodig zijn voor aanvullende onderzoeken die niet onder de expert teams vallen. Daarnaast is naast het overleg via de expertise teams intensivering van andere overleggen nodig vanuit het vakdepartement met de vitale aanbieders over bijvoorbeeld de uitwerking van de mitigerende maatregelen, (crisis)scenario's en dient de samenhang te worden bewaakt met overige (markt)ontwikkelingen, die zich in een sector voortdoen.

Effecten, voor- en nadelen

- + Vergroten zicht op en weerbaarheid van de vitale infrastructuur tegen huidige en toekomstige dreiging vanuit geavanceerde actoren, waaronder digitale spionage.
- + Bundelen van kennis, techniek en veiligheidspartners
- + Sneller, adequater en meer gezamenlijk inspelen op geopolitieke, Europese en technische ontwikkelingen
- + Actiever en structureel inzetten op het integreren van nationale veiligheidsaspecten in bestaande en toekomstige ontwikkelingen zoals standaardisering en diversificatie.
- + Beter en eerder zicht op te beschermen belangen, dreigingen en kwetsbaarheden
- + Binnen publiek-private samenwerking en/of (sectorale) wetgeving mogelijkheid om in een vroegtijdig stadium risico's te mitigeren, waarmee strategische afhankelijkheden voorkomen kunnen worden, de continuïteit van vitale processen beter geborgd kan worden en gevoelige of vertrouwelijke informatie beschermd kan worden.
- + Vitale aanbieders kunnen gerichter worden voorzien van dreigingsinformatie en advies
- + De positie van de toezichthouders wordt versterkt zodat zij waar nodig in kunnen grijpen
- Uitvoeringskosten voor overheid en bedrijfsleven.
- Mogelijk diplomatieke consequenties wanneer naar aanleiding van een risicoanalyse een aanvullende maatregel genomen wordt zoals eisen aan toeleveranciers.
- Wanneer de aanpak resulteert in onvoorspelbaar en fors overheidsingrijpen, kan dit leiden tot onzekerheid bij bedrijven en daardoor minder investeringen in vitale infrastructuur.

Uitvoering

NCTV, NCSC, AIVD, MIVD, EZK, AT, IenW

Budgettaire gevolgen mln. euro's (+ = saldoverslechterend)

	2022	2023	2024	2025	2026	Struc.
Maatregel 1 en 2 ¹⁰						
Deelmaatregel 3 ¹¹						

5.1.2i

Let op:

Het hier opgenomen bedrag voor de AIVD/MIVD betreft een onderdeel van de totale claim voor de AIVD/MIVD zoals opgenomen in het fiche "Versterking inlichtingenpositie".

10

[Redacted text block]

5.1.2i

Fiche 5. Veilige inkoop en aanbesteding rijksoverheid

Context

De Nederlandse economie is hoogontwikkeld, innovatief en internationaal georiënteerd. Dit biedt niet alleen kansen maar brengt ook risico's met zich mee. Het is van belang om op economisch vlak de risico's voor de nationale veiligheid nauwlettend in de gaten te houden. De economische veiligheid kan op verschillende manieren in het geding zijn. Allereerst kan autonomie van en beschikking over de vitale infrastructuur worden aangetast als gevolg van buitenlandse investeringen of technologie. Ten tweede kan het bedrijfsleven als gevolg van technologiediefstal worden aangetast, waarbij intellectueel eigendom, innovatie- en concurrentievermogen verloren gaan. De dreiging kan zich manifesteren als heimelijke staatsinvloed achter buitenlandse overnames en investeringen, inlichtingenvergaring, het verwerven van kennis in Nederlandse bedrijven en kennisinstellingen.

De Rijksoverheid is in toenemende mate afhankelijk van producten en diensten uit het bedrijfsleven. Het functioneren van deze logistieke keten is van belang voor een goede werking van de overheid. Het is dan ook van belang om deze logistieke keten op adequate wijze te beveiligen. Zeker daar waar het staatsgeheime of departementaal vertrouwelijke informatie (of producten) betreft die zich bij bedrijven bevinden.

Bij de overgrote meerderheid van aanbestedingen van overheidsopdrachten zal geen sprake zijn van een nationale veiligheidsdimensie. Echter, daar waar nationale veiligheidsbelangen bij aanbestedingen wel in het geding zijn, is voorzichtigheid geboden. In algemene zin is er bij aanbestedingen namelijk altijd sprake van een nieuwe of aanvullende afhankelijkheidsrelatie met een externe partij. Of deze afhankelijkheid een probleem vormt voor de nationale veiligheid, hangt sterk af van de sector c.q. het type product of dienst dat geleverd wordt, de opdrachtgever/afnemer en het bedrijf dat de opdracht wordt gegund.

De opdracht die voorligt is het vooraf blijvend mitigeren van risico's voor de nationale veiligheid bij inkoop en aanbestedingen. Naast dat de signalering van mogelijke risico's ingebed dient te worden binnen het inkoopproces, dient instrumentarium beschikbaar te worden gesteld en zo nodig geactualiseerd te worden. Binnen de Rijksinkoop, en bij de behoeftesteller en de BVA, dient er voldoende bewustwording te zijn van de mogelijke risico's en hier dient doorlopend aandacht aan te worden besteed door middel van voorlichting en opleiding. Het borgen van nationale veiligheidsrisico's bij aanbesteden door de Rijksdienst kan gezien worden als een stelselverantwoordelijkheid, passend bij de verantwoordelijkheid van de minister van BZK voor het Rijksinkoopstelsel. Doordat het beheer onder is gebracht binnen de afdeling Inkoop en Aanbesteden (IenA) van DGOO wordt de mogelijkheid geboden aanpassingen in nationale veiligheidsrisico's te vertalen in rijksbreed inkoopbeleid, de toepassing van het instrumentarium rijksbreed te monitoren en aanpassingen in het instrumentarium ook rijksbreed te delen.

Daarnaast kunnen korte communicatielijnen worden onderhouden met de NCTV en de CPO Rijk. Vanuit IenA wordt ervoor gezorgd dat producten worden vastgesteld en zo nodig worden geactualiseerd. Ook kan IenA adequaat reageren op knelpunten, incidenten en voortschrijdend inzicht.

Toenemende casuïstiek illustreert dat de omvang en diversiteit van de economische veiligheid (EV) dreiging toeneemt. Het beleidskader en -instrumentarium om op te treden is momenteel in ontwikkeling, en diverse beleidsopties op dit gebied zijn in BMH 16 uitgewerkt. Uit de probleemanalyse economische veiligheid is naar voren gekomen dat meer aandacht nodig is voor veilige inkoop en aanbesteding binnen de rijksoverheid¹². Dit fiche gaat in op voorstellen in deze.

¹² Aanvankelijk betrof het fiche de veilige inkoop en aanbesteding binnen de Rijksoverheid en Vitaal. Maar in het overleg is aangegeven dat de vitale processen niet gelijk zijn aan speciale sector bedrijven (bedrijven die dus te maken hebben met aanbestedingsregelgeving). Het fiche wekte daardoor de indruk dat de voorgestelde

(A - huidige ambitie)

Omschrijving voorgestelde maatregelen

Meer bewustwording creëren bij Rijkinkopers d.m.v. het verder ontwikkelen van het instrumentarium dat toeziet op het identificeren en mitigeren van nationale veiligheidsrisico's bij inkoop en aanbesteding. Momenteel bestaat er al een bewustwordingsmodule, maar deze opleiding wordt nog door onvoldoende inkopers en behoeftestellers gevolgd en is nog te vrijblijvend. Verdere ontwikkeling van de bewustwordingsmodule en het aanbieden van de module binnen de verschillende Rijksinkoop- en trainee opleidingen zal de effectiviteit vergroten. Verder zal evaluatie van de bewustwordingsmodule nieuwe inzichten kunnen opleveren.

Ook met het inzetten van de juiste communicatiekanalen zal de awareness van rijksinkopers en behoeftestellers op het gebied van nationale veiligheid bij rijksinkoop verbeteren.

Omdat er bij veel overheidsopdrachten geen risico zal zijn voor de nationale veiligheid is geconcludeerd dat het een te zware last is voor inkopers om bij elke aanbesteding de quickscan te doorlopen met de opdrachtgever. Daarom is doorlopende aandacht voor bewustwording van de mogelijke risico's en de beschikbaarheid van het instrumentarium essentieel. Inkopers moeten de risico's herkennen zodat ze de opdrachtgever kunnen informeren over de mogelijke risico's en deze gezamenlijk kunnen identificeren en mitigeren.

Het gewenste doel is dat bij inkoop en aanbesteding nationale veiligheidsrisico's worden meegewogen. Naast het doorontwikkelen van het instrumentarium kunnen de volgende activiteiten bijdragen aan de gewenste eindsituatie:

- Periodieke bewustwordingsactiviteiten (o.a. workshops en presentaties op netwerkdagen voor inkopers)
- Bestendigen contactpunt voor vragen (bestaat al maar wordt nog niet altijd gevonden)
- Begeleiden van risicoanalyses
- Inbedden van instrumentarium in inkoopproces
- Onderwijsmodules uitrollen

Het behalen van het gewenste einddoel zal de volgende effecten hebben:

- Inkopers zijn zich bewust van het onderwerp Nationale Veiligheid;
- Inkopers weten wanneer ze vanuit het oogpunt van risico-signalering en -mitigatie de quickscan moeten inzetten.
- Inkopers die risico's voor de nationale veiligheid signaleren weten welke maatregelen ze kunnen overwegen.
- Inkopers die informatie nodig hebben over risico's en maatregelen kunnen dit makkelijk vinden en gebruiken

Voor inkopers is het ook lastig om eisen t.a.v. ICT-producten en -diensten te formuleren en mee te geven aan met de RFP en het contract. Er is een hulpmiddel beschikbaar (gebaseerd op de BIO) waarmee het mogelijk wordt snel en volledig de juiste eisen te bepalen. De zogenaamde ICO-wizard is in beta-modus op internet beschikbaar. Het leert o.a. inkopers maar ook aanbieders van ICT-producten en -diensten te begrijpen welke concrete eisen relevant zijn om op te nemen in contracten. Met het gebruik van de wizard wil de overheid de vraag naar digitaal veilige ICT-producten en diensten stimuleren, haar eigen veiligheid verhogen en goed voorbeeld geven. Het gebruik van de wizard helpt de inkopers bewust te worden van wat er komt kijken bij inkoop van veilige hard- en software en diensten.

maatregelen voor alle bedrijven kunnen gelden die vitale processen "uitvoeren" en dat is niet het geval. Om die reden is "vitaal" ook uit de titel verwijderd.

Hoewel veel van de eisen in de inkoopwizard ook bruikbaar zijn binnen het totale eisenpakket van vitale processen, zijn geen verzwaarde eisen meegenomen die in vitale processen vaak een rol spelen. Er zal onderzocht worden in hoeverre de wizard verrijkt kan worden met extra eisen voor deze processen. De ABDO van Defensie kan daarbij mogelijk als referentie worden gebruikt.

Effecten, voor- en nadelen

- + Het zorgt voor awareness bij inkopers en opdrachtgevers op het gebied van nationale veiligheid bij inkoop en aanbesteden
- + Met verbeterd instrumentarium kan sneller worden bepaald *of* er mogelijke risico's zijn voor de nationale veiligheid bij een te gunnen opdracht.
- Meer administratieve handelingen voor inkopers en behoeftestellers binnen het inkoopproces.

Uitvoering

De maatregelen zullen worden uitgevoerd door de CPO Rijk.

Budgettaire gevolgen

Budgettaire gevolgen in mln. euro's (+ = saldooverslechterend)

	2022	2023	2024	2025	2026	Struc.
Deelmaatregel 1 BZK	■	■	■	■	■	■
Deelmaatregel 2	■	■	■	■	■	■
...	■	■	■	■	■	■

5.1.2i

(B – uitgebreide ambitie)

Omschrijving voorgestelde maatregelen

Het ontwikkelen van een rijksbrede regeling voor 'industrieveiligheid' door het oprichten van een centrale regeling gebaseerd op de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) van het ministerie van Defensie dat op gerubriceerde aanbestedingen van de hele Rijksoverheid verplichtend wordt toegepast¹³. Deze regeling voor industrieveiligheid betreft de beveiliging van gerubriceerde en/of vitale opdrachten bij bedrijven. Het huidige ABDO bevat bepalingen m.b.t. de fysieke beveiliging, cybersecurity, (wijzigingen in) eigendomsstructuren, economische veiligheid, screening van personeel en procedures bij incidenten. Hierdoor wordt voorkomen dat bedrijven slachtoffer worden van bv. (digitale) spionage, het weglekken van kennis en ongewenste overnames. Bedrijven worden contractueel verplicht deze beveiligingseisen in te voeren. De MIVD (Bureau Industrieveiligheid) verzorgt vanuit (regie) de toetsing van de naleving hiervan en adviseert bedrijven bij de implementatie van de maatregelen.

Op dit moment is de regeling alleen van toepassing op defensieopdrachten, of opdrachten van andere ministeries waar het ministerie van Defensie aan meedoet. De Rijksoverheid kan door het omarmen van deze ambitie meeliften op de processen, ervaring en netwerk van Defensie. Daarnaast wordt onderzocht of de regeling ook breder dan enkel de Rijksoverheid toegepast kan worden, bijv. door de speciale sector-bedrijven, zoals drinkwaterbedrijven, energiebedrijven en vervoersdiensten als Schiphol en de NS en als (vrijwillige) handreiking naar overige vitale bedrijven, kennisinstituten en decentrale overheden.

Effecten, voor- en nadelen

- + Het is voor bedrijven eenduidig en kosten efficiënt om één veiligheidsregime te hebben voor gerubriceerde en/of vitale opdrachten dan aparte regimes voor de verschillende ministeries. Veel bedrijven die onder de nieuwe Rijksbrede beveiligingseisen zouden

¹³ Vanaf een nog te bepalen TBB

komen te vallen, vallen nu al onder de ABDO-regeling van Defensie en zijn hier mee bekend.

- + Het is efficiënter en effectiever om dit bij één overheidsdienst te organiseren.
- + De (digitale) weerbaarheid van de Nederlandse industrie neemt toe, waarmee de nationale veiligheid verhoogt.
- + De economische veiligheid van de Nederlandse industrie neemt toe, waarmee de nationale veiligheid verhoogt.
- + De Rijksoverheid heeft een mechanisme waarmee bedrijven verplicht kunnen worden om maatregelen te implementeren op het moment dat het dreigingsniveau verandert. Toename administratieve lasten voor bedrijven die thans niet onder een rijksbrede regeling zouden komen te vallen. Mogelijk dat het met name voor mkb-bedrijven moeilijker is om aan dergelijke voorwaarden te voldoen en dus deel te nemen aan overheidsaanbestedingen. Onderzocht kan worden hoe dit kan worden ondervangen.

Uitvoering

De uitvoering van de maatregelen blijven ongewijzigd belegd bij Bureau Industrieveiligheid van de MIVD van het Ministerie van Defensie¹⁴ omdat veruit het grootste deel van gerubriceerde aanbestedingen binnen de Rijksoverheid bij Defensie plaatsvinden en BIV een rol speelt in de operationele gereedstelling van de krijgsmacht, daarnaast is BIV afhankelijke van de (contra-)inlichtingenteams van MIVD voor een goede uitvoering de taken in het kader van een rijksbrede regeling voor 'industrieveiligheid'.

De baten van de maatregelen vloeien echter terug naar de gehele rijksoverheid.

Budgettaire gevolgen

Budgettaire gevolgen in mln. euro's (+ = saldooverslechterend)

	2022	2023	2024	2025	2026	Struc.
Deelmaatregel 1						
Defensie						

5.1.2i

¹⁴ Het Ministerie van Defensie doet dit sinds 1965 met behulp van Bureau Industrieveiligheid die namens de beveiligingsautoriteit van Defensie toezicht houdt op bijzondere (gerubriceerde) informatie en te beschermen belangen bij de industrie. Bureau Industrieveiligheid heeft ongeveer 1000 bedrijven in portefeuille en is een kennis en expertisecentrum ten aanzien van supply chain security.

De beveiliging van de logistieke keten is op basis van de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). De ABDO richt zich op de bescherming van de industrie tegen statelijke dreiging. Hierdoor zijn de bedrijven tegen "lagere" dreigingen automatisch ook beveiligd. Bureau Industrieveiligheid werkt nauw samen met buitenlandse partners. Op het moment dat Defensie met buitenlandse bedrijven samenwerkt, houdt de partner toezicht op de Defensiebelangen in dat land. Bureau Industrieveiligheid doet dat op haar beurt weer voor buitenlandse Defensies.

Bureau Industrieveiligheid is onvervreemdbaar van Defensie vanwege de rol die zij speelt in de operationele gereedstelling van de krijgsmacht. Daarnaast is Bureau Industrieveiligheid onvervreemdbaar van de Militaire Inlichtingen- en Veiligheidsdienst omdat de nauwe samenwerking met de (contra)inlichtingenbureaus noodzakelijk is om de dreiging richting de industrie om te zetten in concreet te implementeren maatregelen.

Overkoepelend fiche 1. Versterken inlichtingenpositie EV

Uitgangspunten

- Structureel geld / capaciteit voor economische veiligheid;
- Een structurele eigenstandige inlichtingenpositie zorgt voor een betere en meer geïnformeerde afweging tussen publieke belangen en het kunnen treffen van de juiste maatregelen.
- Vraag en noodzaak om de awareness en weerbaarheid bij vitale (en top) sectoren en de defensieindustrie te verhogen.
- Dit geeft invulling aan het besluit van kabinet om een versterkte aanpak van de bescherming van economische veiligheid te ontwikkelen (Nationale Veiligheid Strategie 2019).
- Samenhang met lopende traject (o.a. cyber claim)

Context / wat is het probleem?

De Nederlandse economie is hoogontwikkeld, innovatief en internationaal georiënteerd. Dit biedt niet alleen kansen maar brengt ook risico's met zich mee. Het is van belang om op economisch vlak de risico's voor de nationale veiligheid nauwlettend in de gaten te houden. De dreiging kan zich manifesteren als een fysieke obstructie van economische chokepoints, het opleggen van sancties door vreemde mogendheden, heimelijke staatsinvloed achter buitenlandse overnames en investeringen (aantasting *level-playing field*¹⁵), inlichtingenvergaring op monopolieposities, het verwerven van kennis in Nederlandse bedrijven (waaronder defensie industrie) en kennisinstellingen, aantasting van de kenniseconomie, en afhankelijkheden in de supply-chain en technologisch ontwikkeling. Dit wordt vergroot door de kwetsbaarheid van een transparante overheid en de toenemende technologisering. Daarbij speelt mee dat statelijke actoren die een bedreiging vormen voor de Nederlandse economische veiligheid een *whole of government approach* kunnen toepassen, waardoor de verhouding tussen staten en particuliere bedrijven op scherp komt te staan.

Toenemende casuïstiek illustreert dat de omvang en diversiteit van de economische veiligheid (EV) dreiging toeneemt. De vraag naar EV-inlichtingen vanuit de publieke sector, bedrijven en kennisinstellingen neemt hierdoor toe. Het beleidskader en -instrumentarium om op te treden is momenteel in ontwikkeling. De maatregelen op het gebied van EV vereisen zo concreet mogelijke inlichtingen om beleid te onderbouwen of richting te geven. De diensten kunnen momenteel niet voorzien in de toegenomen behoefte aan inlichtingen ten behoeve van EV. Kortom: de behoefte aan inlichtingen ten behoeve van economische veiligheid is zowel verdiept als verbreed.¹⁶

Wat doen we met de huidige middelen?

De diensten doen nu geen structureel operationeel onderzoek naar bedreiging van de Nederlandse economische veiligheidsbelangen. De huidige EV-onderzoeks aanpak is als gevolg van geringe onderzoekscapaciteit reactief ('incident-driven') en beperkt in focus. Dit resulteert in een zeer beperkt zicht op de omvang, aard en impact van de EV-dreiging tegen NL belangen. Incidenteel kunnen de diensten concrete casussen onderzoeken waarmee zij de behoeftestellers handelingsperspectief bieden en bijdragen aan het vergroten van de weerbaarheid. Dit is een probleem, omdat inlichtingen van de diensten in belangrijke mate bijdragen aan de effectiviteit van het Rijksbrede beleidskader en -instrumentarium (in ontwikkeling) voor EV. Binnen deze capaciteit dragen de diensten Rijksbreed bij aan o.a.:

- Een handelingsperspectief voor cyber(incidenten);
- De regeling ongewenste kennisoverdracht (OCW)
- Project Sensitieve technologie
- Investeringsstoetsen (EZK)
- Exportcontrole (BZ)

¹⁵ Een gelijk speelveld tussen ondernemingen op de interne markt.

¹⁶ Dit is in lijn met de oprichting van de Ministeriele en hoog ambtelijke commissie voor Economie & Veiligheid in 2019.

- Structurele samenwerking telecom
- Awareness en weerbaarheid(sverhogende maatregelen) bij vitale sectoren en de defensie-industrie.

Waarvoor zijn aanvullende middelen noodzakelijk?

Met aanvullende middelen kunnen de diensten structureel onderzoek doen naar de bedreiging van de Nederlandse economische veiligheidsbelangen, wat zal bijdragen aan het onderkennen, voorkomen en tegengaan van activiteiten die een dreiging vormen voor de Nederlandse en bondgenootschappelijke belangen en/of nationale veiligheid. Om de publieke en private sector, waaronder de defensie-industrie, te voorzien van structurele en proactieve dreigingsinformatie zijn additionele investeringen nodig. Hiermee kunnen de diensten tegemoet komen aan de toenemende vraag. Zowel in uitbreiding en verdieping van kennis en capaciteit op traditionele onderwerpen als landenonderzoek, contra-inlichtingen (CI) en Cyber, maar ook uitbreiding op 'nieuwe' expertisegerieden, zoals financieel-economisch onderzoek naar bijv. financierings- en eigendomsconstructies rondom investeringen (verhullen staatsleningen) en exportvergunningen (coverbedrijven om staatsbetrokkenheid te verhullen). Hierbij wordt ook extra geïnvesteerd in Open Source Intelligence (OSINT).

Het is van belang om in het kader van EV, en de te beschermen belangen, zowel naar diversiteit in actoren als doelwitten te kijken. Een substantiële verhoging van de capaciteit geeft de diensten de mogelijkheid om meer diepteonderzoeken te doen, wat zal leiden tot beter zicht, concrete casuïstiek en daarmee tot meer mogelijkheden voor awareness- en outreach activiteiten, ook gericht op het nemen van gerichte maatregelen. Daarnaast kan geïnvesteerd worden in het aantrekken van middelen en mensen met de juiste expertise om te adviseren over weerbaarheidverhogende maatregelen.

Met aanvullende middelen voor EV kunnen we:

- Een betere inlichtingenpositie opbouwen meer zicht op de intenties en inzet van economische (machts)middelen door staten.
- Preventie: in het kader van EV potentiële doelwitten binnen Nederlandse bedrijfsleven alsmede kennisinstellingen en beleidsmakers informeren en hen voorzien van relevante dreigingsinformatie over intenties, werkwijzen en aanvalskennmerken.
- Detectie: Tijdig onderkennen van heimelijke (inlichtingen)activiteiten die een dreiging kunnen vormen voor de Nederlandse EV-belangen.
- Respons: (Actief) frustreren dan wel verstoren van (digitale) inlichtingenoperaties om vroegtijdig dreigingen tegen Nederlandse belangen weg te nemen. Daarnaast in de diepte en de breedte een handelingsperspectief betreffende economische veiligheid (mede-) ontwikkelen.

Hoe moeten we het (succes) meten?

- Periodiek normbeeld van de dreiging
- Zicht op trends en ontwikkelingen (bijv. op sensitieve technologieën)
- Uitgebrachte dreigingsanalyses en inlichtingenproducten (casuïstiek gebaseerd)
- Naslagverzoeken en mededelingen hierover (zie exportcontrole regime en investeringstoets)
- Dreigingspresentaties en beveiligingsadviezen publieke en private sector
- Het behalen van de dekkingsgraad GA

Effecten, voor- en nadelen

- + Een betere inlichtingenpositie geeft meer zicht op de intenties en inzet van economische (machts)middelen door staten.
- + Met een betere inlichtingenpositie wordt het beleidsinstrumentarium / -kader gevoed met inlichtingen

- + Een betere inlichtingenpositie zorgt voor een betere appreciatie van de dreiging gericht tegen de Nederlandse economische belangen
- + Een betere inlichtingenpositie zorgt voor een betere en meer geïnformeerde afweging tussen publieke belangen en het kunnen treffen van de juiste maatregelen
- + Een betere inlichtingenpositie is ondersteunend aan een breed scala aan beleidsopties.
- + Met versterking van de weerbaarheid verhogende taak van de diensten zijn de AIVD en de MIVD beter in staat om publieke en private partijen en vitale sectoren te adviseren over weerbaarheid verhogende maatregelen.
- De inlichtingenpositie zal niet van de een op de andere dag verbeteren, dit is een geleidelijk proces.
- De kwantitatieve effecten van de beleidsopties zijn moeilijk meetbaar.

Uitvoering

AIVD + MIVD

Budgettaire gevolgen

Het hier opgenomen bedrag is inclusief de posten van AIVD en MIVD die betrekking hebben op de fiches "Expertise teams en expertise eenheid vitaal", "Voorkomen ongewenste zeggenschap", "Kennispbouw sensitieve technologie" en het fiche "Beschermen Technologie en Kennis". Deze posten zijn opgenomen in betreffende fiches, waarbij is aangegeven dat de betreffende bedragen onderdeel vormen van onderstaande claims.

MEUR

	2021	2022	2023	2024	2025	2026
AIVD						
MIVD						

5.1.2i

Koppeling andere thema's

- Cyber fiche
- Nationale cryptostrategie
- Fiche Veilige Inkoop en aanbestedingen Rijksoverheid

Overkoepelend fiche 2. Versterken kennisbasis overheid sensitieve technologie en afhankelijkheden

Probleemanalyse

Nationale veiligheidsbeleid richt zich van oorsprong met name op vitale processen en rijksoverheid. Steeds vaker zien we dat de risico's voor de nationale veiligheid ook breder spelen. Op het gebied van technologie, kennis en in de waardeketen rondom vitale processen zijn onderdelen waarvan we het onwenselijk achten dat die in handen komen van andere staten. Dit om te voorkomen dat andere staten controle kunnen uitoefenen over onze vitale processen, toegang krijgen tot gevoelige kennis en informatie of dat ongewenste asymmetrische afhankelijkheden ontstaan.

Om ongewenste overdracht van technologie en kennis tegen te gaan heeft Nederland drie hoofd instrumenten: exportcontrole, investeringstoetsing en een (in ontwikkeling zijnde) kennisregeling voor toetsing van studenten en wetenschappers. Deze drie instrumenten moeten in samenhang worden gezien. Wanneer bijvoorbeeld een exportvergunning met het oog op de nationale veiligheid niet wordt afgegeven moet die techniek niet via een bedrijfsovername alsnog in de verkeerde handen vallen.

Op een aantal terreinen is de afgelopen jaren in kaart gebracht (d.m.v. ex ante analyses) welke belangen moeten worden beschermd in de vitale infrastructuur. Over gehele breedte van de overheid is echter nog onvoldoende zicht op de technologische toepassingen die mogelijk risico's opleveren voor de nationale veiligheid. Om veiligheidsrisico's van nieuwe technologische toepassingen adequaat en eigenstandig in te kunnen schatten, moet de Rijksoverheid over de juiste kennisbasis beschikken om hierover te kunnen adviseren en te acteren. Binnen de Rijksoverheid is momenteel slechts beperkte kennis over nieuwe, opkomende technologieën; en waar deze kennis wel aanwezig is, wordt deze niet altijd bij elkaar gebracht. Kennisdeling tussen marktpartijen, semipublieke partijen en overheid vindt nu ad hoc plaats.

Eigenstandig beleid op het gebied van sensitieve technologie vereist ook een eigenstandige kennisbasis. Het investeren in voldoende kennis en expertise ten behoeve van de overheid voor beleidsontwikkeling en toepassing van beleid (casuïstiek) vraagt de komende jaren dan ook meer aandacht. Daarbij is het belangrijk dat er inzicht wordt verkregen in welke technologische toepassingen - en innovaties voor Nederland (en daarbuiten) sensitief zijn en welke dat (op termijn) kunnen worden. Deze kennis dient gekoppeld te worden aan inzicht in de (heimelijke) agenda's van statelijke actoren.

Naast het versterken van onze kennispositie op sensitieve technologieën is het daarom ook van belang meer inzicht te krijgen in afhankelijkheden. Er bestaat een sterke wisselwerking tussen technologie enerzijds en afhankelijkheden anderzijds. Een versterkte kennisbasis van sensitieve technologie draagt bij aan het beter inzichtelijk maken van technologische afhankelijkheden. Tegelijkertijd zijn er reeds bestaande afhankelijkheden bijvoorbeeld via productieketens die de ontwikkeling van nieuwe technologie kunnen beïnvloeden.

Maatregelen

De eerste stappen voor het versterken van de kennisbasis zijn gezet in het kader van het interdepartementale traject sensitieve technologie. Binnen dit traject worden (door een extern kennisnetwerk) een begrippenkader en dynamische en toekomst robuuste systematiek ontwikkeld om sneller inzicht te krijgen welke kennis en technologieën mogelijk een risico vormen voor de nationale veiligheid. Deze systematiek en de daarmee opgebouwde kennis stelt de overheid beter in staat om relevant beleid bij te sturen en (bestaande) instrumenten toe te passen.

De ontwikkeling van de systematiek en het begrippenkader moet de Rijksoverheid de komende jaren in staat stellen, met gebruik van de juiste expertise van het bedrijfsleven en kennisinstellingen, eigenstandig opkomende technologische toepassingen en innovaties te wegen op risico's voor de nationale veiligheid. Om de opgebouwde kennis en het gebruik van het begrippenkader en de systematiek te borgen, is voldoende capaciteit nodig bij de verschillende

departementen. Het gaat hier dan om capaciteit voor het gebruik van de methodiek en de implementatie van de uitkomsten in beleid (instrumenten) en uitvoering. Een ander element van de langetermijnborging van de kennis en systematiek, is het bij elkaar brengen van de al aanwezige kennis (o.a. bij BHOS, DEF, EZK en de I&V-diensten) die op dit moment te versnipperd en ad hoc wordt ingezet. Daarbij leunen veel departementen voor technologische kennis in relatie tot nationale veiligheid nu op de expertise van specialistische afdelingen. Zoals de afdeling Export Strategische Goederen (BZ) en de NCSC (JenV).

Om aan de huidige ambitie te voldoen zijn er bij alle departementen die met sensitieve technologie te maken hebben extra middelen nodig. De huidige ambitie gaat er vanuit dat alle departementen zelf en los van elkaar de kennisbasis borgen die zij nodig hebben.

De uitgebreide ambitie tracht om meer samenhang in de kennisbasis van de overheid te brengen. Onder dit scenario hebben alle betrokken departementen net als in het basis scenario extra middelen nodig. Daarvoor bundelen deze departementen hun kennis via een kennisnetwerk.

De next level ambitie gaat nog een stap verder. Hierin wordt een zelfstandige kennisunit Technologie en Nationale Veiligheid opgericht binnen de Rijksoverheid. Deze unit voorziet alle departementen van kennis en advies over sensitieve technologieën.

CONCEPT

Fiche A – Ad hoc advisering sensitieve technologie**Omschrijving voorgestelde maatregelen**

- Ieder departement claimt eigen FTE en blijft op basis van casuïstiek vanuit eigen expertise bijdragen aan de afweging voor wat betreft eigen instrumentarium.
- Concrete maatregelen voor exportcontrole en de toetsing van studenten en wetenschappers staan beschreven in het fiche 'Beschermen Technologie en Kennis'
- Concrete maatregel voor de investeringstoets staan in het fiche 'Voorkomen Ongewenste Zeggenschap'.

Effecten, voor- en nadelen

- Budgettaire beslag.
- Uitdagingen betreffen het borgen, delen en toegankelijk maken van informatie.
- Aanpak blijft ad hoc en beperkt gestructureerd, wat minimale bijdrage levert aan behalen doel van een versterkte kennisbasis.

Uitvoering

Alle departementen die momenteel ook betrokken zijn bij het interdepartementale traject (BZ, BZK, DEF, EZK, JenV en OCW).

Budgettaire gevolgen**Budgettaire gevolgen in mln. euro's (+ = saldoerslechterend)**

	2022	2023	2024	2025	2026	Struc.
Ad hoc advisering ¹⁷						

5.1.2i

¹⁷ Door alle betrokken departementen (BZ, BZK, DEF, EZK, JenV en OCW).

Fiche B – Interdepartementaal kennisnetwerk sensitieve technologie

Omschrijving voorgestelde maatregelen

Kennisnetwerk Technologie en Nationale Veiligheid

- Inrichten kennisnetwerk sensitieve technologie relevant voor NV. Dit kennisnetwerk brengt de expertise van verschillende departementen bijeen. Het kennisnetwerk vormt een verzamelpunt voor de kennis van o.a. exportcontrole, het stelsel van investeringstoetsing en in het kader van de brede kennisregeling. Het kennisnetwerk borgt dat er voldoende kennis en expertise binnen de rijksoverheid is voor beleidsontwikkeling en casuïstiek.
- Ook biedt het inzicht in wat kritische technologieën en strategische afhankelijkheden zijn en zullen worden. Daarmee vormt het een structurele inbedding van de dynamische methodiek die middels de verkenning sensitieve technologie wordt uitgewerkt. De deelnemers aan het kennisnetwerk moeten allen over de benodigde screening beschikken.
- Om doelgroeporganisaties met actuele kennis van zaken te adviseren wil het NCSC zijn kennispositie versterken, onder andere op het gebied van operationele technologie in de vitale infrastructuur (Industrial and Automated Control Systems (IACS)) en andere relevante technologische ontwikkelingen (o.a. Artificial Intelligence, machine learning, zero-trust encryptie, containerisation).
- Versterking adviesfunctie operationele technologie (IACS). De digitalisering van productieprocessen neemt de komende jaren verder toe en daarmee groeide de afhankelijkheid van IACS in onze samenleving. Naast ICT moeten ook vitale productieprocessen daarom goed worden beschermd. Het NCSC wil mede daarom opvolging geven aan het advies van de Cybersecurity Raad ten aanzien van OT.

Effecten, voor- en nadelen

- + Meer gestructureerde en geïnstitutionaliseerde borging van kennisbasis.
- + Opgebouwde kennis en gebruik van begrippenkader en systematiek over sensitieve technologie wordt geborgd.
- Extra aandacht nodig voor vertrouwelijkheid door nauwe samenwerking met private partijen en kennisinstellingen in combinatie met NV vraagstukken.
- Budgettaire beslag.

Uitvoering

Betrokkenheid van alle departementen die momenteel ook betrokken zijn bij interdepartementale traject (BZ, BZK, DEF, EZK, JenV en OCW). Wanneer het kennis of casuïstiek bij een ander departement betreft wordt ook dit departement betrokken (bijv. LNV, VWS, I&W).

Budgettaire gevolgen

Budgettaire gevolgen in mln. euro's (+ = saldooverslechterend)

	2022	2023	2024	2025	2026	Struc.
Inrichten van een kennisnetwerk ¹⁸						2
Sensitieve technologie specialisten en ondersteuning ¹⁹						
Opbouw specifieke technische kennis AIVD ²⁰	-	-	-	-	-	-
Opbouw specifieke technische kennis MIVD ²¹						

¹⁸ Interdepartementale claim (BZ, BZK, DEF, EZK, JenV en OCW).

¹⁹ 5 FTE voor specialisten op gebied van (1) natuurkunde en fysica; (2) chemisch/biologisch; (3) informatica en elektrotechniek; (4) lucht- en ruimtevaart en rader en; (5) maritiem en navigatie. Incl. 0,5 FTE ondersteuning komt op 715k. Plus jaarlijkse scholing en outreach (50k + 10k).

²⁰ AIVD bijdrage hierop is onderdeel van de totale claim voor de AIVD zoals opgenomen in het fiche 'Versterking inlichtingenpositie'.

²¹ Het hier opgenomen bedrag betreft een onderdeel van de totale claim voor de MIVD zoals opgenomen in het fiche 'Versterking inlichtingenpositie'.

Versterken adviesfunctie NCSC



5.1.2i

CONCEPT

Fiche C – Kennisunit sensitieve technologie

Omschrijving voorgestelde maatregelen

Kennisunit Technologie en Nationale Veiligheid

- Inrichten zelfstandige kennisunit binnen de overheid, met betrokkenheid van bedrijfsleven en kennisinstellingen, die eigenstandig met systematiek sensitieve technologie en kennisbasis adviseert over beleid t.a.v. sensitieve technologieën. Verantwoordelijkheid voor verschillend instrumentarium blijft wel bij bevoegde ministers.
- De kennisunit bedient de uitvoerders van Exportcontrole, Investeringsstoetsing en de (in ontwikkeling zijnde) Kennisregeling.
- Door de samenwerking wordt bewustwording en draagvlak bij bedrijven en kennisinstellingen vergroot. Tegelijkertijd wordt expertise vanuit bedrijven en kennisinstellingen beter benut. Het team jaagt de ontwikkeling van een kennisecosysteem aan waarin kennis van nieuwe technologieën van publieke en private partijen bijeen wordt gebracht.
- Alle betrokken departementen detacheren experts bij de centrale eenheid. Daarnaast heeft de eenheid eigen personeel nodig (directeur, bedrijfsvoering, ondersteuning etc.) en huisvesting.
- Zie voorgestelde maatregelen van fiche B voor inzet NCSC.

Effecten, voor- en nadelen

- + Intensieve vorm van samenwerking om juiste kennis en expertise bijeen te brengen, kan proactief en adequaat reageren op ontwikkelingen.
- + Kennis en expertise centraal binnen de Rijksoverheid belegd en op afstand van uitvoerders. Dit borgt zicht op te beschermen technologieën en meer integrale besluitvorming.
- + Maakt het borgen, delen en toegankelijk maken van informatie efficiënter.
- Extra aandacht nodig voor vertrouwelijkheid door nauwe samenwerking met private partijen en kennisinstellingen in combinatie met NV vraagstukken.
- Kent een groter budgettaire beslag.

Uitvoering

Betrokkenheid van alle departementen die momenteel ook betrokken zijn bij interdepartementale traject (BZ, BZK, DEF, EZK, JenV en OCW). Wanneer het kennis of casuïstiek bij een ander departement betreft wordt ook dit departement betrokken (bijv. LNV, VWS, I&W).

Budgettaire gevolgen

Budgettaire gevolgen in mln. euro's (+ = saldooverslechterend)

	2022	2023	2024	2025	2026	Struc.
Inrichten van een kennisunit ²²						
Sensitieve technologie specialisten en ondersteuning ²³						
Opbouw specifieke technische kennis AIVD ²⁴	-	-	-	-	-	-
Opbouw specifieke technische kennis MIVD ²⁵						
Versterken adviesfunctie NCSC						

5.1.2i

²² Interdepartementale inzet (BZ, BZK, DEF, EZK, JenV en OCW).

²³ 11 FTE voor specialisten op gebied van (1) quantum; (2) kernfysica; (3) biologie; (4) chemie; (5) AI; (6) cyber; (7) mechatronica en halfgeleiders; (8) lucht- en ruimtevaart; (9) maritieme techniek; (10) materiaalkunde en; (11) radar- en navigatie technologie. Incl. 1 FTE ondersteuning komt op 1,560M. Plus jaarlijkse scholing en outreach (110k + 20k).

²⁴ AIVD bijdrage hierop is onderdeel van de totale claim voor de AIVD zoals opgenomen in het fiche 'Versterking inlichtingenpositie'.

²⁵ Het hier opgenomen bedrag betreft een onderdeel van de totale claim voor de MIVD zoals opgenomen in het fiche 'Versterking inlichtingenpositie'.

Overkoepelend fiche 3. Strafbaarstelling spionage

Probleemanalyse

Buitenlandse mogendheden kunnen op allerlei manieren op heimelijke wijze gevoelige informatie verzamelen in en over Nederland waardoor Nederlandse belangen kunnen worden geschaad. Buitenlandse mogendheden proberen o.a. binnen te komen bij ministeries, opsporings- en veiligheidsdiensten, politieke partijen en cultureel-maatschappelijke organisaties. De door politieke spionage verkregen informatie dient als voorkennis voor staten om in te kunnen spelen op politieke of maatschappelijke ontwikkelingen. De verkregen informatie kan ook worden ingezet om besluitvorming te beïnvloeden. Dit is schadelijk voor de soevereiniteit en het handelingsvermogen van de Nederlandse overheid, alsmede het functioneren van de democratische rechtsorde en de daarin gedeelde waarden.

Daarbij zijn er landen met een diaspora in Nederland die hier -openlijk en heimelijk- persoonsgegevens verzamelen vanuit een intern veiligheidsbelang. Deze landen schrikken er niet voor terug leden van de diasporagemeenschap te mobiliseren om tegenstanders en critici binnen de gemeenschappen de mond te snoeren of onder druk te zetten om anderszins mee te werken. Dit kan leiden tot spanningen binnen de gemeenschappen. Het effect van het verzamelen van persoonsgegevens (middels spionage) is een inbreuk op de persoonlijke levenssfeer en vormt een bedreiging voor de (beleefde) veiligheid van burgers in Nederland, alsmede de sociale cohesie.

De Nederlandse economie is hoogontwikkeld, innovatief en internationaal georiënteerd. Daardoor is Nederland in toenemende mate een doelwit van economische spionage, wat schadelijk is voor het verdienvermogen van Nederland en daarmee de economische veiligheid. Uit onderzoek blijkt dat meerdere Nederlandse topsectoren doelwit zijn (geweest) van (digitale) spionage. Daarbij kan via spionage ook informatie worden verkregen t.b.v. de mogelijkheid tot sabotage.

Ook het feit dat Nederland gastland is voor een groot aantal internationale organisaties maakt Nederland een interessant doelwit voor spionage.

De aanpak voor het tegengaan van statelijke dreigingen is uiteengezet in de Kamerbrief Tegengaan statelijke dreigingen²⁶. Hierin wordt het brede palet aan maatregelen geschetst voor het tegengaan van onder andere ongewenste buitenlandse inmenging en het bevorderen van de economische veiligheid. De mogelijkheden om in repressieve zin op spionage te reageren zijn echter beperkt. Indien het inlichtingenofficiërs betreft met een diplomatieke status, kan een diplomaat worden uitgezet (met veelal als gevolg een spiegeling en uitzetting van NL-diplomaat). Tegen agenten en niet-diplomatieke inlichtingenofficiërs kan een dergelijk middel niet worden ingezet. Wel zijn er verschillende strafrechtelijke mogelijkheden om personen die betrokken zijn bij spionage daarvoor te vervolgen. In de eerste plaats kan gedacht worden aan misdrijven die verband houden met de schending van staats-, ambts- en (bedrijfs)geheimen en omkoping/corruptie. Maar ook bijvoorbeeld de strafbaarstelling van bijvoorbeeld tappen, de vernieling van infrastructuur en verschillende computerdelicten, kunnen ingezet worden. De Wet computercriminaliteit III heeft hieraan nog enkele strafbaarstellingen toegevoegd. Heimelijke samenwerking of het hebben van (structureel) contact met een buitenlandse inlichtingendienst/mogendheid is op zichzelf op dit moment niet strafbaar. Dit betekent dat in gevallen waarin de 'informant' geen ambtenaar is, waarin er (nog) geen digitale spionageactiviteiten hebben plaatsgevonden of waarin de verstrekte informatie niet (staats)geheim is, de mogelijkheden om strafrechtelijk op te treden ontbreken. Hieraan bestaat wel behoefte omdat, zoals hiervoor aan de orde kwam, ook in dergelijke gevallen reeds activiteiten plaatsvinden en informatie wordt verstrekt die de Nederlandse belangen kan schaden. Een dergelijke strafbaarstelling biedt meer mogelijkheden om (al in een eerdere fase) strafrechtelijk op te treden tegen spionageactiviteiten en vergroot de kans op een succesvolle vervolging. Het ontbreken van een specifieke strafbaarstelling heeft tot gevolg dat er geen duidelijke normstelling is vanuit de overheid ten aanzien van dergelijke inlichtingenactiviteiten, terwijl deze een ernstige inbreuk vormen op de Nederlandse soevereiniteit. Inmiddels hebben verschillende landen specifieke

²⁶ TK 2018-2019, 30821, NR. 72

wetgeving op dit gebied geïntroduceerd. Denemarken, Duitsland en Frankrijk hebben reeds wetgeving geïntroduceerd; in het Verenigd Koninkrijk is men bezig met de ontwikkeling hiervan. Ook gelet op deze ontwikkeling lijkt het aangewezen dat Nederland met wetgeving op dit terrein komt, om te voorkomen dat Nederland een relatief aantrekkelijk land wordt voor andere mogelijkheden om spionageactiviteiten te ontplooiën.

Gelet op bovenstaande wordt geadviseerd om een nieuwe strafbaarstelling te introduceren waarin het werven van informanten en het delen van informatie met een buitenlandse inlichtingendienst of een buitenlandse mogendheid strafbaar wordt gesteld.

Omschrijving voorgestelde maatregelen

- Introductie van een nieuwe strafbaarstelling waarin het werven van informanten en het delen van informatie met een buitenlandse inlichtingendienst of een buitenlandse mogendheid strafbaar wordt gesteld.

Effecten, voor- en nadelen

- + Strafbbaarstelling van spionage biedt extra bescherming voor de belangen van de Nederlandse Staat en Nederlandse burgers d.m.v. de mogelijkheid voor de inlichtingen- en veiligheidsdiensten om een ambtsbericht uit te brengen, waarna de nationale politie onderzoek kan doen en het OM over kan gaan tot vervolging.
- + Van dergelijke wetgeving gaat een preventieve werking uit (personen kunnen minder snel geneigd zijn te spioneren voor buitenlandse mogendheden, het kan mensen die 'geworven' worden weerbaarder maken omdat zij kunnen wijzen op het strafrechtelijk verbod en ook mogelijkheden zelf zullen terughoudender worden).
- + Normstelling overheid ten aanzien van spionage en bescherming soevereiniteit.
- Vergt een wetswijziging (aanpassing van het Wetboek van Strafrecht).
- Strafbbaar gedrag moet voldoende concreet omschreven worden. Voorkomen moet worden dat personen die onbewust worden ingezet door buitenlandse mogendheden of die zelf een doelwit zijn van een buitenlandse mogendheid daarvoor strafbaar worden. Ook is nog een vraag in welke mate het delen van niet geheime informatie strafbaar kan worden gesteld, mede in het licht van de vrijheid van meningsuiting en de vrijheid van informatie. Dit zal mede afhankelijk zijn van de mate waarin de schadelijkheid van een dergelijke gedraging kan worden onderbouwd.
- Bewijsbaarheid en handhaving is naar verwachting lastig, maar niet onmogelijk bij goede samenwerking tussen de I&V-diensten, OM en opsporingsdiensten.

Uitvoering

Inlichtingen- en Veiligheidsdiensten, opsporingsdiensten, openbaar ministerie, rechterlijke macht.

Budgettaire gevolgen

Op het moment dat wetgeving van kracht is, is de inschatting dat het zal gaan om slechts een aantal zaken per jaar (in bovenstaande tabel wordt uitgegaan van 3 zaken per jaar). Daar zullen de volgende kosten uit voortvloeien:

- Kosten voor DJI indien gevangenisstraffen worden opgelegd.
- Politie: Een grootschalige zaak (TGO) kost ongeveer 10 tot 15 FTE per zaak, per jaar (1,5 miljoen euro). Deze behoefte zal voor een spionage zaak vergelijkbaar zijn gezien de complexiteit.
- Opleiding / training politie: Een E-learning ontwikkelen kosten ong. 30.000 euro. Daarnaast komen er kosten voor uitrol E-learning, aanpassing ICT middelen etc.

- Opleiding / training OM: Ontwikkelen en uitvoeren van een ééndaagse basiscursus én een ééndaagse verdiepingscursus voor de relevante clusters binnen het Landelijk Parket zal ongeveer 28.000 euro kosten. Als de cursus jaarlijks aangeboden wordt voor eventueel nieuw personeel binnen het CT cluster zijn er extra uitvoeringskosten; gemiddeld 2000 euro voor een groep/klas van 20 personen.
- Gezien de inschatting van enkele zaken per jaar verwacht het openbaar ministerie dit met de huidige personele capaciteit op te kunnen vangen. Als blijkt dat het aantal zaken per jaar een stuk hoger ligt kunnen de opgegeven kosten voor het OM hoger uitvallen.

Budgettaire gevolgen in mln. euro's (+ = saldoverslechterend)²⁷

	2022	2023	2024	2025	2026	Struc.
Deelmaatregel 1 ²⁸						

5.1.2i

²⁷ De bedragen zijn gebaseerd op de inschatting van 3 zaken per jaar.

²⁸ Financiële onderbouwing in voetnoot uitsplitsen per departement.

Overkoepelend fiche 4. Effectieve internationale inzet

Wat in het buitenland gebeurt, raakt rechtstreeks aan de veiligheid van Nederland. Effectieve internationale inzet is daarom nodig in het Nederlands belang. Veiligheid is cruciaal voor het Nederlandse buitenlandbeleid. De internationale veiligheidssituatie is de afgelopen jaren verslechterd. Dit vraagt om extra inzet. De extra inzet richt zich op: I) digitale veiligheid en II) economische veiligheid. Dit is hieronder verder uiteen gezet.

Deel II: Economische Veiligheid

Essentie: Nederland en zijn bondgenoten zien zich in toenemende mate geconfronteerd met rivaliteit en instabiliteit in de internationale politiek-economische rechtsorde en veiligheid.

Autocratische, centraal geleide staten zetten in toenemende mate in op het bereiken van strategische dominantie en het creëren van eenzijdige strategische afhankelijkheden op economisch en technologisch gebied. Nederland moet zich daar in toenemende mate tegen verweren, om de politieke en economische vrijheden te waarborgen.

Samenwerking met autocratische landen moet op evenwichtige, gelijkwaardige en strategisch autonome wijze verder vormgegeven worden. Samenwerking met Europese, trans-Atlantische en andere internationale bondgenoten is daarbij cruciaal. Dit vereist extra inzet om dreigingen en kansen te identificeren en de Europese, trans-Atlantische en internationale samenwerking te versterken. Samenhang van en balans in het EV-beleid, met oog voor diplomatieke consequenties, dient geborgd te worden.

Ontwikkelingen

Nederland is een open en internationaal verweven land, dat brengt ons veel welvaart. Tegelijkertijd staat die openheid in de huidige geopolitieke situatie onder druk door dreigingen van buitenaf. Een integrale aanpak is essentieel om de openheid van de Nederlandse samenleving te behouden en tegelijk de nationale veiligheid te borgen. Zowel beleidsinhoudelijk ('economie-veiligheid') als langs de as 'internationaal-Europees-nationaal' is het noodzakelijk alle belangen in samenhang te bezien.

Technologie staat meer dan ooit centraal in nationale veiligheidsvraagstukken. Dit is onder andere het gevolg van de toenemende inzet van technologie in een internationale geopolitieke strijd, het *dual-use* karakter van technologie en de grote verwevenheid van technologieën in het maatschappelijk functioneren (IoT, AI, Robotics). Dit leidt tot nieuwe vragen over de relatie tussen technologie, veiligheid en economie.

NL belangen

Wereldwijde technologische ontwikkelingen zijn van grote invloed op de Nederlandse concurrentiekracht en het innovatievermogen van de Nederlandse economie. Alleen door zelf een leidende kenniseconomie te zijn kunnen we het Nederlandse verdienvermogen behouden. Internationale samenwerking op terrein van technologie, innovatie en wetenschap is voor de Nederlandse kenniseconomie en speciaal voor de topsectoren van cruciaal belang. Tegelijkertijd worden Nederland en Europa als kenniseconomie weerbaarder tegen dreigingen van buitenaf. Het fiche 'offensief industriebeleid en concurrentiekracht' doet voorstellen om deze leidende kenniseconomie in stand te houden. Daarnaast gaat het fiche 'beschermen technologie en kennis' in op maartregelen om de ongewenste overdracht van kennis en technologie te voorkomen.

Ook op veiligheidsgebied zal kennis en technologie hoge prioriteit hebben. In relatie tot cyber en kritische infrastructuur w.o. telecom maar ook in relatie tot militaire toepassing w.o. wapensystemen en *dual-use* goederen in het kader van non-proliferatie als ook hybride oorlogsvoering. Tegelijkertijd gaat het, mede in het kader van sensitieve technologie, ook over (voorkomen van) strategische afhankelijkheden. Deze tech hoeft zelf niet direct *high-tech* van aard maar wel belangrijk zijn zoals op gebied van grondstoffen zoals als kritieke aardmetalen en -gas, of vrije en veilige toegang tot strategisch belangrijk aanvoerroutes bijv. maritieme veiligheid in de regio Zuidoost Azië maar ook in de *Arctic* en *space*.

Internationale opgave

Dit fiche voegt daar de rol van Nederland in het buitenland aan toe. EV is in hoge mate een internationaal vraagstuk. Concreet stelt het EV vraagstuk NL voor de volgende internationale opgaven:

- (1) beschermen van NL en EU veiligheidsbelangen in de economische sfeer.
- (2) voorkomen dat EV vraagstukken de betrekkingen met het buitenland, bondgenoten en anderen aantasten. Denk hierbij aan de maatregelen die NL heeft getroffen op het gebied van 5G.
- (3) voorkomen of minimaliseren van economische schade agv EV maatregelen van derde landen. Denk aan verscherpte exportcontroleregimes in [REDACTED], die NL bedrijven voor nieuwe uitdagingen stellen.

5.1.2a

Hierbij zijn de volgende zaken instrumenteel:

-Daarbij is het van belang om verder helder te krijgen wat de EV-dreigingen zijn. Enerzijds om risico's van buitenaf te mitigeren (defensief) en anderzijds om onze economie en die van bondgenoten sterker te maken (offensief). Ook de innovatie attachés van EZK zijn op dit offensieve terrein al actief en betrokken bij de (inschatting van de effecten van) defensieve maatregelen. Dit vergt kennisopbouw op het gebied van technologie en veiligheidsaspecten van de economie. Traditioneel wordt vooral gekeken naar internationale aspecten van militaire en dual use technologie. De reeks van technologieën die gevoelig is, breidt zich de laatste jaren sterk uit. Nederland kijkt traditioneel naar de internationale economie als een proces vrij optreden van marktpartijen en wederzijds voordeel centraal staan. Deze blijft relevant. Maar dit is niet meer voldoende. NL moet zich opmaken om de taal van de macht te verstaan, ook in de economische sfeer. Ook dit vergt extra kennisopbouw en analytische capaciteit.

- Mogelijkheden voor samenwerking in kaart brengen en benutten, zoals die leven bij verschillende bondgenoten, andere partners en in internationale gremia, en te onderzoeken met welke staten er in coalitieverband of partnerschap geopereerd kan worden. NL is internationaal een weerbare partner. Internationale partnerschappen en coalitievorming met bondgenoten en andere partners (zie ook financiële onderbouwing), in Europees (eerste en tweede pijler o.a. GBVB/GVDB), trans-Atlantisch (o.a. NAVO) en internationaal verband, worden de komende jaren nog belangrijker. Belangrijk is ook om op die basis de samenwerking met de staten waar de dreigingen uit komen op evenwichtige, gelijkwaardige, strategische autonome wijze verder vorm te geven. Tweezijdige, internationale, strategische afhankelijkheden zijn op lange termijn de beste garantie voor het borgen van EV en de nationale veiligheid.

-Diplomatieke bemiddeling bij concrete problemen. Dit is een belangrijk instrument in EV.

A. versterking van de internationale inzet door:

- Personele versterking van de meest relevante posten (politieke afdelingen, economische afdelingen, JenV- en/of innovatie-attachenetwerk – 'one-team') t.b.v. de nexus 'economie-veiligheid-technologie' in het kader van de brede politieke relatie. Dit netwerk richt zich op de volgende taken in het kader van EV:
 - Versterking van Europese en Trans-Atlantische samenwerking en samenwerking met overige relevante internationale partnerlanden en fora op het gebied van economische veiligheid:
 - intensievere monitoring ('early warning & action') en advisering over ontwikkelingen op gebied van EV ('nexus') in deze landen en fora;
 - uitvoeren van kabinetsbeleid, in het bijzonder het aangaan en verdiepen van coalities en partnerschappen met deze Europese en Transatlantische bondgenoten en andere relevante internationale partners en fora.
 - Vroegtijdige signalering van ontwikkelingen op EV en strategische afhankelijkheden in landen die niet direct tot bondgenoten worden gerekend. Ontsluiten van informatie in vreemde taal ter ondersteuning van strategisch nationaal beleid.
- Ondersteunend hier aan: programmabudget t.b.v. kleinschalige netwerk-, outreach-, kennis, onderzoeks- en andere samenwerkingsprojecten op het terrein van EV ('early warning & action').
- Versterking van de Rijksbrede faciliteiten t.b.v. beveiligde VTC-verbindingen met Europese, trans-Atlantische en internationale bondgenoten, partners en fora.

- Formeren van integrale (economie, veiligheid en brede relatie), coördinerende en ondersteunende BZ/BHOS-taakgroep op economische veiligheid:
 - De taakgroep bundelt en overziet het BZ/BHOS-brede netwerk, informatie en kennis (zowel in Den Haag als in het postennet) op gebied van economie/handel, veiligheid, geopolitiek en landenspecifieke kennis.
 - Op deze basis identificeert de taakgroep sterkten en zwakten in en bedreigingen en kansen voor de BZ/BHOS- resp. Nederlandse aanpak op EV en doet het adviezen daarover.

Financiële onderbouwing:

BZ:

i: personele capaciteit in het postennet (PA en/of EA: veiligheid en economie, brede politieke relatie en coherentie) c.q. die landen die meest relevant zijn: Berlijn, Parijs, Londen, Ottawa, Washington, Beijing, Moskou, New Delhi, Canberra, Tokio, Seoul, Brussel (PVEU/PVNAVO), Geneve (ITU, WIPO, WTO) - 13 uitgezonden fte.

ii: programmamiddelen voor kleine activiteiten in het postennet t.b.v. het versterken van de diplomatiek respons denk aan financiële bijdragen aan kleine onderzoeksprojecten, studies, seminars, overige netwerk, outreach en communicatie-activiteiten, etc.)

iii: beveiligde VTC-verbindingen voor overleg met landen, EU en multilaterale fora die Rijksbreed ter beschikking worden gesteld (via 3W als reeds bestaande Rijksbrede shared service organisatie voor de buitenlandfunctie).

iv: personele capaciteit in Den Haag (EAB, DVB) t.b.v. de BZ/BHOS-brede taakgroep (secretariaat)- 2 fte in Den Haag.

EZK:

I: personele capaciteit in het IA postennet c.q. de landen die het meest relevant zijn zoals hierboven genoemd: DU, FRA, VK, VS, China, Rusland, India, Tokio, Seoul, en voor EZK ook Taiwan, 10 fte.

Ii: EZK: bij directie I&K en TOP: 2 FTE in Den Haag.

JenV: 4 FTE NCTV.

Overkoepelende economische analyse EV-fiches

Openheid, economie en veiligheid

Open markten en een sterke verwevenheid met andere economieën brengt Nederland al eeuwen welvaart. Handel is goed voor één derde van het inkomen in Nederland en voor één op de drie banen en buitenlandse investeringen goed voor één miljoen banen.

Deze (internationale) verwevenheid is een motor voor economische groei. Buitenlandse investeringen brengen kennis met zich mee en zorgen voor het uitwisselen van technologieën en ideeën. Handel en concurrentie met buitenlandse bedrijven creëren prikkels om te innoveren. Daarnaast maakt internationale handel het mogelijk dat ieder land doet waar het beste in is en we elkaars comparatieve voordelen benutten. In het bijzonder van een klein land als Nederland geldt dat we simpelweg niet alles zelf kunnen.

Een open economie komt ook onze nationale veiligheid ten goede. Dat gebeurt op vier manieren:

1. Open markten zorgen voor verwevenheid, wat bijdraagt aan vreedzame samenwerking en de kans op conflicten verlaagt, simpelweg omdat we elkaar nodig hebben.
2. Daarnaast zorgen open markten voor meer economische groei, waarmee we onze collectieve arrangementen, ook ten aanzien van onze nationale veiligheid, veilig kunnen stellen.
3. Buitenlandse oplossingen voor veiligheidsrisico's kunnen ook in Nederland toegepast worden. Zo maken wij dankbaar gebruik van in het buitenland ontwikkelde vaccins of cyberwalls en beschermen derde landen zich tegen overstromingen met behulp van Nederlandse expertise over de Deltawerken.
4. Tot slot draagt openheid bij aan kennisuitwisseling en creëren handel en concurrentie met buitenlandse bedrijven prikkels om te innoveren. Een innovatief Nederland (en Europa) is ook een minder kwetsbaar Nederland (en Europa).

Tegelijkertijd kan internationale openheid ook afbreuk doen aan onze economische veiligheid. Het kan ons bijvoorbeeld kwetsbaar maken voor (cyber)spionage en sabotage, manipulatie en beïnvloeding als ook ongewenste buitenlandse inmenging in het Nederlandse bedrijfsleven, kennisinstellingen en lokale overheden. De combinatie van geopolitieke en technologische ontwikkelingen versterken deze kwetsbaarheden. Dit kan niet alleen leiden tot een aantasting van onze fysieke veiligheid, maar kan ook leiden tot economische schade voor onze economie en bedrijfsleven.

Dit vraagt enerzijds om een effectieve aanpak van veiligheidsrisico's. Daarnaast is een proportionele aanpak minstens zo belangrijk, gegeven de (economische en veiligheids-)voordelen die openheid ons biedt.

Voorliggende beleidsaanbevelingen

Economische veiligheid gaat om het ongestoord functioneren van Nederland als effectieve en efficiënte economie. Dit omvat de continuïteit van vitale processen, de integriteit en exclusiviteit van informatie en kennis en het voorkomen van ongewenste strategische afhankelijkheden. De voorliggende beleidsaanbevelingen dragen hier op verschillende manieren aan bij.

Fiche 1, het versterken van de concurrentiekracht, begint bij het fundament. Een goede concurrentiepositie vergroot ons verdienvermogen en stelt ons in staat onze collectieve arrangementen te kunnen blijven betalen. Daaronder vallen ook publieke voorzieningen die in het belang zijn voor onze nationale veiligheid. Denk daarbij aan goed functionerende inlichtingendiensten en defensie-eenheden, maar ook aan de continuïteit van vitale processen als telecommunicatie, drinkwater en energievoorziening. Het versterken van onze concurrentiekracht is een *offensieve* strategie om ons economisch fundament te versterken. De overige fiches hebben een *defensief* karakter, dat zijn ingrepen om kwetsbaarheden in onze veiligheid zo proportioneel mogelijk adresseren:

1. Het kennisniveau van relevante actoren binnen de overheid vergroten, zodat de overheid niet alleen effectief, maar ook doelmatig kan optreden:
 - a. Beter positie **inlichtingendiensten** (overkoepelend fiche 1).
 - b. Versterking van de kennisbasis over **sensitieve technologie en technologische afhankelijkheden** (overkoepelend fiche 2). Dit stelt de overheid in staat om veiligheidsrisico's van technologieën beter in te schatten.

- c. Het inrichten van expertise teams op **vitale processen** (fiche 4), om Nederland te beschermen tegen risico's.
 - d. Bewustwording bij inkopers en opdrachtgevers bij het **internationaal aanbesteden** (fiche 5).
 - e. **Bescherming van onze technologie en kennis** (fiche 2) door bewustwording van risico's bij kennisinstellingen.
 - f. **Versterking van diplomatie en internationale samenwerking** (overkoepelend fiche 4) op het gebied van cybersecurity.
2. Aanpassen wet- en regelgeving om bestaande kwetsbaarheden te adresseren:
- a. Strafbaar stellen **spionage** (overkoepelend fiche 3).
 - b. Screening en toetsing van **buitenlandse investeringen** (fiche 3) in NL op nationale veiligheidsaspecten.
 - c. **Bescherming van onze technologie en kennis** (fiche 2) door toetsing van buitenlandse studenten of het versterken van de exportcontrole op kritische technologieën.
 - d. Een veiligheidsregeling invoeren voor de **aanbesteding van voor gerubriceerde en/of vitale opdrachten** (fiche 5).

De kosten van ingrijpen versus de kosten van niets doen

In sommige gevallen gaan de bescherming van onze nationale veiligheid en het versterken van onze concurrentiepositie in directe zin hand in hand. Dat geldt bijvoorbeeld bij de opbouw van een stevige positie op sleuteltechnologieën die ook relevant zijn voor de nationale veiligheid (fiche 1) en het bestrijden van spionage (overkoepelend fiche 3).

Tegelijkertijd hangen er in veel gevallen twee soorten kosten aan maatregelen voor de bescherming van onze nationale veiligheid. Veel van de voorgestelde veiligheidsmaatregelen leggen niet alleen een beslag op de overheidsfinanciën, maar zijn ook marktversturend en maken de economie minder efficiënt. Op het eerste gezicht gaat het dus ten koste van economische groei en de concurrentiepositie. Veel van de voorgestelde maatregelen komen in economische macro-modellen – en dus ook bij de doorrekening van dergelijke maatregelen uit bijv. verkiezingsprogramma's door het CPB – dan ook slecht uit de bus.

Dit schetst echter een eenzijdig beeld. Dergelijke macro-modellen zijn doorgaans slechts beperkt in staat incidenten in de calculeren die slechts een kleine kans hebben om zich voor te doen, maar aanzienlijke gevolgen hebben zodra ze zich voor doen. Dit zijn doorgaans het type incidenten waar de voorgestelde veiligheidsmaatregelen op zien. Veel veiligheidsmaatregelen gaan in economische modellen ten koste van groei, maar kunnen in werkelijkheid juist economische groei behouden. Veel veiligheidsrisico's gaan immers in potentie ook gepaard met aanzienlijke economische kosten.

Denk bijvoorbeeld aan het uitvallen van het Nederlandse telecomnetwerk door sabotage van buitenaf. De kans dat dit gebeurt is zeer beperkt, maar kan gepaard gaan met aanzienlijke economische schade. Gegeven dat eenvoudig de helft van de Nederlandse economie direct afhankelijk is van telecommunicatie en internet, kan een verstoring van bijvoorbeeld een week al snel oplopen tot meer dan 10 miljard euro.¹ Door maatregelen op het gebied als cybersecurity of ten aanzien van aanbestedingen voor vitale opdrachten (fiche 5) wordt de risico op een dergelijk incident verkleind.

Dit neemt natuurlijk niet weg dat het in alle gevallen belangrijk is het om maatregelen doeltreffend en proportioneel in te zetten om zowel onze concurrentiekracht als onze nationale veiligheid zo min mogelijk aan te tasten.

¹ Voor een gemiddelde week, waarbij 2/3* van de economie stilvalt (€812 mrd / 52 weken *(2/3) = ca. €10 mrd).

Bijlage 1. Taxatie individuele fiches

Beleidsaanbeveling	Bijdrage effectiviteit adresseren veiligheidsrisico's	Bijdrage proportionaliteit adresseren veiligheidsrisico's	Potentiele (economische) schadeposten bij niets doen
Fiche 2: Offensief industriebeleid en concurrentiekracht	<ul style="list-style-type: none"> Een goede concurrentiepositie vergroot ons verdienvermogen en stelt ons in staat onze collectieve arrangementen te kunnen blijven betalen. Daaronder vallen ook publieke voorzieningen die in het belang zijn voor onze nationale veiligheid. Investerings in sleuteltechnologieën kunnen hieraan bijdragen. Voor zover sleuteltechnologieën ook militaire toepassingen kennen of binnen (toekomstige) vitale processen worden gebruikt, kan het ook een meer directe bijdrage leveren aan de veiligheidsbelangen. Draagt bij aan het voorkomen of beperken van eenzijdige afhankelijkheden van niet-EU partijen. 	<ul style="list-style-type: none"> Brengt geen restricties aan in het vrije verkeer van goederen, diensten en kapitaal. Legt een relatief groot beslag op de overheidsfinanciën, maar kent bredere economische en maatschappelijke baten dan het vergroten van weerbaarheid alleen. Indien wordt geïnvesteerd in sleuteltechnologieën die o.m. leiden tot grote kennisspillovers wordt weerbaarheid tegen relatief lage netto-maatschappelijke kosten gerealiseerd. Wel bestaat het risico van overheidsfalen bij investeringen in sectoren en ondernemingen die economisch en maatschappelijk niet blijken te renderen. Dit risico doet zich m.n. voor wanneer ingezet wordt op sectoren i.p.v. missies of sleuteltechnologieën. 	<ul style="list-style-type: none"> Risico op ongewenste afhankelijkheden van derde landen in sleuteltechnologieën, wat mogelijk kan leiden tot geopolitieke kwetsbaarheden en kwetsbaarheden in vitale processen. Aansluiting EU-bondgenoten (en mogelijke toegang tot toekomstige EU-fondsen) kwijtraken. Zwakkere concurrentie positie en vestigingsklimaat en kan daarmee ons groeipotentieel en welvaartsgraad verlagen. Onvoldoende grip op sleuteltechnologieën > nadelige maatschappelijk-ethische gevolgen. Cyberinbraken kennen directe economische en maatschappelijke schade en indirect kan te beperkte bescherming vanuit de overheid bijdragen aan het vertrek van bedrijven naar landen die hier meer beleid op voeren.
Fiche 2 (overkoepelend): Kennisbasis overheid sensitieve technologie en afhankelijkheden	<ul style="list-style-type: none"> Effectievere inzet ander overheidsinstrumentarium (investeringsstoets, exportcontrole, kennisregeling) 	<ul style="list-style-type: none"> Legt slechts een zeer beperkt beslag op de overheidsfinanciën. 	<ul style="list-style-type: none"> Slecht zicht op wat sensitieve technologieën zijn en waar mogelijke afhankelijkheden bestaan of kunnen ontstaan, zou waarschijnlijk leiden tot minder gerichte inzet van ander overheidsinstrumentarium, zoals de investeringsstoets. Dit leidt tot meer marktverstoring dan mogelijk noodzakelijk. Tegelijkertijd kan het er ook toe leiden dat risico's en afhankelijkheden door slechter zicht worden onderschat. Dit kan risico's voor de continuïteit van bepaalde vitale processen met zich mee brengen en ons onnodig vatbaar maken voor geopolitieke druk via een eenzijdige strategische afhankelijkheid. Wat hiervan de economische gevolgen zijn is op voorhand moeilijk in te schatten.

**Fiche 3: Voorkomen
ongewenste
zeggenschap**

Tijdig zicht op en in kunnen grijpen bij veiligheidsrisico's (opbouw strategische afhankelijkheden, continuïteit vitale processen en bescherming gevoelige of vertrouwelijke informatie) als gevolg van wijzigingen van zeggenschap.

Legt slechts beperkt beslag op de overheidsfinancien.
Verhoogt voor bedrijven onder de reikwijdte van de toets de transactiekosten (investeringsonzekerheid en administratieve kosten) van zeggenschapswijzigingen en beperkt daarmee het vrije verkeer van kapitaal.
Door de reikwijdte zoveel mogelijk te beperken en aan de voorkant duidelijkheid te verschaffen in de toetsingscriteria, worden de kosten voor onze economie beperkt.
Biedt mogelijkheden om mitigerende maatregelen in te stellen alvorens blokkering van de zeggenschapswijziging wordt overwogen.

Draagt bij aan het voorkomen van verstoringen van vitale processen, die gepaard kunnen gaan met bijzonder hoge economische en maatschappelijke kosten. Verstoring van bijvoorbeeld de telecom- of energie-infrastructuur kan grote delen van de economie (langdurig en hevig) ontregelen en kan al snel oplopen tot vele miljarden.



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

9 december 2020

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	16 december 2020, 16:00-17:30 uur
Vergaderplaats	N36.10 - Noord-Brabantzaal (Turfmarkt 147)

1. Opening en mededelingen

2. Verslag TFEV 25 november 2020 [REDACTED]

5.1.2i

3. Structurele samenwerking

- a. Dreigingsappreciatie Telecom [REDACTED] -
mondelinge toelichting AIVD en MIVD
- b. Opvolging dreigingsappreciatie – mondelinge toelichting NCTV

5.1.2i

4. Risicoanalyse [REDACTED] - mondelinge toelichting NCTV

5.1.2i

5. [REDACTED]

5.1.1b +

5.1.2a +

6. Internationaal/Europees

5.1.2i

7. Parlementair

8. Rondvraag en sluiting

Schriftelijke reacties:

IenW:

Akkoord met opdrachtverlening agendapunt 5

Nationale politie:

[REDACTED] 5.1.1b
[REDACTED]

[REDACTED]
[REDACTED] 5.1.1b
[REDACTED]



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

P1

Dep. **VERTROUWELIJK**

TFEV leden

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

9 februari 2021

agenda

TFEV

Omschrijving
Vergaderdatum en -tijd
Vergaderplaats

TFEV
17 februari 2021, 16:00-17:30 uur
ICCb/MCCb-zaal (derde etage)

1. Opening

2. Verslag TFEV 16 december 2020

Bijlage 1. Verslag TFEV 16122020 [REDACTED]

5.1.2i

3. Beschikkingen en zienswijze: stand van zaken – toelichting door EZK

Bijlage 2. Gebruik [REDACTED] rapport in bezwaar en beroep

5.1.2i

Bijlage 3. Ter informatie: Nadeelcompensatiekader (*wordt nagezonden*)

4. Risicoanalyse [REDACTED] – toelichting door [REDACTED], NCTV, EZK

Bijlage 4. Opties t.a.v. voorstel [REDACTED]

5.1.2i

Bijlage 4A. Ter achtergrond: [REDACTED]-rapport [REDACTED] risicoanalyse

5.1.2i

[REDACTED]

5.1.2i

5.1.2i en 5.1.2e

5. Expertise team digitale overheid – toelichting door CIO Rijk

Bijlage 5. Oprichting Expertiseteam Veilige Digitale Overheid

5.1.2i

Bijlage 5A. [REDACTED]

Bijlage 5B. Heroverweging maatregel antivirussoftware

Kaspersky

6. Internationaal/Europees

7. Parlementair

8. Rondvraag en sluiting

Dep. **VERTROUWELIJK**



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

P3

Dep. **VERTROUWELIJK**
TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[REDACTED]

5.1.2e

[REDACTED]

Datum

11 februari 2021

Ons kenmerk

5.1.2i

nota

Gebruik [REDACTED] rapport in bezwaar en beroep

Van
EZK, NCTV

Gevraagd besluit

1. Instemming met de voorgestelde lijn in de bijlage
2. Mandaat voor het zo nodig bespreken of schriftelijk kenbaar maken van dezelfde voorgestelde lijn aan [REDACTED]

5.1.2i

Toelichting

- In 2019 hebben de telecomaanbieders het [REDACTED] rapport 2019 in handen gekregen. Het rapport is gerubriceerd als Staatsgeheim-confidentieel. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- Tijdens de voorbereiding van de beschikkingen (april 2020) heeft [REDACTED] aan EZK gevraagd hoe de rechtsbescherming van [REDACTED] afdoende kan worden gewaarborgd in een bezwaar- en/of beroepsprocedure als belangrijke onderliggende informatie, namelijk het gerubriceerde [REDACTED] rapport 2019, vertrouwelijk dient te blijven.
- Voor gerubriceerde informatie is in het Besluit voorschrift informatiebeveiliging Rijksdienst bijzondere informatie 2013 (VIRBI 2013) voorgeschreven welke eisen aan de beveiliging hiervan worden gesteld. Dit Besluit geldt strikt genomen alleen voor de Rijksdienst zelf. Wel wordt hierin ook bepaald dat bij het buiten de rijksdienst brengen van gerubriceerde informatie dezelfde beveiligingseisen blijven gelden.
- In situaties waarin van overheidswege gerubriceerde informatie ten grondslag ligt aan een besluit kan de overheid normaal gesproken op grond van artikel 8:29 van de Algemene wet bestuursrecht (Awb) de rechter mededelen dat uitsluitend hij kennis zal mogen nemen van die vertrouwelijke informatie, met een toelichting op de hiervoor vereiste gewichtige redenen. Indien de rechter hierop beslist dat de beperking van

5.1.2i

5.1.2i

5.1.2i

5.1.2i

5.1.2i

de kennisneming gerechtvaardigd is, kan hij mede op grondslag van de betrokken informatie uitspraak doen, mits de andere partij daarvoor toestemming verleent. Op die manier kan de rechter zich een oordeel vormen over de motivering van het overheidsbesluit, maar blijft de vertrouwelijkheid van de informatie in elk geval gewaarborgd. Nu de telecomaانبieders het [REDACTED] rapport 2019 echter al in handen hebben, kan deze procedure geen toepassing vinden, omdat niet kan worden uitgegaan van de fictieve situatie dat de telecomaانبieders het [REDACTED] rapport 2019 niet kennen.

5.1.2i

5.1.2i

- De vraag die voorligt is hoe in juridische zin voor alle partijen zo bevredigend mogelijk kan worden omgegaan met de gerezen situatie waarin het rapport gerubriceerd is én van overheidswege dus gehecht wordt aan het vertrouwelijk blijven hiervan, maar de telecomaانبieders dit wel hebben gekregen en zouden willen gebruiken in aankomende bezwaar- en/of beroepsprocedures.
- Dezelfde vraag kan overigens ook betrekking gaan hebben op het [REDACTED] rapport van 2021, betreffende de beveiligingswaarde van de aanvullend door [REDACTED] voorgestelde maatregelen, met name ook indien [REDACTED] op verstrekking hiervan zal aandringen. Voor dit (tweede) rapport geldt voorts nog dat [REDACTED] dit nog niet heeft ontvangen; een eerder concept is ten behoeve van bespreking onder strikte voorwaarden tijdelijk ter beschikking gesteld en geretourneerd.
- Over deze kwestie heeft ambtelijk afstemming plaatsgevonden tussen EZK/WJZ, de NCTV en de AIVD. Daaruit is een lijn naar voren gekomen waarin uitgangspunt is dat telecomaانبieders de mogelijkheid wordt geboden om zich in een bezwaar- en beroepsprocedure inhoudelijk (zowel schriftelijk als tijdens een zitting) te verweren tegen het [REDACTED] rapport en waarin tegelijkertijd procedurele mogelijkheden worden benut om de vertrouwelijkheid van het rapport zo goed mogelijk te waarborgen (zie bijlage).
- Tevens zal dezelfde voorstelde lijn worden toegepast met betrekking tot de gerubriceerde bijlage van de beschikking (Departement-vertrouwelijk). De bijlage bevat een opsomming van de kritieke onderdelen.
- Op 23 februari aanstaande vindt er een gesprek plaats met [REDACTED], [REDACTED], EZK/WJZ en de NCTV over het gebruik van het [REDACTED] rapport in een eventuele bezwaar- en/ of beroepsprocedure. [REDACTED]

5.1.2i

5.1.2i

5.1.2i

5.1.2i

5.1.2i

5.2.1

Bijlage:

1. Bezwaar- en beroepsprocedures van de telecomaanbieders:

- In bezwaar kan EZK beslissen dat de (hoor)zitting achter gesloten deuren plaatsvindt. Op die manier kunnen de aanbieders zowel in het bezwaarschrift als tijdens de hoorzitting zich op het [REDACTED] rapport beroepen, zonder dat anderen daarvan daardoor kennis kunnen nemen.
- De beslissing op bezwaar wordt zodanig verwoord dat de inhoud van het rapport niet openbaar wordt.
- In de beroepsprocedures van de telecomaanbieders wordt aan de rechtbank verzocht om de zitting achter gesloten deuren te behandelen op grond van art. 8:62 lid 2 Awb. Daarnaast wordt, voor het geval ook beroep wordt ingesteld door leveranciers, aan de rechtbank verzocht om splitsing van de behandeling van de beroepszaken (artikel 8:14, lid 2, Awb).
- Als het [REDACTED] rapport in een (hoger) beroepsprocedure onderwerp van de behandeling is, dan kan het voor de rechters mogelijk lastig zijn om de inhoud van het rapport buiten de uitspraak te houden. Om die reden wordt aan de rechtbank aandacht gevraagd voor het [REDACTED] rapport buiten de uitspraak kunnen houden.

5.1.2i

5.1.2i

5.1.2i

2. Bezwaar- en beroepsprocedure leveranciers:

- De kans is aanwezig dat niet alleen de telecomaanbieders, maar ook de leveranciers bezwaar en/of beroep zullen instellen tegen de beschikking, zodra zij van het stuk op de hoogte raken. De leveranciers hebben het [REDACTED] rapport niet in handen.
- In de bezwaarprocedure kan EZK gebruik maken van de mogelijkheid van artikel 7:4 lid 6 Awb (geheimhouding om gewichtige redenen), waardoor het rapport in de bezwaarfase geheim blijft voor de leveranciers.
- In een beroepsprocedure zal EZK, met een beroep op artikel 8:29 Awb, aan de rechtbank mededelen dat uitsluitend de rechter kennis zal mogen nemen van het rapport, met een toelichting op de gewichtige redenen hiervoor. Van belang is daarbij wel dat de redengeving duidelijk zal maken dat het rapport specifiek niet aan leveranciers bekend moet worden.
- Van belang is voorts dat de beroepsprocedures van de aanbieders en van de leveranciers gescheiden blijven en dus niet gevoegd worden. Hierover dient een gemotiveerd verzoek te worden gedaan aan de rechtbank (artikel 8:14 lid 2 Awb) op het moment dat de leveranciers beroep instellen.

5.1.2i



P5

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK

TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[REDACTED]

5.1.2e

T 070 751 50 50

nota

Opties tav voorstel [REDACTED]

Datum

11 februari 2021

Ons kenmerk

3218540

5.1.2i

Aanleiding

In 2019 is door de TFEV gekeken naar risico's van spionage door statelijke actoren door misbruik van producten en diensten van leveranciers in de telecomsector. Op basis daarvan zijn aanvullende beheersmaatregelen genomen en is besloten bepaalde leveranciers te weren uit kritieke onderdelen van telecomnetwerken. [REDACTED] heeft in september 2020 aan de NCTV een voorstel gedaan als alternatief voor het uitschakelen van [REDACTED] in een kritiek onderdeel van hun netwerk [REDACTED]. [REDACTED]

5.1.2i

5.1.2i

5.1.2f

5.1.2i

De beveiligingswaarde van dit voorstel is in de afgelopen maanden beoordeeld door de technische werkgroep (hierna: TW, bestaande uit AIVD, MIVD, NCSC, AT, [REDACTED] NCTV)¹. De werkgroep concludeert dat de maatregelen [REDACTED] de weerbaarheid verbeteren, maar dat de risico's, gezien de aard van de dreiging, ook met deze maatregelen [REDACTED] zeer moeilijk beheersbaar blijven. Het weren en dus ook uitschakelen van de betrokken leveranciers is daarom onverminderd noodzakelijk. Wel kan overwogen worden of het [REDACTED] voorgestelde pakket aan beveiligingsmaatregelen van invloed kan zijn op de termijn waarop in het [REDACTED] moet worden uitgefaseerd. In deze nota worden daarom in twee opties de mogelijke reacties en hun implicaties geschetst ten aanzien van het voorstel [REDACTED].

5.1.2i

5.1.2i

5.1.2i

5.1.2f

5.1.2i

Gevraagd besluit

- Een keuze uit een van de twee opties:

- 1) Vasthouden huidige ontwerpbeschikking [REDACTED]
[REDACTED]
[REDACTED]
- 2) Termijn voor uitschakeling verlengen met als uitgangspunt een verlenging naar [REDACTED] onder de voorwaarde [REDACTED] aanvullende maatregelen neemt. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.1c en

5.2.1

5.1.1b

5.1.2i

5.2.1

¹ Gebruikmakend van dezelfde methodiek als de risicoanalyse in 2019. Zie [REDACTED] -rapport 'veiligheid telecomapparatuur en software', mei 2019.

5.1.2i

Datum
11 februari 2021

Ons kenmerk
3218540

5.2.1

• Instemmen met het volgende proces:

- VZ TFEV (NCTV) en EZK gaan langs bij [REDACTED] om de noodzaak van uitfasering toe te lichten
- Indien wordt gekozen voor optie 2 krijgen zij het mandaat van de TFEV om het gesprek aan te gaan over een aangepaste uitfaseringstermijn in combinatie met het voorgestelde maatregelenpakket [REDACTED].

5.1.2i en

5.1.2e

5.1.2i

Toelichting

Voorstel [REDACTED]

5.1.2i en

5.1.1c

[REDACTED]

Conclusies TW tav beveiligingswaarde voorstel [REDACTED]

5.1.2i

[REDACTED]

5.1.1b

[REDACTED] Het volledige rapport (rubricering: stg confi) is toegevoegd als bijlage.

Toelichting opties

Optie 1 - Vasthouden huidige ontwerpbeschikking [REDACTED]

5.1.1b

Op grond van de dreigingsanalyse kunnen de nationale veiligheidsrisico's alleen beheersbaar worden gemaakt door het uitfaseren van deze leverancier. Tegelijkertijd duurt het minimaal [REDACTED] voordat deze uitfasering voltooid is en de kans op vertraging is daarbij groot. [REDACTED]

5.1.1b

5.1.2i 5.1.2f

[REDACTED]

[REDACTED]

5.2.1 +

5.1.2i +

5.1.2f

² Zoals de implementatie van de beveiligingsmaatregelen op basis van de ministeriële regeling en vervanging van het mobiele kernnetwerk.

In deze optie is het juridisch gezien tevens van belang dat de uitfaseertermijn van [REDACTED] voldoende lang is om de continuïteit van dienstverlening te garanderen. Hoewel daar ten tijde van het nemen van de ontwerp-beschikking (op basis van de op dat moment ingediende stukken) voldoende onderbouwing voor was, is, gelet op de door [REDACTED] ingediende zienswijze, van belang dat de termijn van [REDACTED] nog steeds met het oog op de continuïteit kan worden onderbouwd. Op dit moment wordt gezien door Agentschap Telecom of en in hoeverre de zienswijze van [REDACTED] om redenen van continuïteit van de dienstverlening aanleiding geeft tot verlenging van de uitfaseertermijn.

5.1.1b

5.1.2i

5.1.1b

5.1.2i

Optie 2 - Termijn voor uitfasering verlengen. [REDACTED]

5.1.2i +

5.1.2f

Deze optie houdt in dat wordt afgeweken van de termijn die in de ontwerp-beschikking [REDACTED] was opgenomen [REDACTED], onder de voorwaarde dat de extra [REDACTED] voorgestelde aanvullende maatregelen zo snel mogelijk worden uitgevoerd en de overheid op de naleving daarvan kan toezien.

5.1.2i

5.1.2f

5.1.2i

5.1.2i

De aanvullend [REDACTED] voorgestelde maatregelen (meer in het bijzonder [REDACTED]) zorgen ervoor dat de moeilijkheidsgraad voor de actor om ongezien informatie te exfiltreren wordt verhoogd. [REDACTED]

5.1.2i

5.1.2f

5.1.2f

In deze optie zal, alvorens de nieuwe uitfaseertermijn in de definitieve beschikking te kunnen vaststellen, bestuurlijk [REDACTED] moeten worden besproken welke maatregelen aanvullend moeten worden geïmplementeerd en welke uitfaseringstermijn dan komt te gelden. Als uitgangspunt kan daarbij een verlenging [REDACTED] worden genomen, zodat rekening wordt gehouden met mogelijke vertraging in de uitfasering. [REDACTED]

5.1.2i

5.1.2i

5.2.1 +

5.1.2i

Vanuit juridisch perspectief gelden met betrekking tot optie 2 de in bijlage C toegelichte randvoorwaarden en risico's. Samengevat betreffen die het volgende:

- 1) De AMvB waarop de beschikkingen gebaseerd zijn maakt het alleen mogelijk om in het belang van de continuïteit van dienstverlening een uitfaseringstermijn te bepalen of te verlengen. Een eventuele verlenging van de termijn kan dus op basis van de beschikking alleen worden beargumenteerd als de [REDACTED] niet voldoende zou zijn om de continuïteit van de dienstverlening te kunnen garanderen. Andere redenen kunnen hieraan niet ten grondslag worden gelegd. [REDACTED]

5.1.1b

Dep. VERTROUWELIJK

Datum
11 februari 2021
Ons kenmerk
3218540

- [REDACTED]
- 2) Voorts moet een verlenging van de uitfaseertermijn, in combinatie met stellen van aanvullende maatregelen, overtuigend kunnen onderbouwd op grond van de specifieke situatie [REDACTED]. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- 3) Voor het [REDACTED] stellen van aanvullende beveiligingseisen kan in beginsel gebruik worden gemaakt van een afzonderlijke beschikking op grond van de Telecomwet.

5.1.2i

5.1.2i +
5.2.1

5.1.2i

Daarnaast zijn in de bilaterale relatie met betrokken landen bij deze optie nadeligere consequenties te verwachten. Richting bondgenoten wordt het signaal afgegeven dat Nederland geen urgentie ziet om de waargenomen dreiging te mitigeren en zal het de perceptie versterken dat Nederland economische belangen belangrijker acht dan veiligheid. Verlengen van de uitfaseringstermijn kan mogelijk het verkeerde signaal afgeven dat de Nederlandse overheid te beïnvloeden is en de huidige woordvoeringslijn verzwakken dat deze maatregelen noodzakelijk zijn voor de nationale veiligheid. Mocht er voor optie twee gekozen worden dan is het voor de diplomatieke relaties essentieel om een strakke woordvoeringslijn te handhaven.

Bijlagen:

- Bijlage A - Huidige situatie [REDACTED]
- Bijlage B - Terugblik proces en huidige omstandigheden
- Bijlage C - Impact opties per dimensie
- Bijlage D - Kosten vervanging systemen en nadeelcompensatie

5.1.1b +
5.1.2i

Bijlage A - Huidige situatie

[REDACTED]

Datum
11 februari 2021
Ons kenmerk
3218540

5.1.1b +
5.1.2i

5.1.1b +
5.1.2f + 5.1.1c

Uitfaseringstermijn

[REDACTED]

5.1.2f

Voorstel

[REDACTED]

5.1.2i

³ Ontwerpbeschikking op grond van artikel 2 van het Besluit veiligheid en integriteit telecommunicatie. Zienswijze [REDACTED]

5.1.2i

Dep. VERTROUWELIJK

[REDACTED]

Datum
11 februari 2021
Ons kenmerk
3218540

5.1.2i

Ter vergelijking: huidige situatie

[REDACTED]

5.1.2i +
5.1.2f +
5.1.1c

Bijlage B - Terugblik proces en huidige omstandigheden

Besluit 2019

Op basis van het rapport van de technische werkgroep uit 2019 werd geconcludeerd dat aanvullende maatregelen nodig zijn om de beveiliging van zowel de huidige (2,3 en 4G) als de toekomstige (5G) telecomnetwerken te versterken. Het kabinet besloot op basis van het advies van de TFEV tot het nemen van de volgende maatregelen:

- 1) Telecomaanhouders worden verplicht om aanvullende technische en organisatorische beveiligingsmaatregelen te nemen om de weerbaarheid te verhogen (via een ministeriële regeling).
- 2) Bepaalde leveranciers worden geweerd uit de kritieke onderdelen in het telecomnetwerk (via beschikkingen per MNO).
- 3) De werkwijze van de Taskforce Economische Veiligheid (dreiging - risicoanalyse - maatregelen) wordt bestendigd in een structurele samenwerking tussen IV-diensten, departementen, toezichthouders en vitale partijen, zoals de MNO's.

Voor maatregel 2 is besloten om zo snel mogelijk over te gaan tot uitfaseren. Uit de nota van mei 2019 (p. 7), specifiek over maatregel 2: "vanuit het oogpunt van nationale veiligheid wordt geadviseerd om zo snel als mogelijk maatregelen te nemen, waarbij rekening gehouden wordt met het waarborgen van de continuïteit van de dienstverlening. Voor zover de nationale veiligheid niet in het geding komt, wordt rekening gehouden met de bedrijfseconomische aspecten".

Na deze beslissing heeft AT [REDACTED] verzocht om een plan op te leveren voor een zo snel mogelijke uitfasering van de in de beschikking genoemde leveranciers, zonder de continuïteit van de dienstverlening in gevaar te brengen. Deze plannen, met uitfaseringstermijnen van [REDACTED], dienden als basis voor de conceptbeschikkingen, die in de TFEV van 14 oktober 2020 zijn besproken. Het uitgangspunt van de daar genomen beslissing om verder te gaan met de conceptbeschikkingen was het besluit uit 2019 dat zo snel als mogelijk moet worden uitgefaseerd. Op 10 november 2020 zijn de conceptbeschikkingen voorgelegd aan de telecombedrijven ter consultatie. Inmiddels zijn er echter enkele nieuwe aspecten opgekomen die van belang zijn om te worden meegenomen in de besluitvorming over [REDACTED].

5.1.2i

5.1.1b

5.1.2i

Wat is veranderd sinds de laatste beslissing

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Bij de nadere uitwerking van

5.1.2i en
5.1.2b

4

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2i

- het nadeelcompensatiekader⁵ is in januari echter geconstateerd dat [REDACTED]
- Tegelijkertijd is duidelijk geworden dat vervanging van [REDACTED] in vergelijking met vervanging van andere kritieke systemen tot veruit de grootste kosten leidt (zie bijlage C en D). Dat betekent dat het doorzetten van de huidige beschikkingen een proportioneel zwaardere maatregel is dan aangenomen tijdens eerdere besluitvorming.
- Bij het nemen van de beslissing tot uitfasering in 2019 was nog niet bekend dat [REDACTED] 5.1.2i
 - [REDACTED] 5.1.2f
 - [REDACTED] 5.1.2i
 - [REDACTED] 5.1.2i
- Hoewel eerder is vastgesteld dat deze theoretisch maximaal haalbare beveiligingswaarde niet voldoende is (en er dus moet worden uitgefaseerd), is in de TFEV nog niet expliciet overwogen of een dergelijk pakket aan beveiligingsmaatregelen [REDACTED] (plus eventuele aanvullende eisen vanuit de overheid) van invloed kan zijn op de termijn waarop moet worden uitgefaseerd.
- Wat is er niet veranderd**
- De dreiging die de AIVD en MIVD zien en die zich richt op de Nederlandse telecominfrastructuur en de leverancier in kwestie is sinds het eerste onderzoek in 2019 niet veranderd. [REDACTED] 5.1.1b
- [REDACTED] Het oorspronkelijke dreigingsbeeld en de aanvullende inlichtingen zijn zowel in 2019 als zeer recent gedeeld [REDACTED]. 5.1.2i

⁵ Pels Rijcken, *Kader nadeelcompensatie*, januari 2021 en Dialogic, *Tentatieve geschatte schadebegroting MNO's*, januari 2021

Bijlage C – Impact opties per dimensie

Datum
11 februari 2021
Ons kenmerk
3218540

Dimensies om de impact van verschillende opties te wegen

Om de impact te kunnen bepalen van een besluit van de overheid over hoe om te gaan met het alternatieve plan van aanpak [REDACTED], moeten twee verschillende opties en hun impact worden bekeken. De impact wordt bepaald aan de hand van de volgende dimensies⁶:

- a) *Nationale veiligheid*: gaat in op de mate waarin de geconstateerde dreiging wordt geadresseerd, dit betreft een afweging van de volgende drie factoren:
 - o De snelheid van uitfaseren [REDACTED].
 - o De inhoud van het aanvullende maatregelenpakket (aanvullend ten opzichte van TFEV maatregel 1, de maatregelen die al dmv de MR zijn opgelegd) [REDACTED].
 - o Mate van zekerheid waarmee maatregel 3 van de TFEV (het besluit van 2019), de structurele samenwerking, kan worden opgebouwd.
- b) *Financieel-economisch*: deze dimensie valt uiteen in twee soorten elementen:
 - o *Nadeel* [REDACTED]: Hieronder vallen de directe kosten die een telecombedrijf moet maken en de kosten die daaraan gerelateerd zijn, zoals mogelijke omzetsderving en reputatieschade.
 - o *Kosten voor de maatschappij*: Deze impact op de samenleving in de vorm van misgelopen economische groei wordt vooral bepaald door de mate waarin de maatregelen een negatief effect hebben op de effectieve en duurzame concurrentie tussen de MNO's en de investeringsmogelijkheden van marktpartijen met betrekking tot uitrol en innovatie.
- c) *Juridisch*: Hierbij wordt gekeken naar of er zonder goede grond verschillen in behandeling ontstaan tussen de MNO's en de kans op en impact van mogelijke rechtszaken.
- d) *Diplomatiek*: De Nederlandse besluitvorming m.b.t. de veiligheid en integriteit van (5G) telecomnetwerken wordt door verschillende landen met grote belangstelling gevolgd. Het dossier is voor meerdere landen van groot strategisch belang, waarbij geldt dat nationale maatregelen die door bondgenoten positief gewaardeerd worden kunnen leiden tot voor Nederland onwenselijke represailles uit een ander land. De Nederlandse besluitvorming is ingebed in verschillende binnen de EU gecoördineerde trajecten, waaronder de EU 5G Security toolbox met mitigerende maatregelen.

5.1.2i

5.1.2f

5.1.2f

5.1.2i

⁶ Impactcriteria zoals eerder gebruikt binnen TFEV (verwijzing nota)

Opties

Datum

11 februari 2021

Ons kenmerk

3218540

1. Vasthouden huidige beschikking

5.1.1b

a) Nationale veiligheid:

De nationale veiligheidsrisico's kunnen alleen beheersbaar worden gemaakt door het uitfasen van deze leverancier. Tegelijkertijd duurt het minimaal [REDACTED] voordat deze uitfasering voltooid is en de kans op vertraging is daarbij groot. [REDACTED]

5.1.1b

5.1.2i

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

5.1.2i +

5.2.1

b) Financieel-economisch:

Nadeel [REDACTED]

5.1.2i

De landsadvocaat is gevraagd om in samenwerking met Dialogic en onafhankelijke economen een inschatting te maken [REDACTED] wat de verwachte kosten zijn in verband met het vervroegd vervangen van de in de beschikking genoemde systemen zijn en in hoeverre wordt verwacht dat de schade ten gevolge van de beschikkingen het normaal bedrijfsrisico zal overschrijden⁷. Omdat het gaat om een inschatting van toekomstige bedragen is gebruik gemaakt van drie verschillende scenario's (laag, midden, hoog). Omdat sprake kan zijn van een flinke onderschatting van de daadwerkelijke schade bij migratietrajecten van dit soort complexe IT-systemen en er vaak verborgen kosten blijken te zijn is in de ook gerekend met een kolom [REDACTED]. De ingeschatte kosten in de verschillende scenario's zijn weergegeven in tabel 1. In bijlage D is dit verder uitgewerkt.

5.1.2i

5.1.1b

Tabel 1 – Directe vervangingskosten

5.1.2i

⁷ Daarnaast is de implementatie van de beveiligingsmaatregelen op basis van de ministeriële regeling nog niet meegenomen, wat tot verdere vertraging kan leiden.

⁸ Pels Rijcken, *Kader nadeelcompensatie*, januari 2021 en Dialogic, *Tentatieve geschatte schadebegroting MNO's*, januari 2021 (NB stukken volgen nog, ook met definitieve cijfers)

Schadecijfers voor twee kostenposten die in ieder geval voor nadeelcompensatie in aanmerking komen. Cijfers zijn schattingen van onafhankelijke experts en niet gebaseerd op cijfers van de MNO's.

Naast een effect op kosten in verband met het vervroegd moeten vervangen van apparatuur stelt [REDACTED] dat zij ook andere schade heeft, namelijk omzetsderving ten gevolge van een versnelde vervanging [REDACTED] :

5.1.2i

5.1.1b

- [REDACTED]
- [REDACTED]

5.1.2i

[REDACTED]

5.1.2i

[REDACTED]

5.1.2i

Kosten voor de maatschappij

De inschatting is dat het overheidshandelen geen langdurig negatief effect heeft op de effectieve en duurzame concurrentie tussen de MNO's en de investeringsmogelijkheden van marktpartijen met betrekking tot uitrol en innovatie.

c) Juridisch:

[REDACTED]

5.1.2i

⁹ Op basis van vertrouwelijk, informeel verkregen informatie met een grove schatting [REDACTED]. Formele inbreng van de zijde [REDACTED] wordt nog verwacht.

5.1.2i

Datum
11 februari 2021
Ons kenmerk
3218540

In deze optie is het juridisch gezien tevens van belang dat de dat de uitfaseertermijn van [REDACTED] voldoende lang is om de continuïteit van dienstverlening te garanderen. Hoewel daar ten tijde van het nemen van de ontwerp-beschikking (op basis van de op dat moment ingediende stukken) voldoende onderbouwing voor was, is, gelet op de door [REDACTED] ingediende zienswijze, van belang dat de termijn van [REDACTED] nog steeds met het oog op de continuïteit kan worden onderbouwd. Op dit moment wordt bezien (door AT) of en in hoeverre de zienswijze van [REDACTED] om redenen van continuïteit van de dienstverlening aanleiding geeft tot verlenging van de uitfaseertermijn.

5.1.2i

5.1.1b

5.1.2i

5.1.1b

5.1.2i

d) *Diplomatiek:*

Bij het vasthouden aan de huidige beschikking zal er geen verandering zijn in de te verwachten impact van de maatregel op de diplomatieke dimensie.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2a

5.1.2i

[REDACTED] Het vasthouden aan de huidige beschikking betekent in deze dat de huidige, zo transparant mogelijke, communicatie over de robuustheid van de Nederlandse maatregelen richting bondgenoten voortgezet kan worden. Nederland laat daarmee zien dat het de waargenomen dreiging serieus neemt en een passende eigenstandige afweging heeft gemaakt om risico's voor de nationale veiligheid te mitigeren.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2a

2. **Termijn voor uitfasering verlengen.**

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2i

Deze optie houdt in dat wordt afgeweken van de termijn die in de huidige beschikking [REDACTED] is opgenomen voor [REDACTED] onder voorwaarde dat de extra [REDACTED] voorgestelde aanvullende maatregelen zo snel mogelijk worden uitgevoerd en de overheid op de naleving daarvan kan toezien. [REDACTED]

5.1.2i

5.1.2f

[REDACTED]
[REDACTED]

5.1.2i

a) *Nationale veiligheid:*

De aanvullende maatregelen [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.1.2f

Datum
11 februari 2021

Ons kenmerk
3218540

5.1.2f
5.1.2i

b) *Financieel economisch:*

Nadeel

5.1.2i

5.1.2i

Door het verlengen van de vervangingstermijn zullen de vervangingskosten substantieel afnemen en dichterbij de buurt komen van de kosten waarmee rekening moet worden gehouden gegeven haar eigen life cycle management.

5.1.2i

5.1.2i

Kosten voor de maatschappij

Geen verschil met optie 1, behalve dat mogelijk extra capaciteit benodigd is bij de overheid voor het controleren van de extra maatregelen afhankelijk hoe dit concreet wordt ingevuld.

c) *Juridisch:*

5.2.1

Wel gelden vanuit juridisch perspectief met betrekking tot optie 2 de volgende randvoorwaarden en, bij niet-inachtneming daarvan, risico's:

5.1.2i

- Als er aanvullende maatregelen worden opgelegd, dan is hiervoor een wettelijke grondslag nodig. Voor de beschikking krachtens het Besluit (met artikel 11a.1, vierde lid, Telecomwet als grondslag) geldt dat het Besluit op zich niet de mogelijkheid biedt om hierin een (langere) uitfaseringstermijn te koppelen aan aanvullende beveiligingseisen. Naar het oordeel van de juristen van EZK kan voor het stellen van die aanvullende eisen echter in beginsel wel gebruik worden gemaakt van de in artikel 11a.1, vijfde lid, Telecomwet aan de minister van EZK gegeven bevoegdheid om telecomaانبieders te verplichten om binnen een bepaalde termijn (beveiligings)maatregelen te treffen. Er is dus in beginsel een wettelijke grondslag waarvan hiervoor gebruik kan worden gemaakt.
- Op grond van artikel 2, derde lid, van het Besluit wordt in de beschikking in het belang van de continuïteit van dienstverlening een termijn vastgesteld voor de uitfasering. Dit betekent dat er vanuit de continuïteit van dienstverlening onderbouwd moet worden dat niet een termijn maar noodzakelijk is. Nu er vanuit continuïteit van dienstverlening in het voornemen is uitgegaan van een termijn van, zullen er nieuwe argumenten gevonden moeten worden die maken dat de termijn met het oog op de continuïteit beredeneerd te kort is gebleken.

5.1.1b

5.1.1b

5.2.1 +

5.1.2i

- [REDACTED]

5.1.2i +
5.2.1

d) *Diplomatiek:*

[REDACTED]

5.1.2a

Bondgenoten keken met zorg en belangstelling naar de breed in de publiciteit uitgemeten [REDACTED]

5.1.2i

[REDACTED] NL wordt hierover met regelmaat bevraagd en ontwikkelingen [REDACTED] worden met zeer veel belangstelling gevolgd¹⁰.

5.1.2i

[REDACTED] De
aanpassing kan daarnaast een verkeerd signaal afgeven:

5.1.2a

- Verlenging van de uitfaseringstermijn verzwakt de huidige woordvoeringslijn dat deze maatregelen noodzakelijk zijn voor de nationale veiligheid.
- Het veranderen van het huidige overheidsbeleid kan het signaal afgeven dat de Nederlandse overheid nog te beïnvloeden is. [REDACTED]

5.1.2a

[REDACTED]

5.1.2a

[REDACTED]

5.1.2a

Dep. VERTROUWELIJK



Datum
11 februari 2021
Ons kenmerk
3218540

5.1.2a

Biilage D - Kosten vervanging systemen en nadeelcompensatie

Het nadeelcompensatierecht kent geen integrale vergoeding van alle schade die ten gevolge van een rechtmatig genomen overheidsbesluit wordt geleden. Een deel van de schade zal voor eigen rekening van de MNO's blijven. Alleen de schade die het normaal bedrijfsrisico overschrijdt, komt voor vergoeding in aanmerking. Door de landsadvocaat is in samenwerking met Dialogic en onafhankelijke economen bevestigd in hoeverre wordt verwacht dat de schade ten gevolge van de beschikkingen het normaal bedrijfsrisico zal overschrijden¹¹. Dit leidt tot onderstaand beeld.

In de onderhavige casus doet het nadeel van de MNO's zich in ieder geval voor aan de kostenkant¹². Het moeten vervangen van apparatuur in kritieke onderdelen leidt in ieder geval tot de volgende kosten voor de MNO's: (1) het vervroegd afschrijven van bestaande apparatuur (restwaarde vervroegd afschrijven) en (2) het nadeel dat verband houdt met het in tijd naar voren halen van de investering in nieuwe apparatuur (kapitaalkosten vervroegde investering). Voor zover deze kosten het normaal bedrijfsrisico overstijgen, komen zij voor vergoeding in aanmerking omdat er een rechtstreeks causaal verband is tussen het overheidshandelen en deze kosten. Het normaal bedrijfsrisico wordt gesteld op een percentage van de kosten van de MNO's, de zogenaamde drempel. Het bepalen van een drempelwaarde in een unieke case als deze is maatwerk. De landsadvocaat is daarom gevraagd met een bandbreedte voor een drempelwaarde te komen binnen welke een vergoeding als rechtmatig kan worden gezien. Bij een lager percentage dan de ondergrens zal er al gauw sprake zijn van staatssteun, bij een hoger percentage dan de bovengrens, wordt onvoldoende recht gedaan aan het egalité-beginsel. Afwijken van de boven- of ondergrens vormt daarmee een juridisch risico.

Per getroffen MNO is de schade geschat voor de twee hiervoor benoemde kostenposten die in ieder geval in aanmerking komen voor compensatie. Omdat er geen exacte cijfers voorhanden zijn over het exacte moment van aankoop door de MNO's van de te vervangen onderdelen en het daarbij behorende investeringsbedrag, is gewerkt met drie scenario's. Deze geven uitdrukking aan het minimale nadeel bij de MNO's voor deze kosten ('laag'), het maximale nadeel ('hoog') en het meest waarschijnlijke scenario ('midden').

Tabel 1 (zelfde tabel als in bijlage C) – Directe vervangingskosten

5.1.2i

¹¹ Pels Rijcken, *Kader nadeelcompensatie*, januari 2021 en Dialogic, *Tentatieve geschatte schadebegroting MNO's*, januari 2021 (NB stukken volgen nog, ook met definitieve cijfers)

¹² In de financieel-economische paragraaf wordt ingegaan op mogelijke omzeteffecten

Schadecijfers voor twee kostenposten die in ieder geval voor nadeelcompensatie in aanmerking komen. Cijfers zijn schattingen van onafhankelijke experts en niet gebaseerd op cijfers van de MNO's.

Voor de vraag of er nadeelcompensatie moet worden betaald, is bepalend of het nadeel (de schade als benoemd in de tabel) als onevenredig moet worden aangemerkt. Om dat te bepalen, is het gebruikelijk te bekijken hoe het nadeel zich verhoudt tot de totale kosten van de betreffende ondernemingen. Als het nadeel in verhouding wordt gezien tot de omvang van de kosten, gaat het om een percentage van 0,4%. Ook als het nadeel wordt afgezet tegen de omzet of de winst van [REDACTED], dan is deze niet van een zodanige omvang dat gezegd kan worden dat voornoemde schade als onevenredig moet worden aangemerkt. Afhankelijk van de vergelijkingsgrondslag lopen de percentages van 0,0% tot maximaal 3,4%.

5.1.2i

In het advies meent de landsadvocaat dat van een (minimale) drempel uitgegaan zou kunnen worden van ongeveer 3-4% van de kosten van de onderneming. Dat is een aanzienlijk lager percentage dan gebruikelijk binnen het nadeelcompensatierecht¹³. Dit lage percentage is met name ingegeven door het feit dat de maatregel zoals die uiteindelijk is opgelegd, als zodanig naar het voorlopige oordeel van de landsadvocaat niet in de lijn der verwachtingen lag. Concreet betekent dit dat in alle verkende scenario's het nadeel beneden de laagste drempelwaarde zou blijven waardoor de compensatie nihil is.

De gekozen methodiek voor het bepalen van de waarde van de vervroegde afschrijving werkt goed als er sprake is van aanschaf van een asset op één moment in de tijd. [REDACTED]

5.1.2f

¹³ Gebruikelijk is een drempelwaarde tussen de 8 en 15% van de kosten of omzet



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Departementaal vertrouwelijk

Taskforce Economische Veiligheid

PNDV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

5.1.2e

nota

Oprichting Expertiseteam Veilige Digitale Overheid

Datum

17 februari 2021

Ons kenmerk

-

Bijlagen

2

Van

CIO Rijk

Datum/eindparaaf

NCTV

Datum/paraaf

Aanleiding

Recente ontwikkelingen rondom producten van [Redacted] en Kaspersky die implicaties kunnen hebben voor al dan niet gebruik van de producten door de (rijks)overheid.

5.1.2i

Gevraagde besluiten

- 1) Akkoord met oprichting expertiseteam Digitale Overheid voor de betreffende casussen, onder voorzitterschap BZK met deelname van de NCTV, NCSC, AIVD, MIVD, EZK en BZ.
- 2) Akkoord met de inzet op de twee genoemde casussen rondom [Redacted] (bijlage 1)
- 3) Akkoord met inzetten van heroverweging Kaspersky antivirussoftware, zoals uiteengezet in bijgevoegde nota (bijlage 2)
- 4) Akkoord met eerstvolgende terugkoppeling in de TFEV voorzien voor medio april

5.1.2i

Toelichting

Expertiseteam Digitale Overheid

De vraagstukken zoals die voorliggen op de verschillende producten (zie uitgebreide toelichting in de bijlagen en overzicht op hoofdlijnen beneden) gaan in de kern over de vraag welke maatregelen de (rijks)overheid moet treffen om zichzelf en zijn dienstverlening te beschermen op digitaal vlak. Om hierover onderbouwd besluiten te kunnen nemen dienen de te beschermen belangen, dreigingen en mogelijke weerbaarheidsverhogende maatregelen in kaart te worden gebracht.

Een methodiek om dit te doen is inmiddels ontwikkeld in het kader van de inzet op de telecomsector. Er wordt daarom voorgesteld een zogenaamd "Expertiseteam Veilige Digitale Overheid" (EVDO) op te richten om beide casussen op te pakken. Hierbij zal net als voor de telecomsector technisch feitelijk

PNDV

Ons kenmerk

•

5.1.2i

5.1.2i

100

Group	Yes	No	Don't know
All respondents	80%	15%	5%
Rep/Lean Rep	80%	15%	5%
Dem/Lean Dem	80%	15%	5%

5.1.2i

5.1.2i

- a. Bijlage 1 Besluit 2018 zoals gecommuniceerd aan de Tweede Kamer
- b. Kamerbrief over heroverweging in 2019
 - i. Briefwisseling met Kaspersky Labs hieromtrent

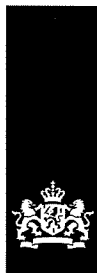
PNDV

Datum

17 februari 2021

Ons kenmerk

-



P8

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Departementaal vertrouwelijk
Taskforce Economische Veiligheid (TFEV)

BIJLAGE 2 BIJ AGENDAPUNT 'OPRICHTING EXPERTISETEAM DIGITALE
OVERHEID

Programma Nederland Digitaal
Veilig

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[Redacted]
[Redacted]

5.1.2e

nota

Heroverweging maatregel antivirussoftware Kaspersky

Datum
2 februari 2021

Ons kenmerk

Visie vooraf
NCTV Juridisch Advies
Datum/eindparaaf

Bijlagen
Kamerbrief
Voorzorgsmaatregel ten
aanzien van gebruik
Kasperskyantivirussoftware
d.d. 14 mei 2018
Kamerbrief Reactie Kaspersky
Lab inzake rol van de overheid
en IT-branche in cybersecurity
d.d. 9 juli 2019
Brief aan Kaspersky Lab d.d. 9
juli 2019
Brief aan Kaspersky Lab d.d.
13 september 2019

1. Doel nota

Besluitvorming over het onderzoeken of de maatregel van mei 2018, inhoudende dat het gebruik van antivirussoftware van Kaspersky wordt uitgefaseerd binnen de Rijksoverheid en organisaties die deel uitmaken van de vitale infrastructuur en ABDO-bedrijven wordt geadviseerd hetzelfde te doen, heroverwogen moet worden.

2. Aanleiding/gevraagde actie/advies

Aanleiding voor deze nota zijn:

- Stappen die Kaspersky in een persbericht aangeeft te hebben ondernomen op het gebied van hun gegevensopslag- en verwerkingsactiviteiten, namelijk verhuizing van deze activiteiten van Rusland naar Zwitserland;
- De doorontwikkeling van de overwegingen op basis waarvan wordt beoordeeld of maatregelen dienen te worden genomen met het oog op risico's ten aanzien van onder meer spionage en sabotage door statelijke actoren of andere partijen bij digitale producten, zoals vermeld in de TK-brief over C2000 en ook gehanteerd bij het nemen van 5G-beslissingen;

[Redacted]

5.1.2i

Gevraagde actie en tevens advies is akkoord te gaan met het verrichten van nader onderzoek naar de gewijzigde omstandigheden zoals hierboven geschetst en op basis daarvan de afweging te maken of daarin reden is gelegen om tot heroverweging van de maatregel te besluiten, vanuit het in de oplegnota genoemde Expertiseteam Veilige Digitale Overheid (EVDO), zoals geagendeerd in de TFEV van 17 februari 2021.

3. Toelichting

In mei 2018 is bovengenoemde maatregel genomen vanwege de risico's voor de nationale veiligheid in geval van gebruik van antivirussoftware van Kaspersky, waarbij is overwogen dat (a) antivirussoftware diepgaande toegang tot ICT-systemen heeft en daardoor voor bijvoorbeeld spionage kan worden misbruikt, (b) Kaspersky onder Russische wetgeving valt en die wetgeving bedrijven als Kaspersky verplicht mee te werken aan Russische inlichtingenactiviteiten, en (c) Rusland eenoffensief (cyber)programma heeft dat onder meer is gericht op Nederlandse belangen. Nadien zijn deze criteria nader aangepast c.q. aangevuld in bovengenoemde C2000-brief, waarbij onder meer uitdrukkelijk is opgenomen dat (ook) beoordeeld wordt of er beheersmaatregelen mogelijk of realiseerbaar zijn die de betrokken nationale-veiligheidsrisico's voldoende beschermen. Ook is verduidelijkt dat maatregelen ook partijen kunnen betreffen die onder controle staan van partijen uit een land met wetgeving die tot medewerking aan overheidsactiviteiten verplicht. In het 5G-traject heeft de beoordeling of er reden is voor het nemen van beschikkingen strekkend tot het weren van partijen in kritieke onderdelen van netwerken van telecomaانبieders in lijn met deze criteria plaatsgevonden.

In 2019 is op twee heroverwegingsverzoeken schriftelijk beslist dat hierin geen reden wordt gezien om tot heroverweging van de maatregel van 2018 over te gaan. Over de eerste beslissing is de Kamer bericht. Op dit moment loopt een hoger beroep in de WOB-procedure bij de Raad van State.

5.2.1

De vraag of de overheid gelet op bovenbedoelde verhuizing van de gegevensopslag en -verwerking aanleiding ziet tot heroverweging van de maatregel van 2018 verdient serieus aandacht. Van die verhuizing was in de heroverwegingsverzoeken van Kaspersky van 2019 nog geen sprake (er werd namelijk gemeld dat hiermee een aanvang werd gemaakt). Voltooiing van de verhuizing is een nieuwe omstandigheid die mogelijk implicaties kan hebben voor het al dan niet handhaven van de maatregel van 2018, met name ook als deze verhuizing een striktere compartimentering zou betekenen tussen de Russische vestiging en de activiteiten in Nederland of ten behoeve van Nederlandse klanten. Van belang is in dit verband dan in het bijzonder de toets aan de bovengenoemde criteria, zoals die met de C2000-brief en het 5G-AMvB nader zijn geformuleerd: (a) "zijn er beheersmaatregelen ... die de nationale veiligheidsrisico's ... voldoende beschermen?" en (b) "... staat de partij onder controle van een partij uit een land met wetgeving die commerciële ... partijen verplicht samen te werken met de overheid ...?". Om te beoordelen of de nieuwe omstandigheid inderdaad een striktere compartimentering tot gevolg heeft en of er daarnaast mogelijk ook in juridische zin sprake is van een verminderde controle van het bedrijf in Rusland ten opzichte van de Nederlandse vestiging, of er daardoor werkelijk sprake is van een minder groot risico voor de nationale veiligheid, is nader onderzoek daarnaar nodig. Dat is aan de hand van het persbericht van Kaspersky niet op voorhand te zeggen.

Nader onderzoek naar de technische en juridische structuur in bovenvermelde zin kost veel tijd en afstemming, zo blijkt bijvoorbeeld uit de trajecten rondom C2000 en 5G, maar het doen van dit onderzoek in het kader van een ambtshalve overweging ligt om de navolgende redenen in elk geval wel in de rede:

- [Redacted]
- [Redacted]
- [Redacted]

Programma Nederland
Digitaal Veilig

Datum
2 februari 2021

Ons kenmerk

5.1.2i en 5.2.1

5.1.2i en
5.2.1

- Tenslotte past het bij een pro-actieve en rechtvaardige overheid om ambtshalve zelfkritisch de eigen besluiten te monitoren en daarop terug te komen indien nodig, gelet op veranderende omstandigheden en voortschrijdend inzicht.

Er wordt tevens voorgesteld om het in de oplegnota voorgestelde Expertiseteam Veilige Digitale Overheid deze heroverweging ter hand te laten nemen.

Bijlagen:

1. Besluit 2018
2. Kamerbrief over heroverweging 2019
 - a. Briefwisseling met Kaspersky Labs



> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Directie Analyse en
Strategie**

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
2268367

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 14 mei 2018
Onderwerp Voorzorgsmaatregel ten aanzien van gebruik Kaspersky
antivirussoftware

Met deze brief informeer ik uw Kamer over de voorzorgsmaatregel die door het kabinet is genomen ten aanzien van het gebruik van antivirussoftware van Kaspersky Lab. Het zorgelijke beeld op het terrein van digitale dreigingen heeft, met het oog op het waarborgen van de nationale veiligheid, geleid tot aangescherpte afwegingen ten aanzien van het gebruik van digitale producten en diensten. In dat kader heeft het kabinet bepaald dat, als voorzorgsmaatregel, Kaspersky antivirussoftware bij de Rijksoverheid zal worden uitgefaseerd. Bedrijven en organisaties met vitale diensten en processen en bedrijven die vallen onder de Algemene Beveiligingseisen Defensie Opdrachten (ABDO) worden geadviseerd hetzelfde te doen. Aanleiding voor deze stap door het kabinet zijn zorgen ten aanzien van nationale veiligheidsrisico's die het gebruik van Kaspersky antivirussoftware met zich mee kan brengen. Het kabinet wil deze risico's waar mogelijk voorkomen.

Antivirussoftware is verbonden met, en/of heeft rechten over netwerken en systemen en daarmee uitgebreide en diepgaande toegang tot ICT-systemen om computervirussen te bestrijden. Dergelijke software kan echter, vanwege de uitgebreide toegang die deze biedt, ook misbruikt worden om digitale spionage en sabotage mogelijk te maken.

Kaspersky Lab is een Russisch bedrijf met haar hoofdkantoor in Rusland en valt daarmee onder Russische wetgeving. Deze wetgeving vereist dat bedrijven zoals Kaspersky de Russische inlichtingendiensten ondersteunen in de uitvoering van hun taken, indien deze diensten daarom vragen. De Nederlandse inlichtingen- en veiligheidsdiensten geven in hun jaarverslagen aan dat is geconstateerd dat de Russische Federatie al jarenlang zeer aanzienlijke capaciteiten in het digitale domein ontwikkelen. De Russische Federatie heeft een actief offensief cyberprogramma dat onder meer is gericht op Nederland en Nederlandse belangen.

De software waar het hier om gaat in combinatie met de Russische wetgeving en offensieve cybercapaciteiten, maakt dat het kabinet heeft geconcludeerd dat het risico op digitale spionage en sabotage bij de Rijksoverheid, de Nederlandse vitale infrastructuur en ABDO-bedrijven via de antivirussoftware van Kaspersky aanwezig is.

Hoewel er geen concrete gevallen van misbruik in Nederland bekend zijn, kan dit niet worden uitgesloten. Het kabinet wil een dergelijk risico waar mogelijk voorkomen en acht het bovengenoemde als de aangewezen voorzorgsmaatregel. Deze voorzorgsmaatregel ziet alleen op het gebruik van de antivirussoftware van Kaspersky binnen de Rijksoverheid, de vitale infrastructuur en ABDO-bedrijven, en dus niet op andere producten of diensten van dit bedrijf.

**Directie Analyse en
Strategie**

Datum
14 mei 2018

Ons kenmerk
2268367

Er is kennisgenomen van de aanpak en afwegingen van de Verenigde Staten en het Verenigd Koninkrijk die beiden hebben gewaarschuwd tegen het gebruik van Kaspersky antivirussoftware. Het kabinet heeft een eigenstandige inventarisatie en analyse uitgevoerd op basis waarvan een zorgvuldige afweging is gemaakt.

De betrokken partijen binnen de Rijksoverheid, de vitale infrastructuur en ABDO-bedrijven worden respectievelijk door de NCTV en Defensie geïnformeerd. Zij worden gewezen op de afwegingen die het kabinet heeft doen besluiten om deze software niet langer te gebruiken en het advies om Kaspersky antivirussoftware uit te faseren.

Kaspersky Lab is op de hoogte gebracht van deze maatregel van het kabinet. Wanneer de omstandigheden die aanleiding geven tot deze stap veranderen, kan dat aanleiding zijn voor de Nederlandse overheid om een nieuwe afweging te maken ten aanzien van het gebruik van de antivirussoftware van Kaspersky Lab.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus



Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Binnenhof 4
Den Haag

**Nationaal Coördinator
Terrorismebestrijding en
Veiligheid
Programma Nederland
Digitaal Veilig**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum 9 juli 2019
Onderwerp Reactie Kaspersky Lab inzake rol van de overheid en IT-branche in cybersecurity

Onze Referentie
2019Z05647/2019D15161

Naar aanleiding van het verzoek van de vaste commissie voor Justitie en Veiligheid van uw Kamer van 11 april 2019¹ om mijn reactie op het e-mailbericht van Kaspersky Lab over de rol van de overheid en IT-branche in cybersecurity, informeer ik u als volgt.

In het e-mailbericht, gedateerd 19 maart 2019, concludeert Kaspersky Lab dat onvoldoende inzichtelijk is geweest en niet helder is gecommuniceerd hoe de voorzorgsmaatregel met betrekking tot het gebruik van antivirussoftware van Kaspersky Lab, waarover uw Kamer op 14 mei 2018 is geïnformeerd,² tot stand is gekomen. Daarnaast wordt betoogd dat er vanuit de overheid geen objectieve richtlijnen zijn opgesteld, waardoor een schijn van willekeur gecreëerd wordt. Naar het oordeel van Kaspersky Lab is er vanwege nieuw beschikbaar gekomen informatie aanleiding tot heroverweging van genoemde voorzorgsmaatregel.

Zoals blijkt uit de bijlage bij genoemd e-mailbericht, heeft Kaspersky Lab bij brief van 1 maart 2019 aan de plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid van mijn ministerie een verzoek om heroverweging van bovenbedoelde voorzorgsmaatregel gedaan. Ik heb de reactie op dat verzoek eerder deze week, met als conclusie dat er naar mijn oordeel geen aanleiding is om de voorzorgsmaatregel te heroverwegen, aan Kaspersky Lab gestuurd. De conclusie van deze reactie houdt in dat de huidige omstandigheden geen aanleiding geven tot heroverweging van de getroffen voorzorgsmaatregel. Graag licht ik daarover het volgende toe.

Bij bovengenoemde brief van 14 mei 2018 aan uw Kamer, alsook bij brief van 27 juni 2018 aan Kaspersky Lab, is medegedeeld dat het kabinet, vanwege de mogelijke risico's voor de nationale veiligheid, besloten heeft tot het nemen van de voorzorgsmaatregel om het gebruik van de antivirussoftware van Kaspersky Lab bij de rijksoverheid uit te faseren en aan vitale en ABDO-bedrijven te

¹ Uw kenmerk: 2019Z05647/2019D15161.

² Kenmerk 2268367,

<https://www.rijksoverheid.nl/documenten/kamerstukken/2018/05/14/voorzorgsmaatregelen-aanzien-van-gebruik-kaspersky-antivirussoftware>.

adviseren hetzelfde te doen. Daarbij is in het bijzonder het volgende in samenhang van belang geacht:

- 1) Antivirussoftware heeft uitgebreide en diepgaande toegang tot ICT-systemen, waardoor deze ook misbruikt kan worden voor digitale spionage en sabotage;
- 2) Kaspersky Lab is een Russisch bedrijf en kan krachtens Russische wetgeving verplicht worden om de Russische inlichtingendiensten desgevraagd te ondersteunen in de uitvoering van hun taken;
- 3) De Russische Federatie heeft een actief offensief cyberprogramma dat onder meer is gericht op Nederland en Nederlandse belangen.³

Minister van Justitie en Veiligheid

Datum
9 juli 2019

Onze Referentie
2019Z05647/2019D15161

Deze voorzorgsmaatregel is, zoals hierboven aangegeven, genomen vanwege de mogelijke risico's voor de nationale veiligheid. Het besluit van het kabinet om een dergelijke maatregel te nemen is uiteraard genomen op basis van een zorgvuldige voorafgaande beoordeling van de mogelijke risico's. Daarbij is overigens sprake geweest van een beoordeling aan de hand van bovengenoemde factoren, die het kabinet ook in andere gevallen, zoals bij de vernieuwing van C2000, hanteert.⁴

Kaspersky Lab heeft in de bovengenoemde brief van 1 maart 2019 aangevoerd dat de beoordeling aan de hand van bovenvermelde factoren deels op onjuiste aannames berust en daarnaast gewezen op maatregelen die zij getroffen hebben om de integriteit van hun antivirussoftware te borgen. Zoals ik in mijn brief in reactie op deze brief van 1 maart 2019 aan Kaspersky Lab heb laten weten, ben ik na beoordeling hiervan nog steeds van oordeel dat het gebruik van de antivirussoftware van Kaspersky mogelijke risico's voor de nationale veiligheid heeft en er geen aanleiding is de voorzorgsmaatregel te heroverwegen.

Onverminderd geldt dat wanneer de omstandigheden die het kabinet hebben doen besluiten bovenbedoelde voorzorgsmaatregel te nemen, veranderen, dat aanleiding kan zijn om dat besluit te heroverwegen. Indien dit het geval is, zal uw Kamer hierover worden geïnformeerd.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

³ Deze specifieke omstandigheid is dit jaar opnieuw onder de aandacht gebracht in het Cybersecuritybeeld Nederland 2019, het jaarverslag van de AIVD en het jaarverslag van de MIVD.

⁴ Kenmerk 2565880,
<https://www.rijksoverheid.nl/documenten/kamerstukken/2019/04/26/beveiliging-nieuwe-infrastructuur-mobiele-communicatie-c2000>.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

Kaspersky Lab
T.a.v. [REDACTED]
Papendorpseweg 79
3528 BJ Utrecht
[REDACTED]

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

5.1.2e

T 070 751 50 50

Ons kenmerk
2481812

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 9 juli 2019
Onderwerp Uw brief van 1 maart 2019

Geachte [REDACTED],

5.1.2e

Op 1 maart 2019 heeft u, naar aanleiding van een gesprek tussen u en de [REDACTED] Nationaal Coördinator Terrorismebestrijding en Veiligheid, [REDACTED], op 17 januari jl., een brief gestuurd aan het NCSC, [REDACTED], met als onderwerp "**Reactie: voorzorgsmaatregel uitfaseren gebruik antivirussoftware Kaspersky Lab, 27 juni 2018**". In dit gesprek heeft u aangegeven reden te zien voor heroverweging van de vorig jaar door het kabinet genomen voorzorgsmaatregel ten aanzien van de antivirussoftware van Kaspersky Lab.

5.1.2e

Deze voorzorgsmaatregel houdt, zoals is toegelicht in de brief aan de Tweede Kamer van 14 mei 2018 en de brief aan uw bedrijf van 27 juni 2018, in dat, vanwege de mogelijke risico's voor de nationale veiligheid, het gebruik van antivirussoftware van Kaspersky Lab bij de rijksoverheid wordt uitgefaseerd en dat aan vitale en ABDO-bedrijven wordt geadviseerd hetzelfde te doen.

In uw brief van 1 maart 2019 schetst u ten eerste de inspanningen van Kaspersky Lab ten behoeve van de digitale weerbaarheid van Nederland en de gevolgen voor Kaspersky Lab van bovenbedoelde voorzorgsmaatregel. Ten tweede verduidelijkt u in uw brief, aan de hand van de drie factoren waarvan onder meer in mijn brief aan uw bedrijf van 27 juni 2018 is vermeld dat die aanleiding zijn geweest voor genoemde voorzorgsmaatregel, waarom u meent dat deze aanleiding berust op verkeerde aannames. Die verduidelijking en de opening van een Transparency Center in Zurich waar diverse onderdelen van uw producten onder de loep genomen kunnen worden, geven volgens u reden tot heroverweging van deze maatregel.

Op 15 maart 2019 is de ontvangst van deze brief schriftelijk aan u bevestigd. Op 3 juni is aan u een brief gestuurd waarin, naar aanleiding van uw opmerking dat deze op verzoek zal worden verstrekt, om het rapport van de heer K. Hober, waarnaar u in uw brief verwijst, is verzocht. Bij brief van 19 juni 2019 is u bericht dat streven erop is gericht om binnen uiterlijk vier weken na ontvangst van uw reactie op de brief van 3 juni, te reageren op uw verzoek om heroverweging.

Ik heb het in uw brief vermelde verzoek om heroverweging van bovenbedoelde voorzorgsmaatregel bestudeerd. Naar aanleiding hiervan ben ik tot het oordeel gekomen dat er geen aanleiding is tot heroverweging van die voorzorgsmaatregel. Ik licht dit graag ter motivering als volgt toe.

Programma Nederland
Digitaal Veilig

Datum
9 juli 2019

Ons kenmerk
2481812

Uitgebreide en diepgaande toegang tot ICT-systemen

In uw brief schrijft u het ermee oneens te zijn dat antivirussoftware uitgebreide en diepgaande toegang tot ICT-systemen heeft en dat dergelijke software vanwege de uitgebreide toegang die deze biedt, ook misbruikt kan worden om digitale spionage en sabotage mogelijk te maken. U geeft daarvoor enkele redenen.

Uw stelling onder punt I dat antivirussoftware slechts op één systeem draait en daarom geen diepe en brede toegang tot ICT-systemen heeft, deel ik niet. Bij bedrijfsmatige netwerk- en informatiesystemen is antivirussoftware doorgaans geïnstalleerd op meerdere servers of werkstations die met elkaar in verbinding staan dan wel op een centrale plek in die systemen waar al het dataverkeer doorheen komt. Antivirussoftware heeft vergaande rechten op een systeem om goed te kunnen functioneren. Zonder die rechten zou de effectiviteit beperkt zijn. Om te kunnen doen wat het moet doen, heeft antivirussoftware diepgaande toegang tot systemen, onder meer de bestanden die erop staan, en moet deze die bestanden kunnen scannen en in quarantaine kunnen zetten bij detectie van malware of virussen.

De door u onder punt II genoemde maatregelen die Kaspersky Lab treft om de integriteit van producten te waarborgen sluiten de risico's op spionage en sabotage niet uit. Ook zonder telemetrie is compromittering van netwerk- en informatiesystemen bijvoorbeeld nog steeds mogelijk. In de broncode is niet na te gaan of de AV-handtekeningen kwetsbaarheden bevatten. Inzage in de softwarebroncodes biedt geen soelaas, gelet op de omvang van de code, de veranderlijkheid daarvan bij updates en de kleine, moeilijk vast te stellen afwijkingen daarin die zouden kunnen duiden op kwetsbaarheden of backdoors. Daaraan toegevoegd de omstandigheid, dat voor een betrokken organisatie die gebruik maakt van de antivirussoftware onder meer onvoldoende controleerbaar is welke data door die software wordt verzameld en waarnaar die wordt verstuurd, maakt dat de geschetste maatregelen uitgebreide en diepgaande toegang van antivirussoftware tot de systemen waarop deze geïnstalleerd is niet uitsluiten, noch dat deze toegang gebruikt kan worden ten behoeve van digitale spionage en sabotage. De opening van een Transparency Center in Zurich, waarvan u in uw brief melding maakt, doet aan het voorgaande niet af.

De Russische wetgeving

In uw brief geeft u, onder verwijzing naar een rapport van de heer Hober, aan dat uw bedrijf niet krachtens Russische wetgeving verplicht is om de Russische inlichtingendiensten desverzocht te ondersteunen in de uitvoering van hun taken.

In zijn rapport bespreekt de heer Hober het rapport van de heer P.B. Maggs, die wetgeving van de Russische Federatie heeft benoemd op grond waarvan onder meer private organisaties verplicht kunnen worden om medewerking te verlenen aan activiteiten van de Russische inlichtingendiensten. Over de toepasselijkheid van enkele wetsartikelen verschillen Hober en Maggs van mening. Het rapport van

de heer Hober betwist echter niet dat verschillende andere wetsartikelen wel van toepassing zijn. Dit rapport doet dan ook niet af aan de conclusie dat ondernemingen in de Russische Federatie de verplichting hebben om, bijvoorbeeld door het ophalen van digitale gegevens, de Russische inlichtingendiensten assistentie te verlenen. Daarbij wijs ik in het bijzonder op artikel 15 van de Wet op de federale veiligheidsdienst (no. 40-FZ) en artikel 6 van de Wet op operationele onderzoeksactiviteiten (no. 144-FZ). Hierdoor kan ook Kaspersky Lab daartoe verplicht worden. Dit geldt niet alleen voor bijvoorbeeld organisatoren van verspreiding van informatie, daargelaten of Kaspersky Lab al dan niet als zodanig kan worden aangemerkt.

Programma Nederland
Digitaal Veilig

Datum
9 juli 2019
Ons kenmerk
2481812

Het offensieve cyberprogramma van de Russische Federatie

Tenslotte benadrukt u in uw brief, ten aanzien van de capaciteiten die de Russische Federatie in het digitale domein ontwikkelt en hun onder meer op Nederland gerichte cyberprogramma, dat Kaspersky Lab een privaat en onafhankelijk bedrijf is en dat de meerderheid van uw activiteiten buiten Rusland plaatsvindt.

De jaarverslagen van de AIVD en de MIVD over 2018 schetsen – net als vorig jaar – het beeld dat de Russische Federatie een actief en offensief cyberprogramma heeft, dat zich onder meer richt op spionage en gericht is tegen Nederland en Nederlandse belangen. Het Cybersecuritybeeld Nederland 2019 bevat ditzelfde beeld. Dit wordt in uw brief ook niet betwist.

Voorts merk ik, in reactie op uw opmerking dat de afwegingen van een aantal landen inzake het gebruik van de antivirussoftware van Kaspersky Lab verschillen, op dat het kabinet, onder kennisneming daarvan, een eigenstandige beoordeling heeft uitgevoerd en vanwege de op basis daarvan gebleken mogelijke risico's voor de nationale veiligheid de bovengenoemde voorzorgsmaatregel heeft genomen. Van belang is dat deze afweging een risico-afweging is en dat, zoals in de Kamerbrief van 14 mei 2018 is benadrukt, er geen concrete gevallen van misbruik in Nederland bekend zijn.

Tenslotte verzoekt u om een besprekingsverslag van het gesprek dat op 17 januari 2019 tussen u en [REDACTED] heeft plaatsgevonden. Ten aanzien daarvan wordt u verwezen naar de brief van 1 februari 2019 die aan u is verstuurd en die de inhoud van dit gesprek weerspiegelt.

5.1.2e

Op grond van het voorgaande zie ik in uw brief geen aanleiding de voorzorgsmaatregel, zoals die u bij brief van 27 juni 2018 is medegedeeld, te heroverwegen.

Ik hecht er hierbij aan duidelijkheidshalve op te merken dat de vorig jaar genomen voorzorgsmaatregel alleen betrekking heeft op het gebruik van de antivirussoftware van Kaspersky Lab en er derhalve geen belemmering is als het gaat om het gebruik van andere producten van, of het aangaan van een samenwerking met, uw bedrijf door de rijksoverheid, vitale bedrijven en ABDO-bedrijven.

Daarnaast geldt uiteraard dat wanneer er in de aankomende periode sprake zal zijn van een wijziging van de omstandigheden op basis waarvan tot het nemen van bovengenoemde voorzorgsmaatregel is besloten, dit aanleiding kan zijn om dat besluit te heroverwegen.

Ik hoop u hiermee voldoende geïnformeerd te hebben.

Hoogachtend,
De Minister van Justitie en Veiligheid,

Programma Nederland
Digitaal Veilig

Datum
9 juli 2019

Ons kenmerk
2481812

Ferd Grapperhaus



Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Kaspersky
T.a.v. [REDACTED]
Papendorpseweg 79
3528 BJ Utrecht
[REDACTED]

Minister van Justitie en
Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

5.1.2e

[REDACTED] 5.1.2e

Ons kenmerk
2700172

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 13 september 2019
Onderwerp Uw brief van 25 juli 2019 met kenmerk 2481812

Geachte [REDACTED],

5.1.2e

Op 25 juli 2019 heeft u, in reactie op mijn brief van 15 juli 2019, een brief gestuurd met als onderwerp "**Reactie: Uw brief van 15 juli 2019, kenmerk 2481812**". In die brief verzoekt u om heroverweging van de in mei vorig jaar door het kabinet genomen voorzorgsmaatregel ten aanzien van de antivirussoftware van Kaspersky Lab. Ook verzoekt u om het verstrekken van een aantal documenten die ten grondslag hebben gelegen aan het nemen van genoemde voorzorgsmaatregel.

Ik heb het in uw brief vermelde verzoek om heroverweging van bovenbedoelde voorzorgsmaatregel bestudeerd. Naar aanleiding hiervan ben ik tot het oordeel gekomen dat er geen aanleiding is voor heroverweging van die voorzorgsmaatregel. Graag merk ik hierbij het volgende op.

Voor anti-virussoftware geldt dat het software betreft met uitgebreide en diepgaande toegang tot ICT-systemen en dat dergelijke software daardoor ook misbruikt kan worden om digitale spionage en sabotage mogelijk te maken. Inzage in de broncode en het uitvoeren van audits, waarvan u melding maakt in uw brief, nemen dit niet weg en laten onverlet dat de kans op tijdige detectie van eventueel misbruik van die toegang – op welke wijze dan ook; via telemetrie, de broncode, een update daarvan of een AV-handtekening – gering is gelet op de complexiteit en omvang van de software in verhouding tot de subtiliteit van een mogelijke kwetsbaarheid of backdoor. Ten aanzien van de Russische wetgeving, die verplicht tot het verlenen van ondersteuning aan Russische inlichtingendiensten, is van belang dat deze, ongeacht de statutaire zetel van uw bedrijf, op Kaspersky van toepassing is. Daarnaast geldt onverminderd, en wordt door u ook niet betwist, dat er sprake is van een offensief cyberprogramma van de Russische Federatie, gericht tegen Nederlandse belangen.

Van belang hierbij is dat het kabinet bij het beoordelen van risico's van het gebruik van bijvoorbeeld antivirussoftware voor de nationale veiligheid, vanwege de mogelijkheid van spionage of sabotage door statelijke actoren of andere partijen, op een *case-by-case* basis geschiedt en dat beoordeling aan de hand van de factoren, zoals die vorig jaar zijn gehanteerd in relatie tot het nemen van bovengenoemde voorzorgsmaatregel, plaatsvindt.

Daarnaast verwijs ik in reactie op uw verzoek om verstrekking van een aantal documenten, die betrekking hebben op het nemen van de bovengenoemde voorzorgsmaatregel en naar aanleiding van uw Wob-verzoek hierover niet (volledig) openbaar zijn gemaakt, naar mijn besluit op laatstbedoeld Wob-verzoek van 25 juli 2019 met kenmerk 2658402.

**Minister van Justitie en
Veiligheid**

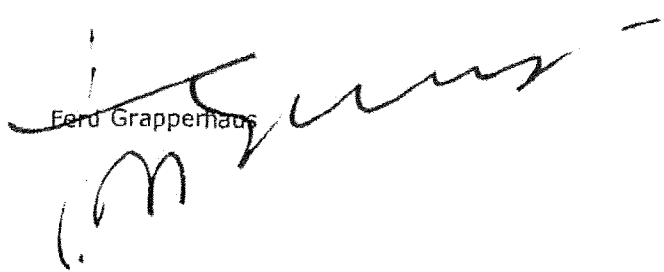
Datum
13 september 2019

Ons kenmerk
2700172

Zoals eerder benadrukt blijft gelden dat wanneer sprake is van wijziging van de omstandigheden op basis waarvan tot het nemen van de genoemde voorzorgsmaatregel is besloten, dit aanleiding kan zijn om het besluit te heroverwegen.

Ik hoop u hiermee voldoende geïnformeerd te hebben.

De Minister van Justitie en Veiligheid,


Ferd Grapperhaus



Contactpersoon

[Redacted]

T 070 751 50 50

5.1.2e

Datum

11 maart 2021

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	18 maart 2021, 15:30-17:00 uur
Vergaderplaats	MinJenV, ICCb/MCCb-zaal (3e etage)

1. Opening en mededelingen

2. Verslag TFEV 17 februari 2021

Bijlage 1. Verslag TFEV 17022021 [Redacted]

5.1.2i

3. Beschikkingen

a. Uitfaseringstermijn [Redacted] (EZK)

Stukken worden dinsdag nagezonden

5.1.2i

b. Diplomatieke woordvoeringslijn (BZ)

Bijlage 3. Oplegnota diplomatieke woordvoeringslijn beschikkingen

Bijlage 3a. Woordvoeringsstrategie [Redacted]

Bijlage 3b. Woordvoeringsstrategie [Redacted]

5.1.2a

4. Expertise team telecom/structurele samenwerking (NCTV, AIVD, MIVD)

Bijlage 4. Prioritering dreigingen telecomsector [Redacted]

5.1.2i

5. [Redacted]

5.1.1b + 5.1.2a +
5.1.2i

6. Toolkit Economische Veiligheid (EZK)

Bijlage 6. Oplegnota Toolkit Economische Veiligheid

Bijlage 6a. Toolkit Economische Veiligheid

7. Internationaal/Europees

8. Parlementair

9. Rondvraag en sluiting

MEMO van EZK

Aan: Leden Task Force Economische Veiligheid

Onderwerp: Uitsluitingstermijn [REDACTED] (agendapunt 3a)

5.1.2i

Datum: 16-3-2021

Inleiding

Er zijn concept beschikkingen opgesteld die telecomaانبieders verplichten om in kritieke onderdelen alleen gebruik te maken van vertrouwde leveranciers (zie bijlage). Een van de elementen in die beschikking is het stellen van een termijn waarbinnen kritieke onderdelen vervangen moeten worden. De vorige TFEV is stilgestaan bij de vervangingstermijn van [REDACTED] [REDACTED] aangegeven dat de voorgenomen vervangingstermijn [REDACTED] een risico oplevert voor de continuïteit van haar dienstverlening. Het besluit in de TFEV was [REDACTED] een nadere onderbouwing hiervan te vragen en aan te laten geven wat wel een haalbare vervangingstermijn is.

5.1.1c

5.1.2i

5.1.1b

5.1.2i

Advies

In de beschikking [REDACTED] vasthouden aan een vervangingstermijn [REDACTED]. Daarbij in de beschikkingen aan alle mobiele netwerkkoperators aan te geven dat mocht de implementatie buiten de invloed van een operator stagneren en de continuïteit van dienstverlening in gevaar komen indien zou worden vastgehouden aan de geldende termijn, een operator een aanvraag voor een verlenging van de vervangingstermijn kan indienen bij het Agentschap Telecom (AT). Deze aanvraag zal dan worden beoordeeld op de vraag of verlenging gerechtvaardigd is vanuit de continuïteit van dienstverlening én oorzaken buiten de invloed van een operator liggen.

5.1.2i

5.1.1b

Kernpunten

- EZK heeft [REDACTED] een nadere uitleg gevraagd over de vervangstermijn [REDACTED]. 5.1.2i
- In reactie daarop [REDACTED] 5.1.1c
- AT is gevraagd te beoordelen of het verzoek voor een langere termijn gerechtvaardigd is vanuit het perspectief van continuïteit van dienstverlening en of de ingebrachte zienswijze [REDACTED] zich voldoende concreet laat vertalen naar een verlenging van de termijn. 5.1.2i
- Voor de beoordeling heeft AT deskundigen van Dialogic geraadpleegd.
- De conclusie van AT en Dialogic luidt dat het aannemelijk is dat een vervanging [REDACTED] langer duurt [REDACTED], maar dat de zienswijze [REDACTED] onvoldoende zeker (in het manifest [REDACTED] benoemde potentiële risico's) en concreet is om nu te kunnen vertalen naar een langere vervangingstermijn. 5.1.1.c
5.1.2i
- Daarom is het advies de huidige vervangingstermijn [REDACTED], welke is gebaseerd op eerdere plannen [REDACTED] en beoordeling door AT en Dialogic, te handhaven. 5.1.1b
5.1.2i(2x)
- Mochten de [REDACTED] benoemde potentiële risico's die tot een verlenging van de termijn nopen zich daadwerkelijk voordoen, hetgeen lastig te voorzien is bij dit soort complexe IT projecten, dan kan [REDACTED] een verzoek voor verlenging van de vervangingstermijn indienen bij AT. 5.1.2i
- AT zal de onderbouwing van een verzoek beoordelen en een advies uitbrengen aan EZK. EZK zal de voorgenomen reactie op een verzoek voor verlenging voorleggen aan de TFEV.
- De planning is om de definitieve beschikkingen eind april 2021 uit te sturen, na behandeling in ACEV (30 maart), MCEV (13 april) en MR (16 april).

Toelichting

In opvolging van besluitvorming in de vorige TFEV heeft EZK [REDACTED] verzocht om een nadere uitleg van eerdere opmerkingen [REDACTED] dat de in de concept beschikking genoemde termijn voor het vervangen van [REDACTED] niet kan worden gehaald en dat een langere termijn noodzakelijk is. [REDACTED] heeft dit nader toegelicht in brieven van 25 februari 2021 en 8 maart 2021.

5.1.2i (2x)

5.1.1c

5.1.2i

EZK heeft AT vervolgens gevraagd om te beoordelen of en in hoeverre de nadere toelichting [REDACTED] een langere termijn [REDACTED] rechtvaardigt vanuit het perspectief van de continuïteit van

5.1.2i

5.1.1c

dienstverlening. En of de ingebrachte zienswijze [redacted] zich op dit moment voldoende concreet laat vertalen naar een verlenging van de termijn. 5.1.2i

AT heeft de argumenten [redacted] beoordeeld, met inschakeling van deskundigen van Dialogic. Zij komen samen tot de conclusie dat het aannemelijk is dat een vervanging van [redacted] langer zal duren dan [redacted] maar dat de onderbouwing van de gevraagde (langere) termijn naar ongeveer [redacted] onvoldoende zeker (in het manifest worden [redacted] benoemde potentiële risico's) en concreet is om nu te kunnen vertalen naar een verlenging van de termijn [redacted]. Het is onvoldoende zeker dat de continuïteit van dienstverlening in gevaar komt bij de vervangings-termijn [redacted]. 5.1.2i (1x)
5.1.1c
5.1.1b
5.1.2i
5.1.1b (2x)

Behoud van de termijn [redacted] als vervangingstermijn [redacted] is goed te onderbouwen. De termijn [redacted] is overgenomen uit eerder ingediende plannen [redacted] voor vervanging [redacted]. Deze termijn is destijds door AT en Dialogic beoordeeld als realistisch, waarbij tegelijkertijd werd aangegeven dat het plan [redacted] minder concreet is uitgewerkt en meer onzekerheden kent dan de plannen voor vervanging van de andere kritieke onderdelen. Deze onzekerheden zijn het gevolg van het feit [redacted] een uiterst complex IT systeem betreft met veel interfaces naar andere systemen. 5.1.1b 5.1.1c
5.1.1b 5.1.2i
5.1.1c
5.1.1c
5.1.1c

[redacted] in haar nieuwe zienswijze met name op deze onzekerheden en (bijbehorende) risico's in en betoogt dat als deze daadwerkelijk optreden, dit noopt tot een langere vervangingstermijn. De conclusie van AT en Dialogic is dat de nieuwe informatie [redacted] het inderdaad aannemelijk maakt dat een vervanging [redacted] langer duurt dan [redacted], maar dat de onderbouwing onvoldoende zeker (treden die potentiële risico's daadwerkelijk op) en concreet is om nu te kunnen vertalen naar een langere vervangingstermijn. 5.1.2i
5.1.2i
5.1.1c
5.1.1b

Op basis van de nieuw verkregen informatie [redacted] is het zeker voorstelbaar dat een langere termijn uiteindelijk noodzakelijk zal zijn. Daarom wordt in de beschikking een passage opgenomen dat, mochten de [redacted] benoemde potentiële risico's die tot een verlenging van de termijn nopen met het oog op de continuïteit van dienstverlening zich daadwerkelijk voordoen, [redacted] verzoek voor verlenging van de vervangingstermijn kan indienen bij AT. Op basis van de zich dan voordoende feiten en beoordeling van de vraag of verlenging gerechtvaardigd is vanuit de continuïteit van dienstverlening én oorzaken buiten de invloed van een operator liggen, kan een beter oordeel worden geveld over een eventuele verlenging van de vervangingstermijn [redacted]. 5.1.2i (3x)
5.1.1c

De bewijslast voor een verlenging van de termijn ligt bij de operator. AT zal de onderbouwing van de operator met inschakeling van externe deskundigen beoordelen en een advies uitbrengen aan EZK. EZK zal de voorgenomen reactie op een verzoek voor verlenging vervolgens voorleggen aan de TFEV.

Vervolg

November 2020 zijn de voornemens voor de beschikkingen veiligheid en integriteit telecomnetwerken aan de mobiele netwerk operators verstuurd. Eind december 2020 zijn hun zienswijzen ontvangen.

De beschikkingen zijn op basis van de verkregen zienswijzen op een aantal punten verduidelijkt. Indien de TFEV akkoord is met het voorstel voor de vervangingstermijn [redacted] zoals omschreven in deze memo, is er geen sprake van principiële wijzigingen in de definitieve beschikkingen ten opzichte van de eerder aan de TFEV voorgelegde voornemens voor de beschikkingen. 5.1.1c

De planning is om de definitieve beschikkingen eind april 2021 uit te sturen, na behandeling in ACEV (30 maart), MCEV (13 april) en MR (16 april).

[redacted]
[redacted]@minezk.nl

5.1.2e



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

18

Dep.-VERTROUWELIJK
TFEV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
18 maart 2021

Ons kenmerk

oplegnota

Toolkit Economische Veiligheid

Gevraagde beslissing/doel
Samenvatting

Ter kennisneming

EZK heeft een *Toolkit Economische Veiligheid* ontwikkeld.

Aanleiding

Economische veiligheid is een onderwerp waar steeds meer EZK medewerkers in hun werk zijdelings mee te maken krijgen. Bijvoorbeeld wanneer ze de aanvraag voor een PPS-toeslag moeten beoordelen of een samenwerkingsverband tussen een kennisinstelling en bedrijf faciliteren. Om hen een handreiking te bieden in het constateren van mogelijke risico's en wat mogelijke handelingsopties zijn, heeft EZK een *Toolkit Economische Veiligheid* ontwikkeld.

Toelichting

Economische veiligheidsrisico's kunnen zich voordoen binnen verschillende werkterreinen van EZK. Wanneer medewerkers denken met een economisch veiligheidsrisico te maken te hebben, is momenteel weinig praktische informatie ter beschikking. Hierdoor worden EV overwegingen soms te weinig meegenomen of blijven medewerkers juist zitten met onbeantwoorde EV vraagstukken.

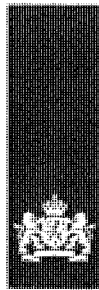
- De *Toolkit Economische Veiligheid* heeft drie doelen:
 1. Bewustwording creëren over EV bij EZK medewerkers die zijdelings met EV-vraagstukken te maken kunnen krijgen.
 2. Een handreiking bieden aan medewerkers die tegen een specifieke casus aanlopen.
 3. Structuur en houvast geven voor het afwegingsproces voor EV casuïstiek.
- De toolkit is nadrukkelijk niet bedoeld als antwoord op casuïstiek waarbij complexere economische-, veiligheids- en diplomatieke belangen spelen, maar voornamelijk als handreiking voor een eerste analyse door de dossierhouder. In de toolkit wordt dan ook

expliciet verwezen naar het tijdig betrekken van relevante collega's binnen de Rijksoverheid, die zulke casuïstiek in de daartoe bijpassende gremia behandelen (bijv. de TFEV).

- De toolkit zal middels een pagina op het Rijksportaal beschikbaar worden gesteld voor alle EZK medewerkers. Om het actief te gaan gebruiken zal het team EV bij een aantal directies binnen EZK langsgaan om casuïstiek langs de toolkit houden en de formats te toetsen. Daarnaast kan het (onder begeleiding) worden gebruikt door bijvoorbeeld de RVO of andere diensten.
- Als het gebruik van de toolkit goed bevalt zou deze, in de huidige vorm of in een aangepaste vorm, ook interdepartementaal of in samenwerking met universiteiten of bedrijven kunnen worden gebruikt.

Afstemming

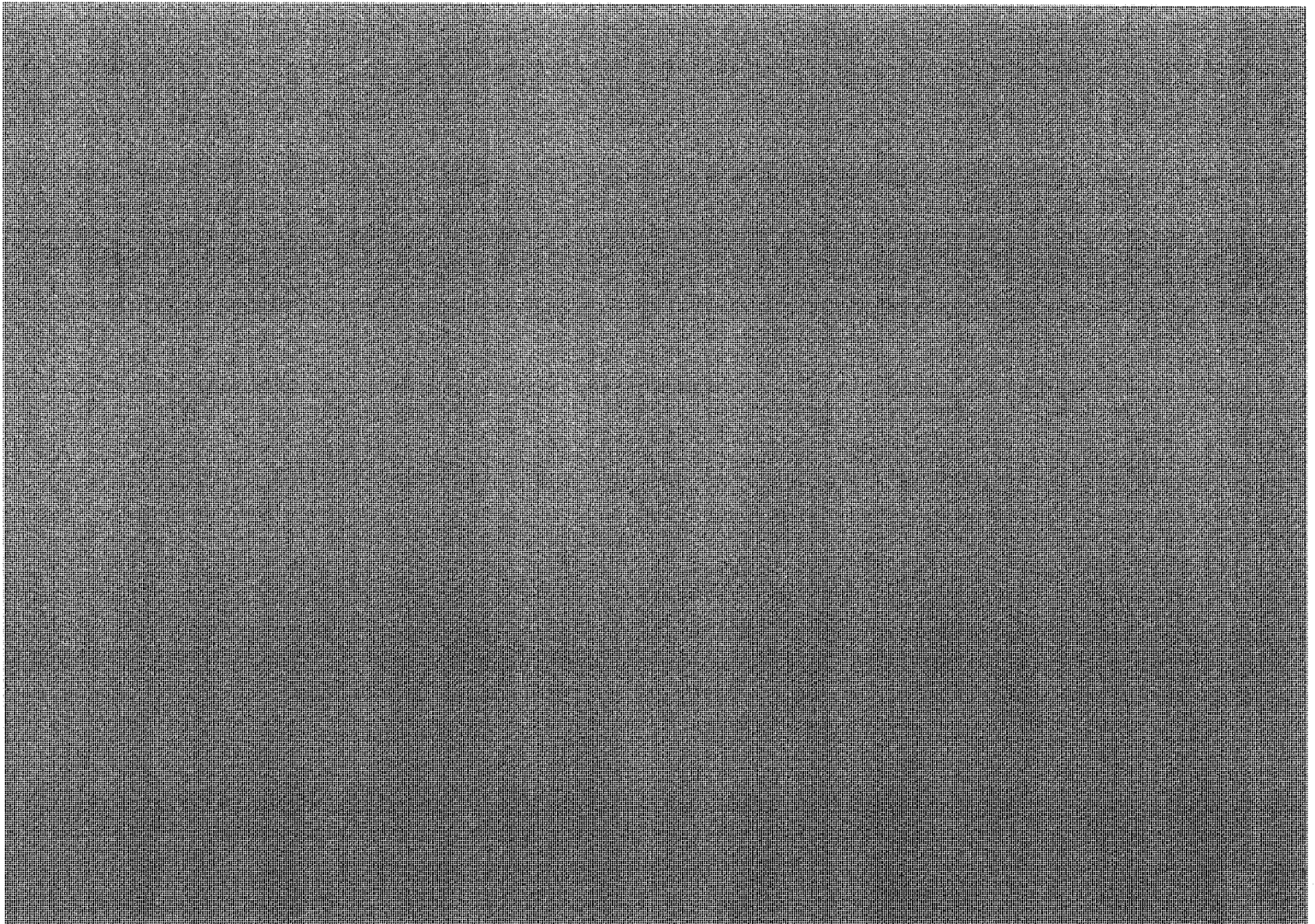
Conceptversies van de toolkit zijn besproken met de NCTV en BZ. Hierop is nuttige input ontvangen, met name over de scoping en opbouw van de toolkit. De opbouw is nu geïnspireerd op de documenten over nationale veiligheid bij inkoop en aanbesteden die door de NCTV en BZK zijn ontwikkeld. Ook feedback over het verduidelijken van de reikwijdte en het proces rondom de toolkit (zoals 'wanneer schakel je als dossierhouder wie in?' en 'wanneer vindt interdepartementale afstemming plaats?') is meegenomen.

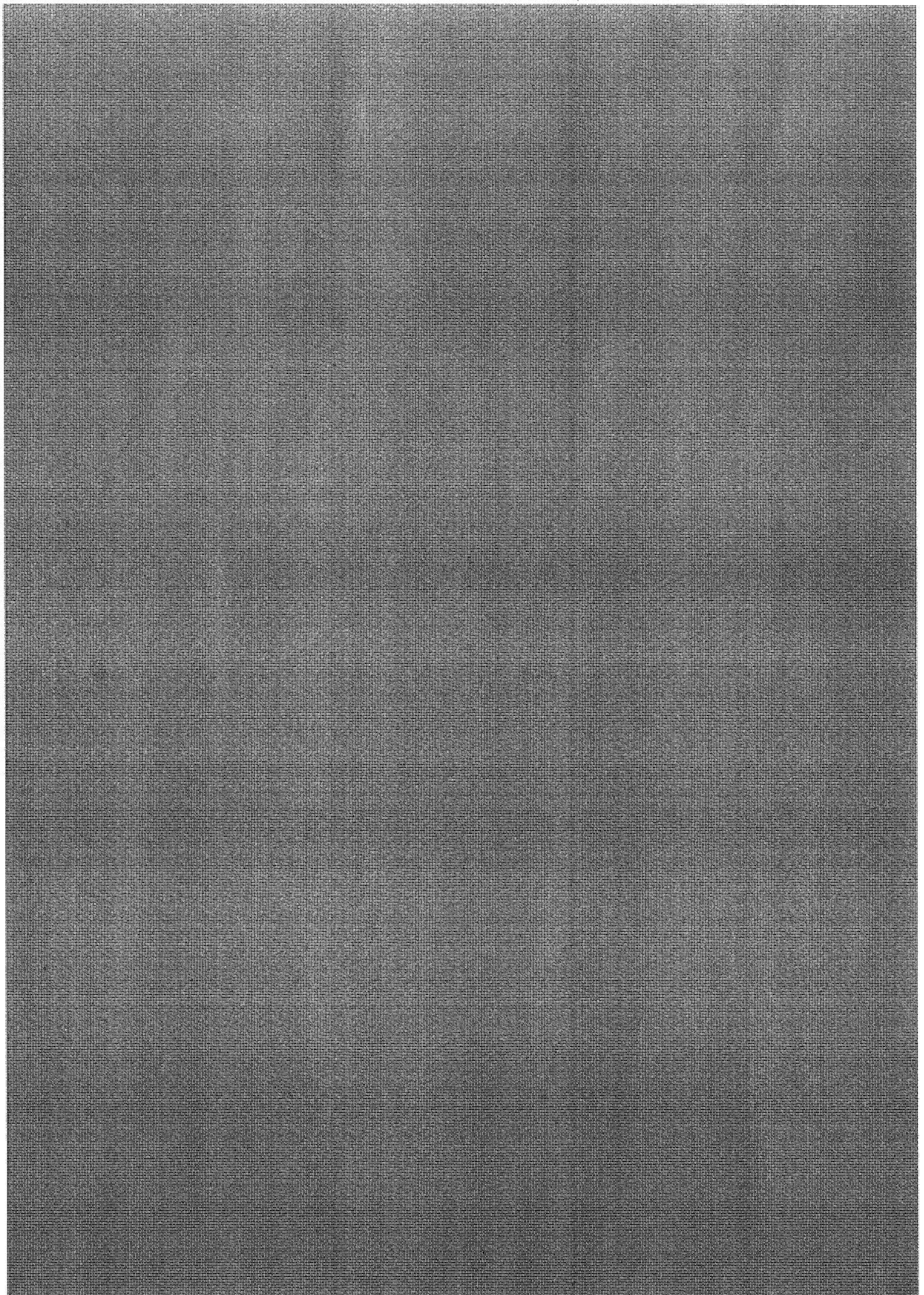


Q12

Ministerie van Economische Zaken
en Klimaat

Toolkit Economische Veiligheid





Inhoudsopgave

Inleiding	4
Gebruiksaanwijzing	5
1 Quickscan nationale veiligheidsrisico's	6
2 Risicoanalyse	8
3 Handvatten voor maatregelen	9
4 Impactanalyse	10
5 Besluit	13

Inleiding

Open markten en sterke verwevenheid van landen in mondiale waardeketens zorgen voor meer welvaart en toegang tot de beste productiefactoren. Bovendien stimuleert het de ontwikkeling van kennis en innovatie. Open markten en een sterke internationale verwevenheid brengen echter ook kwetsbaarheden en dreigingen voor de nationale veiligheid met zich mee. In het bijzonder gaat het om drie dreigingen:

1. sabotage of verstoring van onze vitale infrastructuur;
2. het weglekken sensitieve technologie en kennis;
3. het ontstaan van strategische afhankelijkheden binnen vitale infrastructuur of sensitieve technologie waarmee Nederland politiek onder druk kan worden gezet.

Bij het mitigeren van deze dreigingen spreken we van het borgen van de economische veiligheid van Nederland.

De economische veiligheid kan op verschillende manieren in het geding komen. Vitale processen worden niet alleen door publieke partijen en overheidsonderdelen uitgevoerd en aangeboden, maar veelal ook door het (private) bedrijfsleven. Sensitieve technologie die gevolgen kan hebben voor de nationale veiligheid wordt niet alleen ontwikkeld door het bedrijfsleven, maar ook door universiteiten en toegepaste kennisinstellingen. Een economisch veiligheidsvraagstuk kan op de radar verschijnen als gevolg van de uitvoering van een instrument – bijvoorbeeld subsidieverlening of aanbesteding – maar soms komt het juist in beeld door handelingen van andere staten of bedrijven die een link hebben met een buitenlandse overheid.

Veel instrumentarium is al in werking of wordt op dit moment ontwikkeld als gevolg van dreigingen voor de economische veiligheid van Nederland. Zo zijn er maatregelen op het gebied van investeringstoetsing en op gebied van kennisveiligheid in ontwikkeling.

Waarom deze toolkit?

Het kan zijn dat u in aanraking komt met een casus in het economisch domein waarbij u twijfels heeft over de impact op de veiligheid van Nederland en bovendien het idee heeft dat het niet past bij bestaand instrument voor de economische veiligheid (zoals exportcontrole of de investerings-

toets). Om na te gaan of er sprake is van zo'n risico is deze toolkit opgesteld, bestaande uit 5 hulpmiddelen:

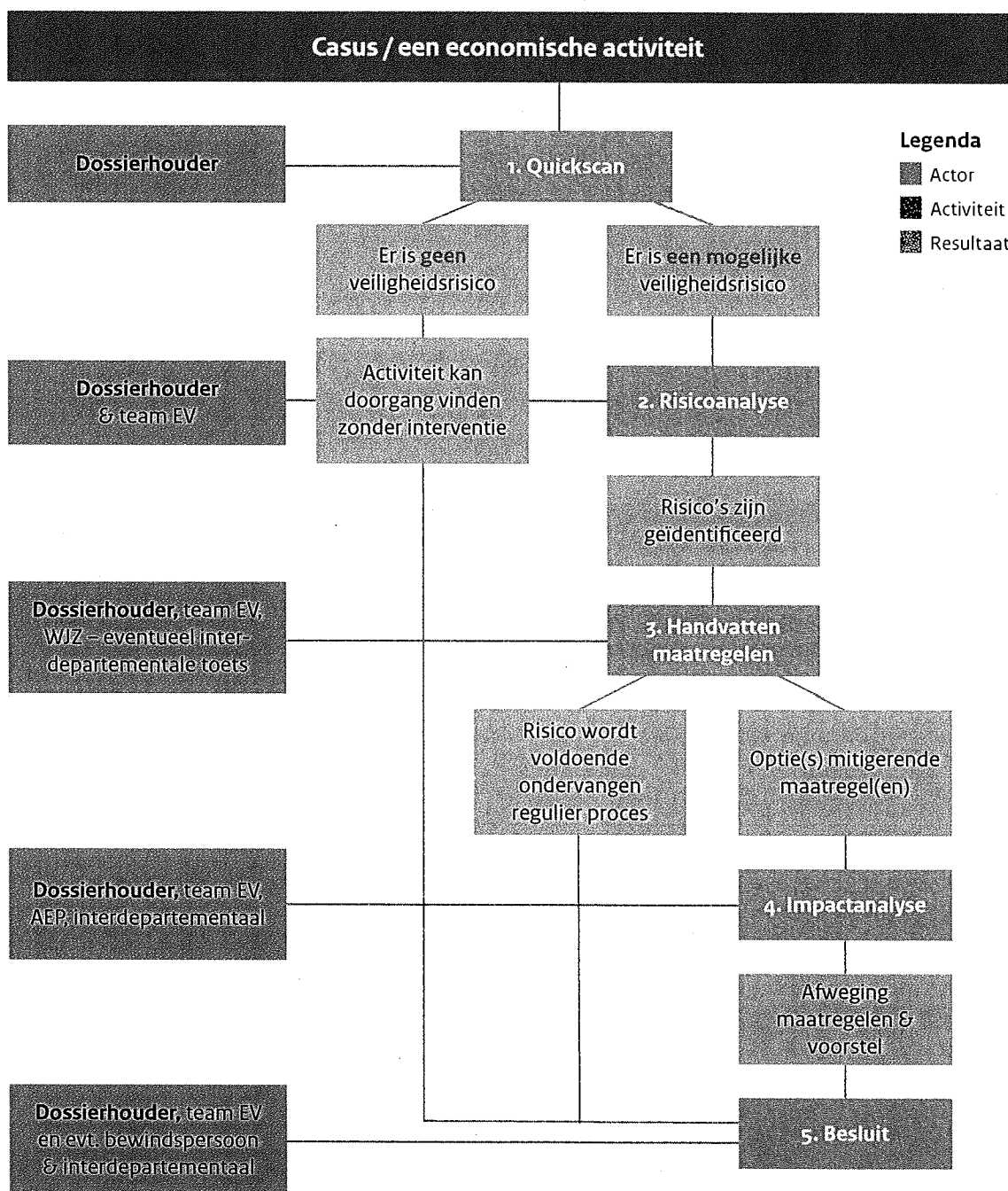
1. **Quickscan** - Door middel van de quickscan kunt u nagaan of u te maken zou kunnen hebben met een economisch veiligheidsrisico.
2. **Risicoanalyse** - Indien er 'orange' of 'red flags' volgen uit de risicoanalyse, vervolgt u met het maken van een uitgebreide analyse, mogelijk in samenwerking met team Economische Veiligheid (EV). Hiervoor schakelt u externe bronnen in en kunt u deze interdepartementaal laten toetsen.
3. **Handvatten voor maatregelen** - Vervolgens zijn er enkele suggesties voor maatregelen opgenomen in de toolkit, zonder de pretentie uitputtend te zijn. Met behulp van de directie Wetgeving en Juridische Zaken (WJZ) kunnen de maatregelen worden uitgedacht.
4. **Impactanalyse** - Na het inventariseren van maatregelen gaat u over naar de impactanalyse. Bij het nemen van een maatregel, brengt u eerst de impact daarvan in kaart op de economie (bezien in tijd en schaal), de diplomatieke betrekkingen en de nationale veiligheid. Het ligt voor de hand deze maatregel gezamenlijk met de probleemanalyse interdepartementaal door te denken en af te stemmen.
5. **Voorgenomen besluit** - het ligt voor de hand het voorgenomen besluit interdepartementaal af te stemmen afhankelijk van de schaal/fase van het probleem op een passend niveau. Ook de eigen bewindspersoon wordt indien nodig geïnformeerd.

Het is goed mogelijk dat u niet alle stappen van de toolkit hoeft te gebruiken, bijvoorbeeld omdat u er al snel achter komt dat er geen belangrijk veiligheidsrisico is. Zie hiervoor ook het stroomschema op pagina 5.

Deze toolkit biedt geen blauwdruk voor elke casus, maar een handreiking om de te nemen stappen van te voren te overzien. Team Economische Veiligheid verleent hulp bij inhoud en proces; u blijft als dossierhouder zelf verantwoordelijk voor de uitvoering van uw instrument.

Gebruiksaanwijzing

Deze toolkit bestaat uit een aantal formats die u kunt gebruiken voor het afhandelen van een casus met een mogelijk economisch veiligheidsrisico. Onderstaand vindt u het bijbehorende proces. De grijze blokjes zijn de formats die u in de toolkit vindt. De actoren die nodig zijn om de formats in te vullen staan in onderstaand stroomschema en bovenaan de formats aangegeven in geel.

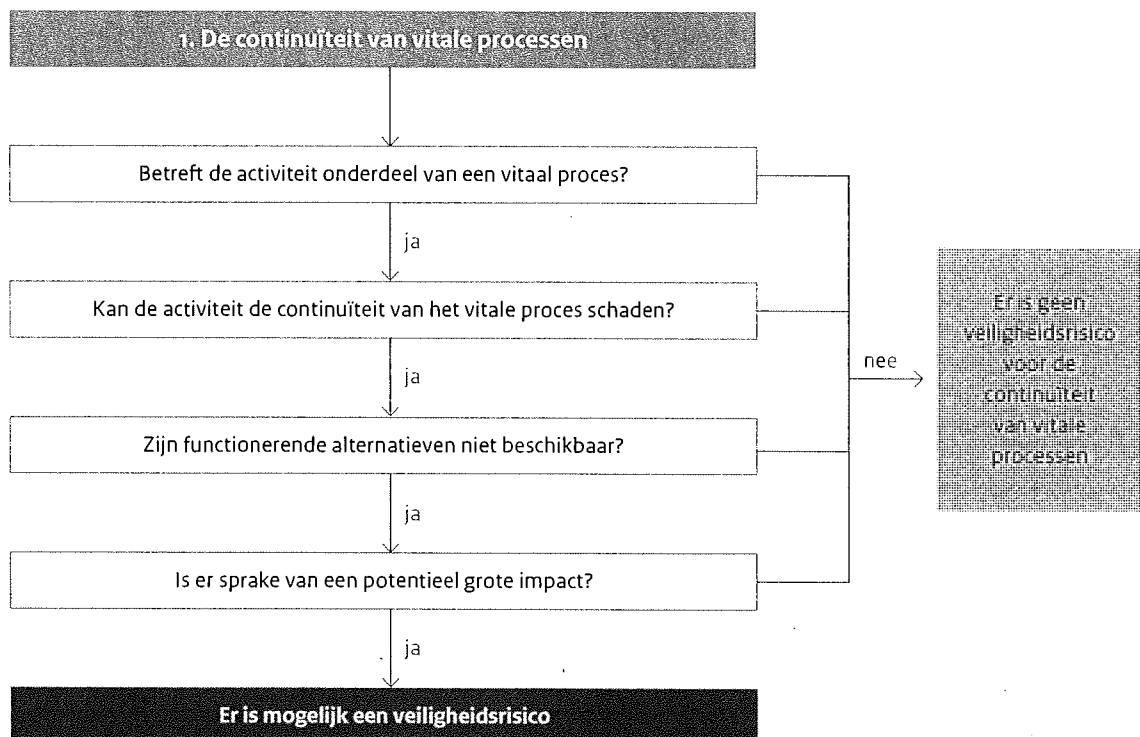


1 Quickscan nationale veiligheidsrisico's

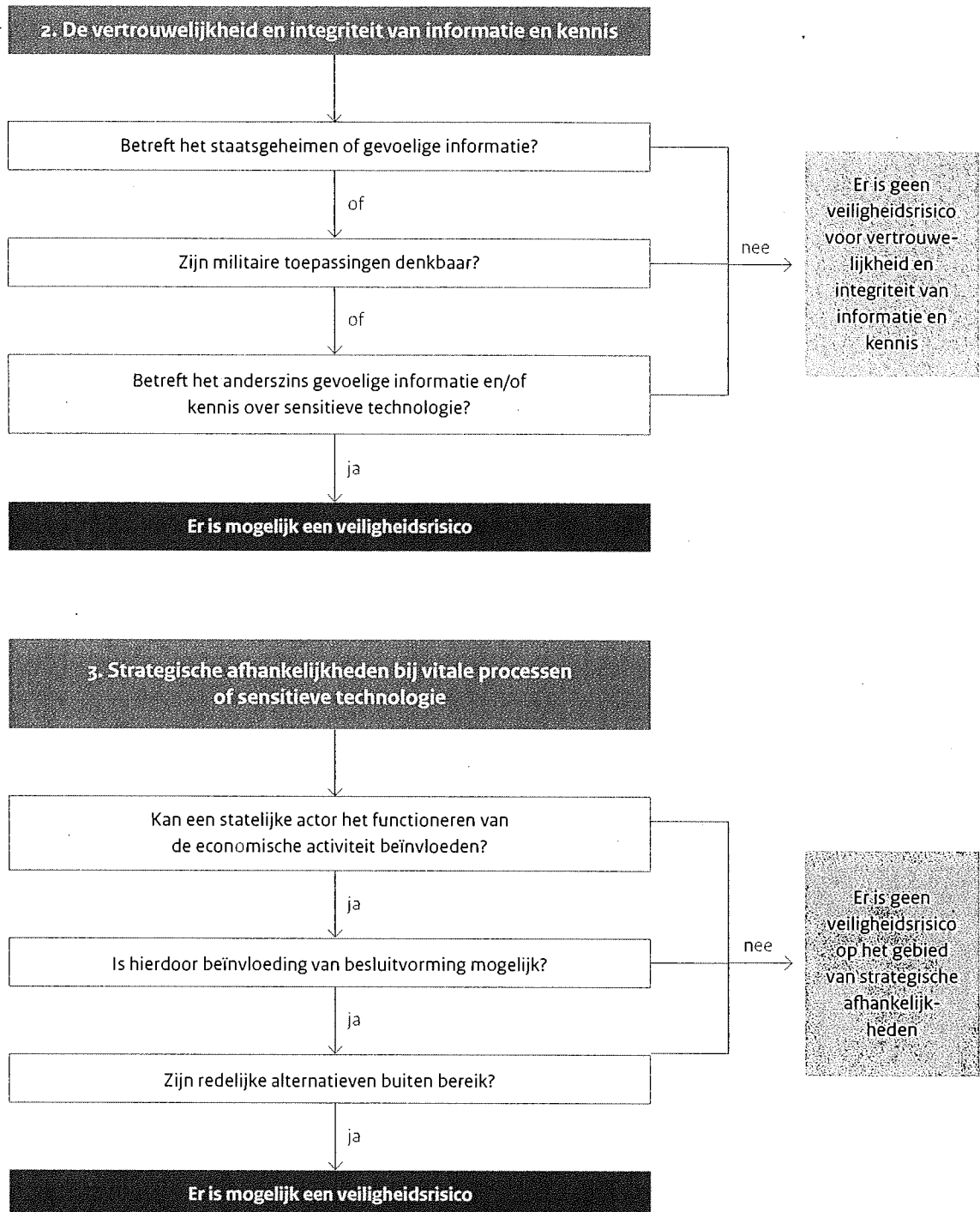
In deze stap kijken we of er mogelijk sprake is van een nationaal veiligheidsrisico bij het uitvoeren van de economische activiteit. Dit doen we aan de hand van de eerder genoemde drie categorieën: de continuïteit van vitale processen, de vertrouwelijkheid en integriteit van informatie en kennis en strategische afhankelijkheden. Alle vragen in de categorie moeten met 'ja' worden beantwoord om een veiligheidsrisico te vormen. Wanneer 'nee' wordt geantwoord in één van de drie categorieën, kan door worden gegaan naar de volgende categorie.

Legenda

- I. **Vitaal proces:** zijn processen die bij uitval of verstoring tot ernstige maatschappelijke ontwrichting kunnen leiden. Zie ook: <https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen>.
- II. **Staatsgeheim/ gevoelige informatie:** vertrouwelijke informatie, waarvan het grote nadelige gevolgen heeft voor de nationale veiligheid als het openbaar wordt of in verkeerde handen komt.
- III. **Militaire toepassing:** de techniek of kennis is te gebruiken voor militaire/defensie toepassing.
- IV. **Sensitieve technologie:** technologie die een impact kan hebben op de nationale veiligheid, door het mogelijke gebruik in vitale processen of voor proliferatiedoelinden. In het bijzonder gaat het om technologieën die nu al gecontroleerd zijn onder het exportcontroleregimes of anderszins zijn aangewezen als *dual-use*.
- V. **Statelijke actoren:** de overheid van een land.
- VI. **Economische activiteit:** het leveren, verwerken en produceren van diensten en goederen.



Dossierhouder



Als u uit de quickscan opmaakt dat er mogelijk sprake kan zijn van een nationaal veiligheidsrisico, neem dan contact op met ev@minezk.nl. Het team Economische Veiligheid kan u begeleiden in het maken van een uitgebreidere risicoanalyse en eventuele volgende stappen.

2 Risicoanalyse

In deze stap kijken we of er mogelijk sprake is van een nationaal veiligheidsrisico bij het uitvoeren van de economische activiteit. Dit doen we aan de hand van de eerder genoemde drie categorieën: de continuïteit van vitale processen, de vertrouwelijkheid en integriteit van informatie en kennis en strategische afhankelijkheden. Alle vragen in de categorie moeten met 'ja' worden beantwoord om een veiligheidsrisico te vormen. Wanneer 'nee' wordt geantwoord in één van de drie categorieën, kan door worden gegaan naar de volgende categorie.

1. Risico's voor de continuïteit van vitale processen	
Kan de activiteit leiden tot verstoringen, aantasting of uitval in de dienstverlening?	
Kan de activiteit (op korte termijn) leiden tot verstoring, aantasting of uitval van de productie, distributie en aanlevering van goederen/ producten?	
Kan de activiteit (op korte termijn) leiden tot gebrek aan toegang tot vitale infrastructuur?	
Is de actor leverancier van producten of diensten die in Nederland niet of moeilijk substitueerbaar zijn en die voorwaardelijk zijn voor de continuïteit van het vitaal proces?	
Is er sprake van een activiteit in een doelonderneming dat beschikt over cruciale kennis of technologie waarvan de gegarandeerde toegankelijkheid van essentieel belang is voor de continuïteit van een vitaal proces?	
2. Risico's voor de integriteit en vertrouwelijkheid van kennis en informatie	
Kan de activiteit leiden tot toegang tot (of juist tot het verhinderen van toegang tot), of het weglekken of verdwijnen van hoogwaardige en specialistische kennis en informatie, wat potentiële implicaties heeft voor de nationale veiligheid?	
Kan de activiteit leiden tot ongeoorloofde/ ongewenste kennisname en stelen van (met andere woorden: spionage op) hoogwaardige specialistische kennis en informatie en grootschalige privacy schending, wat potentiële implicaties heeft voor de nationale veiligheid?	
3. Risico's op strategische afhankelijkheden	
Hoezeer is NL afhankelijk van levering/productie door betreffende statelijke actor?	
Is het aannemelijk dat geen tijdig alternatief beschikbaar is?	
3. Risico's op strategische afhankelijkheden	
Is Nederland kwetsbaar voor invloed uit het land dat het functioneren van de economische activiteit kan beïnvloeden?	
Kan de activiteit leiden tot pressie, chantage en manipulatie (door statelijke actoren), wat onder meer kan leiden tot een strategische afhankelijkheid van die statelijke actoren?	
Is er sprake van een onlogische verhouding tussen de activiteit en het Bruto Nationaal Product (BNP) van het deel van het Koninkrijk waar de activiteit betrekking op heeft?	
4. Land van herkomst	
Is er sprake van inmenging of beïnvloeding door een statelijke actor? Met andere woorden: wordt de actor gedreven door een statelijke actor en/of is er sprake van (zakelijke) banden of eigendomsverhoudingen tussen de verwerver en een statelijke actor?	
Is de actor ingezetene van een staat, waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze geen of ontoereikende of niet-transparantie scheiding heeft tussen civiele en militaire onderzoeks- en ontwikkelingsprogramma's?	
Is er een negatieve staat van dienst van deze statelijke actor, kent deze bijvoorbeeld offensieve programma's, gericht op het verstoren of aantasten van de integriteit van een vitaal proces en/of het verwerven van sensitieve technologie om een technologische of strategische machtspositie te verwerven?	
Is de actor of staat de actor onder invloed van een natuurlijke persoon, rechtspersoon of niet-statale entiteit die is onderworpen aan beperkende maatregelen zoals sancties door NL, de EU of VN?	
Is de actor ingezetene van een staat, waar (1) geen exportcontrolebeleid aanwezig is, of die (2) een slechte staat van dienst heeft inzake exportcontrole, of die (3) niet gebonden is aan relevante verdragen of besluiten van volkenrechtelijke organisaties inzake beveiliging, rubricering of exportcontrole, of die (4) een slechte staat van dienst heeft in de naleving van deze verdragen?	

Als uit de risicoanalyse blijkt dat de activiteit risico's voor de nationale veiligheid met zich mee kan brengen, kunt u gaan kijken naar in hoeverre de risico's mogelijk al worden afgevangen door een regulier proces. Het kan bijvoorbeeld zijn dat er al bestaande wet- en regelgeving is om risico's te ondervangen. Wanneer dit niet het geval is, kan worden gekeken naar bestaande mitigerende maatregelen of aanvullende mitigerende maatregelen.

3 Handvatten voor maatregelen

In de vorige stappen heeft u in kaart gebracht welke kenmerken de casus heeft, daarbij zijn er o.a. de volgende mogelijkheden:

Kenmerken van de casus:
Import/aanbesteding
Export
Investeren
Personeel
Aanbesteden
Innovatie samenwerking
Fallosceneit

Veiligheidsrisico
Verstoring vitale processen
Proliferatie sensitieve kennis / technologie
Strategische afhankelijkheden

Nu het potentiële economische veiligheidsrisico is geïdentificeerd, kunt u geschikte maatregelen identificeren.

Vier instrumenten vangen op dit moment een groot deel van de casuïstiek op, waarmee mitigerende maatregelen te nemen zijn, namelijk:

1. Exportcontrole
2. Investeringsstoetsing
3. Kennisveiligheid
4. Aanbestedingsinstrumenten

Economische veiligheidsvraagstukken zijn doorgaans complex en vereisen maatwerk. U gebruikt deze toolkit omdat de casus nog niet in een bestaand proces wordt gemitigeerd, of weliswaar gerelateerd is aan één van bovenstaande instrumenten maar daarmee wordt het risico niet volledig afgedicht. Er blijft dan een rest risico over. Vaak heeft een casus bijvoorbeeld meer dimensies waardoor er aan meerdere instrumenten gedacht kan

worden, valt de casus inhoudelijk buiten de reikwijdte van het instrument, of bevindt de casus zich in een stadium waarbij voor de hand liggende instrumenten nog niet in beeld komen. De volgende lijst is niet volledig en niet direct te gebruiken voor mitigerende maatregelen, maar dient ter inspiratie en bespreking met team EV, WJZ en ter interdepartementale toetsing, als potentiële mitigerende maatregelen.

Mitigerende maatregelen
Informatie rubriceren
Contractuele afspraken
Geheimhoudingsplicht
DTC/NCSC instakken
Scheringsmaatregelen nemen
Financiering/steun
Vertrouwensfuncties instellen
Opzeggen van opdracht

Voorbeeld: Indien de casus te maken heeft met PPS en uit de risicoanalyse is gebleken dat er een risico is op weglekken van sensitieve technologie, is het mogelijk om, in samenwerking met WJZ, contractuele afspraken op te stellen over openbaarmaking van kennis.

4 Impactanalyse

Nu de risico's in beeld zijn gebracht en naar mogelijke maatregelen is gekeken, gaan we naar de impactanalyse. In deze stap wordt gekeken naar de economische impact van mogelijke maatregelen door op bedrijfsniveau, waardeketen/ecosysteem en nationale economie aan te geven wat de economische gevolgen zijn.

Als blijkt dat de economische effecten van de maatregelen mogelijk erg groot kunnen zijn, moet worden overwogen of deze maatregel wel de juiste is om het geïdentificeerde risico te mitigeren. Het kan zijn dat het dan handig is om

weer terug te gaan naar de stap waarin wordt gekeken naar mitigerende maatregelen om te kijken of andere maatregelen wellicht beter passen. De hamvraag is dan: wegen de kosten van de maatregel op tegen de baten van het minimaliseren van het rest risico?

Hieronder is een lijst met vragen weergegeven die als leidraad kunnen dienen, maar zullen ook in consultatie met andere medewerkers moeten worden aangevuld en beantwoord, afhankelijk van de casus.

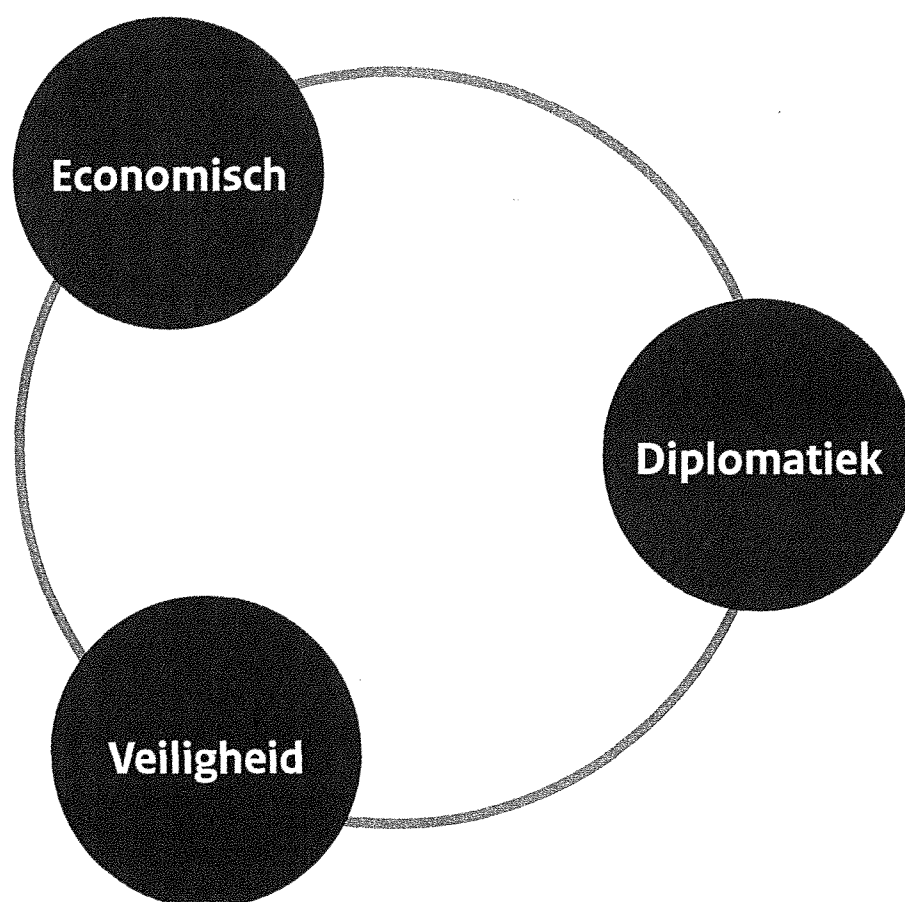
Vraag	Nu	Over een jaar	Meer dan een jaar
Bedrijfsniveau			
Wat is de impact op de concurrentiepositie van het bedrijf? (inclusief R&D/kennis/patenten/afzetmarkt/omzetflexibiliteit/ bedrijfsvoering)	Kies: <div> <div></div> <div></div> <div></div> </div>	Kies: <div> <div></div> <div></div> <div></div> </div>	Kies: <div> <div></div> <div></div> <div></div> </div>
Hoe beïnvloedt de maatregel het gelijk speelveld ten opzichte van concurrenten?			
Wat is de invloed van de maatregel op de continuïteit van het bedrijf?			
Waardeketen en ecosystemen			
Wat is de grootte van het bedrijf?			
Wat is de betekenis van deze bedrijfsactiviteit voor de regionale economie en kennisontwikkeling?			
Hoe zijn de effecten van de maatregel op de positie van het bedrijf in de waardeketen?			
Hoe zijn de effecten van de maatregel op de concurrentiepositie van de sector?	Open vraag		
Hoe zijn de effecten van de maatregel op de ontwikkeling van de sector?	Open vraag		
Nationale economie			
Wat zijn de effecten van de maatregel op het vestigingsklimaat van NL?			
In welke mate kan de maatregel effect hebben op het vestigingsklimaat van NL?			

Effecten v/d maatregelen

- Hoog
- Middelmatig
- Laag

Dossierhouder, team EV, AEP, interdepartementaal

Tot slot moet er gekeken worden naar de cascade effecten van het nemen van de mitigerende maatregelen, op diplomatiek en veiligheidsaspect. Deze analyse moet gemaakt worden in consultatie met andere medewerkers, mogelijk interdepartementaal, via het team EV.

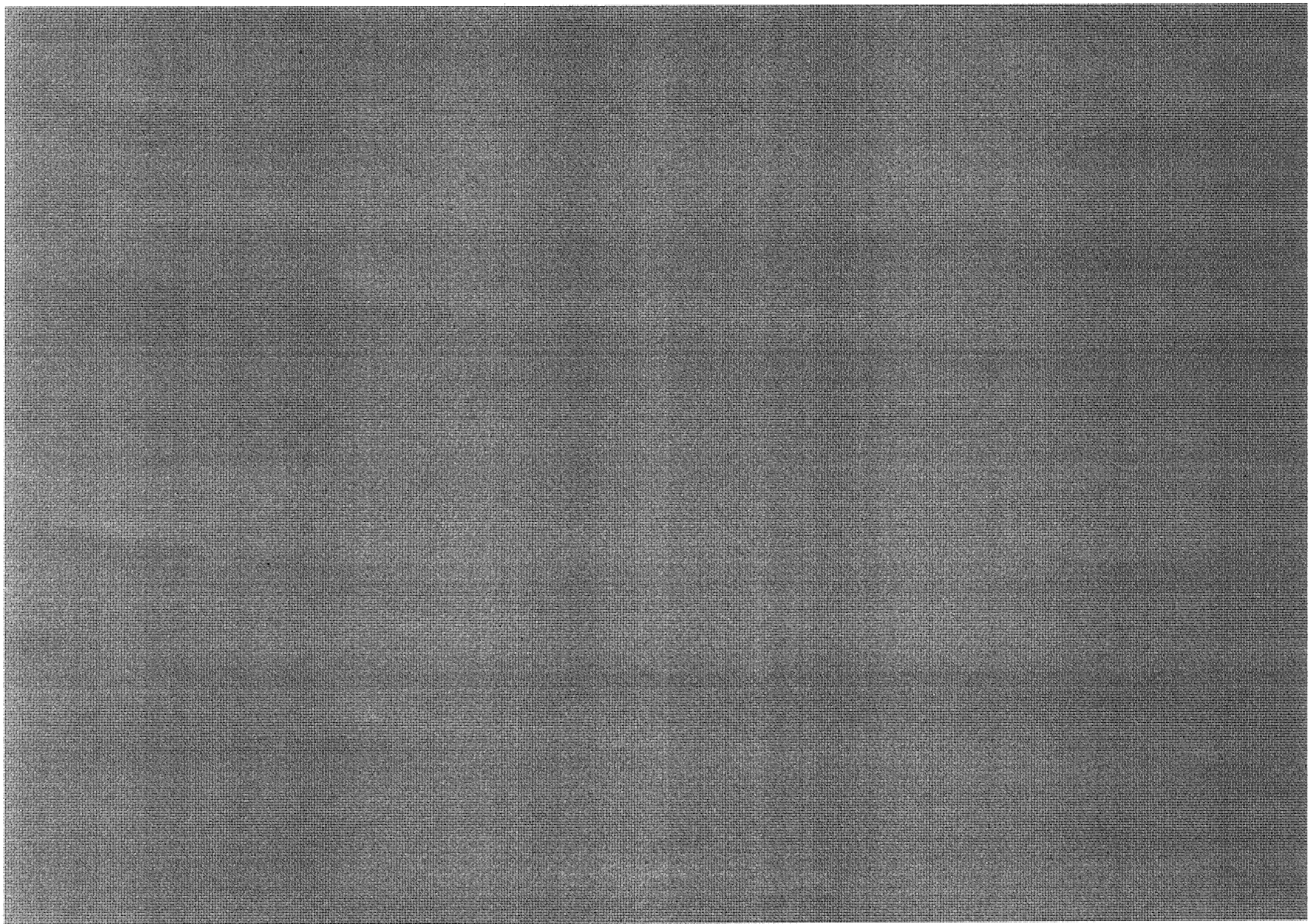


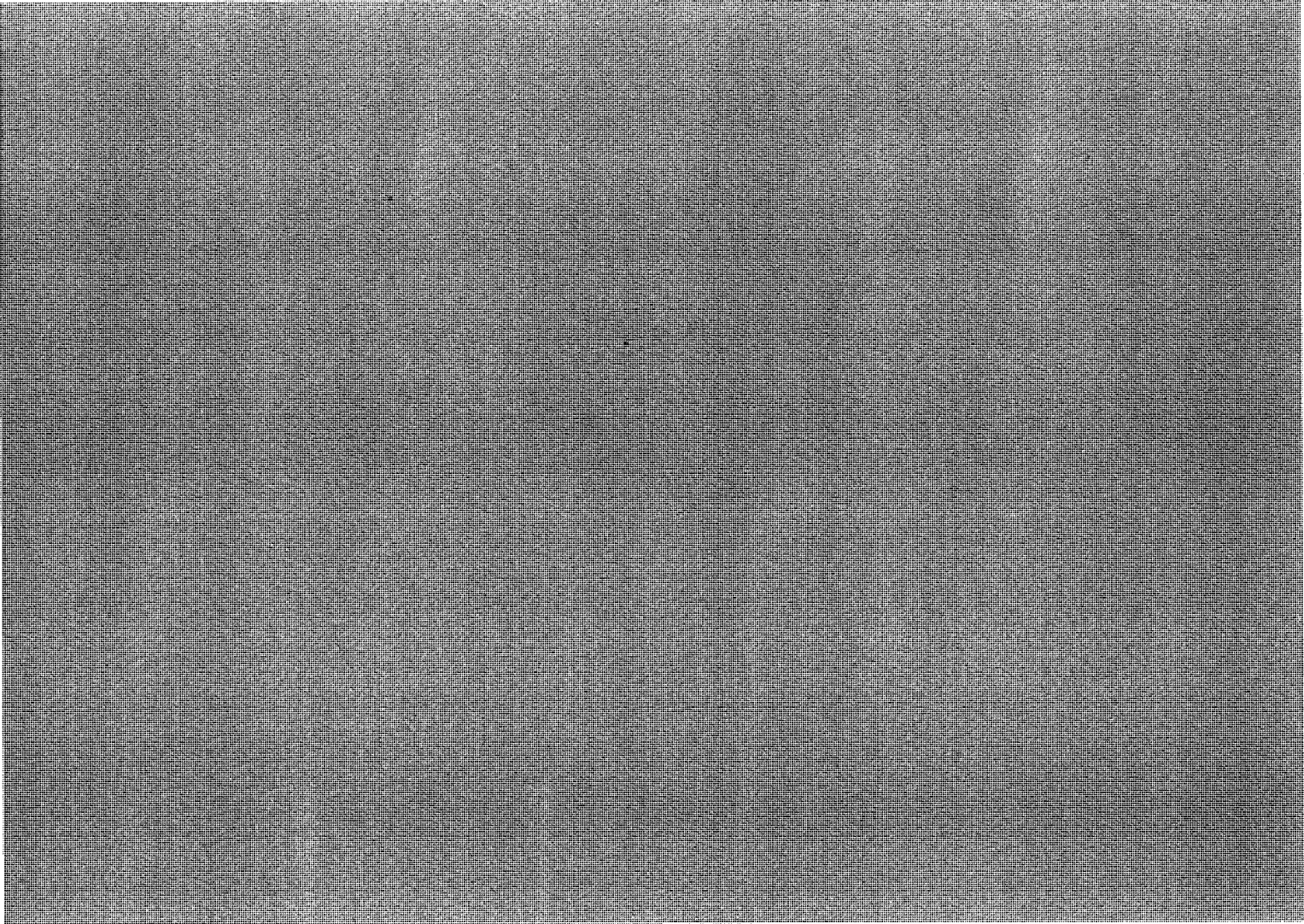
Dossierhouder, team EV en eventueel bewindspersoon en interdepartementale collega's

5 Besluit

Als u de toolkit volgens het stroomschema heeft gebruikt en bent aangekomen bij het besluit, zijn er verschillende vervolgstappen mogelijk. Het kan zijn dat er gebleken is dat er geen sprake is van een significant veiligheidsrisico. Dan is er geen noodzaak tot mitigerende maatregelen en kunt u de activiteit door laten gaan. Het kan ook zijn dat u samen met het team EV en andere experts de conclusie heeft getrokken dat er sprake zou kunnen zijn van een veiligheidsrisico. In

dat geval kunt u samen met deze collega's afspraken maken over welke vervolgstappen er ondernomen moeten worden en in welk gremium een besluit moet worden genomen. Ook als u uit de quickscan al denkt op te maken dat er geen veiligheidsrisico is maar u toch twijfels heeft, verzoeken we u contact op te nemen met EV@minezsk.nl. Dan kunnen we samen met u meer onderzoek doen naar de casus en de mogelijke handelingsopties.

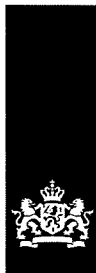




Dit is een uitgave van:

Ministerie van Economische Zaken en Klimaat
Postbus 20401 | 2500 EK Den Haag
T 070 379 8911

Maart 2021 | Publicatie-nr. 21400910



R1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK

Contactpersoon



5.1.2e

Datum

14 april 2021

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	22 april 2021, 16:00-17:30 uur
Vergaderplaats	3 ^e etage (tijdelijke ICCb/MCCb-zaal), Turfmarkt 147

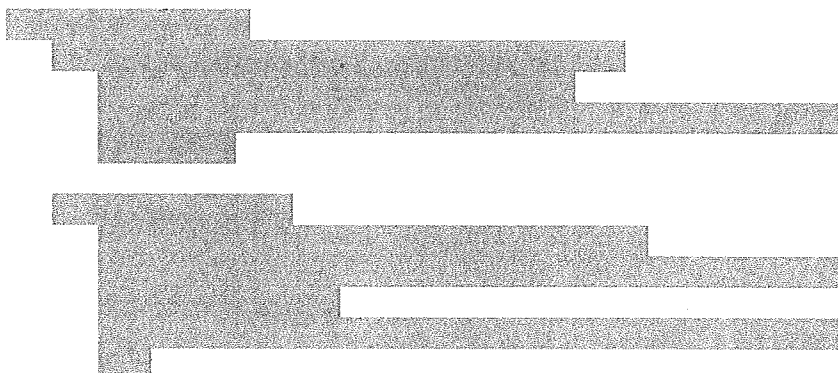
1. Opening en mededelingen

2. Verslag TFEV 18 maart 2021

Bijlage 1. Verslag TFEV 18032021

5.1.2i

3.



5.1.1b +
5.1.2a +
5.1.2i

5.1.1b +
5.1.2a +
5.1.2i

4. Expertise team veilige digitale overheid (BZK)

Bijlage 7. Nota EVDO update en gevraagde prioritering

5. Beschikkingen: communicatie leverancier (EZK)

Bijlage 8. Communicatiestrategie leveranciers bij beschikkingen
o.b.v. Besluit veiligheid en integriteit telecommunicatie

6. Internationaal/Europees

7. Parlementair

8. Rondvraag en sluiting

Dep. VERTROUWELIJK

Ministerie van Binnenlandse Zaken en
KoninkrijksrelatiesDEPARTEMENTAAL-VERTROUWELIJK
TER BESLUITVORMING

Aan

TFEV leden

DG00/CIO Rijk

Ministerie van Binnenlandse
Zaken en Koninkrijksrelaties

Contactpersoon

5.1.2e

Datum

12 april 2021

Kenmerk

Bijlage(n)

nota

EVDO update & gevraagde prioritering

Aanleiding

Na het TFEV besluit tot oprichting van Expertiseteam Veilige Digitale Overheid (EVDO) is gestart, met een Programma Overleg (EVDO-PO) en met een Technische Werkgroep (EVDO-TW), op basis van opgedane ervaringen in de Telecom sector. Wij vragen uw instemming met de hieronder voorgestelde prioritering van de werkzaamheden.

Kern

In de EVDO-TW wordt onderzocht hoe de technische risico's en te beschermen belangen in de voorliggende casussen kunnen worden gewogen. Het EVDO-PO zal dit met breder, beleidsperspectief verrijken in een voorstel aan het TFEV. Inhoudelijke analyses zijn nog niet voor de EVDO-PO beschikbaar. Gezien de opbouwfase waarin beide teams zich bevinden en de complexiteit van de vraag heeft dit enige tijd nodig. Op basis van input vanuit de NCTV wordt door het EVDO-PO de volgende prioritering voorgesteld:

1. Casus herziening Kaspersky
2. Casus [REDACTED] bij de Rijksoverheid en in de vitale sector
3. Casus ondersteuning NL burgers met [REDACTED]

5.1.2i

Communicatie en vervolgstap

[REDACTED] is schriftelijk geïnformeerd dat CIO Rijk hun verzoek voor [REDACTED] heeft overgenomen. Toch blijven zij de Belastingdienst benaderen over de status van hun vragen. Als voorbereiding op een escalatie, wordt een woordvoeringslijn voorbereid.

5.1.2i

Toelichting

De hoogste prioriteit krijgt de casus herziening Kaspersky vanwege een langere historie [REDACTED]. Onze acties zijn erop gericht om een inhoudelijk advies ter besluitvorming in de volgende TFEV van juni aan u voor te leggen.

5.1.2i

De daarop volgende prioriteit krijgt de casus van [REDACTED] bij de Rijksoverheid en in de vitale sector, vanwege het grote belang van de doelgroep. In de TFEV van juni ontvangt u tenminste een stand van zaken.

5.1.2i

DEPARTEMENTAAL-VERTROUWELIJK

Datum
12 april 2021
Kenmerk

De casus van het ondersteunen van NL burgers met [REDACTED]
[REDACTED], krijgt pas daarna aandacht omdat het marktaandeel van
[REDACTED] klein is geworden in het afgelopen jaar daar
deze minder aantrekkelijk zijn ([REDACTED]).

5.1.2i



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

5.1.2e

Datum

26 mei 2021

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	3 juni 2021, 13:00-14:30 uur
Vergaderplaats	Rolzaal (AZ)

1. Opening en mededelingen

2. Verslag TFEV 22 april 2021

Bijlage 1. Verslag TFEV 22042021

5.1.2i

3. [Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

5.1.1b + 5.1.2a +
5.1.2i

- [Redacted]
- [Redacted]

4. Internationaal/Europees

5. Parlementair

6. Rondvraag en sluiting



T1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

[REDACTED]

5.1.2e

[REDACTED]

Datum

6 september 2021

agenda

TFEV

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	15 september 2021, 14:00-16:00 uur
Vergaderplaats	AZ, Rolzaal

1. Opening en mededelingen

2. Verslag TFEV 3 juni 2021

Bijlage 1. Verslag TFEV 03062021 [REDACTED]

5.1.2i

[REDACTED]

[REDACTED]

[REDACTED]

5.1.1b + 5.1.2a
+ 5.1.2i

4. Structurele samenwerking Telecom

- a. Stand van zaken (NCTV) – mondelinge toelichting
- b. Kamerbrief n.a.v. Motie van Ginneken (EZK) – zie bijlage 3 en 3a
- c. Ministeriele regeling - De-rubricering kritieke gegevens (EZK) – zie bijlage 3b (nazending)

5. Expertiseteam Scan

Opdracht oprichting expertiseteam Scan – zie bijlage 4, 4a en 4b.
(nazending)

6. Expertiseteam Veilige Digitale Overheid

EVDO prioritering heroverweging Kaspersky (NCTV) – zie bijlage 5

[REDACTED]

[REDACTED]

[REDACTED]

5.1.2a

8. Internationaal/Europees

9. Parlementair

10. Rondvraag en sluiting

Dep.-VERTROUWELIJK

Datum
6 september 2021

Ministerie van Economische Zaken
en Klimaat

TER INFORMATIE

Aan
De leden van de TFEV

Directoraat-generaal
Bedrijfsleven & Innovatie

Auteur
[REDACTED] 5.1.2e
[REDACTED]
[REDACTED]

Datum
8 september 2021

Kenmerk
DGBI / 21230658

nota

Discussienotitie ten behoeve van o.a. [REDACTED]
[REDACTED]

5.1.1b + 5.1.2a + 5.1.2i

Kopie aan

Bijlage(n)

Aanleiding

Begin juni hebben de leden van de TFEV ingestemd met het opstellen van een korte notitie ten behoeve van een hoogambtelijke richtinggevende discussie over een aantal fundamentele vraagstukken over statelijke dreigingen, economische veiligheid en strategische autonomie. [REDACTED]
[REDACTED]

5.1.1b + 5.1.2a +
5.1.2i

Tegelijkertijd zijn ze projectoverschrijdend en ook relevant voor andere (lopende en toekomstige) trajecten binnen dit beleidsdomein.

Kernpunten

- Parallel aan de werkzaamheden voor [REDACTED] heeft een schrijfteam van BZ, EZK en NCTV in opdracht van het projectteam voorliggende discussienotitie opgesteld.
- De genoemde dilemma's komen voort uit [REDACTED], maar raken ook aan andere beleidstrajecten in het kader van EV, strategische autonomie en statelijke dreigingen.
- Doordat ze raken aan de kern van dit beleidsdomein, kan deze notitie gezien worden als het startpunt van een bredere discussie over de richting van de komende jaren – mede afhankelijk van een nieuw regeerakkoord.
- [REDACTED]
[REDACTED]
- Desgewenst kan deze discussie ook richting ACEV/MCEV-niveau worden gebracht.

5.1.1b + 5.1.2a +
5.1.2i

5.1.1b + 5.1.2a +
5.1.2i

5.1.1b + 5.1.2a +
5.1.2i

TFEV discussienotitie

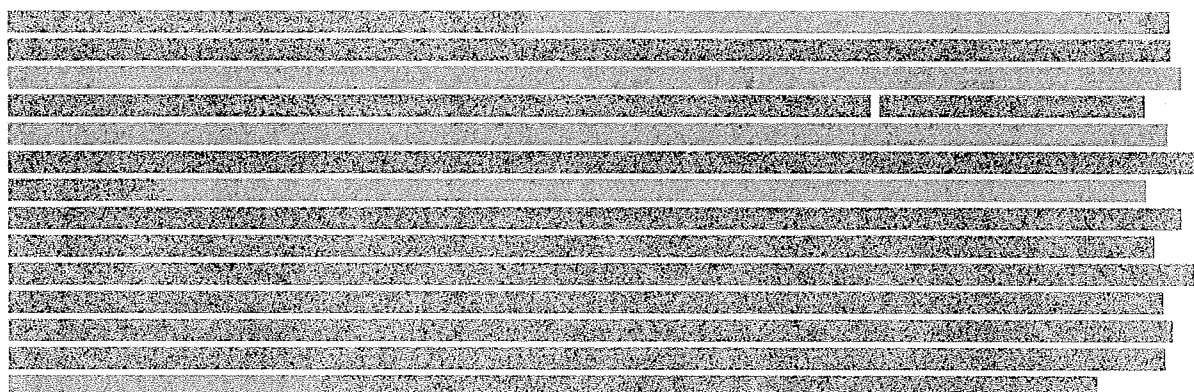
Doel discussienotitie: Richting de TFEV-leden duidelijk maken tegen welke trajectdoorsnijdende dilemma's wij als beleidsmakers aanlopen en waarom we antwoorden op deze vragen nodig hebben.

De Nederlandse samenleving en economie zijn hoogontwikkeld, innovatief en sterk internationaal verbonden. Deze factoren vormen de basis van de Nederlandse welvaart. Sinds enige tijd veroorzaken verschuivingen in de wereldorde ook een verschuiving van economische machtsverhoudingen en wordt Nederland geconfronteerd met vormen van "economic statecraft", die effect hebben op het dreigingsbeeld: van cybercriminaliteit, (digitale) spionage, kwalijke handelspraktijken, ongewenste buitenlandse overnames en investeringen, inmenging tot aan sabotage. In toenemende mate zijn we ons als overheid ervan bewust dat het handelen van andere overheden in ons eigen land kan leiden tot een aantasting van Nederlandse belangen, zoals de verstoring van vitale processen, aantasting van de integriteit en exclusiviteit van informatie en/of het ontstaan van ongewenste strategische afhankelijkheden die ons speelbal kunnen maken van het geopolitiek spel van derde landen.

Niet voor niets zijn er de afgelopen jaren interdepartementaal diverse beleidsinitiatieven gestart om onszelf weerbaarder te maken tegen deze risico's, veelal te vangen onder de term statelijke dreigingen, economische veiligheid en strategische autonomie. Over de gehele linie – zowel in Nederland als EU – wordt gewerkt aan het vergroten van onze weerbaarheid en ons geopolitiek handelingsvermogen: van de ontwikkeling van wetgeving om ongewenste investeringen tegen te gaan tot aan de uitrol van beleid op het gebied van kennisveiligheid, de instrumenten die worden ontwikkeld om aandacht voor veiligheidsrisico's onderdeel te laten maken van inkoop en aanbestedingen, het identificeren en adresseren van kwetsbare strategische afhankelijkheden tot aan het versterken van onze kennis- en innovatiepositie.

In eerste instantie lag het zwaartepunt op de ontwikkeling van onze defensieve maatregelen. Daarnaast is in de laatste twee jaar is het besef steeds verder ingedaald dat onze veiligheids- en geopolitieke positie op de lange termijn vooral door onze economische en technologische capaciteiten wordt bepaald. Daarmee is er zowel breder in Europa als in Nederland een hernieuwde interesse in de rol van bijvoorbeeld innovatie- en industriebeleid voor onze veiligheid.

Kortgezegd is er de afgelopen jaren enorm veel gebeurd en het denken staat verre van stil. De structuren zijn gebouwd, de departementen zijn aangesloten, informatie wordt uitgewisseld en het bewustzijn m.b.t. nationale veiligheid is enorm toegenomen. Voorafgaand aan een nieuw kabinet is een goed moment om de balans op te maken. Doen we nog de juiste dingen, waarom doen we ze en wat is de richting die we op willen gaan?



5.1.1b +

5.1.2a +

5.1.2i

5.2.1

Technologisch leiderschap

De laatste jaren is het besef gegroeid dat de geopolitieke- en veiligheidspositie op lange termijn in grote mate bepaald worden door de economische en technologische capaciteiten van een land of machtsblok. Eén van de meest vergaande scenario's is dat bepaalde landen op middellange termijn zowel economisch als technologisch een koploperspositie zullen verkrijgen en deze positie zullen aanwenden om de op regels gebaseerde internationale orde te ondermijnen. Dit kan schade op leveren voor de borging onze publieke belangen, waaronder onze (nationale) veiligheid. De beste verzekering tegen toekomstige veiligheidsrisico's lijkt daardoor een inzet op het behoud van technologisch leiderschap.

Dilemma 1 In hoeverre is het behoud van (democratisch) technologisch leiderschap de doelstelling achter ons veiligheidsbeleid? Hoe ver willen en kunnen we gaan om technologisch leiderschap te behouden?

Dilemma 2 *Hoe en met wie* behouden we technologisch leiderschap? Is de overheid in staat om te identificeren op *welke terreinen* een technologische voorsprong wenselijk (en mogelijk) is?

Kennisoverdracht

De uitwisseling van kennis en informatie is een belangrijke aanjager van innovatie en vooruitgang en is daarmee belangrijk voor het functioneren van onze samenleving en economie. Tegelijkertijd kan een overdracht van kennis en technologie in sommige gevallen ook leiden tot een erosie van een technologische leiderschapspositie. Een belangrijke vraag is wanneer kennisoverdracht ongewenst is. De huidige insteek (waarop beleid is gebaseerd) is : "Open waar mogelijk, gesloten/beschermd waar nodig", maar wanneer is het nodig? In sommige gevallen is het duidelijk dat verspreiding van kennis en informatie direct onze veiligheidsbelangen schaadt of kan schaden, zoals waar het gaat om militaire toepassingen die tegen ons kunnen worden ingezet. In andere situaties is het minder duidelijk, omdat die veiligheidsbelangen pas op langere termijn kunnen worden geschaad door bijvoorbeeld een verschuiving van technologisch leiderschap op het wereldtoneel.

5.1.2i

Dilemma 3 Wanneer is de overdracht van kennis via legitieme kanalen ongewenst?

Bereidheid treffen maatregelen strijdig met fundamentele waarden

5.1.2i

Dilemma 4 In welke gevallen wijken we af van kernwaarden zoals economische/wetenschappelijke openheid of vrijheid van vereniging? Hoe wijken we hier van af en hoe ver wensen we daarin te gaan?

Verantwoordelijkheidsverdeling overheid en bedrijfsleven

Voor het verkrijgen van kennis en technologie schromen statelijke actoren niet om een breed palet aan acties in te zetten. Variërend van de inzet van samenwerkingsverbanden, economische instrumenten, talent werving tot aan spionageactiviteiten. Tot op zekere hoogte hebben bedrijven zelf een prikkel en verantwoordelijkheid om zich te beschermen tegen de overdracht van kennis en informatie die hun eigen bedrijfsvoering schaadt. Tegelijkertijd ligt er ook een overheidsrol om illegitieme vormen van kennisoverdracht tegen te gaan en is het de vraag of bedrijven opgewassen zijn tegen staatsgedreven spionage. In bijvoorbeeld de telecomsector wordt een structurele aanpak opgezet waarbinnen telecomoperators en overheid informatie uitwisselen over ontwikkelingen in dreigingen en techniek zodat snel maatregelen genomen kunnen worden waar ontwikkelingen dat nodig maken. Een soortgelijke aanpak wordt ook voorzien voor andere vitale sectoren. De overheid is hierbij eindverantwoordelijk voor de belangenafweging bij het nemen van beleidsmaatregelen. Ook hier speelt echter de vraag in welke mate de te treffen maatregelen vanuit de bedrijven zelf of de overheid dienen te komen.

Dilemma 5 Wat is de verantwoordelijkheidsverdeling tussen de Nederlandse overheid en Nederlandse bedrijven/kennisinstellingen in het tegengaan van ongewenste kennis- en technologieoverdracht?



Aan
Leden van de Taskforce Economische Veiligheid

Directoraat-generaal
Bedrijfsleven & Innovatie

Behandeld door
5.1.2e

Datum
10 september 2021

Kenmerk
DGBI / 21232746

Kopie aan

Bijlage(n)
2

memo

Regeling veiligheid en integriteit telecom –
De-rubricering kritieke gegevens

Gevraagd Besluit

EZK is bezig om de ministeriële regeling veiligheid en integriteit af te ronden. Hierin zijn de technische maatregelen opgenomen die de mobiele netwerk-aanbieders moeten treffen teneinde de veiligheid en integriteit van hun mobiele netwerken te verhogen.

Dit conform eerdere besluitvorming in de Taskforce Economische Veiligheid.

5.1.2i

De kritieke gegevens zijn als onderdeel van het voor de TFEV gemaakte rapport STG-C geclassificeerd (16 mei 2019). Deze rubricering leidt er echter toe dat het in de praktijk onuitvoerbaar is voor de mobiele netwerkoperators (MNO's) om invulling te geven aan de uitwerking van deze maatregel. Om de balans te vinden tussen uitvoerbaarheid en vertrouwelijkheid wordt instemming gevraagd de lijst met kritieke gegevens te de-rubriceren naar dep-v (het voornoemde rapport zelf zal STG-C blijven). Dit overeenkomstig wat eerder is gedaan met de lijst van kritieke onderdelen, welke als dep-v met de beschikkingen is meegestuurd.

5.1.1b

Toelichting

- Om dit mogelijk te maken en de maatregel voor de operators goed uitvoerbaar te maken is het voorstel van EZK om dat te doen overeenkomstig de procedure die de TFEV in 2020 heeft gekozen bij het delen van de kritieke onderdelen in het kader van de beschikkingen.
- Een de-rubricering naar dep-v maakt het voor EZK mogelijk richting de MNO's te communiceren dat zij de lijst met kritieke gegevens moeten behandelen volgens het bij hen bekende TLP (Traffic Light Protocol¹) AMBER.
- Dat betekent dat de kritieke gegevens alleen worden gedeeld met personen die ten behoeve van de MNO () nodig zijn voor

5.1.2i

5.1.2i

¹ <https://www.first.org/tlp/docs/tlp-v1-nl.pdf>

het voorbereiden van en uitvoering geven aan de eisen uit de regeling en dan alleen die kritieke gegevens die zij nodig hebben (alleen delen op "need to know" basis). Deze personen kunnen ook externen zijn, indien deze noodzakelijk zijn om voor het bedrijf uitvoering te geven aan de (voorbereiding van de) implementatie van voornoemde beheersmaatregel. Dit is overeenkomstig de werkwijze zoals eerder gehanteerd met de lijst van kritieke onderdelen in het kader van de beschikkingen.

- [REDACTED]
[REDACTED]
[REDACTED]

5.1.2i



TER BESLUITVORMING
DEPARTEMENTAAL-VERTROUWELIJK

Aan
TFEV

Directoraat-Generaal
Douane
Directie Bedrijfsvoering
Inlichtingen

5.1.2e

www.minfin.nl

Datum
9 september 2021

Van
Douane 5.1.2e
NCTV

notitie

Opdracht oprichting expertiseteam Scan

Aanleiding

Begin 2021 zijn Kamervragen gesteld over mogelijke spionage via scanners van het Chinese bedrijf Nuctech bij de Douane. Zoals aangekondigd in de beantwoording van de Kamervragen vindt er een onderzoek plaats dat inzicht moet geven in mogelijke risico's voor de nationale veiligheid die kunnen ontstaan bij het gebruik van buitenlandse toeleveranciers door de Douane.

Gevraagd besluit

De TFEV wordt gevraagd in te stemmen met de volgende besluiten:

- De oprichting van het expertiseteam Scan, onder voorzitterschap Douane en NCTV, met deelname van BZ, BHOS, Defensie, EZK, Financiën, I&W, AIVD, MIVD en NCSC;
- Het uitvoeren van een onderzoek door het expertiseteam naar risico's voor de nationale veiligheid in verband met het gebruik van buitenlandse toeleveranciers (in het bijzonder [REDACTED])

5.1.2i

Toelichting

In de beantwoording van de genoemde Kamervragen is aangegeven dat de Douane een externe audit laat uitvoeren naar de informatiebeveiliging van de scan- en detectieprocessen. De resultaten hiervan worden in september opgeleverd.

Daarnaast is aangekondigd dat er een "aanvullend onderzoek" zal plaatsvinden, waarbij alle relevante overheidspartijen aansluiten. Dit onderzoek moet inzicht geven of, en zo ja welke, risico's voor de nationale veiligheid er mogelijk ontstaan door de inkoop en inzet van apparatuur van buitenlandse toeleveranciers (waaronder [REDACTED]).

5.1.2i

In het onderzoek worden de nationale veiligheidsrisico's voor de vitale infrastructuur voor de scan- en detectieprocessen van de Douane in kaart gebracht, in relatie tot de te beschermen belangen en de dreiging. Daaropvolgend wordt gezien welke mitigerende maatregelen nodig zijn om eventueel geïdentificeerde risico's voor de nationale veiligheid beheersbaar te maken. De uitkomsten van de externe audit worden in het onderzoek meegenomen. Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij (digitale) producten worden de overwegingen gehanteerd die zowel bij c2000 als bij de veiligheid van de telecomnetwerken zijn gebruikt.

Voor de uitvoering van dit onderzoek wordt geadviseerd een expertiseteam op te richten, dat gebruik maakt van de methodiek en *governance*-structuur die ook wordt toegepast binnen de structurele samenwerking telecom. Het expertiseteam Scan wordt opgericht voor de duur van het genoemde onderzoek.

Het expertiseteam Scan zal bestaan uit twee onderdelen:

Technische werkgroep - onder voorzitterschap en secretariaat Douane.

- De technische werkgroep zal zich richten op het uitvoeren van het onderzoek.
- De werkgroep levert hiertoe een technisch rapport op, met daarin:
 1. Risicoanalyse op basis *belangen, dreigingen, weerbaarheid*
 2. Een overzicht van eventuele weerbaarheid-verhogende maatregelen en de beveiligingswaarde die daarvan uitgaat.
- Deelname vanuit NCTV, AIVD, NCSC (I&W agendalid). [REDACTED] is betrokken als procesbegeleider.

5.1.2i

Programmaoverleg - onder voorzitterschap en secretariaat NCTV.

- Het programmaoverleg zal het technisch rapport van de werkgroep duiden (brede belangenafweging) en een beleidsadvies opstellen voor de TFEV.
- Naast het onderzoek dat betrekking heeft op de Douane zal het programmaoverleg ook benut worden om zicht te houden op overige ontwikkelingen/casuïstiek rondom [REDACTED]
- Deelname vanuit BZ, BHOS, Defensie, EZK, Financiën/Douane, I&W, AIVD, MIVD en NCSC.

5.1.2i

De **TFEV** dient als stuurgroep voor het expertiseteam Scan. [REDACTED] Douane sluit voor dit agendapunt incidenteel aan.

5.1.2e

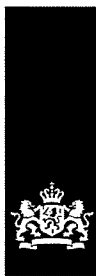
Planning

Uitvoering van het onderzoek start in september 2021. De verwachting van [REDACTED] is dat het onderzoek 6 tot 8 maanden zal duren. Gedurende het onderzoek zal de TFEV waar nodig geïnformeerd worden over de voortgang. Het rapport zal met een beleidsadvies van het programmaoverleg worden geagendeerd in de TFEV.

5.1.2i

Bijlagen

- Beantwoording Kamervragen 19-04-2021



U1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep.-VERTROUWELIJK

Contactpersoon

5.1.2e

Datum

9 november 2021

agenda

TFEV

Omschrijving	Taskforce Economische Veiligheid
Vergaderdatum en -tijd	17 november 2021, 16:00-17:30 uur
Vergaderplaats	AZ, Rolzaal

1. Opening en mededelingen

2. Verslag TFEV 15 september 2021

Bijlage 1. Verslag TFEV 15092021

5.1.2i

3. Expertiseteam Veilige Digitale Overheid

5.1.2i

a. Casus 1: Kaspersky

Bijlage 2. Oplegnota EVDO

5.1.2i

Bijlage 3. Advies heroverweging Kaspersky antivirus

5.1.2i

Achtergrondstukken:

Bijlage 3A. Bedrijf Kaspersky

5.1.2i

Bijlage 3B. Maatregelen andere landen

5.1.2i

Bijlage 3C. Duiding TBB's NV

5.1.2i

Bijlage 3D. Rapport Technische Werkgroep EVDO

5.1.2i

Bijlage 3E. Advies Landsadvocaat (*nazending via reguliere lijn*)

b. Casus 2: Verbreden scope

Bijlage 4. Verbreden Scope EVDO voor mobiele OS

4. Internationaal/Europees

5. Parlementair

6. Rondvraag en sluiting

Dep.-VERTROUWELIJK

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

DEPARTEMENTAAL-VERTROUWELIJK

TER BESLUITVORMING

Datum
4 oktober 2021

Onze referentie

Opgesteld door 5.1.2e
DG00 CIO Rijk

Samengewerkt met

Bijlage(n)
0Aan
TFEVVan
EVDOAan
VanTFEV
EVDO

nota

Verbreden scope EVDO voor mobiele OS

Aanleiding

Recente gesprekken binnen het EVDO en gestelde Kamervragen over het gebruik van mobiele OS.

Geadviseerd besluit

Akkoord gaan met de verbreding van de scope van het te behandelen vraagstuk omtrent het gebruik van bepaalde mobiele OS binnen overheidscontext en het beschikbaar stellen van overheidsapps in verschillende appstores naar een landen- en merkenneutrale aanpak.

Toelichting

In het TFEV van 17 februari is besloten dat het EVDO besluitvorming rond de casus Kaspersky en casus [REDACTED] zou voorbereiden. De vraagstukken gaan in de kern over de vraag welke maatregelen de (rijks)overheid moet treffen om zichzelf en zijn dienstverlening te beschermen op digitaal vlak. Om hierover onderbouwd besluiten te kunnen nemen dienen de te beschermen belangen, dreigingen en mogelijke weerbaarheidsverhogende maatregelen in kaart te worden gebracht.

5.1.2i

Op basis van input vanuit de NCTV werd door het EVDO-PO de volgende prioritering voorgesteld:

1. Casus herziening Kaspersky
2. Casus gebruik [REDACTED] bij de Rijksoverheid en in de vitale sector
3. Casus [REDACTED]

5.1.2i

5.1.2i

5.1.2i

Naar aanleiding hiervan heeft:

- 1) De Chief Technology Officer raad (CTO Raad), onder voorzitterschap van CIO Rijk, gevraagd of er richtlijnen zijn voor gebruik/aanschaf van [REDACTED] voor de rijksoverheid.

5.1.2i

- 2) [REDACTED] Vanuit CIO Rijk is

5.1.2i

inmiddels een ontvangstbevestiging gestuurd richting [REDACTED] waarin is aangegeven dat er nog een inhoudelijk antwoord zal komen.

Datum
4 oktober 2021

5.1.2i

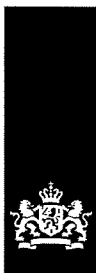
Onze referentie

Inmiddels zijn door de VVD fractie Kamervragen gesteld over het gebruik van Xiaomi telefoons.¹ [REDACTED]

5.1.2i

¹

<https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2021Z16201&did=2021D34921>



V1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Contactpersoon

[Redacted]

[Redacted]

5.1.2e

Datum

9 december 2021

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	16 december 2021, 13:30-15:00 uur
Vergaderplaats	AZ (Rolzaal)

1. Opening en mededelingen

2. Verslag TFEV 17 november 2021

Bijlage 1. Verslag TFEV 17112021 [Redacted]

5.1.2i

3. [Redacted]

[Redacted]
[Redacted]
[Redacted]

5.1.1b

+

5.1.2a

+ 5.1.2i

b. [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

5.1.1b +

5.1.2a +

5.1.2i

4. Richtinggevende principes technologisch leiderschap (EZK)

Bijlage 5. Nota technologisch leiderschap

Bijlage 5a. Technologisch leiderschap

Bijlage 5b. Stellingen over technologisch leiderschap

5. Formatie en begroting 23-27

6. Internationaal/Europees

7. Parlementair

8. Rondvraag en sluiting

Datum
9 december 2021

Prioriteiten fiches cybersecurity, economische veiligheid en vitaal**Aanleiding**

In de ACEV van januari is er gesproken over prioriteren binnen de fiches voor het geval maar een deel van het gevraagde bedrag wordt toegekend. Hierbij heeft de ACEV aangegeven liever niet te willen 'kaasschaven' maar gezamenlijk te kijken naar wat de prioriteiten zijn. In deze nota wordt een voorstel gedaan voor een gezamenlijke prioritering per fiche.

Kernpunten

In de fiches en de bijbehorende financiële onderbouwing zit weinig lucht, alles in de fiches is hoogst noodzakelijk. Schrappen van specifieke elementen hierin zal daarmee nadelige consequenties hebben voor de geïntegreerde inzet die nodig is om de nationale veiligheid te waarborgen. Het volledige pakket is dan ook de inzet voor de formatietafel. De prioritering is in beginsel bedoeld om snel gericht te kunnen antwoorden bij vragen van de formatietafel.

Onderwerp: Prioriteren formatiefiche cybersecurity

Namens: Directeuren Overleg Cyber Security (DOCS)

Werkwijze

De cyberclaim is een geïntegreerd pakket met een brede focus en is opgesteld vanuit verschillende invalshoeken (i.e. een veilige digitale overheid, digitale slagkracht, internationale samenwerking) omdat digitalisering en digitale veiligheid zo'n breed thema is. Het is inmiddels van dagelijks belang voor de burger, het MKB, de vitale infrastructuur, onderwijs- en wetenschappelijk instellingen en zorginstellingen en de overheid.

Eventuele vragen vanuit de formatietafel kunnen daarmee aan verschillende kanten van cybersecurity raken, en kunnen niet met één standaard antwoord worden beantwoord. Ook de hoogte van het eventuele bedrag dat aan het onderwerp cyber wordt toegekend is uiteraard niet vooraf duidelijk. Daarom wordt er geen scenario voorgesteld, maar zijn in plaats daarvan gezamenlijk een prioritaire onderwerpen vastgesteld.

Prioritaire onderwerpen

- Versterken weerbaarheid vitale veiligheidsbelangen (incl. toezicht) (t.b.v. AIVD, MIVD, NCSC, NCTV, EZK, IenW, BZK)¹
- Versterken informatiebeveiligingsbeleid en weerbaarheid overheid (t.b.v. BZK, AIVD, DEF)
- Versterken van informatiedeling en verdere opbouw van het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (informatie-uitwisseling, stimuleren vorming OKTT's en CERTs, versterking sectorale expertise (t.b.v. VWS, OCW, EZK/DTC, NCSC)
- Versterken informatie en inlichtingenpositie (t.b.v. AIVD, MIVD, NCSC, NP)
- Digitale slagkracht (t.b.v. DEF, NCSC)
- Nationale cryptostrategie (t.b.v. BZK, AIVD)
- Veilige hard- en software (t.b.v. EZK, AIVD)
- Kennis en innovatie (t.b.v. EZK, JenV, VWS, OCW, BZ, DEF)
- Weerbaarheid burger (campagnefonds t.b.v. EZK, JenV, BZK)
- (Diplomatieke) respons op kwaadaardige cyberoperaties van statelijke actoren (t.b.v. BZ, DEF, AIVD, MIVD)
- Oefenen en testen (t.b.v. NCSC, EZK, IenW, DEF)

¹ Dit thema staat niet in het fiche cybersecurity maar gezien het belang van digitale weerbaarheid van de vitale aanbieders voor het cybersecuritystelsel hechten de betrokken partijen eraan om het hier op te nemen.

Onderwerp: Prioriteren formatiefiche economische veiligheid

Namens: Voorbereidingsgroep TFEV

Werkwijze

- Voor het EV-fiche is interdepartementaal geprioriteerd binnen de defensieve maatregelen.
- Er is hierbij gewerkt aan een 40% en 10% scenario.
- Over het 10% scenario is overeenstemming, over het 40% bestaan verschillende inzichten. Voor beide scenario's geldt dat de pakketten niet afdoende zijn om onze economische veiligheid te beschermen. Ook wordt met de pakketten niet voldaan aan de toezeggingen van de Kamer.
- Voorstel is om het noodzakelijke scenario (40%) niet vast te stellen maar als uitgangspunt te zien. Afhankelijk van het toegekende geld en de vragen en wensen vanuit de formatietafel kan worden bepaald op welke thema's wordt ingezet (en welke maatregelen daarbinnen). Hierbij zullen maatregelen worden getoetst middels de toekenningscriteria. De uitwerking hiervan heeft al deels plaatsgevonden en wordt de komende weken verder uitgewerkt.
- Voor het offensieve deel van de claim ('Versterken van de eigen kracht en soevereiniteit door middel van een offensief industriebeleid') is geen prioritering gemaakt, onder meer omdat de gevraagde bedragen al een minimum betreffen – zeker in vergelijking met andere Europese landen. Ook valt door verder te korten het te bereiken effect weg om daadwerkelijk een bijdrage te kunnen leveren aan het versterken van onze eigen slagkracht en strategische autonomie.

10%-scenario:

- Voor het 10% scenario zal worden ingezet op het versterken van de kennisbasis van de overheid m.b.t. sensitieve technologieën en afhankelijkheden en bijbehorende inzet van de inlichtingen en veiligheidsdiensten op dit thema. Belangrijke motivatie voor dit pakket is dat er geen maatregelen genomen kunnen worden als niet duidelijk is wat we willen beschermen op het gebied van sensitieve technologieën.
- Dit betreft nadrukkelijk alleen het versterken van de kennisbasis: ontwikkeling en implementatie van maatregelen valt buiten dit scenario.

40% scenario:

- Bij het 40% scenario zijn er twee voorlopige opties uitgewerkt. Beide opties hebben hetzelfde doel: beschikken over benodigde kennis en adequate instrumenten om overdracht van kennis, technologie en/of zeggenschap tegen te gaan.
- Consensus in de beide opties is er rondom inzet op:
 - het versterken van de kennisbasis van de overheid op sensitieve technologieën en afhankelijkheden;
 - het tegengaan van ongewenste kennis en technologieoverdracht (exportcontrole en kennisveiligheid);
 - veilige inkoop en aanbesteding Rijksoverheid;
 - gedeeltelijke inzet van de inlichtingen- en veiligheidsdiensten.

Deze vier bouwstenen vormen de basis van het 40% scenario.

- Belangrijke verschillen in beide opties zijn:
 - Optie 1 zet naast de genoemde bouwstenen in op strafbaarstelling spionage en het volledige pakket m.b.t. veilige inkoop en aanbesteding Rijksoverheid (ABRO + bewustwording en instrumentarium). Optie 1 maakt de keuze om niet in te zetten op internationale samenwerkingen ongewenste zeggenschap. Optie 1 gaat uit van een intensivering van 23,5 miljoen in 2022, oplopend tot 46,5 miljoen structureel.
 - Optie 2 zet naast de genoemde bouwstenen in op ongewenste zeggenschap, internationale samenwerking en een gedeelte van het pakket m.b.t. veilige inkoop en aanbesteding Rijksoverheid (bewustwording en instrumentarium). Optie 2 maakt de keuze om niet in te zetten op de ABRO en strafbaarstelling spionage. Optie 2 gaat uit van een intensivering van 29,3 miljoen in 2022, oplopend tot 39,9 miljoen structureel (incl. gedeeltelijke inzet inlichtingen- en veiligheidsdiensten, anders resp. 25 miljoen in 2022 en 23 miljoen structureel).

Onderwerp: Prioriteren formatiefiche versterken weerbaarheid vitale veiligheidsbelangen

Namens: Werkgroep fiche vitale belangen

Scenario's fiche Versterken weerbaarheid vitale veiligheidsbelangen

Maatregel / Scenario	10%	40%	100%
1. Oprichting unit vitale belangen	Geen unit	Oprichting minimale unit, beperkte ondersteuning	Oprichting unit conform fiche
2. Oprichting expertise teams op specifieke vitale belangen	1 team	2 teams	3-5 teams
3. Beleidsopvolging en adaptief toezicht	Specifieke beleidsopvolging en toezicht voor dit team.	Specifieke beleidsopvolging en toezicht voor deze teams	Beleidsopvolging en adaptief toezicht conform fiche.

Kernpunten

- In het 10% en 40% scenario is het niet mogelijk om te voldoen aan moties uit de Kamer (o.a. versterken aanpak vitaal en verbreden werkwijze telecom naar andere sectoren)
- Het is geen optie om geen opvolging te geven aan gesignaleerde risico's. In de praktijk zien we dat actualiteit en casuïstiek aanleiding geeft voor de oprichting van meerdere expertiseteams.
- Met minder middelen ligt het voor de hand om fors te prioriteren, wat er concreet toe leidt dat er minder expertise teams worden opgericht. Het is niet haalbaar om met minder middelen hetzelfde aantal teams (+ bijbehorende ondersteuning en opvolging) te draaien. Uitzondering hierop is het expertiseteam watermanagement, dat ook in een 'light'-versie kan bestaan.

Toelichting

- De maatregelen in het fiche vitaal worden door iedereen als een hoge (zo niet hoogste) prioriteit gezien omdat een verstoring in vitale processen tot grote maatschappelijke ontwrichting en grote economische gevolgen kan leiden.
- Het is belangrijk dat de drie maatregelen in het fiche in samenhang worden gezien. Hoe meer expertise teams, hoe meer behoefte aan een unit, beleidsopvolging en toezicht nodig is.
- Dit schema geeft een versimpelde versie van de scenario's. Specifieke submaatregelen (zoals CSIRT) komen hierin omwille van de helderheid niet in terug.
- Deze maatregelen zijn echter wel van belang en zullen bij uiteindelijke verdeling van eventuele middelen wel meegenomen moeten worden mede omdat de inzet voor bijvoorbeeld CSIRT/DSP voortvloeit uit de verplichtingen vanuit de NIS-richtlijn.

Nota agendapunt Technologisch leiderschap

- Deze notities zijn het vervolg op een discussiestuk over technologisch leiderschap in de TFEV van september jl. Vanuit [REDACTED] ontstond namelijk de behoefte aan richtinggevende principes o.a. voor technologisch leiderschap. 5.1.1b + 5.1.2a + 5.1.2i
- EZK, BZ en de NCTV zijn gezamenlijk tot dit stuk gekomen met het doel om de verhouding te duiden tussen technologie, economie en veiligheid in een geopolitieke context.
- De notities laten zien waar verschillende belangen met elkaar schuren en werpt stellingen op waar nog geen consensus over is. Bijlage 1 geeft een conceptueel kader, bijlage 2 geeft richtinggevende stellingen.
- Het huidige stuk moet worden gezien als een tussenproduct en is bedoeld om het gesprek te voeren over deze dilemma's op basis van een aantal – deels prikkelende – stellingen die hieronder zijn geformuleerd. Insteek is om op basis van deze discussie verder te werken aan richtinggevende principes die helpen bij het bepalen van de overheidsinzet op technologisch leiderschap.
- Het blijft lastig om algemeenheden te formuleren op deze complexe thematiek. Veel is krachtenveld- en casusafhankelijkheid. Principes kunnen dus niet meer dan richting geven en zullen geen pasklaar antwoord verschaffen.
- Belangrijk is dat steeds wordt gekeken naar de gehele keten van de desbetreffende technologie, de technologische positie van Nederland, de EU, bondgenoten en andere spelers daarin en de belangen die spelen.
- **Bespreekpunt:**
 - Kan de TFEV zich vinden in de beleidsanalyse over technologisch leiderschap? Welke gedachten en aandachtspunten heeft de TFEV bij deze werkversie die we mee kunnen nemen bij de verdere uitwerking?

Een conceptueel kader voor technologisch leiderschap

Opmerking vooraf: voor het lezen van deze notitie kan het helpen eerst kennis te nemen van de terminologie op de laatste pagina.

Noodzaak voor richtinggevende stellingen/vragen

Economische belangen enerzijds en nationale veiligheidsbelangen anderzijds kunnen leiden tot verschillende perspectieven. Economische productiviteit en welvaart worden in internationale context gedreven door comparatieve voordelen en de voordelen van internationale vrijhandel. Internationale economische betrekkingen kennen dan ook een 'positieve som benadering': door internationaal economisch verkeer gaan alle deelnemers er op vooruit. Veiligheid, in ieder geval daar waar het geopolitiek en nationale veiligheid betreft, wordt daarentegen gemeten aan de hand van het vermogen van een partij om macht uit te oefenen. Dit wordt niet zozeer bepaald door hoe dit vermogen in absolute termen toe- of afneemt, maar door hoe het zich verhoudt tot de toe- of afname van het vermogen om macht uit te oefenen van tegenstanders of concurrenten.

In de huidige verschuivende geopolitieke orde worden Nederland en de EU geconfronteerd met nieuwe strategische vragen. Economische omvang en technologische positie waren altijd onderdeel van geopolitieke macht. Nederland en de EU worden echter in toenemende mate geconfronteerd met geopolitieke concurrentie tussen staten. Deze nieuwe verhoudingen brengen risico's voor de borging van Nederlandse en Europese publieke belangen met zich mee, waaronder de nationale veiligheid. Openheid en internationale samenwerking blijven de vertrekpunten voor zowel Nederland als de EU, maar risico's voor de borging van publieke belangen kunnen aanleiding geven tot nieuwe vormen van overheidsingrijpen.

In het Nederlandse beleid is economische openheid het vertrekpunt. Bij economische veiligheid is ons uitgangspunt "Open waar het kan, beschermen waar het moet, altijd alert, nooit naïef". Als EU-lidstaat draagt Nederland bij aan de open strategische autonomie van de EU, oftewel "haar vermogen om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes haar publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld."

Eventuele beleidsinzet zal altijd op basis van zorgvuldige afwegingen moeten plaatshebben. Bovenstaande uitgangspunten geven richting, maar laten nog de nodige ruimte voor concrete invulling.

Een aantal ontwikkelingen maakt het nodig het denken over technologie, economie en veiligheid aan te scherpen. Ten eerste raakt technologie zoals AI, semicon en quantum steeds meer vervlochten in onze economie, onze veiligheid en onze maatschappij. Technologie wordt in het internationale speelveld dan ook een steeds belangrijkere machtsfactor. Ten tweede zetten landen economische instrumenten, waaronder technologie en de strategische grondstoffen¹ die nodig zijn voor de ontwikkeling ervan, steeds vaker in voor geopolitieke doeleinden. Deze ontwikkeling bemoeilijkt onbelemmerde toegang tot technologie elders. Deze toegang omvat o.a. de markttoegang tot derde landen als afgesproken onder het op regels gebaseerde handelssysteem voor de verschillende onderdelen in de technologische waardeketen (van intellectueel eigendom, grondstoffen tot een technologisch eindproduct).² De Westerse aanname dat alle landen – waaronder opkomende economieën – zich zouden voegen naar het multilaterale stelsel gebaseerd op verdragen is niet uitgekomen. De omgeving kan worden gekarakteriseerd door de term 'comprehensive cooperative competition': staten concurreren met elkaar en werken tegelijk met elkaar samen om mondiale uitdagingen aan te gaan, terwijl onderwerpen en beleidsterreinen aan elkaar verbonden worden. Verbindingen kunnen tot wederzijds voordeel strekken maar ook gebruikt worden als machtsmiddelen.³

Aangezien technologie zo sterk samenhangt met zowel onze economische welvaart als onze veiligheidspositie, zijn nadere richtinggevende principes nodig. Idealiter geven we daarmee bij onze afwegingen en beleid voldoende rekenschap van zowel onze economische als onze

¹ Grondstoffen zijn relevant, maar vergen een aparte analyse en vallen buiten de scope van deze notitie.

² Zie uitleg van het begrip 'technologie' in de bijlage.

³ Zie bv Mark Leonard, *The Age of Unpeace: How Connectivity Causes Conflict*, London, Bantam Press 2021

veiligheidsbelangen. Zowel waar ze complementair zijn als waar er juist spanning tussen zit en een zorgvuldige balans gevonden dient te worden. Het krachtenveld is te vatten in een driehoek van technologie, veiligheid en economie (waarbij die laatste o.a. verdienvermogen en bedrijfsbelangen omvat). Veiligheid, een gezonde economie en technologie zijn op hun beurt weer nodig om maatschappelijke uitdagingen zoals klimaat, volksgezondheid en onderwijs te kunnen aangaan. Deze notitie beoogt de krachten in de driehoek technologie, veiligheid en economie in kaart te brengen tegen de hierboven geschetste geopolitieke achtergrond. Dat stelt ons in staat beleid te maken dat slim en gebalanceerd inspeelt op het samenspel tussen technologie, veiligheid en economie.

Conceptueel kader: 1) relatie economie en veiligheid

Economie en veiligheid zijn met elkaar verweven. In de meest traditionele zin omdat een stabiele en veilige omgeving een randvoorwaarde is voor economische welvaart. Omgekeerd hangt onze veiligheid ook af van onze economische positie. Er zijn namelijk mensen, geld en kapitaal nodig om veiligheid te borgen en het versterken van de veiligheid is gebaat bij ontwikkelingen in onze (technologische) kennis en innovatie. Daarbij geeft een grote economische voetafdruk landen ook gelegenheid politieke punten onder de aandacht te brengen en is de economische voetafdruk een belangrijk onderdeel van de *deterrence posture* van een land. Internationaal gezien versterken wederzijdse economische afhankelijkheden de stabiliteit.

Er bestaan ook afruilen tussen economie en veiligheid. Het borgen van veiligheid legt een beslag op middelen (mensen, geld, kapitaal) die ook elders in de economie hadden kunnen renderen. Daarnaast kunnen ingrepen ten behoeve van de veiligheid een versturende werking hebben op innovatie, markten en op de economie in zijn geheel. Te stringente veiligheidsmaatregelen kunnen op korte termijn nodig lijken maar op langere termijn kostbaar blijken. Aan de andere kant kan het negeren of onderschatten van veiligheidsrisico's, bijvoorbeeld vanwege korte termijn bedrijfsbelangen, leiden tot kwetsbaarheden in de vorm van dwang, manipulatie en chantage. Veiligheidsmaatregelen kunnen dus op korte termijn kostbaar zijn, maar op langere termijn grotere economische en maatschappelijke schade voorkomen.

De verwevenheid tussen economie en veiligheid neemt toe doordat andere landen economische instrumenten steeds vaker inzetten voor geopolitieke doeleinden, met technologie als machtsfactor.

Conceptueel kader: 2) relatie technologie en economie

De technologische positie draagt, met name via de kanalen van efficiëntie en innovatie, bij aan zowel het verdienvermogen als het aangaan van maatschappelijke uitdagingen. Technologische vooruitgang is nodig om onze maatschappelijke uitdagingen - bijvoorbeeld op het gebied van klimaat - aan te gaan en tegelijkertijd onze productiviteit - en daarmee ons verdienvermogen - op peil te houden. Dat geldt voor zowel binnenlandse technologische capaciteiten als toegang tot technologie elders.

Daarbovenop heeft het voordelen om binnen de eigen landsgrenzen te beschikken over technologische capaciteiten:

- Geografisch gebonden uitstralingseffecten (spillover): dit betreft regionale kennisoverlovers, met name kennis die niet-tijdelijk is en moeilijk repliceerbaar is, zoals de ontwikkeling van hoogwaardige regionale toeleveringsketens. Hieronder valt ook de aanzuigende werking van meer bedrijvigheid en hoogopgeleide kenniswerkers.
- Toegang tot technologie elders en tot technologische vooruitgang: de kennis en sleutelposities die Nederland in huis heeft geven ons toegang tot nuttige technologie elders in de wereld die vervolgens ons verdienvermogen kunnen versterken. Ook bieden ze een basis om bij te dragen aan de ontwikkeling van verdere technologische capaciteiten, wat ons verdienvermogen van de toekomst verstevigt.

Er zijn dus voordelen van binnenlandse technologische capaciteiten bovenop toegang tot technologie elders. Hoe groot die voordelen zijn is niet kwantificeerbaar. Daarnaast is het een gegeven dat een land niet alle technologische capaciteiten zelf in huis kan hebben, zeker een klein land als Nederland niet.

*Ook de economische voordelen van technologisch leiderschap - geavanceerder zijn dan andere landen - bovenop het hebben van capaciteiten zijn lastig in te schatten. In markten waar er maar één winnaar kan zijn, doorgaans markten met groot *first-mover-advantage* en *winner-takes-all* dynamiek, kan leiderschap economische voordelen hebben. Dergelijke markten zijn overigens lastig te betreden vanuit een achterstandspositie. Markten waar *first-mover-disadvantage* of *catching-up effecten* de overhand hebben zijn juist wel vanuit een achterstand te betreden en geven de technologisch leider niet veel profijt. Dit zijn over het algemeen technologieën die relatief gemakkelijk over te nemen zijn en lage toetredingsbarrières kennen.*

Conceptueel kader: 3) relatie technologie en veiligheid

De technologische positie draagt ook bij aan de nationale veiligheid. Dat gaat via twee kanalen: (1) de toepassing van de technologie en (2) de geopolitieke positie die gepaard gaat met de technologie. Het dual use karakter van veel technologieën maakt dat deze kunnen worden ingezet voor zowel vreedzame maatschappelijke doeleinden als voor militaire, politieke of inlichtingenmatige doeleinden. Belangrijk is dat een technologie alleen in een specifieke context en met een specifieke toepassing een potentieel gevaar voor de nationale veiligheid oplevert. Omdat dat risico altijd bestaat voor dual use technologieën, bestaat daarvoor een uitputtende lijst waarmee Nederland werkt, op basis van EU-wetgeving (op haar beurt gebaseerd op een internationaal verdrag).

Met betrekking tot toepassing:

- Beschikbaarheid van technologie noodzakelijk voor de continuïteit en veiligheid van vitale processen. De absolute positie is hier van belang (beschikken over capaciteiten).
- Voorsprong bij ontwikkelen militaire- en veiligheidstechnologie (w.o. cyber). Voor een achterstand geldt uiteraard het omgekeerde. De relatieve positie (leiderschap) is hier van belang.
- Invloed op normen en standaarden en op eindgebruik van gevoelige technologie in de keten. De relatieve positie (leiderschap) is hier van belang.

Bovenstaande laat zien dat het bij nationale veiligheid duidelijker dan bij het verdienvermogen gaat om de relatieve technologische positie – dus om technologisch leiderschap.

Met betrekking tot geopolitieke positie: de technologische capaciteiten van ons land (of de EU) verminderen kwetsbare strategische afhankelijkheden. Dat werkt twee kanten op: het buitenland wordt meer afhankelijk van ons en wij worden minder afhankelijk van het buitenland. Dit geldt in het bijzonder wanneer Nederland (of de EU) beschikt over een sleutelpositie. Het verminderen van kwetsbare afhankelijkheden en sleutelposities kunnen op de volgende manieren de geopolitieke positie beïnvloeden:

- Nederland en de EU invloed verschaffen die het kan gebruiken wanneer het onder geopolitieke druk gezet wordt. De technologie kan dan gebruikt worden als geopolitieke tegendruk, vooral wanneer die technologie of het onderdeel in de keten slechts beperkt beschikbaar is in de wereld. De relatieve positie (leiderschap) is hier van belang.
- de geopolitieke invloed van Nederland en de EU vergroten via technologische capaciteiten:
 - door een relevante (gespreks)partner te zijn voor geopolitieke grootmachten. De relatieve positie (leiderschap), in het bijzonder een sleutelpositie, is hier van belang.
 - door geopolitieke invloed op een ander land uit te oefenen. Dit geldt voor zowel derde landen alsook binnen de EU en bondgenootschappen als de NAVO. Ook hier is de relatieve positie (leiderschap) van belang.
 - door een bijdrage te leveren aan het in stand houden van een op regels gebaseerde internationale orde met respect voor universele mensenrechten. Bv door bij te dragen aan normontwikkeling op tech-gebied. Ook hier is de relatieve positie (leiderschap) van belang.

Een gebalanceerde beleidsinzet

Een goede technologische positie is dus dienstbaar aan de publieke belangen van veiligheid en welvaart (verdienvermogen en kunnen aangaan van maatschappelijke uitdagingen), al is de bijdrage aan welvaart moeilijk te kwantificeren. De overheid kan het beleid daarom op een goede

technologische positie richten. Afhankelijk van de context, de technologie en de belangen die in het geding zijn varieert de overheidsinzet op:

1. Technologisch leiderschap (van NL, de EU of andere bondgenoten)
2. Binnenlandse technologische capaciteiten (van NL, de EU of andere bondgenoten)
3. Toegang tot technologie elders (bondgenoten of daarbuiten)

Hierbij geldt in algemene zin dat de kosten van inzet op leiderschap en op eigen technologische capaciteiten hoger zullen zijn dan de kosten van inzet op toegang tot technologie elders. Bovendien is technologisch leiderschap niet af te dwingen en kan het inzetten op technologische capaciteiten en/of leiderschap een hoge prijs hebben. Nederland kan niet op alles inzetten en moet hier dus een balans in vinden. Gezien de toenemende rol van technologie voor veiligheid en economie maar ook gezien de beperkte sturende rol die de overheid kan spelen, is goede communicatie met het bedrijfsleven van groot belang.

Hoe, met wie, wanneer en wat

Het concretiseren van de beleidsinzet (hoe, met wie, wanneer en wat) vergt antwoord op meerdere kennisvragen en parkeren we derhalve voor nader onderzoek. Bij een volgende slag zetten we de ingrediënten hiervoor op een rijtje.

Bijlage: Terminologie

Om de discussie op dit nog deels onontgonnen kennisgebied goed te kunnen voeren is het belangrijk definities te geven van de begrippen die in deze notitie centraal staan.

Land: we spreken hieronder vaak over een land, maar dat kan ook een groep landen (bijvoorbeeld de EU, de NAVO of ander partner-/bondgenootschap of coalitie) zijn. Welke landen (EU, 'like-minded', NAVO, of anders) we als partners beschouwen hangt af van de context en is grotendeels een politieke vraag. De richtinggevende principes gaan hierop in.

Economie: wanneer er in deze notitie wordt gesproken over economie of economisch belangen bedoelen we het verdienvermogen (zie hieronder) van een land. Dit hangt sterk samen met bedrijfsbelangen, maar is breder dan dat. Het verdienvermogen van een land komt namelijk niet alleen tot stand door bedrijven, maar ook door de beroepsbevolking en de economische structuur (infrastructuur, instituties, wet- en regelgeving, etc.) van een land; beide zijn ook bepalend voor het vestigingsklimaat.

Verdienvermogen: het bruto binnenlands product dat een land op structurele basis kan genereren.

Nationale veiligheidsbelangen: Nederland definieert zijn nationale veiligheid in termen van het Voorkomen van maatschappelijke ontwrichting en het beschermen van de democratische rechtsorde. Hiervoor worden zes nationale veiligheidsbelangen onderkend: (1) Territoriale veiligheid, (2) fysieke veiligheid, (3) economische veiligheid, (4) ecologische veiligheid (5) sociale en politieke stabiliteit en (6) internationale rechtsorde.

Technologie: De term technologie verwijst naar de kennis en vaardigheden om een bepaald product (goed of dienst) te kunnen vervaardigen. Daarbij kan technologie gebruikt worden om een overkoepelend kennisgebied, een onderdeel daarvan en/of een toepassing daarvan aan te duiden. Relevant om te noemen is dat grondstoffen (lithium, magnesium, etc.) onmisbaar zijn voor technologieën, maar dat die buiten de scope van deze notitie vallen.

Technologie omvat meerdere dimensies: (1) binnenlands/buitenlands, (2) absoluut/relatief, (2) (3) niche/keten, (4) nu/later. Deze dimensies komen terug in onderstaande begrippen die het begrip 'technologie' verfijnen.

Technologische capaciteiten: de technologieën waartoe een land binnen de eigen landsgrenzen over beschikt. Technologische capaciteiten van een land zijn niet strak afgebakend en statisch. De bedrijven en mensen die de capaciteiten (kennis, assets, vaardigheden) bezitten zijn namelijk vrij om te komen en vertrekken en nemen die capaciteiten dan vaak mee.

Technologische positie: alle technologie waar een land gebruik van kan maken. Bestaat uit (1) de eigen technologische capaciteit in eigen land, (2) toegang tot technologie in andere landen, (3) de mogelijkheden om eigen technologie/toegang tot technologie te verwerven.

Absolute positie: de staat van de technologie waar een land over beschikt of toegang toe heeft.

Relatieve positie: is de stand van de technologie van een land ten opzichte van die van andere landen.

Technologisch leiderschap: wanneer de eigen technologische positie geavanceerder is dan die van een ander land (de relatieve positie). Technologisch leiderschap kan gaan over een individuele technologie of een deel daarvan, of over de hele set aan technologieën binnen een land.

First-mover-(dis)advantage: PM

Winner-takes-all dynamiek: PM

Catching-up effecten: PM

Keten: PM

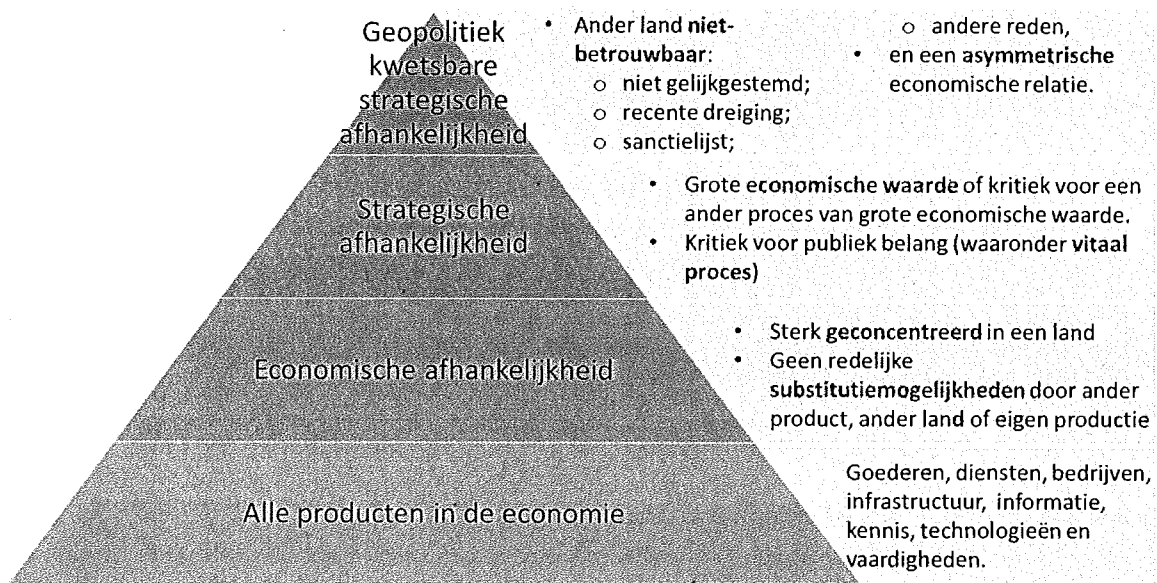
Niche: een schakel binnen de technologische keten.

Sleutelpositie: PM.

Technologische autonomie: wanneer een land beschikt over technologische capaciteiten (binnen de eigen landsgrenzen) over de hele keten van de technologie en niet afhankelijk is van andere landen.

Technologische vooruitgang (ook wel innovatie): het opdoen van nieuwe kennis en vaardigheden om bestaande technologie te verbeteren of tot nieuwe technologie te komen. Technologieën en toepassingen ontwikkelen zich continu. Technologische capaciteiten nu zijn daarom niet hetzelfde als de technologische capaciteiten later.

Kwetsbare strategische afhankelijkheid: een combinatie van: (1) economische afhankelijkheden (2) die strategisch zijn en (3) die betrekking hebben op een land dat hier mogelijkgevoors geopolitiek gebruik van maakt (zie figuur hieronder).



Stellingen voor het denken over technologisch leiderschap

1. Uitgangspunt is en blijft een zo open mogelijke economie en eerlijke concurrentie. Nederland is ervan overtuigd dat deze principes op lange termijn de meeste welvaart, maatschappelijke vooruitgang en stabiliteit opleveren. Ook wanneer andere landen in strijd met deze principes handelen.
2. Het al dan niet streven naar technologisch leiderschap, technologische capaciteiten en toegang tot technologie is in beginsel aan marktpartijen. Een technologische positie is slechts in beperkte mate maakbaar door de overheid.
3. Omdat technologie een machtsfactor vormt en niet meer in alle gevallen vrij toegankelijk is, is Nederland zich bewust van de technologische positie van ons eigen land en die van de EU. Die bestaat uit een combinatie van toegang tot technologie, technologische capaciteiten en technologisch leiderschap.
4. Waar een technologie nodig is om publieke belangen, waaronder nationale veiligheid en verdienvermogen, te borgen, kan de overheid maatregelen nemen om ook de toegang tot die technologie te borgen. In uiterste/bepaalde gevallen kan de overheid streven naar eigen capaciteiten of leiderschap.
5. Eventueel overheidsingrijpen is nauwkeurig en contextafhankelijk. Nauwkeurig betekent dat de inzet steeds een balans zal zijn tussen beschermen en versterken en tussen (nationale) veiligheidsbelangen, andere publieke belangen en economische belangen. De algemene principes van doelmatigheid, doeltreffendheid en proportionaliteit gelden onverkort.
6. Generiek stimulerend beleid is op lange termijn het meest doelmatig en toekomstbestendig, mede omdat dat technologieën van de toekomst nu nog niet bekend zijn. De overheid kan onze technologische positie versterken door te zorgen voor stimulerende randvoorwaarden als een goed opgeleide beroepsbevolking, een goed vestigingsklimaat en een dynamische en diverse economie en door innovatie in algemeen te subsidiëren.
7. Nederland kiest ervoor om in te zetten op een stevige technologisch positie wanneer er sprake is van een sensitieve technologie waar Nederland een positie op heeft of kan verkrijgen en die raakt aan het publieke belang, waaronder het nationale veiligheidsbelang, zoals in het bijzonder territoriale integriteit en economische veiligheid (continuïteit van vitale processen en infrastructuur, integriteit en exclusiviteit van kennis en informatie). Andere belangen kunnen hierbij ook een rol spelen, zoals ons toekomstig verdienvermogen en het aangaan van maatschappelijke uitdagingen (bv klimaat) waarvoor de technologie essentieel is.
8. Het verdienvermogen is in principe aan de markt en samenleving, maar daarvoor moeten we nu en in de toekomst wel toegang hebben tot bepaalde essentiële technologieën. Daarom zijn semicon, kwantum, fotonica en ai voorbeelden van technologie(deel)gebieden waar Nederland op basis van deze criteria zou kunnen inzetten op een goede technologische positie.
9. Nederland is een klein land, dat geen technologisch leiderschap in isolement kan verwerven. We zetten om die reden in beginsel in EU-verband in op toegang, capaciteiten en waar nodig leiderschap. Daarnaast zetten we in op toegang tot die technologie via betrouwbare partners (bondgenoten en/of like-minded).
10. Indien we kiezen voor overheidsinzet om onze technologische positie te versterken, al dan niet in EU-verband, vergt dat een nadere concretisering van beleidsopties en zorgvuldige afweging van de gevolgen. Dat gaat om systematische afwegingen tussen bijvoorbeeld generiek en/of specifiek beleid, beschermen en/of versterken, welke chokepoints zijn cruciaal, om welke kwetsbaarheden gaat het en in welk internationaal verband of met welke partners werken we samen.
11. Specifieke overheidsinzet op leiderschap is in veel gevallen niet nodig. Met name daar waar het gaat om onze technologische positie op militaire toepassingen en dual use goederen is de relatieve positie wél van belang. Omdat leiderschap niet is af te dwingen, streven we voor deze technologieën naar een combinatie van eigen en bondgenootschappelijke capaciteiten en toegang via NAVO-bondgenoten.

Eerste inventarisatie coalitieakkoord punten cybersecurity, economische veiligheid en vitaal

P. 22: EV - kennisveiligheid

We stimuleren de vrije en veilige uitwisseling van ideeën en borgen de academische vrijheid van wetenschappers. **We stellen kaders vast voor de wetenschappelijke samenwerking met onvrije landen. 'Open science' en 'open education' worden de normen, mits de nationale veiligheid hierbij niet in het geding komt.**

P.22: OBI

We grijpen sneller in bij (informele) onderwijsinstellingen en hun vertegenwoordigers die anti-integratief, anti-democratisch of anti-rechtsstatelijk opereren. We breiden de mogelijkheden om dat te doen uit en onderzoeken op welke manieren dat mogelijk is.

P. 27: OBI

Ongewenste buitenlandse beïnvloeding en financiering worden aangepakt. We nemen maatregelen om ongewenste beïnvloeding zoveel mogelijk tegen te gaan, o.a. door de werkzaamheden van de verder te versterken Taskforce problematisch gedrag en ongewenste buitenlandse financiering (Kamerstuk 35228, nr. 39) en de behandeling van het wetsvoorstel transparantie maatschappelijke organisaties (Kamerstukken 35646) voort te zetten.

P. 28: EV - investeringstoets, offensief industriebeleid & vitaal

We versterken het bedrijfsleven en het vestigingsklimaat en stimuleren met een duidelijke strategie een maakindustrie die vooroploopt. Dat doen we door te voorzien in goed opgeleid personeel en het tekort aan technisch en praktisch opgeleide werknemers aan te pakken. Door het bieden van een stabiel en voorspelbaar ondernemingsklimaat. En door in te zetten op een gelijk speelveld en bescherming te bieden tegen oneerlijke concurrentie van buiten Europa. Andersom vragen we van bedrijven om hun eerlijke bijdrage te nemen en rekening te houden met mensen en leefomgeving. **We zetten in op strategische onafhankelijkheid door productie van cruciale (half)producten in Europa en door het beschermen van vitale processen en het voorkomen van ongewenste zeggenschap in vitale bedrijven.**

P. 30: offensief industriebeleid

Wetenschap, bedrijfsleven, 'startups', 'scale-ups', kenniscoalities en overheid slaan de handen ineen om de kansen die digitale technologie biedt te verzilveren. **We stimuleren innovatie en investeren in chips- en sleuteltechnologieën** zoals kunstmatige intelligentie en quantum computing. We pakken (in Europees verband) de marktmacht en datamacht van grote tech- en platformbedrijven aan om de concurrentiepositie van bedrijven en de privacy van burgers te verbeteren.

P. 30: digitale infrastructuur

Nederland wordt het **digitale knooppunt van Europa** en krijgt robuust, supersnel en veilig internet in alle delen van het land.

P.30 internationale samenwerking digitalisering

We nemen het voortouw en zetten in Europees verband in op **versterking van de samenwerking tussen lidstaten op het gebied van digitalisering**, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en 'open source'.

P. 30 cybercriminaliteit

Cybercriminaliteit zoals 'ransomware' is zeer ondermijnend. We investeren daarom in een brede meerjarige cybersecurity aanpak en in cyberexpertise bij de politie, rechtspraak, het Openbaar Ministerie (OM) en defensie.

P. 30: digitale slagkracht

We willen dat **inlichtingendiensten** beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende **digitale dreigingen en aanvallen assertief op te sporen en te bestrijden**, met waarborgen voor goed en effectief toezicht en digitale burgerrechten.

P. 30: informatiedelen en samenwerken

We beschermen onze **bedrijven, vitale infrastructuur en economisch kapitaal** beter door **centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers**. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en 'hacks'.

P. 31: desinformatie

Grote online platformen worden verantwoordelijk om desinformatie en haatzaaien op hun platforms tegen te gaan. We beschermen kinderen extra tegen niet-passende 'online' reclame en kindermarketing, geven ze het recht om niet gevolgd te worden en geen dataprofielen te krijgen.

P. 37: EV: Offensief industriebeleid

We zetten in op **open strategische autonomie van de EU en stimuleren innovatiekracht en slimme industriepolitiek**. Zo worden we leidend in digitalisering en nieuwe technologieën.

P. 38: EV: Offensief industriebeleid

Wij geven het buitenlandbeleid vorm langs de volgende vijf lijnen: 1) bevorderen van de internationale samenwerking door een voortrekkersrol in de EU en multilaterale organisaties, via het versterken van de trans-Atlantische band en nieuwe partnerschappen, 2) meer focus op onze internationale belangen, 3) **verminderen van de afhankelijkheid voor strategische goederen en grondstoffen**, 4) respect voor mensenrechten blijven bevorderen in ons buitenlands beleid, 5) betere en toegankelijke dienstverlening voor Nederlanders in het buitenland (o.a. via een sterker postennetwerk).

P. 38: strafbaarstelling spionage

Buitenlandse inmenging gaan we tegen, o.a. door **spionage strafbaar te stellen**. Nationale en internationale veiligheid raken steeds meer verweven. Daarom richten we een **nationale veiligheidsraad op**.

P. 39: ihkv notitie technologisch leiderschap

Voor onze strategische onafhankelijkheid houden we, binnen de EU-regels, oog voor een vitale defensiesector in Nederland met een gelijkwaardiger Europees speelveld.

P. 39: ongewenste zeggenschap/investeringstoets

Tegelijkertijd beschermen we onze ondernemers tegen **ongewenste investeringen en oneerlijke concurrentie**. We ondersteunen ondernemers en het mkb om in de wereld succesvol te zijn. We vergroenen onze handelsinstrumenten in lijn met de uitkomsten van de akkoorden van Parijs en Glasgow.

P. 39: versterking defensie

We investeren in **modern materieel** (inclusief digitalisering, innovatie en benodigde nieuwe capaciteiten) en hanteren daarbij een langjarig perspectief.

We versterken onze specialismen in **'cyber' en inlichtingen**. Dit gebeurt in nauw overleg met onze belangrijkste partners.

Overig relevante passages:

P. 28 – kennis en innovatie

Publiek-private samenwerking op het terrein van kennis en innovatie blijft een belangrijk onderdeel van het bedrijfsleven beleid. Het Topsectorenbeleid wordt gecontinueerd. We verhogen onze publieke investeringen in kennis en innovatie door het instellen van een fonds voor onderzoek en wetenschap en een intensivering van de kennis- en innovatiepijlers in het Groeifonds.

P. 9 (budgettaire bijlage) – kennis en innovatie

Voor een nog op te richten **fonds voor onderzoek en wetenschap** wordt incidenteel 5 miljard euro gereserveerd met als doel het inhalen van achtergebleven investeringen in onderzoek en verdere versterking van de onderzoek infrastructuur. Deze middelen worden ook ingezet voor het versterken van de kwaliteit van hoger onderwijs en wetenschap, verlagen van de werkdruk en ruimte voor ongebonden onderzoek.



de ACEV

Datum
17 februari 2021
Ons kenmerk
NCTV
Bijlagen
3

nota

Formatie fiches cybersecurity, economische veiligheid en
vitaal

Aanleiding

In de ACEV van januari 2021 zijn de concept fiches cybersecurity, economische veiligheid en vitaal voor de formatie besproken, vandaag liggen de definitieve fiches voor. Daarnaast is er gesproken over prioriteren binnen de fiches voor het geval maar een deel van het benodigde bedrag wordt toegekend. Er zijn per fiche interdepartementaal gedeelde prioriteiten vastgesteld, deze zijn bijgevoegd in bijlage 3. Deze nota zet uit een hoe het proces tijdens de formatie er uit ziet en op wat voor manier de verschillende stukken zullen worden ingezet.

Gevraagde besluiten

1. Het definitief vaststellen van de fiches en bijbehorende financiële onderbouwing als de inzet voor de formatie op de onderwerpen cybersecurity, economische veiligheid en vitaal.
2. Instemmen met het overzicht van de prioritaire onderwerpen
3. Instemmen met de voorgestelde toekenningsfactoren.
4. Instemmen met de hieronder geschetste werkwijze tijdens de formatie.

1. Definitieve fiches en bijbehorende financiële onderbouwing (bijlage 1 en 2)

Bijlage 1 betreft de fiches cybersecurity, economische veiligheid en vitaal. Bijlage 2 (a,b,c) is de financiële onderbouwing daarvan. Deze documenten vormen de inzet voor de formatietafel. Uw akkoord met beide bijlagen wordt gevraagd.

2. Prioritaire onderwerpen (bijlage 3)

Insteek voor de formatie is altijd de 100% variant zoals in bijlage 1 en 2 geschetst. In het voorkomende geval dat slechts een deel van de benodigde middelen wordt toegekend is het van belang prioritering aan te brengen.

Deze interdepartementaal afgestemde prioritering is uiteengezet in bijlage 3. Dit is in beginsel niet bedoeld om actief te delen met de

formatietafel maar om gericht te kunnen antwoorden bij specifieke vragen of wensen vanuit de formatietafel. Hiermee wordt tevens invulling gegeven aan de wens van de ACEV van januari om 'kaasschaven' te voorkomen als er maar een deel van het bedrag wordt toegekend.

Datum
17 februari 2021
Ons kenmerk
NCTV

Uw akkoord met de prioritering binnen de fiches wordt gevraagd.

3. Toekenningsfactoren

Als ondersteuning in het verder aanbrengen van prioriteiten zijn toekenningsfactoren opgesteld. Deze factoren hebben bijgedragen aan het formuleren van de huidige prioritering en zullen gebruikt worden om keuzes te maken wanneer er naar specifieke thema's gevraagd wordt vanuit de formatietafel (in tegenstelling tot generieke toekenning van geld op thema's).

- Betreft de maatregel toegezegd beleid?
- Sluit de maatregel aan bij de BMH, advies CSR, WRR, DBSA etc.
- Komt de maatregel ten goede van meerdere departementen?
- Volgt de maatregel uit afspraken die zijn gemaakt in EU/NAVO verband.
- Heeft de maatregel een versterkend effect op andere maatregelen?
- Is de maatregel afhankelijk van andere maatregelen?
- Is het mogelijk om de maatregel in afgeslankte vorm uit te voeren?
- Ligt er een duidelijke financiële onderbouwing ten grondslag aan de maatregel?
- In hoeverre is het mogelijk om de maatregel (deels) uit bestaande middelen te financieren? (bijv. middels herprioritering van fte's)
- Hoe verhoudt de maatregel zich tot eerder ontvangen gelden?
- Wat is het effect als de maatregel niet wordt uitgevoerd?

Uw akkoord met het gebruik van de voorgestelde toekenningsfactoren als hulpmiddel voor de beantwoording van formatievraagstukken wordt gevraagd.

Werkwijze tijdens de formatie

In 2017 is de NCTV vanuit de coördinerende rol tijdens de formatie bevraagd op nationale veiligheid thema's (waaronder cybersecurity). Het voorstel is om de NCTV deze keer ook aan te wijzen als eerste aanspreekpunt voor de vragen rond cybersecurity¹, economische veiligheid en vitaal.

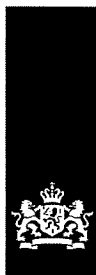
Het is vooraf niet met zekerheid te zeggen voor welke thema's of bedragen er vragen beantwoord zullen moeten worden. Vanwege deze onzekerheid is het vooraf opstellen en uitwerken van

¹ DGRR zal het eerste aanspreekpunt zijn voor vragen rond cybercrime. Indien er naar het fiche over cybersecurity wordt gevraagd zal ook het fiche over cybercrime worden aangeboden en vice versa.

standaardantwoorden niet mogelijk, maar is flexibiliteit gedurende het traject noodzakelijk. Bij vragen vanuit de formatietafel, zal de NCTV op basis van de bijgevoegde fiches input leveren. Indien er sprake is van een generieke toekenning van een deel van het bedrag zal dit ingezet worden t.b.v. de prioritaire onderwerpen per fiche (zie bijlage 3). Wanneer er naar specifieke thema's wordt gevraagd zal er daarnaast gebruik worden gemaakt van de toekenningsfactoren. Afstemming zal altijd plaatsvinden. Echter, de ervaring leert dat de reactietijd kort is, interdepartementale afstemming zal daarom, voor zover mogelijk, plaatsvinden op DG niveau. De ingestuurde reactie richting de formatietafel zal in ieder geval interdepartementaal worden gedeeld.

In de ACEV's gedurende de formatie zal de NCTV de deelnemers informeren over de meest recente stand van zaken. Indien nodig kan de inzet zoals vastgelegd in de bijgevoegde stukken (gericht) worden aangescherpt.

Datum
17 februari 2021
Ons kenmerk
NCTV



W1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Contactpersoon

5.1.2e

Datum

4 februari 2022

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	10 februari 2022, 09:00-10:30 uur
Vergaderplaats	AZ, Rolzaal

1. Opening en mededelingen

2. Verslag TFEV 16 december 2021

5.1.2i

Bijlage 1. Verslag TFEV 16122021

3. Richtinggevende principes technologisch leiderschap (EZK)

Bijlage 2. Oplegnota TFEV technologisch leiderschap

Bijlage 2A. TFEV Criteria en handelingsrichtingen technologisch leiderschap

4. Aanpak ontwikkelingen Oost-Europa (NCTV)

Mondelinge toelichting

5.1.1b +

5.1.2a +

5.1.2i

6. Internationaal/Europees

7. Parlementair

8. Rondvraag en sluiting

Ministerie van Economische Zaken
en Klimaat

TER INFORMATIE

Aan
TFEV ledenDirectoraat-generaal
Bedrijfsleven & Innovatie

Auteur

5.1.2e

[REDACTED]

Datum

3 februari 2022

Kenmerk

DGBI / 22044071

nota

Criteria en handelingsrichtingen voor technologisch
leiderschap

Kopie aan

Bijlage(n)

1

Aanleiding

Op basis van het eerder voorgelegene conceptueel kader voor technologisch leiderschap zijn criteria en handelingsrichtingen voor technologisch leiderschap opgesteld. U wordt gevraagd in te stemmen met de inhoud van de voorliggende notitie en de voorgestelde vervolgstappen.

Voorgenomen besluiten

- Akkoord op de criteria en handelingsrichtingen voor technologisch leiderschap;
- Akkoord op de vervolgstappen:
 - Toepassen van de criteria [REDACTED] technologieën als voorbeelden;
 - Voorbereiden discussiestuk voor politieke niveau (Catshuis of informele RDINEV), met een aantal uitgangspunten en als bijlage een voorlopig overzicht van NL inzet op technologisch leiderschap (dynamisch document);
 - Voorstel voor opdrachtformulering nadere uitwerking van rolverdeling EU-nationaal, inzet op technologische capaciteiten, op toegang tot technologie en tot grondstoffen.

5.1.2i

Toelichting

- In de TFEV van 11 december is een conceptueel kader voor technologisch leiderschap besproken. De criteria en handelingsrichtingen in deze notitie bouwen voort op dit kader.
- Deze notitie vormt het uitgangspunt om het beleid op technologisch leiderschap de komende jaren verder vorm te geven.
- Om dit nader vast te leggen wordt voorgesteld om de criteria en handelingsrichtingen op politiek niveau voor te leggen.
- Op 14 februari vindt tevens een overleg over technologisch leiderschap plaats tussen MinEZK en de boegbeelden van de Topsectoren, waarbij ook NCTV en BZ zullen aansluiten. De input vanuit de Topsectoren zal worden meegenomen in het verder proces.

Criteria en handelingsrichtingen voor technologisch leiderschap

Kern

- Voorliggende notitie biedt criteria voor het identificeren van de technologie(deel)gebieden waar technologisch leiderschap nuttig of nodig is en geeft bijpassende handelingsrichtingen.
- Deze notitie bouwt voort op het conceptueel kader voor technologie dat in de TFEV van december 2021 is besproken. Daarin staat beschreven hoe onze technologische positie nauw samenhangt met zowel onze economische welvaart als onze veiligheidspositie. Daarin wordt de drieslag gemaakt (1) toegang tot technologie elders, (2) technologische capaciteiten en (3) technologisch leiderschap. Deze notitie gaat in op die laatste.

Inleiding

Nederland streeft in Europees verband naar 'open strategische autonomie'. Dat houdt in dat we nu en in de toekomst onze publieke belangen kunnen borgen en weerbaar zijn in een onderling verbonden wereld. Dat doet de EU als mondiale speler en in samenwerking met internationale partners. 'Open' staat voor een economie die openstaat voor internationale handel, met wederzijdse afhankelijkheden en zoveel mogelijk op regels gebaseerde multilaterale samenwerking. Die openheid is belangrijk, omdat het op lange termijn de meeste welvaart, maatschappelijke vooruitgang en stabiliteit oplevert.

Om ook in de toekomst onze publieke belangen – op het vlak van veiligheid, verdienvermogen en maatschappelijke uitdagingen – te kunnen borgen, is het belangrijk om beschikking te houden over enkele cruciale technologieën. Bekende voorbeelden zijn chips, kunstmatige intelligentie en quantum, maar ook technologieën die nodig zijn voor de klimaattransitie. Die vormen op het internationale toneel een steeds grotere machtsfactor. In de huidige verschuivende geopolitieke orde worden Nederland en de EU geconfronteerd met geopolitieke concurrentie, die ook de nationale veiligheid raakt. Nieuwe strategische vragen die hieruit voortkomen, vergen van de overheid om na te denken over nieuwe vormen van ingrijpen.

Tegen die achtergrond schetst het conceptueel kader dat het in veel gevallen voldoende is om via andere landen toegang te hebben tot een bepaalde technologie, maar niet altijd. Soms is toegang tot technologie elders te kwetsbaar en wil de EU over eigen technologische capaciteiten beschikken. Daarbovenop is het voor onze open strategische autonomie belangrijk dat de EU op enkele technologieën een leiderschapspositie inneemt. Dat stelt ons in staat om – langs de weg van wederzijdse afhankelijkheden – toegang te houden tot technologie elders, maar ook om ons te kunnen verdedigen, spelregels internationaal af kunnen te dwingen en de koers van technologische ontwikkeling mede te bepalen langs onze waarden. Dit is geen abstracte discussie: keuzes over bijvoorbeeld semicon worden nú gemaakt, o.a. in het kader van de EU Chips Act en de IPCEI's.

Nederland en de EU menen dat op termijn de economische kernwaarden van openheid, concurrentie en een gelijk speelveld de beste voedingsbodem zijn voor technologisch leiderschap. Daarmee onderscheidt de Europese strategie zich mogelijk van die van andere landen. Daarnaast is een sterke technologische positie (een combinatie van capaciteiten en op sommige gebieden leiderschap) gebaat bij stimulerende randvoorwaarden zoals een goed opgeleide beroepsbevolking, een goed vestigingsklimaat, duidelijke regelgeving en een dynamische, diverse en innovatieve economie. Omdat het in de EU in principe – enkele uitzonderingen daargelaten – clusters van bedrijven en kennisinstellingen zijn die over technologie beschikken, is het met name aan hen om een technologische positie op te bouwen en te beschermen. De overheid kan daarbij wel helpen. Voor de technologieën die de komende jaren belangrijk zijn voor onze open strategische autonomie kan de overheid gericht knelpunten wegnemen die Europese technologieclusters belemmeren bij het verwerven van een leiderschapspositie. Het gericht wegnemen van knelpunten vereist een probleemanalyse, een verantwoordelijkheidsverdeling tussen markt en overheid en maatwerk per technologiecluster.

Deze notitie geeft drie handelingsrichtingen voor overheidsoptreden om technologisch leiderschap te bevorderen door knelpunten weg te nemen. Om te bepalen welke technologieën belangrijk zijn voor de Europese open strategische autonomie en op welke technologieën Nederlandse bedrijven en kennisinstellingen een steentje bij kunnen dragen, stellen we allereerst vier criteria voor. Dan volgen de drie soorten handelingsperspectieven. Tot slot gaan we in op de verhouding tussen Nederland, de EU en andere like-minded-partners in het streven naar open strategische autonomie via technologisch leiderschap. De nuancering dat technologisch leiderschap

moeilijk maakbaar en meetbaar is, is hier op zijn plaats. Dat betekent dat overheidshandelen ter bevordering van technologisch leiderschap een zeker risico met zich brengt.

Deze notitie is een startpunt om nader invulling te geven aan technologisch leiderschap in Europees verband. Het is dus geen allesomvattende strategie om onze publieke belangen in de huidige geopolitieke context te borgen. Ook gaat deze notitie nog niet in op technologische capaciteiten, toegang tot technologie elders of toegang tot grondstoffen¹ (zie vervolgacties 5 op laatste pagina).

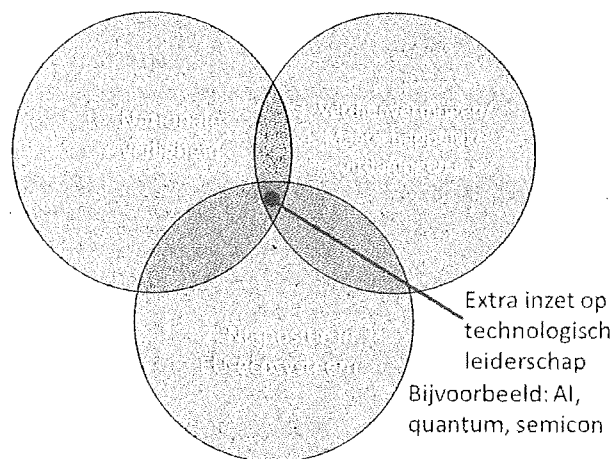
Criteria voor inzet op technologisch leiderschap

Het versterken van een specifieke technologische positie kost inspanning, capaciteit en middelen en kan de binnenlandse economische dynamiek belemmeren. Daarom streven we enkel naar technologisch leiderschap wanneer dat bijdraagt aan het beschermen van publieke belangen. Daarbij valt bijvoorbeeld te denken aan AI-systemen die bijdragen aan onze militaire veiligheid, quantumtoepassingen die bijdragen aan onze digitale veiligheid, of telecom-technologie die een integere omgang met (gevoelige) informatie moet borgen. Belangrijk daarbij is dat overheidsinterventie effectief en proportioneel is en dat er een samenspel is met bedrijven en kennisinstellingen.

Zoals uitgelegd in het conceptueel kader zijn met name de technologieën op het snijvlak van nationale veiligheid, economie en maatschappij (zie figuur) essentieel om Nederlandse en Europese publieke belangen in de toekomst de kunnen blijven borgen. We stellen daarom de volgende vier criteria voor:

Voor de technologie geldt dat:

1. deze een aanzienlijke potentiële impact heeft op onze *nationale veiligheid* (waaronder militaire veiligheid, sensitieve technologie en vitale processen); en
2. een *leidende positie haalbaar* is, doordat er al een ecosysteem in de EU bestaat waarbinnen Nederland een positie van betekenis heeft; en
3. deze nodig is voor ons *verdienvermogen* (omdat de technologie meerdere economische processen en sectoren dient); of
4. deze nodig is voor het aangaan voor een of meer van de door het kabinet vastgestelde *maatschappelijke uitdagingen*².



Toelichting

1. Technologie die aanzienlijke potentiële impact heeft op de nationale veiligheid (sensitieve technologie) is bij uitstek technologie die kan worden ingezet als machtsmiddel en voor militaire- en inlichtingendoeleinden. Zo worden kunstmatige intelligentie en robotica steeds belangrijker in militaire systemen³.
2. De ambitie voor technologisch leiderschap moet haalbaar zijn. Om die reden is het belangrijk dat Nederland en de EU daartoe de potentie hebben. Inzet vanuit Nederland heeft alleen zin als Nederland daadwerkelijk een rol van betekenis speelt binnen het Europese ecosysteem. Hierbij kan bijvoorbeeld worden gedacht aan de (door)ontwikkeling van fotonische chips, die door hun specifieke eigenschappen veel sneller en energiezuiniger zijn dan de gangbare elektronische chips. Ook is

¹ Inzicht in toegang tot grondstoffen is een vraagstuk dat in EU-kader hoog op de agenda staat. Het is een belangrijk element in relatie tot het vraagstuk van technologisch leiderschap. Om die reden is het wenselijk dat bij de uitwerking van dit traject blijvend moet worden meegenomen.

² Het coalitieakkoord spreekt van drie grote transitie: klimaat en energie, digitalisering en sleuteltechnologieën, en de circulaire economie.

³ HCSS, Taming Techno-nationalism, A policy agenda, September 2021

kwantuminternet, dat het mogelijk maakt om internetcommunicatie in extreem hoge mate te beveiligen, een voorbeeld van een opkomende sub-technologie waarin Nederland al een vooraanstaande positie heeft.

3. Het zijn de technologieën waar ook verdienpotentieel in zit die uiteindelijk internationaal het verschil gaan maken en die ons gaan helpen in de toekomst welvarend te blijven en onze maatschappelijke uitdagingen aan te gaan. Daarnaast geldt dat we voor technologieën met verdienpotentieel het innovatief vermogen van het bedrijfsleven kunnen benutten. Er is dan een markt voor de technologie waardoor technologisch leiderschap ook op den duur houdbaar kan zijn, zoals op dit moment al geldt voor kunstmatige intelligentie, maar ook voor bijvoorbeeld 3D-printing³.
4. Sommige technologieën zijn dermate disruptief dat ze zowel maatschappelijke uitdagingen kunnen creëren als oplossen. Dergelijke baanbrekende technologieën, bijvoorbeeld quantumtechnologie en kunstmatige intelligentie, leveren op korte termijn misschien nog geen verdienmodellen op maar zijn in de toekomst mogelijk dermate van belang of disruptief dat het gunstig is om mede de koers van de ontwikkeling ervan te beïnvloeden. Daarnaast zijn er technologieën die onmisbaar zijn voor de transitie naar een klimaatneutrale of circulaire economie.

Deze vier criteria laten zien dat afbakeningen als kunstmatige intelligentie, quantum en semicon⁴, fotonica en robotica te breed zijn. Niet alle technieken binnen deze gebieden voldoen aan alle criteria. De belangrijkste technologie(deel)gebieden moeten zorgvuldig worden geïdentificeerd, samen met bedrijven en kennisinstellingen.

Een leiderschapspositie op alle technologieën binnen het snijvlak van nationale veiligheid, Nederlandse positie in EU-ecosystemen en verdienvermogen/maatschappelijke uitdagingen is niet haalbaar en niet nodig. Een stevige (sleutel)positie op enkele technologieën kan al zorgen voor een gunstige EU-positie op het internationale toneel.

Handelingsbereidheid is nodig om technologisch leiderschap te realiseren

Het voorstel is om enkele handelingsrichtingen overeen te komen die vervolgens nader kunnen worden uitgewerkt. Vooralsnog zijn de volgende handelingsrichtingen te onderscheiden: (1) kennisopbouw, (2) beleidsontwikkeling en (3) middelen.

Handelingsrichting 1: Kennisopbouw over technologie

Voorstel is om (verder) te werken aan kennisopbouw over technologie als machtsfactor. Bijvoorbeeld door onderzoek naar technologie(deel)gebieden die raken aan de nationale veiligheid (sensitieve technologie), zoals al gebeurt in het kader van de Wet vifo en de het toetsingskader voor ongewenste kennis- en technologieoverdracht. Een voorbeeld van een concrete maatregel is om te onderzoeken bij welke sensitieve technologieën een technologische positie bestaat die een voorsprong mogelijk zou maken op andere machtsblokken, of op welke technologieën we juist kwetsbaar zijn. Ook een intensivering van de kennisopbouw over internationale technologieontwikkelingen ligt in de rede en is in de maak.

Handelingsrichting 2: Beleidsontwikkeling voor technologisch leiderschap

Voorstel is om de kennisopbouw doorlopend te benutten voor verdere beleidsontwikkeling. Een voorbeeld van beleidsontwikkeling is om de hierboven genoemde criteria te operationaliseren: hoe verhouden de genoemde criteria zich tot onze huidige inzet op een aantal technologieën, zoals semicon? Op welke technologie(ën) of onderdelen ervan wil Nederland leiderschap nastreven, zelf of met de EU? Bij de beleidsontwikkeling zal ook rekening moeten worden gehouden met de belangen en keuzes van partners (bondgenoten en/of samenwerkingsverbanden). Nederland moet enerzijds bereid moet zijn mee te bewegen met beleidsprincipes van de gewenste partner omwille van de samenwerking en anderzijds in staat zijn de partner te overtuigen van de eigen belangen en keuzes. Een voorbeeld van beleidsontwikkeling op gebied van semicon is de Nederlandse input op de EU Chips Act, de dialoog met de VS en de input in de relevante werkgroep van de EU-VS TTC.

Handelingsrichting 3: Middelen beschikbaar stellen voor technologisch leiderschap

⁴ Zie bijvoorbeeld het Coalitieakkoord van december 2021; Europese Commissie doelstellingen voor 2030 voor semicon en quantum in Digital Compass (EUR-Lex - 52021DC0118 - EN - EUR-Lex (europa.eu)).

Voorstel is om bovenop de huidige middelen voor generiek technologiebeleid, middelen in te zetten voor het behalen of behouden van technologisch leiderschap bij een gericht aantal kennis(deel)gebieden. Bijvoorbeeld door het inrichten van middelen voor deelname aan technologie-, innovatie- en industriesamenwerking in grensoverschrijdend, bilateraal en Europees verband. De middelen zijn dan gericht op voor-en co-financiering van PPS. Daarbij dient eerst geïdentificeerd te worden voor welke (sleutel)technologieën technologisch leiderschap wenselijk en haalbaar is. Vervolgens dient in kaart gebracht te worden wat de knelpunten zijn en waar specifiek behoefte aan is, in aanvulling op middelen die reeds beschikbaar zijn vanuit bijvoorbeeld het Missiegedreven topsectoren en innovatiebeleid (MTIB) en het Nationaal Groeifonds (NGF). Het best en meest toekomstbestendig is om middelen beschikbaar te stellen die een bestaand ecosysteem⁵ versterken. Daarbij investeren we niet in één poot van de technologie, maar versterken we het hele ecosysteem, bijvoorbeeld door een stapje bij te zetten op zwakke punten. Bijvoorbeeld de beschikbaarheid van talent, risicodragend kapitaal, onderzoeksfaciliteiten of valorisatieactiviteiten. Ecosystemen zijn krachtig doordat samenwerking gebaat is bij (fysieke) nabijheid. De aantrekkingskracht van ecosystemen maakt ze toekomstbestendig; ze zijn een voedingsbodem voor niet alleen de technieken van vandaag, maar ook van die van morgen. Een concreet voorbeeld is de IPCEI ME2, waar EU-lidstaten investeren in de productie van chips die niet cutting-edge zijn. Die productie kan toch waardevol zijn om het ecosysteem te versterken en daarmee de productie van cutting-edge chips en/of andere toepassingen in de toekomst wel mogelijk te maken.

Handelen op EU-niveau of nationaal?

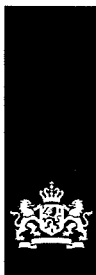
Bij alle drie de bovenstaande handelingsrichtingen is er zowel een EU- als een nationale dimensie. Inzet op Nederlands leiderschap zal vaak samengaan met inzet op capaciteiten in de EU en samenwerking met like-minded landen. Er zal nader moeten worden gezien waarop we primair nationaal willen inzetten, waarop in EU-verband en waarop in/met like-minded landen.

De Nederlandse overheid heeft eigen kennisversterking over technologie nodig in aanvulling op de kennis die in de EU-instellingen en andere lidstaten wordt opgebouwd. Nederland kan zelf beleid maken om technologisch leiderschap te versterken, maar het semicon voorbeeld laat zien dat dat niet tot Nederland beperkt kan blijven: de leiderschapspositie in de semicontekst hangt nauw samen met een ecosysteem met belangrijke onderdelen in andere EU-lidstaten (bv IMEI in BE, Zeiss in DE), in de VS en in andere landen. Nederland speelt daarom ook een actieve rol bij de totstandkoming van EU-beleid, zoals de EU Chips Act, IPCEI's, herziening staatssteunkader en de EU-VS TTC. En bij de financiering zijn in Nederland de middelen relevant die het Coalitieakkoord voorziet voor kennis en innovatie, waaronder het NGF, terwijl in EU-verband zowel delen van het EU-budget (Horizon, RRF) relevant zijn als nationale middelen die in EU-initiatieven worden ingezet (IPCEIs). Zie wederom het voorbeeld semicon: onze positie in het ecosysteem vergt keuzes op bovengenoemde handelingsrichtingen. Daarbij moeten we wel zeker stellen dat onze belangen goed worden behartigd, net als die van kleinere lidstaten.

Voorgestelde vervolgacties

- (1) Bespreking technologisch leiderschap met Boegbeelden (14 februari)
- (2) Toepassen van de criteria op semicon en een of twee andere (delen van) technologieën als voorbeelden
- (3) Voorbereiden discussiestuk voor politieke niveau (Catshuis of informele RDINEV), met een aantal uitgangspunten en als bijlage een voorlopig overzicht van NL inzet op technologisch leiderschap (dynamisch document)
- (4) Voorstel voor opdrachtformulering nadere uitwerking van:
 - a. rolverdeling EU- nationaal;
 - b. inzet op technologische capaciteiten;
 - c. toegang tot technologie;
 - d. toegang tot grondstoffen.

⁵ Zie ook Kabinetsstrategie van onderzoeks- en innovatie-ecosystemen.



X1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep.-VERTROUWELIJK

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

4 april 2022

Bijlagen

2

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	4 april 2022
Vergaderplaats	Schriftelijke ronde

1. Algemeen

- Deze schriftelijke ronde is ter vervanging van de TFEV die op 24 maart 2022 gepland stond. U kunt tot en met 11 april uw reactie op de stukken geven.

2. Ter besluitvorming: Opdrachtformulering EVDO casus gebruik binnen de Rijksoverheid van telefoons uit een land met een offensief cyberprogramma gericht tegen NL belangen (BZK)

- Zie bijlage 1

3. Ter kennisname: Kader Nationale Veiligheid inkoop en gebruik producten en diensten (BZK & NCTV)

- Zie bijlage 2

4. EV-loket RVO (EZK)

- In de TFEV van december 2021 heeft EZK voorgesteld een EV-loket in te richten voor bedrijven. Hierbij is aangegeven dat zal worden aangesloten bij het loket kennisveiligheid, dat sinds januari operationeel is. Een korte update over het loket:
- De RVO is begin deze maand begonnen met een inventarisatie bij bedrijven. Er zullen ca. 10 interviews worden gehouden en er zal een enquête naar 1500 bedrijven worden gestuurd. [REDACTED]
[REDACTED]
[REDACTED]
- Uit de eerste drie interviews die nu zijn gehouden komt naar voren dat er behoefte is aan één aanspreekpunt binnen de overheid. Onderwerpen die spelen zijn o.a. cybersecurity en IT-beheer, human capital en het screenen van medewerkers en het omgaan met IP-gevoelige informatie. Er lijkt behoefte te zijn aan checklists, kaders en advies (m.n. voor kleine en startende bedrijven), maar ook aan een aanjagende functie waarbij bedrijven worden getriggerd om na te denken over EV.

5.1.2i

Dep.-VERTROUWELIJK

Datum
4 april 2022

- In april zullen de resultaten van de quickscan worden gedeeld met de boegbeelden van de topsectoren. Mede op basis hiervan zal de concept quickscan worden afgerond waarna deze zal worden gedeeld in de TFEV. Op basis van de quickscan zal worden gezien of en hoe het loket het beste ingericht kan worden.

5.

[REDACTED]

5.1.1b + 5.1.2a +
5.1.2i

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

DEPARTEMENTAAL-VERTROUWELIJK

TER BESLUITVORMING

Nota actief openbaar
NeeOnze referentie
2022-0000163712Datum
21 maart 2022

Opgesteld door

 5.1.2.e
 Samengewerkt met
 Leden EVDO
Bijlage(n)
0Aan
VanLeden TFEV
EVDO

nota

opdrachtformulering EVDO casus gebruik binnen de
Rijksoverheid van telefoons uit een land met een offensief
cyberprogramma gericht tegen NL belangen**Aanleiding**

In de nota 'Verbreden scope EVDO voor mobiele OS' die in de TFEV van 17 november '21 is besproken is aangegeven dat het EVDO een risicoanalyse zou uitvoeren naar het gebruik binnen de Rijksoverheid van telefoons uit een land met een offensief cyberprogramma. Dit wordt gedaan op basis van een set aan criteria waarover de Tweede Kamer in de C2000-casus is geïnformeerd¹

Het EVDO heeft de eerste verkennende fase afgrond en stelt voor om de vervolg analyse langs onderstaande lijnen uit te voeren. De structuur van de risicoanalyse komt overeen met de eerder gebruikte methodiek, die ook in de Kaspersky casus is gebruikt. Deze methodiek wordt vanuit de NCTV en NCSC verder ontwikkeld zodat mogelijke risico's voor de nationale veiligheid en beheersmaatregelen binnen dergelijke casuïstiek op een gestructureerde en gestandaardiseerde wijze kunnen worden beoordeeld. Met die methodiek wordt een analyse gemaakt van de nationale veiligheidsbelangen, dreigingen en weerbaarheid.

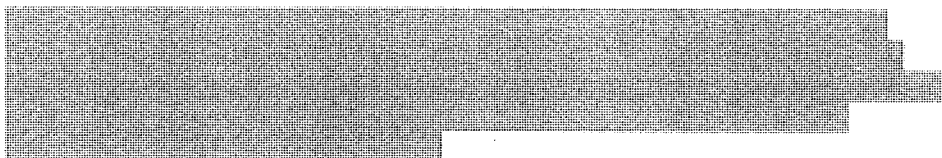
Daarnaast wordt in deze nota inzicht gegeven welke andere casuïstiek op dit moment op de agenda van het EVDO staat om risicoanalyses op uit te voeren.

Geadviseerd besluit

Akkoord met deze opzet en scope van de risicoanalyse.

Kern

Bij het bepalen van de scope is gebruik gemaakt van de risicoleidraad nationale veiligheid, met een overzicht van nationale veiligheidsbelangen en impactcriteria, zodat kan worden aangegeven wanneer sprake is van een risico dat mogelijk de nationale veiligheid raakt. Deze risicoleidraad is een onderdeel van de Nationale Veiligheidsstrategie.



5.1.2i

¹ Kst 25124-96

Onze referentie
2022-0000163712

Datum
21 maart 2022

5.1.1b

Toelichting

Om te komen tot mogelijke proportionele maatregelen, wordt een verdiepende technische analyse uitgevoerd. Op basis daarvan wordt een beleidsadvies opgesteld met mogelijke beheersmaatregelen.

Overige onderwerpen op de agenda van het EVDO

5.2.1

Nast de telefooncasus heeft het EVDO onderstaande onderwerpen op de voorraadagenda staan. Deze vloeien voort uit zowel internationale ontwikkelingen, als vragen vanuit bijvoorbeeld de Tweede Kamer. De voorraadagenda is daarmee inherent dynamisch.

Het oppakken van een casus kost inzet van capaciteit vanuit de betrokken organisaties. Deze is inherent begrensd, waardoor er steeds gekozen moet worden waarop wordt ingezet. Hiertoe zal in de volgende TFEV een voorstel worden gedaan in welke volgorde deze onderwerpen kunnen worden opgepakt, en hoe we met die dynamiek kunnen omgaan.

- Risico's smartphones (hardware en OS niveau) uit land X, voor alternatieve doelgroepen en/of andere scope

•

5.1.1b

- Gebruik van camera's uit land X
- Overheidsapps in Appstores uit land X
- Gebruik van 'Certificate Authorities' uit land X

Waarbij 'land X' een land is met een offensief cyberprogramma gericht tegen Nederlandse belangen.

De recente toezegging door de staatssecretaris van Koninkrijksrelaties en Digitalisering aan de Kamer rondom inkoop², valt vanwege het juridische karakter buiten directe scope van het EVDO. De TFEV zal in april worden geïnformeerd over de opzet/uitwerking van dit onderzoek, en samenhang met andere lopende trajecten rondom inkoop.

Het streven van de betrokken organisaties is om op basis van de opgedane kennis uit de casussen, toe te werken naar een meer algemene beoordelingsmethode

² De volledige toezegging is om onderzoek te doen naar naar inkoop Eisen en – richtlijnen over cyberveiligheid in het overheidsapparaat, voor wat betreft producten (voornamelijk) landen met een offensief cyberprogramma tegen Nederlands en diens belangen. (Definitieve formulering uit het verslag van het Commissiedebat was bij opstellen van nota op 23 maart nog niet beschikbaar.)

rondom producten en diensten. Die methode op basis van concrete ervaringen, maakt het mogelijk om sneller tot afweging en besluitvorming te kunnen komen, dan de arbeidsintensieve casus gebaseerde aanpak zoals die nu wordt gevolgd. Bij het voorstel voor de volgende TFEV zal dit nader worden toegelicht.

Onze referentie
2022-0000163712

Datum
21 maart 2022

Informatie die niet openbaar gemaakt kan worden

Onderliggende stukken worden niet openbaar gemaakt.

Motivering

In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd.



X3

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep- **VERTROUWELIJK**
TFEV

Datum
22 maart 2022

nota

Kader nationale veiligheid: inkoop en gebruik van
producten en diensten

Van
BZK (DGOO), NCTV
Datum/eindparaaf


Doel nota

- TFEV informeren over de huidige inzet om risico's voor de nationale veiligheid te identificeren en mitigeren bij de inkoop en het gebruik van producten en diensten bij de (rijks- en lokale) overheid en vitale aanbieders.

Aanleiding

- TFEV van 10 februari jl. heeft aangegeven behoefte te hebben aan een breder kader waarbinnen casuïstiek gericht op de inkoop en het gebruik van (met name buitenlandse) producten en diensten kan worden geplaatst/opgepakt. Dit kader wordt geschetst in deze nota.

Toelichting

- Met enige regelmaat worden vragen gesteld vanuit de bewindspersonen, parlement of media over het (mogelijke) gebruik van producten en diensten door de Nederlandse (rijks)overheid of binnen de vitale infrastructuur en mogelijke risico's die hieraan verbonden zijn, bijvoorbeeld het risico op spionage of sabotage.
- 
- Het is van belang om bij de aanschaf en in gebruik name maar ook daarna te monitoren op risico's en deze te beheersen. Hier is, en wordt, via diverse trajecten op ingezet. Deze nota schetst de huidige stand van zaken en inzet hierop.
- De inzet komt tot uiting in verschillende beleidskaders. Vanuit nationale veiligheid o.a. in de aanpak Tegengaan Statelijke Dreigingen (specifiek Economische Veiligheid), beleid op Cybersecurity en beleid voor de vitale infrastructuur. Vanuit Rijksinkoopbeleid/BZK krijgt dit vorm via onder

5.1.2i+
5.2.1

meer de regelgeving/kaders voor inkoop, Baseline Informatiebeveiliging Overheid, het CIO-stelsel Rijksdienst. De komende ABRO wordt een aanvullend nieuw instrument in dit geheel.

Datum
22 maart 2022


Inkoop en aanbesteding

Juridisch kader

Voor aanbestedende diensten en speciale sectorbedrijven is het verplicht om bij de inkoop van producten en diensten, indien deze boven een bepaald drempelbedrag uitkomen, volgens voorgeschreven Europese procedures aan te besteden. Het Rijk, evenals een aantal aanbieders van de vitale infrastructuur vallen onder deze aanbestedingsplicht. Hieronder geschetst juridisch kader is hierbij van toepassing.

- Voor het inrichten van het aanbestedingsrechtelijke proces, moet eerst worden vastgesteld welk juridisch kader op de opdracht van toepassing is. Hierbij wordt uitgegaan van de volgende kaders:
 1. Aanbestedingswet 2012 (AW 2012)
 2. Aanbestedingswet op defensie- en veiligheidsgebied (ADV)
- In uitzonderlijke gevallen kan een opdracht geheim worden verklaard op grond van artikel 346 VWEU, waarbij er geen aanbestedingsprocedure hoeft te worden gevolgd.
- Vervolgens zijn er diverse mogelijkheden voor het opnemen van uitsluitingsgronden, geschiktheidseisen, selectiecriteria, gunningscriteria en contractvoorwaarden die risico's voor de nationale veiligheid kunnen beheersen bij toepassing van de AW 2012 of de ADV.

1. *Aanbestedingswet 2012*

- Voor overheidsopdrachten en een deel van de opdrachten van vitale aanbieders geldt dat ze vallen onder de AW 2012.
- De AW 2012 biedt geen directe uitsluitingsgrond om een ondernemer te weren als deze een risico vormt voor de nationale veiligheid.
- 
- Wel kunnen eisen en criteria zo worden vormgegeven dat dit de facto leidt tot uitsluit of niet-gunning aan partijen waarbij risico's voor de nationale en economische veiligheid worden vermoed. Daarvoor is wel vereist dat de aanbestedende dienst zich bewust is van deze risico's bij het ontwerp van de aanbesteding en dat de eisen en criteria voldoende verband houden met de opdracht. Zo kan een aanbestedende dienst voor de inkoop van potloden geen strenge beveiligingseisen stellen, omdat het functioneren van de potloden niet afhangt van die beveiliging.
- Inzet: EZK en NCTV doen momenteel navraag bij Europese lidstaten hoe zij de Europese aanbestedingsrichtlijn hebben geïnterpreteerd en doorgevoerd in nationale wetgeving om te kijken of er meer ruimte nodig is om nationale veiligheid mee te nemen. Mogelijk moet toegewerkt

5.1.2i

worden naar een aanpassing/actualisering van de AW 2012. Dit zal in overleg met EZK als eerste ondertekenaar van de wet worden verkend.

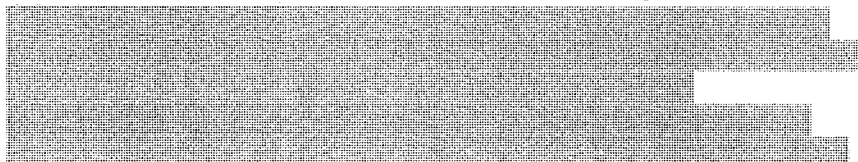
Datum
22 maart 2022

2. *Aanbestedingswet Defensie en Veiligheid (ADV)*

- De ADV biedt, meer dan de AW 2012, opdrachtgevers de mogelijkheid om in het kader van nationale veiligheid bij aanbestedingen de juiste randvoorwaarden te stellen. Als de ADV van toepassing is, wordt er vanuit de wet al vanuit gegaan dat er eisen gesteld moeten worden aan een product of dienst die risico's voor de nationale (en economische) veiligheid tegengaan. Voor een aanbestedende dienst is het dan makkelijker gerichte eisen ten aanzien van o.a. beveiliging, screening, en de herkomst van het product te stellen. De ADV is momenteel toepasbaar voor maar een selecte groep aan aanbestedingen.

Inzet:

- In september jl. ging de ACEV (opnieuw) akkoord met het breder toepasbaar maken van de ADV zodat ook bepaalde aanbestedingen van vitale aanbieders hieronder vallen. Dit draagt bij aan het stellen van de juiste randvoorwaarden in het kader van de nationale veiligheid. Departementen zijn zelf verantwoordelijk voor het uitvoeren van deze opdracht, onder coördinatie van de NCTV en EZK. De CDINEV wordt regelmatig geïnformeerd over de voortgang van dit traject.



5.1.2i

Bewustwording en instrumentarium nationale veiligheid bij inkoop en aanbesteding, waaronder ICO

- Het staande Rijksinkoopbeleid is dat per inkoopopdracht moet worden bezien of er mogelijk risico's zijn voor de nationale veiligheid.
- Als er mogelijke risico's kleven aan een inkoopopdracht wordt geadviseerd een risicoanalyse te doen en waar nodig en mogelijk, mitigerende maatregelen te treffen. Organisaties zijn zelf verantwoordelijk voor het treffen van risicomitigerende maatregelen. Dit kunnen technische of organisatorische maatregelen zijn, maar ook aanbestedingsrechtelijke maatregelen.
- Inkopers kunnen voor het bezien van deze risico's gebruik maken van het instrumentarium nationale veiligheidsrisico's bij inkoop en aanbesteding dat eind 2018 door BZK en NCTV is ontwikkeld. Dit bestaat uit een quickscan, een handleiding risicoanalyse en handvatten risicomitigatie.
- Als onderdeel van de Roadmap Digitaal Veilige Hard- en Software, het programma NL DIGIbeter en het Rijksinkoopbeleid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is in 2021 het instrument Inkoop-eisen Cybersecurity Overheid (ICO) opgeleverd. Met dit instrument, kunnen (overheids)opdrachtgevers ten behoeve van ICT-

inkopen en -aanbestedingen specifieke informatiebeveiligingseisen formuleren.¹ Deze eisen worden vervolgens meegestuurd bij een aanbesteding en kunnen later in een contract met een leverancier worden opgenomen. Door de open toegang is het daarnaast mogelijk voor marktpartijen om gebruik te maken van de mogelijke eisen die de inkopende overheden hanteren. Sinds de start van de ontwikkeling hebben er hebben pilots plaats gevonden met de cybersecurity inkoopseisen bij 35 inkooptrajecten binnen alle overheidslagen inclusief uitvoeringsinstanties.

- ICO bestaat inmiddels uit tien inkoopsegmenten waaronder clouddiensten en serverplatformen. Tegelijkertijd worden ook nieuwe invalshoeken toegevoegd. Zo zijn dit jaar de informatieveiligheidseisen aangevuld met privacy-eisen. Deze aanvulling wordt nu in de praktijk getest. Het beeld dat uit de pilots kwam is dat ICO door de informatiebeveiligingsfunctionarissen als een belangrijk inkoop hulpmiddel wordt gezien. Daarmee verdient ICO een vaste plek in het inkoopproces van de overheid. Tegelijkertijd werd geconstateerd dat inkopers en opdrachtgevers het complex vinden om informatiebeveiligingseisen mee te nemen bij inkooptrajecten omdat ze moeite hebben om een programma van functionele eisen te vertalen naar specifieke ICT-gerelateerde beveiligingseisen. Betere samenwerking tussen ICT-specialisten, opdrachtgevers en inkopers kan dit vraagstuk oplossen.
- Inzet: Er wordt verder in gezet op bewustwording op dit thema en de borging van de instrumenten binnen het Rijksinkoopstelsel. Daarnaast zijn de instrumenten gericht op nationale veiligheid bij inkoop en aanbesteding ook beschikbaar gesteld voor vitale aanbieders en lokale overheden en wordt met enige regelmatig voorlichting gegeven over dit onderwerp bij de vitale aanbieders. Eind 2022 zal het gebruik van ICO worden geëvalueerd.

ABRO (Algemene Beveiligingseisen Rijksoverheid Opdrachten)

- De komende tijd wordt gewerkt aan het ontwikkelen van de ABRO: het nationale veiligheidsraamwerk voor alle gerubriceerde en gevoelige aanbestedingen bij het Rijk en het ministerie van Defensie.
- De huidige Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) dient als basis voor de ABRO waarbij de ABRO de ABDO zal vervangen.
- Het ABRO sluit niets uit, maar biedt een toetsingskader voor aanbestedingen.
- De ABRO kent 3 fasen:
 - I Opzetten projectorganisatie en randvoorwaarden creëren;
 - II Uitvoering geven aan ABRO voor de Rijksoverheid;
 - III Doorontwikkeling en eventueel uitbreiden richting decentrale overheden en vitale sectoren (middellange termijn)
- BZK/DGOO/IFHR, AIVD, MIVD en NCTV zijn betrokken bij uitwerken ABRO.

¹ ICO Wizard - bio-overheid

- Het ABRO-traject zal zich focussen op: bewustwording, regelgeving, toetsing en controle.

Datum
22 maart 2022

Overheid: stelsel en kaders

De (rijks)overheid zet structureel en continu in op de veiligheid en weerbaarheid van zijn digitale systemen. Dit gebeurt onder meer via het CIO-stelsel Rijksdienst en de Baseline Informatieveiligheid Overheid (BIO), waarop hier beneden nader wordt ingegaan. Regels rondom het omgaan met gerubriceerde informatie en bijvoorbeeld de advisering over kwetsbaarheden vanuit het NCSC aan rijksoverheidsorganisaties spelen een rol bij het beheersen van risico's, maar wordt hier niet nader op ingegaan. De inzet op inkoop en aanbesteding, zoals hierboven geschetst, past ook binnen deze structurele inzet.

Besluit CIO-stelsel Rijksdienst 2021

Eind 2020 is het Besluit CIO-stelsel Rijksdienst vastgesteld. Hierin zijn onder meer de positie van de departementale CIO's versterkt, en is de positie van de CIO Rijk verzaamd en geherpositioneerd. Informatiebeveiliging is een integraal onderdeel van het stelsel, waartoe ook de nieuwe positie CISO Rijk is gecreëerd. Binnen dit stelsel zijn onder andere rapportagecycli ingericht, waarin risico's en dreigingen worden geïdentificeerd en een reactie op wordt geformuleerd, waarbij de primaire verantwoordelijkheid binnen de bestaande lijnorganisaties blijft. Zo is er structureel op alle lagen aandacht voor risicomanagement. Ook de ADR kan concrete onderzoeken uitvoeren, en tot aanbevelingen komen.

Baseline informatieveiligheid overheid (BIO)

Voor de gehele overheid geldt de Baseline Informatiebeveiliging Overheid (BIO). De BIO kent een risicogebaseerde aanpak, en is gebaseerd op de internationale standaarden ISO27001 en ISO27002. Dat betekent dat overheidsorganisaties op basis van risicoafweging (nieuwe) dreigingen onderkennen en daarop passende en proportionale beveiligingsmaatregelen treffen. Dit jaar wordt de BIO geëvalueerd. Onderdeel van die evaluatie is de herijking van de dreigingen die richting geven aan de concrete overheidsmaatregelen in de BIO. De BIO bevat ook richtlijnen voor inkoop.

Wet Digitale Overheid


Veel specifieke informatieprocessen van de overheid kennen informatieveiligheidswet- en regelgeving die onderling vergelijkbare algemene informatieveiligheidseisen stellen, die min of meer overeenkomen met de BIO. Voor een aantal van deze processen is verticaal interbestuurlijk toezicht op de naleving van deze regels opgezet. Vooral bij de medeoverheden komen deze regels in de uitvoering weer samen waardoor zij zich geconfronteerd zien met een grote hoeveelheid gelijksoortige toezicht- en verantwoordingsprocessen. Om de lastendruk bij overheden te verminderen en de BIO als juridisch uitgangspunt te hanteren voor informatieveiligheid, bereidt het ministerie van BZK de wettelijke grondslag voor de BIO gaan voor in de volgende tranche van de Wet Digitale Overheid.

In het Commissiedebat met VKC Digitalisering op 22 maart is op verzoek van de VVD door de staatssecretaris voor Koninkrijksrelaties en Digitalisering toegezegd dat er een onderzoek komt naar inkoop-eisen en -richtlijnen over cyberveiligheid in het overheidsapparaat, voor wat betreft producten uit (voornamelijk) landen met een offensief cyberprogramma tegen Nederlands en diens belangen. Over de opzet/uitwerking van dit onderzoek, en samenhang met andere lopende trajecten, waaronder trajecten geschetst in deze nota, wordt de volgende TFEV geïnformeerd.

Expertise teams

Op het moment dat er sprake is van complexe risico's bij inkoop of gebruik van producten en diensten die meerdere departementen raken kan er een interdepartementaal expertiseteam worden opgericht. In de structuur van een expertiseteam wordt een technische analyse gemaakt van NV-risico's en een apart beleidsadvies met beheersmaatregelen, die afhankelijk van de situatie, bij de inkoop (voorkant) of tijdens gebruik (achterkant) kunnen worden geïmplementeerd.

Er zijn op dit moment verschillende expertise teams, gericht op Rijk en diverse vitale processen:

- Expertiseteam Veilige Digitale Overheid (omvat o.a. casuïstiek op antivirussoftware, camera's, mobiele telefoons en overheidapps).
- Expertiseteam Telecom
- Expertiseteam Scan 
- Expertiseteam Electro

5.1.2i

Vervolg

Deze nota schetst het bredere kader waarbinnen casuïstiek rondom de inkoop en het gebruik van producten en diensten kan worden geplaatst. De TFEV wordt apart geïnformeerd over de ontwikkelingen binnen de verschillende dossiers/onderdelen genoemd in deze nota.



X4

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep.-VERTROUWELIJK

Contactpersoon

[REDACTED]
[REDACTED]

5.1.2e

Datum

14 april 2022

verslag

TFEV

Omschrijving
Vergaderdatum en -tijd

TFEV
Schriftelijk

1. Algemeen

- Deze schriftelijke ronde is ter vervanging van de TFEV die op 24 maart 2022 gepland stond.

2. Ter besluitvorming: Opdrachtformulering EVDO casus gebruik binnen de Rijksoverheid van telefoons uit een land met een offensief cyberprogramma gericht tegen NL belangen (BZK)

Schriftelijke reactie TFEV:

- TFEV leden gaan akkoord met gevraagd besluit
- [REDACTED]
- [REDACTED]
- **BZ** leest dat de toezegging van de staatssecretaris van Koninkrijksrelaties en Digitalisering aan de Kamer rondom inkoop van producten uit landen met een offensief cyberprogramma tegen NLse belangen niet zal worden behandeld binnen het EVDO vanwege het juridische karakter en vraagt daarom of BZK een ander gremium voorziet voor interdepartementale afstemming op werkniveau (bijv. IWEV). Daarbij vraagt BZ zich af hoe deze toezegging zich verhoudt tot agendapunt nummer 3.

5.1.2a

3. Ter kennisname: Kader Nationale Veiligheid inkoop en gebruik producten en diensten (BZK & NCTV)

Schriftelijke reactie TFEV:

- **IenW:** het is zeer zinvol om als Rijksoverheid helder en actief te communiceren over de scope, reikwijdte en doelgroepen van desbetreffende regelingen.

4. EV-loket RVO (EZK)

- *In de TFEV van december 2021 heeft EZK voorgesteld een EV-loket in te richten voor bedrijven. Hierbij is aangegeven dat zal worden aangesloten bij het loket kennisveiligheid, dat sinds januari operationeel is. Een korte update over het loket:*
- *De RVO is begin deze maand begonnen met een inventarisatie bij bedrijven. Er zullen ca. 10 interviews worden gehouden en er zal een enquête naar 1500 bedrijven worden gestuurd.* [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- *Uit de eerste drie interviews die nu zijn gehouden komt naar voren dat er behoefte is aan één aanspreekpunt binnen de overheid. Onderwerpen die spelen zijn o.a. cybersecurity en IT-beheer, human capital en het screenen van medewerkers en het omgaan met IP-gevoelige informatie. Er lijkt behoefte te zijn aan checklists, kaders en advies (m.n. voor kleine en startende bedrijven), maar ook aan een aanjagende functie waarbij bedrijven worden getriggerd om na te denken over EV.*
- *In april zullen de resultaten van de quickscan worden gedeeld met de boegbeelden van de topsectoren. Mede op basis hiervan zal de concept quickscan worden afgerond waarna deze zal worden gedeeld in de TFEV. Op basis van de quickscan zal worden gezien of en hoe het loket het beste ingericht kan worden.*

5.1.2i

Schriftelijke reactie TFEV:

- **BZ:** Net als bij het loket kennisveiligheid is verwachtingsmanagement richting bedrijven van groot belang. BZ is benieuwd hoe de gevraagde technisch-inhoudelijk expertise voor het EV loket op het gebied van de onderwerpen die in de interviews genoemd werden georganiseerd zal worden. Daarnaast vraagt BZ zich af of het mogelijk wordt dat het loket voorlichting gaat geven aan bedrijven over bijvoorbeeld spionage, om meer bewustwording te creëren.

- **AIVD:** (1) de AIVD kijkt uit naar de resultaten van de verkenning en (2) in de toekomst zouden we graag verder spreken over coördinatie op (digitale) dienstverlening op dit thema in de richting van het bedrijfsleven.
- **IenW:** Het Kennisloket heeft een grote meerwaarde, niet enkel voor de vitale sectoren en kenniscentra maar ook voor departementen. IenW pleit er dan ook voor om de taak en diensten van het Kennisloket nadrukkelijker te communiceren naar andere kenniscentra/vitale sectoren en andere departementen.
- **NCTV:** Dit initiatief raakt aan - en loopt vooruit op - governance vraagstukken die worden geadresseerd in de NLCS en RbVS. Dit zal vervolgens in de uitvoering (NIB en CER richtlijn) ook een plek moeten krijgen. Zo zal er bijvoorbeeld met de oprichting van de nieuwe CER ondersteuningsorganisatie naar verwachting ook een loketfunctie worden ingericht (ivm meldplicht en zorgplicht onder de CER).

Voorstel is om dit integraal en in gezamenlijkheid uit te lopen (en hiermee het voorstel voor een EV-loket ook voor nu weg te zetten in de tijd). Dit geeft ook tijd om de voor- en nadelen van een frontoffice bij RVO op het gebied van EV en hoe deze zich verhoudt tot CER, NIB, BTI, cyber, statelijk, kennisveiligheid goed uit te werken en te kijken wat werkbaar en toekomstbestendig is. Daarnaast ook van belang om bij dit initiatief de (wettelijke) taken en rol NCSC in ogenschouw te nemen.

5.1.1b + 5.1.2a +
5.1.2i

[REDACTED]

[REDACTED]

Dep. VERTROUWELIJK

Datum
14 april 2022

5.1.1b

[REDACTED]



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**

Contactpersoon

5.1.2 e

Datum
10 mei 2022

Bijlagen
4

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	10 mei 2022, 16:00-17:30
Vergaderplaats	NCTV

1. Opening en mededelingen

2. Verslag schriftelijke TFEV 4 april 2022

Bijlage 1. Verslag TFEV 04042022

5.1.2i

3. Expertiseteam ScaN (Douane)

Bijlage 2. Beleidsnota scan- en detectieapparatuur Douane

5.1.1b

4. Opvolging inventarisatie EV-loket (EZK)

Bijlage 3. Nota opvolging inventarisatie EV-loket

Bijlage 3a. Rapportage Quicksan RVO EV-loket

5.1.1b + 5.1.2a +
5.1.2i

6. Internationaal/Europees

7. Parlementair

8. Rondvraag en sluiting

Ministerie van Economische Zaken
en Klimaat

TER BESLUITVORMING

Aan
TFEVDirectoraat-generaal
Bedrijfsleven & Innovatie

Auteur

5.1.2e

Datum
29 april 2022Kenmerk
DGBI / 22191901

nota

Opvolging inventarisatie EV-loket

Kopie aan

Bijlage(n)

Aanleiding

Naar wens van de TFEV en in opdracht van EZK heeft de RVO een inventarisatie uitgevoerd van de adviesbehoefte bij bedrijven op het gebied van economische veiligheid en de behoefte aan een EV-loket. Er is geconstateerd dat er behoefte is aan een loket. Nu zal worden gezien hoe hieraan vorm kan worden gegeven.

Beslispunten

- Akkoord op de quick scan van de RVO.
- Akkoord op de vervolgstappen:
 1. Afbakenen van het doel, doelgroep en reikwijdte EV-loket op basis van quick scan en reeds bestaande, en ook de verwachte loketten en contactpunten;
 2. Plan van aanpak opstellen voor operationalisering, inclusief inschatting benodigde financiën en personele capaciteiten;
 3. Het plan en een definitief besluit over inrichten van een loket zal worden geagendeerd in de TFEV na de zomer.

Kernpunten

- De quick scan wijst een aantal dingen uit:
 - Er is behoefte bij bedrijven (met name MKB) aan een adviesloket voor vragen over economische veiligheid;
 - De aspecten binnen EV waarop de voornaamste adviesbehoefte bestaat zijn: export, intellectueel eigendom, vermoedens van beïnvloeding/spionage, opzetten van een buitenlands verkoopkantoor of buitenlandse dochter en buitenlandse reizen door medewerkers.
 - Daarnaast wordt aangegeven dat economische veiligheidsrisico's en vraagstukken (middels het loket) in zijn integraliteit beter bekend zouden moeten worden gemaakt bij bedrijven.
- Voor een aantal van bovengenoemde aspecten binnen EV zijn al loketten of contactpunten bij de Rijksoverheid zijn ingericht.
- Tegelijkertijd lopen een aantal beleidstrajecten zoals bijvoorbeeld rondom aanbestedingen en kennismigranten waarvoor het mogelijk wenselijk is om bedrijven ook via het EV-loket te informeren en adviseren.

- Tenslotte komt er Europese wetgeving aan, inzake weerbaarheid van kritieke entiteiten (CER-richtlijn) en cybersecurity (NIB2-richtlijn) die ook ondersteuningstaken verplichten t.b.v. de weerbaarheid waardoor vraagstukken van een dergelijk loket integraal moeten worden gezien.
- Daarom zal in de vervolgstappen goed moeten worden gekeken naar de precieze scope van een nieuw loket en de samenhang met andere contactpunten en beleidstrajecten.
- De vragen van bedrijven lijken veel overeenstemming te hebben met de vragen die spelen bij kennisinstellingen; beide raken voornamelijk aan ongewenste kennisoverdracht.
- In het vervolgtraject zal daarom in het bijzonder worden gekeken naar aansluiting bij het kennisveiligheidsloket.
- Bovendien zal moeten worden gezien hoe het loket tegemoet kan komen aan de behoefte tot meer bewustwording en voorlichting over EV.

Toelichting

- In de TFEV van december 2021 heeft EZK voorgesteld te inventariseren of er bij het bedrijfsleven behoefte is aan een loket voor vragen rondom economische veiligheid.
- Hierop is door de RVO een quick scan uitgevoerd, bestaande uit 10 interviews en een enquête onder ca. 120 bedrijven.
- De volgende stap is om uit te werken hoe de Rijksoverheid tegemoet kan komen aan de adviesbehoefte bij de bedrijven.
- Een uitbreiding van het kennisveiligheidsloket bij de RVO lijkt hierop een voor de hand liggende optie.
- Er zal echter nog specifiekere moeten worden afgebakend wat het loket wel en niet zal gaan doen en hoe dit aan de achterkant (bijv. door middel van tweedelijns expertise) bij de departementen zal worden belegd.
- Dit zal de komende maanden door EZK, in nauwe afstemming met andere departementen, verder worden verkend.
- Beoogd is om na de zomer een definitief besluit te nemen over de inrichten van het loket, met een concreter beeld van de financiën en benodigde capaciteiten.

Inventarisatie adviesloket economische veiligheid

RVO, V 2.0 29 april 2022

VERTROUWELIJK

Inhoud

Inventarisatie adviesloket economische veiligheid.....	1
Managementsamenvatting	4
Opdracht.....	4
Thema's waarop een adviesbehoefte bestaat	Fout! Bladwijzer niet gedefinieerd.
Randvoorwaarden voor een adviesloket economische veiligheid.....	4
Aanbevelingen inrichting adviesloket economische veiligheid.....	6
Hoofdstuk 1. Aanleiding, opdracht en aanpak.....	7
Aanleiding.....	7
Opdracht.....	7
Aanpak.....	7
Over RVO	10
Leeswijzer	11
Hoofdstuk 2. Context thema economische veiligheid	12
Definitie economische veiligheid	12
Economische veiligheid binnen de organisatie	12
Aspecten van economische veiligheid waar bij bedrijven vragen omtrent risico's spelen.....	13
Contact met de Rijksoverheid	14
Onderdelen van de Rijksoverheid waarmee bedrijven contact hebben.....	15
Beoordeling van het contact met de Rijksoverheid	15
Hoofdstuk 3. Rol en reikwijdte van het expertise- en adviesloket economische veiligheid	16
Adviesbehoefte op gebied van economische veiligheid	16
Thema's waarop een adviesbehoefte bestaat	16
Aanspreekpunten economische veiligheid buiten de Rijksoverheid	17
Randvoorwaarden adviesloket economische veiligheid	17
Soorten informatie waarin een adviesloket zou moeten voorzien.....	17
Hoe zou een adviesloket vorm moeten worden gegeven om van meerwaarde te zijn voor bedrijven?.....	18
Overzicht bestaande, gerelateerde loketfuncties	19
Hoofdstuk 4. Praktische inregeling en synergie met het loket kennisveiligheid	23
Voorkeur contactmogelijkheden.....	23
Redelijke termijn van beantwoording van vragen	23
Gebruik van input vragen loket economische veiligheid voor beleidsontwikkeling.....	24
Hoofdstuk 5. Conclusies en aanbevelingen.....	25
Conclusies.....	25
Aanbevelingen	Fout! Bladwijzer niet gedefinieerd.

VERTROUWELIJK

Managementsamenvatting

Opdracht

Om invulling te geven aan de ambitie van de Taskforce Economische Veiligheid, heeft het Ministerie van Economische Zaken en Klimaat (EZK) RVO gevraagd om een kortlopend onderzoek ('quick scan') uit te voeren naar de vraagstukken rondom economische veiligheid die spelen bij bedrijven en de behoeften die bedrijven hebben ten aanzien van het opzetten van een loket economische veiligheid. Daarnaast is aan RVO verzocht om aanbevelingen te doen over de reikwijdte en praktische inrichting van een loket op gebied van economische veiligheid.

Het onderzoek richt zich op bedrijven die actief zijn in vitale sectoren, en/of beschikken over sensitieve technologie en internationaal actief zijn of willen worden, vanuit de aanname dat bij deze bedrijven een breed scala aan vragen leeft rondom verschillende aspecten op gebied van economische veiligheid.

Behoefte aan een loket economische veiligheid

Uit het onderzoek kan worden geconcludeerd dat er een indirecte behoefte aan een adviesloket economische veiligheid is. Ondanks dat het begrip 'economische veiligheid' niet erg bekend is bij bedrijven, is er wel degelijk behoefte aan een contactpunt met verschillende functies dat kan helpen met vraagbeantwoording op een aantal thema's dat onder 'economische veiligheid' valt.

Thema's

Het thema 'economische veiligheid' als overkoepelend begrip is niet erg bekend is bij bedrijven. Dit bleek uit de diepte-interviews, maar dit zou ook een reden kunnen zijn waarom een grote meerderheid van de respondenten nog geen contact met de Rijksoverheid heeft gehad ten aanzien van 'economische veiligheid' en meer dan de helft van de respondenten niet zou weten met wie ze bij de Rijksoverheid contact zouden moeten opnemen.

Desondanks leeft het thema wel, zodra duidelijk wordt wat welke onderwerpen onder 'economische veiligheid' kunnen worden geschaard (zie tabel 1).

Tabel 1

Onderwerpen waar bedrijven vragen over hebben	Onderwerpen waar bij bedrijven een adviesbehoefte van de Rijksoverheid bestaat
<ul style="list-style-type: none">• Intellectueel eigendom;• Buitenlandse reizen door medewerkers;• Export;• <i>Dual-use</i> of andere sensitieve technologieën;• Aannemen/screenen van medewerkers.	<ul style="list-style-type: none">• Export;• Intellectueel eigendom;• Vermoedens van beïnvloeding/spionage;• Opzetten van een buitenlands verkoopkantoor of een buitenlandse dochter;• Buitenlandse reizen door medewerkers.

Randvoorwaarden

Uit het onderzoek blijkt ook dat er behoefte aan een contactpunt is dat verschillende adviesfuncties kan vervullen op deze thema's. Een adviesloket economische veiligheid zou met name nuttig zijn voor het MKB en zou aan een aantal randvoorwaarden moeten voldoen. Het loket zou de volgende functies moeten hebben:

- **Proactief en reactief:** het loket moet bedrijven stimuleren om over economische veiligheid na te denken en moet hen helpen met de juiste vraagformulering. Dit moet via een algemene website en door middel van één-op-één gesprekken met medewerkers;
- **Algemene en specifieke informatie:** bedrijven hebben zowel behoefte aan algemene informatie zoals tools, checklists en updates, maar zoeken ook advies op maat;
- **Deskundigheid:** medewerkers van het loket dienen of zelf deskundig genoeg te zijn voor vraagbeantwoording of moeten efficiënt kunnen doorverwijzen naar een ander onderdeel van de Rijksoverheid wanneer dit geschikter is om de vraag te beantwoorden.
- **Vindbaarheid, bereikbaarheid en responsiviteit:** het loket moet goed vindbaar en bereikbaar zijn. Bedrijven verwachten een reactie binnen één of twee weken.

VERTROUWELIJK

Aanbevelingen inrichting adviesloket economische veiligheid

Op basis van de resultaten van het kortlopende onderzoek 'adviesloket economische veiligheid', te weten de antwoorden op de vragenlijst alsook de diepte-interviews die zijn afgenomen zoals besproken in Hoofdstuk 2 t/m 4 en de conclusies zoals besproken in Hoofdstuk 5, worden hier een aantal aanbevelingen gedaan ten aanzien van de reikwijdte en praktische inrichting van een adviesloket economische veiligheid, alsook hoe het huidige Loket Kennisveiligheid kan worden uitgebouwd.

1. Maak het onderwerp '**economische veiligheid**' in zijn **integraliteit** zichtbaarder bij bedrijven. Het loket moet hiervoor actief bedrijven gaan benaderen en voorlichten. Daarbij is het van belang om uit te leggen aan bedrijven **wáarom** het onderwerp in zijn integraliteit moet worden gezien. Zoek hierbij de synergiën op met lokale en regionale overheden, andere overheidsinstanties, alsook met brancheorganisaties.
2. Gebruik de behoefte-inventarisatie op gebied van thema's als leidraad voor welke informatie er beschikbaar moet worden gesteld door het loket. Zorg er daarbij voor dat het loket optimaal gebruik maakt van **reeds bestaande adviesmogelijkheden** bij de Rijksoverheid zodat het loket een efficiëntieslag betekent voor bedrijven. Dat betekent extra inzet om informatie beschikbaar te stellen op prioriteitsthema's waar nog weinig advies over beschikbaar is, maar met name verwijzen naar andere aanspreekpunten indien deze er al zijn. Breid het overzicht in Hoofdstuk 4 uit als onderdeel van het opzetten van het loket en zoek daarbij ook de synergiën op met lokale en regionale overheden, alsook met brancheorganisaties.
3. Richt het loket in eerste instantie op **kennisintensieve, internationaal actieve bedrijven binnen het MKB**, waar de behoefte ligt. Hierdoor kunnen inhoud en expertise scherper worden afgesteld dan wanneer de doelgroep bedrijven van alle groottes beslaat.
4. Zorg voor een **efficiënte en effectieve vraagafhandeling**, waarbij de duur van de beantwoording maximaal twee weken is en het streven is om vragen binnen één week te beantwoorden.
5. Zorg voor voldoende **deskundigheid** bij medewerkers van het adviesloket zodat zij vragen zelf kunnen beantwoorden of bedrijven kunnen doorverwijzen.
6. Gebruik een website voor **algemene informatie** en biedt tegelijkertijd de mogelijkheid om **maatwerk** te leveren. Dit is voor bedrijven van grote meerwaarde.
7. Het **Loket Kennisveiligheid** biedt op een deel van de thema's die in dit onderzoek naar voren komen aanknopingspunten. Het is dan ook te verwachten dat vragen van kennisinstellingen en bedrijven voor een deel overlappen. Indien de wens bestaat om beide loketten samen te voegen dan dient niet alleen goed te worden gekeken naar het aanvullen van het Loket Kennisveiligheid met de juiste informatie en expertise, maar moet ook vooral worden gelet op naamgeving en communicatie zodat het thema 'economische veiligheid' als zodanig goed onder de aandacht kan worden gebracht.
8. Tot slot: start met een **pilot** van het loket en evalueer deze na een periode van 6-12 maanden. Deze 'quickscan' schetst een goed eerste beeld, maar gezien de breedte van het onderwerp en de grootte van de doelgroep is het verstandig om te werken met een eerste aanloopfase. Wees hier als Rijksoverheid transparant over naar bedrijven toe en vraag aan hen om mee te denken en te helpen evalueren.

Hoofdstuk 1. Aanleiding, opdracht en aanpak

Aanleiding

Sinds januari 2022 is het Rijksbrede Loket Kennisveiligheid¹ operationeel. Het opzetten van dit loket was één van de maatregelen die in de Kamerbrief kennisveiligheid hoger onderwijs en wetenschap van november 2021² is aangekondigd om de kennisveiligheid in het hoger onderwijs en de (toegepaste) wetenschap beter te borgen. Hiertoe is door RVO in opdracht van het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) een inventarisatie uitgevoerd om de behoeften en wensen van het Nederlandse kennisveld en aanbevelingen ten behoeve van het opzetten van een expertise- en adviesloket kennisveiligheid te peilen.

De Taskforce Economische Veiligheid³ heeft naar aanleiding van het opzetten van het Loket Kennisveiligheid in december 2021 interdepartementaal de ambitie uitgesproken om te onderzoeken of het wenselijk is om dit loket uit te bouwen met een Loket Economische Veiligheid, waar naast instanties uit het hoger onderwijs en (toegepaste) wetenschap ook bedrijven terecht kunnen met vragen over onder meer kansen, risico's en praktische aspecten met betrekking tot economische veiligheid.

De reden hiervoor is dat er op dit moment geen centraal, Rijksbreed aanspreekpunt is voor bedrijven die vragen hebben over economische veiligheid. Dit zou kunnen betekenen dat vragen op dit moment niet gesignaleerd en/of niet beantwoord worden, met als potentieel gevolg dat niet alleen bedrijfsbelangen, maar ook de nationale veiligheid in het geding komen.

Opdracht

Om invulling te geven aan de ambitie van de Taskforce Economische Veiligheid, heeft het Ministerie van Economische Zaken en Klimaat (EZK) RVO gevraagd om een kortlopend onderzoek ('quick scan') uit te voeren naar de vraagstukken rondom economische veiligheid die spelen bij bedrijven en de behoeften die bedrijven hebben ten aanzien van het opzetten van een loket op gebied van economische veiligheid. Daarnaast is aan RVO verzocht om aanbevelingen te doen over de reikwijdte en praktische inrichting van een loket op gebied van economische veiligheid.

Het onderzoek richt zich op bedrijven die actief zijn in vitale sectoren, en/of beschikken over sensitieve technologie en internationaal actief zijn of willen worden, vanuit de aanname dat bij deze bedrijven een breed scala aan vragen leeft rondom verschillende aspecten op gebied van economische veiligheid.

Aanpak

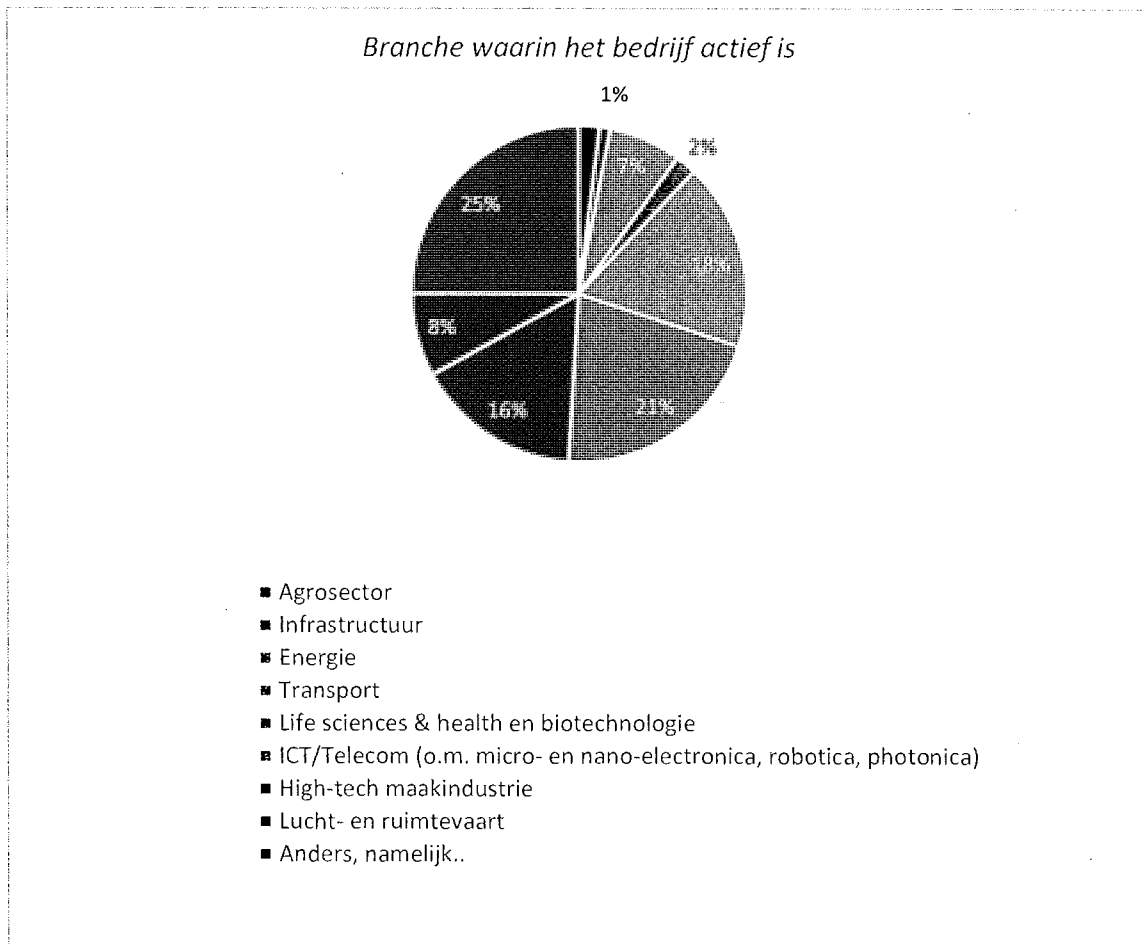
De resultaten van het onderzoek zijn gebaseerd op een online enquête, verspreid onder bedrijven die actief zijn in vitale sectoren, en/of beschikken over sensitieve technologie en internationaal actief zijn of willen worden. Daarnaast zijn diepte-interviews gehouden met 10 bedrijven die ook binnen deze groep vallen, variërend in sector en grootte. De enquête stond open van 22 maart tot en met 7 april 2022. Binnen deze periode hebben in totaal 119 respondenten de enquête ingevuld. De enquête is onder meer ingevuld door bedrijven in de sectoren ICT (21%), Life sciences & health en biotechnologie, en high-tech maakindustrie (16%) (figuur 1). Opvallend is dat 25% van de

¹ <https://www.loketkennisveiligheid.nl/>

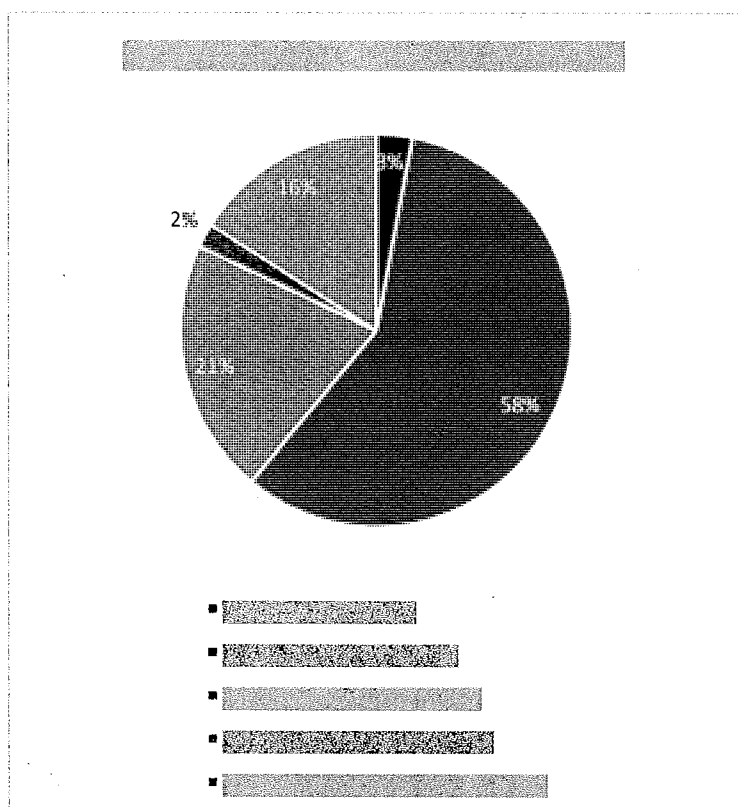
² <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/27/kennisveiligheid-hoger-onderwijs-en-wetenschap>

³ De Taskforce Economische Veiligheid bestaat uit vertegenwoordigers van de Ministeries van Justitie en Veiligheid (NCTV), Economische Zaken en Klimaat, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, Defensie, Financiën, de AIVD en de MIVD.

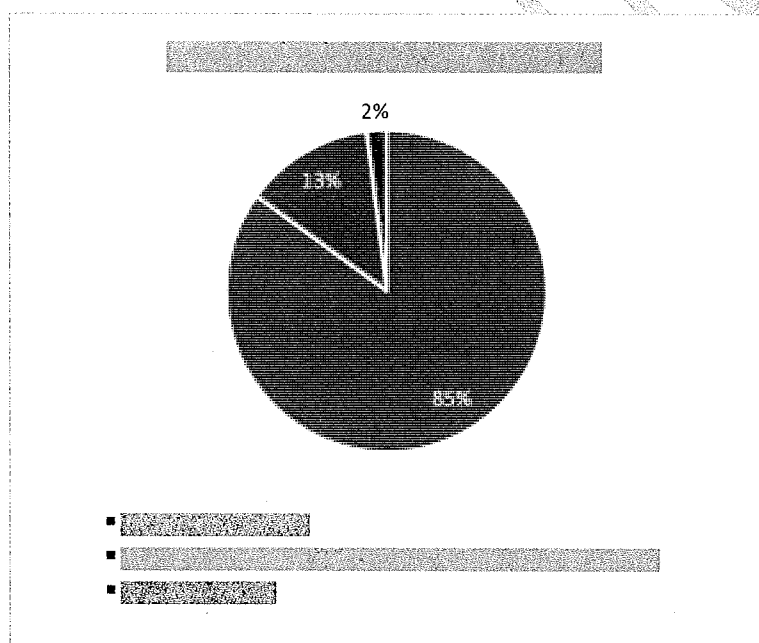
respondenten 'Anders' heeft ingevuld. Uit de antwoorden die binnen deze categorie worden gegeven blijkt dat 8% van het totaal aan respondenten in de zakelijke of technische dienstverlening actief is. Ook komt uit de enquête naar voren dat de meerderheid van de respondenten (58%) werkzaam is binnen een bedrijf met 2-50 werkzame personen (figuur 2). Het grootste deel van de respondenten heeft de enquête namens het gehele bedrijf ingevuld (figuur 3). 34% van de respondenten werkt op gebied van onderzoek en ontwikkeling en 32% van de respondenten kwalificeert zichzelf als 'directie' of 'management' (zo blijkt uit open antwoorden in de categorie 'Anders') (figuur 4).



Figuur 1



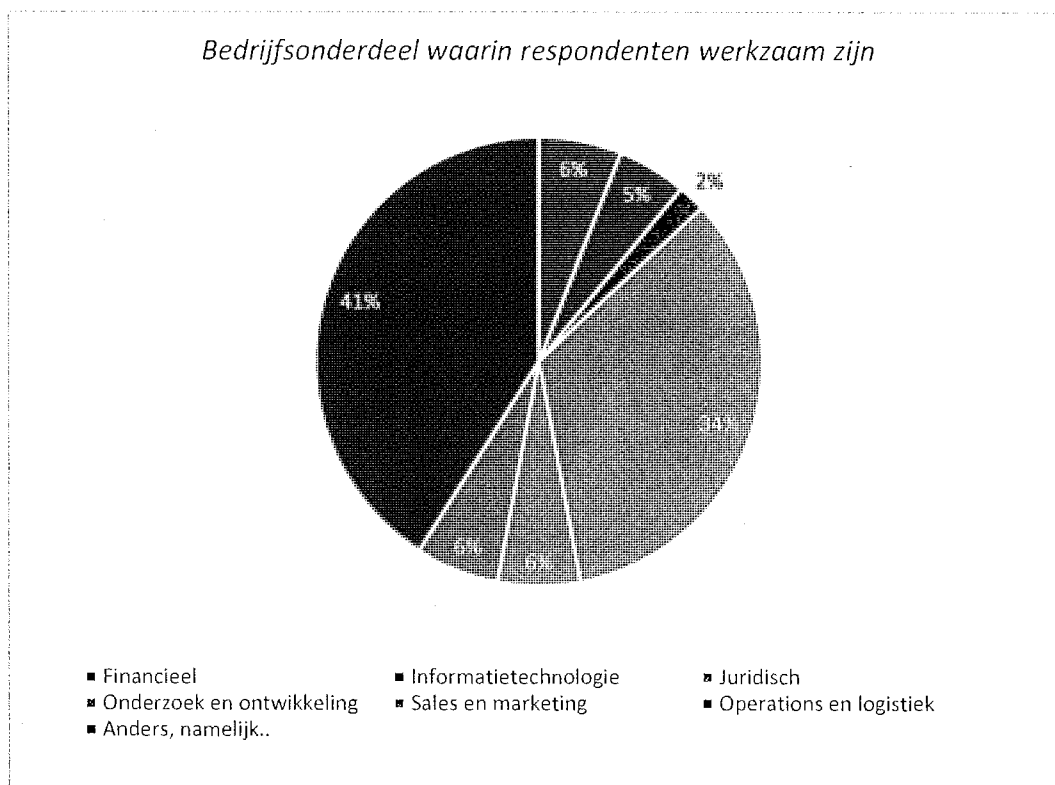
Figuur 2



Figuur 3

5.1.1c

5.1.1c



Figuur 4

Over RVO

De Rijksdienst voor Ondernemend Nederland (RVO) voert beleid uit van de Ministeries ter bevordering van een uitstekend ondernemersklimaat. Dit zijn opdrachten die ondernemende Nederlanders en beleidsmedewerkers vooruithelpen op het gebied van duurzaamheid, zakendoen over de grenzen, agrarisch ondernemen en innovatie, zowel binnen Nederland als daarbuiten. RVO biedt hiertoe voorlichting en advies, financiering, de juiste contacten of is sparringpartner. Er wordt dan ook veel samengewerkt met Nederlandse internationale partners, waaronder kennisinstellingen, MKB en topsectoren.

RVO heeft ruime ervaring met het opstellen van rapportages, uitvoeren van onderzoeken én de inrichting van loketten. In 2019-2020 is binnen de directie Internationale Programma's het onderzoek 'Verkenning wetenschappelijke samenwerking Nederlandse en Chinese kennisinstellingen' uitgevoerd. In 2020 is in opdracht van het Ministerie van OCW de inventarisatie kennisveiligheid uitgevoerd zoals hierboven beschreven.

De uitvoering van deze 'quick-scan' is, net als de inventarisatie kennisveiligheid, ondergebracht bij Team Internationale Research en Innovatiesamenwerking (IRIS). Dit team binnen de afdeling Internationaal Innoveren heeft als één van de voornaamste taken het geven van advies over Europese financieringsinstrumenten (waaronder Horizon Europe en Eurostars/Eureka) aan kennisinstellingen en bedrijven.

Team IRIS beschikt hierdoor over een uitgebreid netwerk van bedrijven, bijvoorbeeld op gebied van High Tech Systemen en Materialen (HTSM) en sleuteltechnologieën (waaronder kunstmatige intelligentie, sensoren, fotonica-, nano- en quantumtechnologie) en is goed op de hoogte van ontwikkelingen in het veld.

Leeswijzer

In Hoofdstuk 1 wordt de aanleiding, opdracht en aanpak van het onderzoek besproken. In Hoofdstuk 2 wordt ingegaan op de definitie van economische veiligheid en bij welke aspecten van economische veiligheid er bij bedrijven vragen spelen. Ook wordt hier het contact met de Rijksoverheid dat bedrijven hebben besproken. Hoofdstuk 3 gaat in op de adviesbehoefte van bedrijven ten aanzien van economische veiligheid en de randvoorwaarden waar een adviesloket economische veiligheid volgens bedrijven aan zou moeten voldoen. Ook wordt hier een globaal overzicht gegeven van reeds bestaande loketfuncties. In hoofdstuk 4 wordt, uitgaande van de inrichting van een adviesloket economische veiligheid, besproken hoe het loket praktisch ingeregeld kan worden. Tot slot worden in Hoofdstuk 5 de conclusies van het onderzoek besproken en worden er een aantal aanbevelingen gedaan ten aanzien van de inrichting van een adviesloket economische veiligheid. In dit rapport is één bijlage opgenomen, te weten de volledige vragenlijst die is gebruikt voor de enquête.

VERTROUWELIJK

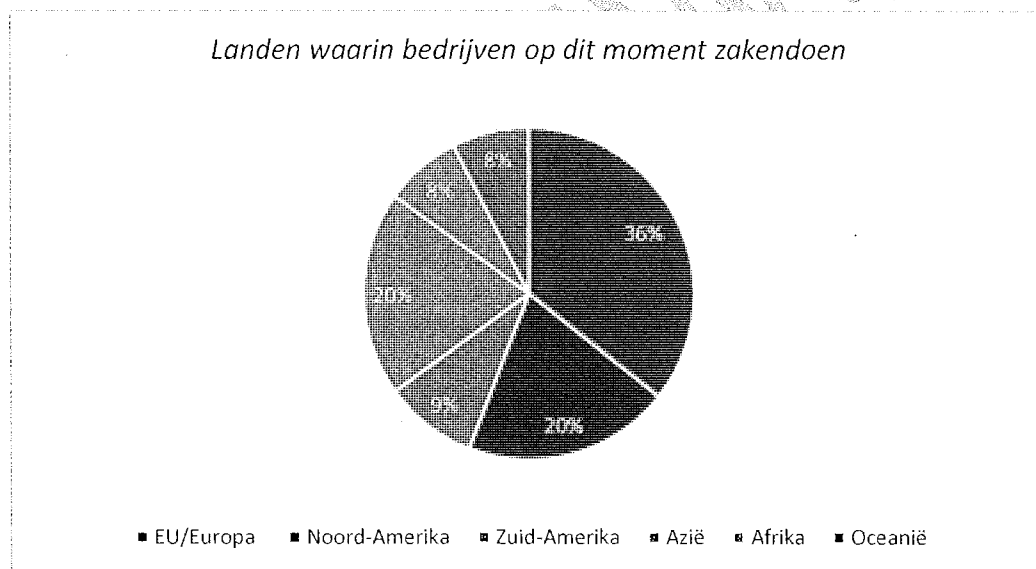
Hoofdstuk 2. Context thema economische veiligheid

Definitie economische veiligheid

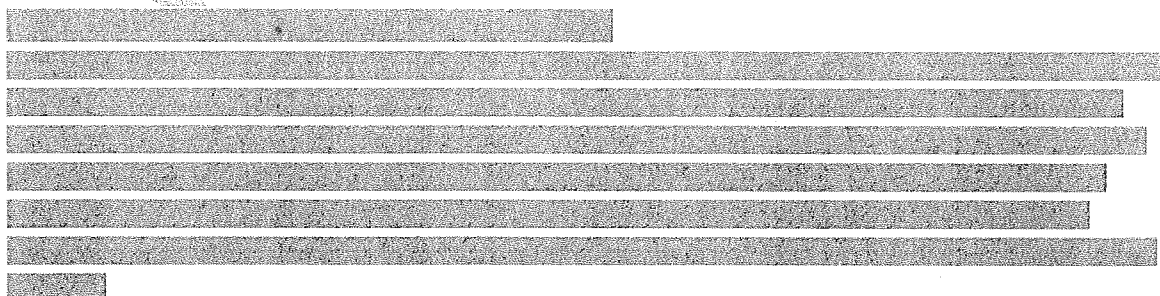
Ten behoeve van dit onderzoek wordt onder economische veiligheid verstaan 'het ongestoord functioneren van Nederland als een effectieve en efficiënte economie' (Nationale Veiligheid Strategie, 2019). Bedreigingen van economische veiligheid kunnen uiteenlopend van aard zijn: het kan gaan om risico's voor vitale processen, risico's op de vertrouwelijkheid en integriteit van gevoelige kennis en informatie of over ongewenste strategische afhankelijkheden. Voor bedrijven kunnen die risico's zich bijvoorbeeld voordoen bij het opzetten van een dochter in het buitenland of bij een investering door een ongewenst bedrijf. In de diepte-interviews is deze definitie besproken en werd deze aangevuld door een aantal geïnterviewden: als voorbeelden van aspecten van economische veiligheid werden ook het niet verkrijgen van cruciale technologie uit het buitenland, het niet kunnen leveren van technologie aan andere landen, en de impact van sancties op Nederlandse bedrijven, genoemd. Uit de diepte-interviews komt ook naar voren dat bedrijven niet goed bekend zijn met 'economische veiligheid' als overkoepelend begrip, aangezien vaak werd gevraagd om dit begrip uit te leggen.

Landen waarin bedrijven actief zijn

Uit de enquête blijkt dat bedrijven het meest zaken doen in Europa/de EU (36%) en daarna in Noord-Amerika en Azië (ieder 20%) (figuur 5). Individuele landen binnen deze regio's die het vaakst werden genoemd zijn Duitsland, de Verenigde Staten en China.



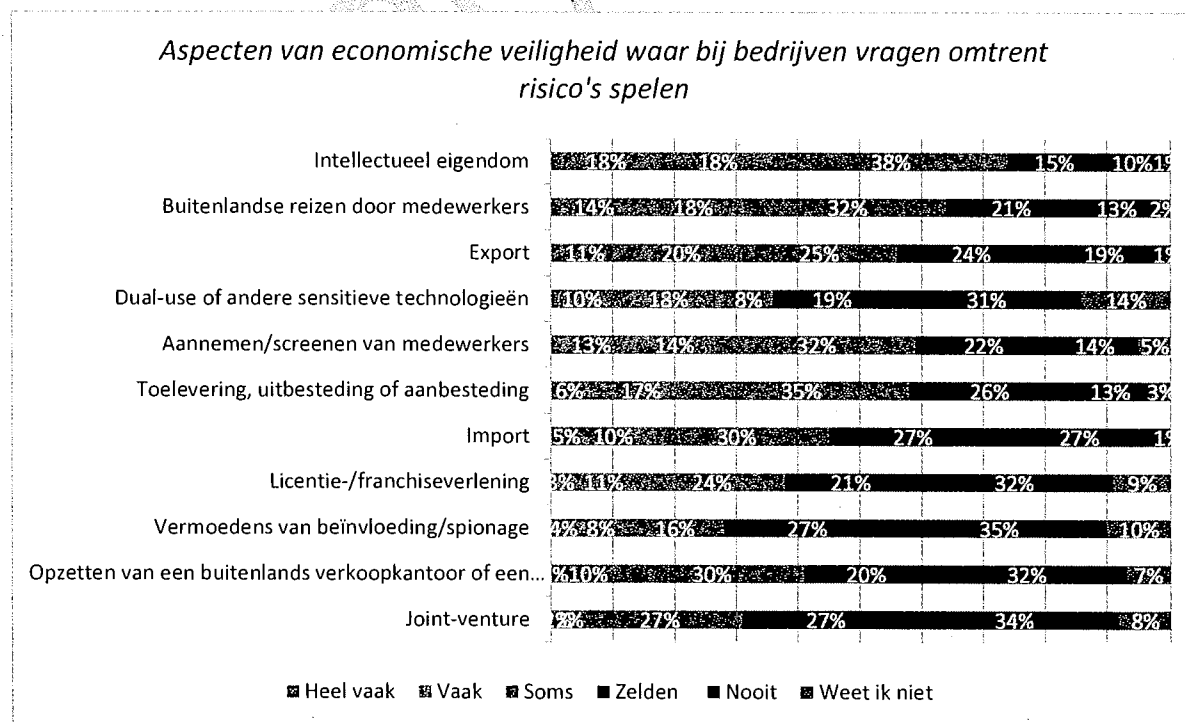
Figuur 5



5.1.1c

Aspecten van economische veiligheid waar bij bedrijven vragen omtrent risico's spelen
In onderstaand diagram (figuur 7) zijn de aspecten van economische veiligheid weergegeven waarbij bedrijven vragen omtrent risico's spelen. Hierbij dient te worden opgemerkt dat het hierbij niet gaat om de aspecten waarbij advies van de overheid wordt gevraagd. Hieruit komen de volgende thema's naar voren waarbij de meeste vragen spelen omtrent risico's ('heel vaak' en 'vaak' bij elkaar opgeteld):

1. Intellectueel eigendom;
2. Buitenlandse reizen door medewerkers;
3. Export;
4. Dual-use of andere sensitieve technologieën;
5. Aannemen/screenen van medewerkers.



Figuur 7

Een aantal respondenten noemde in de enquête nog andere aspecten van economische veiligheid waaromtrent vragen spelen. Daarnaast is ook in de diepte-interviews naar deze aspecten gevraagd. Zowel in de interviews als in enquête werd **cybersecurity** vaak genoemd als terugkerend thema waardoor risico's zoals spionage ontstaan. In de interviews werd **intellectueel eigendom** vaak genoemd, waarbij [REDACTED] een aantal keer werd genoemd als risicoland (bijvoorbeeld in de vorm van een shop-in-shop).

5.1.2a

Omgaan met buitenlandse investeerders werd een aantal keer genoemd. Bijvoorbeeld in de context van intellectueel eigendom (als er gevoelige informatie wordt uitgewisseld met investeerders uit derde landen) of wanneer er een risico is op *dual-use* van technologieën. Een geïnterviewde gaf daarbij aan dat er voor hightech in Nederland weinig investeerders zijn en een andere geïnterviewde uitte bezorgdheid over de gevolgen die de Wet Veiligheidstoets investeringen, fusies en overnames (Vifo) zou hebben op het aantrekken van Aziatische investeerders. In dit verband werd ook één keer **de rol van aandeelhouders bij toeleveranciers** genoemd

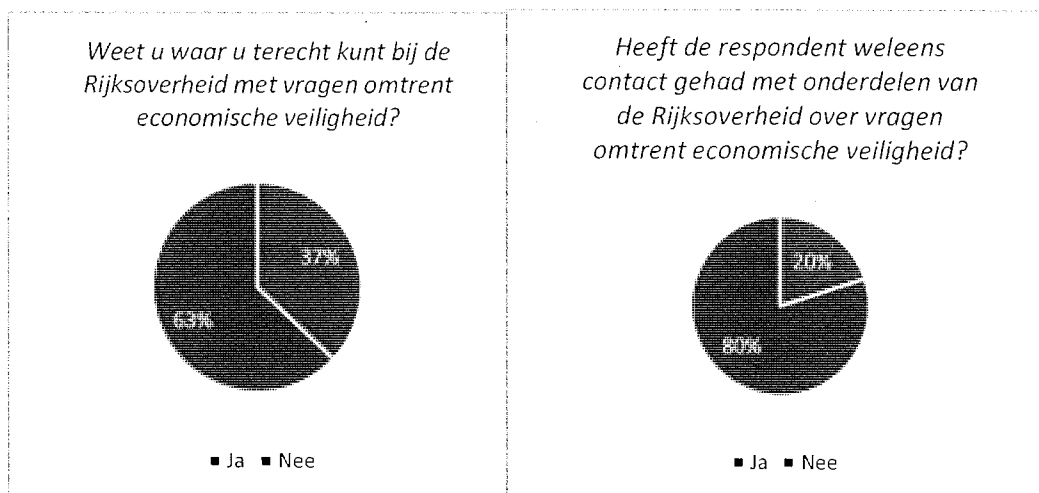
Het **aannemen/screenen van buitenlandse medewerkers** is voor veel bedrijven noodzakelijk omdat er niet genoeg personeel in Nederland beschikbaar is, maar zeker bij medewerkers uit derde landen is het lastig om goed te screenen.

Export(controle) werd een aantal keer genoemd in de interviews. Een aantal bedrijven is zeer sterk afhankelijk van export en de invloed van geopolitieke ontwikkelingen en de hieraan verbonden strategische autonomie zijn thema's die leven.

Het **acquireren van dochterondernemingen** en de **fysieke veiligheid** van het bedrijf werden één keer genoemd in de interviews. Aanvullend op de resultaten die in figuur 7 te zien zijn, bevestigen bovenstaande thema's de diversiteit van het begrip economische veiligheid.

Contact met de Rijksoverheid

Een ruime meerderheid van de respondenten weet niet waar ze bij de overheid terecht zouden kunnen met vragen omtrent economische veiligheid (figuur 8). Een aantal respondenten geeft in de toelichting aan niet te weten waar ze zouden moeten aankloppen of geen noodzaak te hebben gezien om naar de Rijksoverheid te stappen. 80% van de respondenten heeft nog geen contact gehad met onderdelen van de Rijksoverheid met vragen omtrent economische veiligheid. De geïnterviewden hebben wat vaker contact met de Rijksoverheid, maar gaven ook aan veel met commerciële partijen te werken (bijvoorbeeld voor business development in het buitenland of het toetsen van de bedrijfsactiviteiten aan het sanctiebeleid ten aanzien van Rusland) en veel informatie online bij elkaar te zoeken (waarbij de informatie dan vaak van consultancy- of accountancy-bureaus komt).



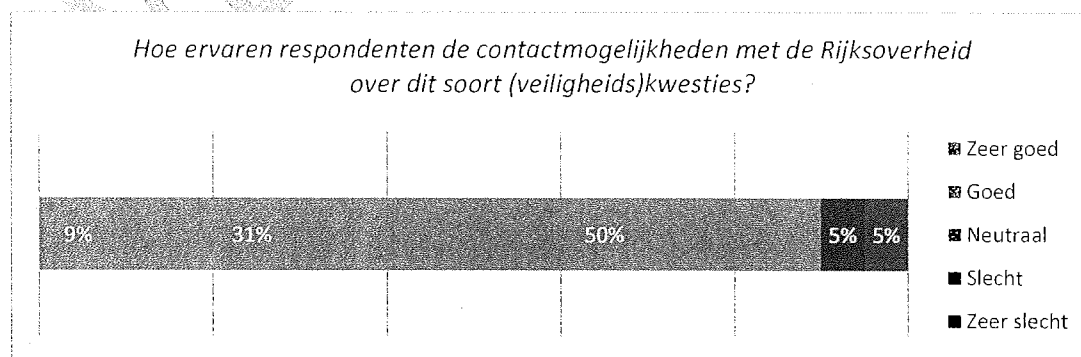
Figuur 8

Onderdelen van de Rijksoverheid waarmee bedrijven contact hebben
 Wanneer er wél contact is geweest met onderdelen van de Rijksoverheid over vragen omtrent economische veiligheid, dan is dit met een groot aantal verschillende partijen. Dit blijkt zowel uit de enquête als uit de diepte-interviews. Onderdelen van de Rijksoverheid waarmee contact is of is geweest:

- Inlichtingendiensten (AIVD en MIVD);
- Ministeries: BZ (onder meer IMH, ambassades), EZK (onder meer Commissariaat Militaire Productie (CMP) en Bureau Toetsing Investerings), OCW, Def, I&W, J&V (onder meer Nationaal Cyber Security Centrum (NCSC) en Immigratie- en Naturalisatiedienst (IND));
- RVO;
- Nationale Politie;
- Belastingdienst (Douane, Centrale Dienst In- en Uitvoer (CDIU)).

Beoordeling van het contact met de Rijksoverheid

Een klein aantal van de respondenten (10%) geeft aan het contact met de overheid als slecht of zeer slecht te ervaren (zie figuur 8). De helft van de respondenten geeft aan het contact als neutraal te ervaren. Uit de diepte-interviews komt naar voren dat men het contact vaak als positief ervaart waarbij werd opgemerkt dat de Nederlandse overheid heel benaderbaar is en dat er gemakkelijk informeel kan worden getoetst. Wel werd een aantal keer genoemd dat de aanspreekpunten erg versnipperd zijn.



Figuur 9

Hoofdstuk 3. Rol en reikwijdte van het expertise- en adviesloket economische veiligheid

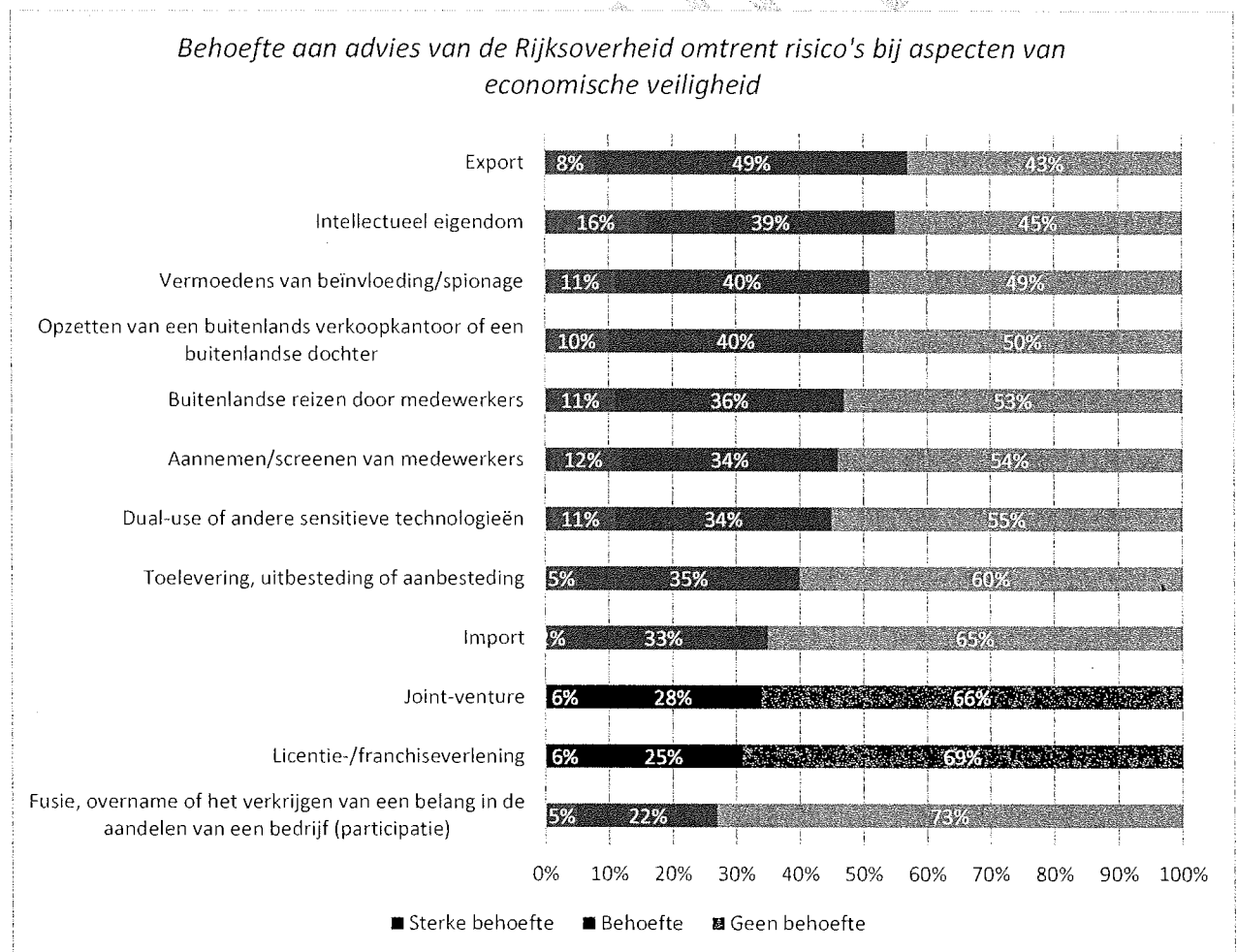
Adviesbehoefte op gebied van economische veiligheid

Aan bedrijven is gevraagd bij welke aspecten zij behoefte hebben aan advies van de Rijksoverheid ten aanzien van economische veiligheidsrisico's. In Hoofdstuk 2 van dit rapport werden de antwoorden besproken op de vraag op welke thema's er vragen spelen bij bedrijven als het gaat om economische veiligheidsrisico's. De vraag in dit hoofdstuk gaat specifiek in op de adviesbehoefte van bedrijven.

Thema's waarop een adviesbehoefte bestaat

Hieruit komen de volgende thema's naar voren waarbij de grootste adviesbehoefte is omtrent economische veiligheidsrisico's ('heel vaak' en 'vaak' bij elkaar opgeteld) (figuur 10):

1. Export;
2. Intellectueel eigendom;
3. Vermoedens van beïnvloeding/spionage;
4. Opzetten van een buitenlands verkoopkantoor of een buitenlandse dochter;
5. Buitenlandse reizen door medewerkers.



Figuur 10

Het overgrote deel van de respondenten (89%) geeft aan geen vragen te hebben over onderwerpen anders dan genoemd in de vragenlijst. Wel werd door één respondent verzocht om een goed beeld van **definities van economische veiligheid**. Door een andere respondent werd gevraagd of informatie kan worden gegeven over **prijzontwikkelingen** (bijvoorbeeld van grondstoffen). Ook **energievoorziening, klimaatontwrichting, economische ongelijkheid en Brexit** werden genoemd door individuele respondenten als thema's waarop er een adviesbehoefte is.

Een aantal keer genoemd door respondenten, maar ook in de diepte-interviews, is het thema **cybersecurity** als onderwerp waar bedrijven vragen over hebben. Een geïnterviewde gaf bijvoorbeeld aan dat het nuttig zou zijn om een checklist te hebben met *best practices* op dit gebied.

Daarnaast komen uit de diepte-interviews de volgende thema's naar voren waar een adviesbehoefte op bestaat:

- De impact van **economische sancties**, alsook een behoefte aan financiële hulp om de impact hiervan op te vangen;
- Advies over **aannemen/screenen van medewerkers**: daarbij noemt één respondent als voorbeeld het geven van trainingen aan HR-afdelingen;
- Advies over **strategische onafhankelijkheid** en in dat verband beperkingen op buitenlandse investeringen;
- Op het gebied van **export** is er behoefte aan begeleiding in het zakendoen in het buitenland, bijvoorbeeld in China. Dit zou bijvoorbeeld een overzicht kunnen zijn van partijen die bedrijven hierin kunnen begeleiden. Daarbij werd ook opgemerkt dat handelsmissies nuttig zijn voor de beeldvorming rondom risico's.

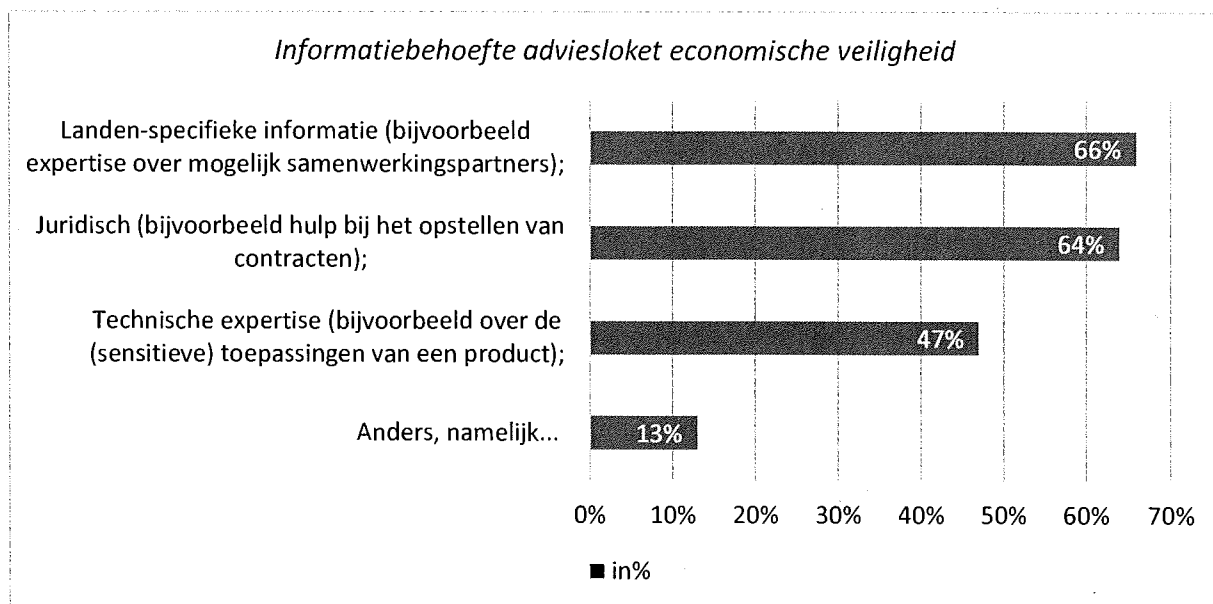
Aanspreekpunten economische veiligheid buiten de Rijksoverheid

Ondanks dat dit geen specifieke vraag was, vroegen een geïnterviewde personen zich af of de Rijksoverheid het meest geschikte aanspreekpunt is voor vragen op gebied van economische veiligheid. Zo werden lokale en regionale partijen (bijvoorbeeld gemeenten en provincies, maar ook regionale ontwikkelmaatschappijen) genoemd als mogelijke partners. Waarbij werd opgemerkt dat gemeenten en provincies op dit moment niet goed op de hoogte zijn, maar dat er vanuit regionale ontwikkelmaatschappijen al één en ander gebeurt op gebied van economische veiligheidsthema's. Daarnaast werd de Kamer van Koophandel genoemd als een plek waar een adviesloket zou moeten worden ondergebracht. Ook zijn brancheorganisaties goed te bereiken voor bedrijven, zowel voor grote bedrijven en voor MKB.

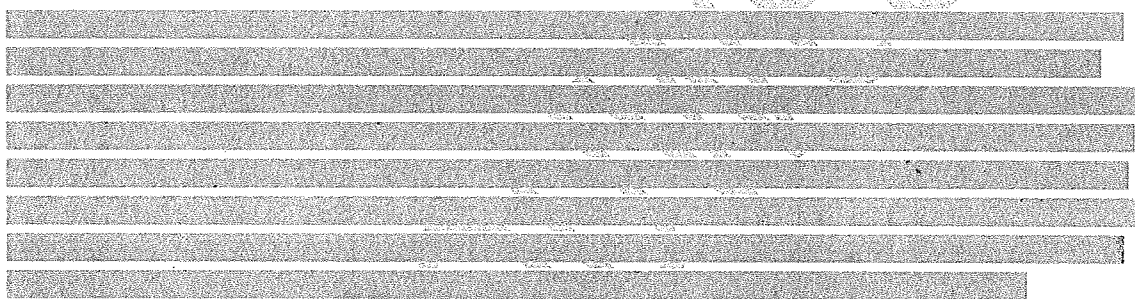
Randvoorwaarden adviesloket economische veiligheid

Soorten informatie waarin een adviesloket zou moeten voorzien

Indien er een adviesloket Economische Veiligheid zou komen, zouden respondenten graag de volgende soorten informatie ontvangen (figuur 11):



Figuur 11



5.1.2f

Hoe zou een adviesloket vorm moeten worden gegeven om van meerwaarde te zijn voor bedrijven?

In de enquête is de open vraag aan respondenten gesteld wanneer een adviesloket echt van meerwaarde is. Hier heeft 22% van de respondenten een antwoord gegeven. Daarnaast is er in de diepte-interviews uitgebreid ingegaan op deze vraag. Uit de enquête en de diepte-interviews komt een aantal elementen naar voren waar het adviesloket aan zou moeten voldoen om meerwaarde te hebben. Daarbij variëren deze elementen onder meer in de mate van pro-activiteit die bedrijven van de overheid verwachten.

- Het loket moet **vindbaar** zijn en er moet duidelijk worden gecommuniceerd wat er van het loket kan worden verwacht.
- Ofwel **deskundigheid** bij het loket zelf waarborgen waarbij één case manager de antwoorden verzameld op een bepaalde vraag. Ofwel efficiënt **doorverwijzen** naar bestaande contactpunten waardoor bedrijven minder last hebben van bestaande versnippering op gebied van economische veiligheid. Bijvoorbeeld via een stroomschema of direct contact.
- Aanbieden van **praktische informatie op maat**: een adviesloket zou bijvoorbeeld op verzoek een **scan of risico-inschatting** moeten kunnen doen voor potentiële zakenpartners (vooral voor kleine bedrijven ontbreekt het vaak aan middelen hiervoor). Of het loket zou een bedrijf moeten kunnen leren hoe het die risico-inschatting zelf kan doen.
- Aanbieden van **algemene, strategische informatie**, bijvoorbeeld in de vorm van checklists, kwartaalscans van risico's in vitale sectoren, jaarlijkse rapportage met risico's, adviezen en

regelgeving, aankomende relevante Nederlandse- en EU-wetgeving en geopolitieke ontwikkelingen. Hierbij belangrijk om een goede zoekfunctie te waarborgen.

- **Bereikbaarheid** (liefst persoonlijk kunnen benaderen of terug gebeld worden), **toegankelijkheid** en **responsiviteit** (vaak snelle terugkoppeling nodig) zijn van belang.
- Aanbieden van **specifieke informatie**, die **up-to-date** is en **compleet**. Er is behoefte aan informatie waar het bedrijfsleven anders geen toegang tot heeft, alsook de mogelijkheid om te worden gekoppeld aan andere bedrijven die ervaringen kunnen delen. Een andere optie zou het publiceren van *use cases* of *best practices* kunnen zijn.
- Het loket moet **met één stem spreken** namens de Rijksoverheid: het is belangrijk dat bedrijven niet met tegenstrijdige informatie worden geconfronteerd.
- **Bedrijven stimuleren om over economische veiligheid na te denken en hen helpen de juiste vragen te stellen** : actief bedrijven benaderen om hen voor te lichten over economische veiligheid en bijbehorende risico's, alsook welke partijen bedrijven hierbij kunnen helpen. Bijvoorbeeld door nieuwsbrieven, bezoeken van bedrijven, masterclasses organiseren of het aanbieden van checklists.
- MKB-bedrijven de mogelijkheid bieden om met de overheid in gesprek te gaan over **beleidsontwikkeling**.
- De **doelgroep beperken**: een loket heeft meerwaarde voor MKB, niet voor grote bedrijven. Grote bedrijven hebben intern afdelingen en compliance-trainingen, alsook al een bestaand netwerk binnen de overheid.

Een klein deel van de respondenten van de gehele enquête (8%) geeft expliciet aan geen behoefte te hebben aan een adviesloket. In de diepte-interviews gaven de grote bedrijven aan geen behoefte te hebben aan een adviesloket economische veiligheid aangezien zij al binnen het bedrijf over voldoende expertise en mankracht beschikken op dit terrein.

Overzicht bestaande, gerelateerde loketfuncties

Een aantal respondenten van de enquête gaf aan dat een adviesloket niet nodig is, maar dat beter gebruik zou kunnen worden gemaakt van bestaande loketten. In de enquête is niet gevraagd naar een overzicht van welke adviesloketten respondenten gebruik maken. Dit element van het onderzoek is na afloop van het uitzetten van de enquête en het afnemen van de interviews toegevoegd. Hieronder (tabel 2) wordt een kort overzicht gegeven van adviesloketten die gerelateerd zijn aan economische veiligheid. Daarbij is alleen gekeken naar loketten die onderdeel uitmaken van de Rijksoverheid en die daarom gratis en openbaar toegankelijk zijn. Dat betekent dat loketten van gemeenten en provincies, of die georganiseerd zijn vanuit koepel- of brancheorganisaties en waarvoor een betaald abonnement moet worden afgesloten, zoals de MKB Servicedesk, hierin niet zijn meegenomen.

Bij de loketten is gekeken of en wat voor informatie er beschikbaar is ten aanzien van de zes meest genoemde onderwerpen waar bedrijven adviesbehoefte op hebben (zie onder hoofdstuk 3), te weten: export; intellectueel eigendom; vermoedens van beïnvloeding/spionage; opzetten van een buitenlands verkoopkantoor of een buitenlandse dochter; buitenlandse reizen door medewerkers; en het aannemen/screenen van medewerkers. Daarnaast is gekeken naar cybersecurity als thema omdat dit zowel in de enquête als in de diepte-interviews vaak werd genoemd, maar dit geen onderdeel was van de keuzes in de vragenlijst. Door het karakter van dit onderzoek ('quick scan') is dit overzicht niet uitputtend, maar schetst het een globaal beeld van waar bedrijven op dit moment al terecht kunnen met vragen.

Tabel 2

Naam en organisatie	Economische veiligheidsthema's	Economische veiligheid als integraal thema?	Website en beschrijving
Ondernemersplein (initiatief van Min EZK en Min BZK; partners: KVK, Belastingdienst, CBS, Min SZK, RDW, RVO, UWV, VNG, Rijksoverheid.nl, Min EZK)	Alle thema's (algemene informatie met verwijzingen naar specifieke loketten/informatiebronnen)	Nee	https://ondernemersplein.kvk.nl/ <i>Via Ondernemersplein.kvk.nl vindt u informatie en advies van de (semi-)overheid. Alles wat u nodig heeft om te ondernemen. Wetgeving, belastingregels maar ook subsidies, ondernemersevenementen en branche-informatie. Door onze krachten te bundelen met die van KVK, kunnen wij u nog beter voorzien van informatie en advies van de overheid. Zo houdt u meer tijd over om te ondernemen.</i>
Bureau Toetsing Investerings (BTI), per 1 september 2022 (Min EZK)	Investerings, fusies en overnames	Ja	Home Bureau Toetsing Investerings <i>Het Bureau Toetsing Investerings (BTI) beoordeelt of meldingen van investeringen, fusies en overnames een risico kunnen ontstaan voor de nationale veiligheid. Als er risico's blijken te zijn adviseert het de minister(s) met welke proportionele maatregelen deze beheersbaar gemaakt kunnen worden.</i>
RVO	Alle thema's	Nee	Rijksdienst voor Ondernemend Nederland (rvo.nl) <i>Wij helpen ondernemende Nederlanders en beleidsmedewerkers vooruit op het gebied van duurzaamheid, zakendoen over de grenzen, agrarisch ondernemen en innovatie. Samen met onze partners maken we Nederland economisch sterker en duurzamer.</i>
Informatie- en Contactpunt China (RVO)	Zakendoen in China	Nee	https://www.rvo.nl/onderwerpen/overheden/informatie-contactpunt-china <i>Nederlandse decentrale overheden en de Trade and Innovate NL-partners (TINL) kunnen voortaan terecht bij het Informatie- en Contactpunt (ICP). Krijgt u een verzoek vanuit China voor een economisch of zakelijk bezoek? Dan kan het ICP u helpen.</i>

Sanctieloket Rusland en Oekraïne (RVO)	Internationaal zakendoen met Rusland en Oekraïne	Nee	<p>Oekraïne en Rusland (rvo.nl)</p> <p><i>Doet u zaken in Oekraïne of Rusland? Op deze pagina vindt u informatie voor ondernemers die te maken hebben met de gevolgen van de oorlog in Oekraïne. Sanctie-informatie, vragen & antwoorden en gratis advies: wij staan klaar om u te helpen.</i></p>
Loket Kennisveiligheid (Rijksbreed, gecoördineerd door RVO)	Kennisveiligheid	Nee	<p>Home Loket Kennisveiligheid</p> <p><i>Het Loket Kennisveiligheid verstrekt informatie en adviseert kennisinstellingen over kennisveiligheidsthema's. De instelling kan het advies gebruiken om kansen en risico's af te wegen. Het loket staat in verbinding met alle relevante onderdelen van de rijksoverheid en de sectororganisaties. Zo is het loket één toegangspunt voor alle vragen over kennisveiligheid.</i></p>
Octrooiencentrum Nederland (onderdeel van RVO)	Intellectueel eigendom	Nee	<p>Over Octrooiencentrum Nederland (rvo.nl)</p> <p><i>Als belangrijkste opdrachten heeft Octrooiencentrum Nederland:</i></p> <ul style="list-style-type: none"> - de octrooiverlenende instantie voor Nederland - voorlichting geven over het octrooisysteem - belangenbehartiger van Nederland in Europese en mondiale organisaties op het gebied van industrieel eigendom
Autoriteit Persoonsgegevens (AP; zelfstandig bestuursorgaan)	Met name relevant in de context van het aannemen/screenen van medewerkers en het voorkomen van spionage binnen de AVG-richtlijnen	Nee	<p>Autoriteit Persoonsgegevens </p> <p><i>Belt u namens een organisatie? En komt u zelf niet uit een meer algemene privacyvraag? Dan kunt u ons bij ons terecht voor informatie over uw verantwoordelijkheden bij het verwerken van persoonsgegevens. Wij leggen u dan uit wat er in de wet staat.</i></p> <p><i>Als onafhankelijk toezichthouder geven wij geen oordeel over uw specifieke situatie. Dus wilt u weten of u volledig aan de regels voldoet? Of in lijn handelt met andere organisaties in uw sector? Dan verwijzen wij u door. Bijvoorbeeld naar een adviesbureau, bedrijfsjurist of een brancheorganisatie.</i></p>

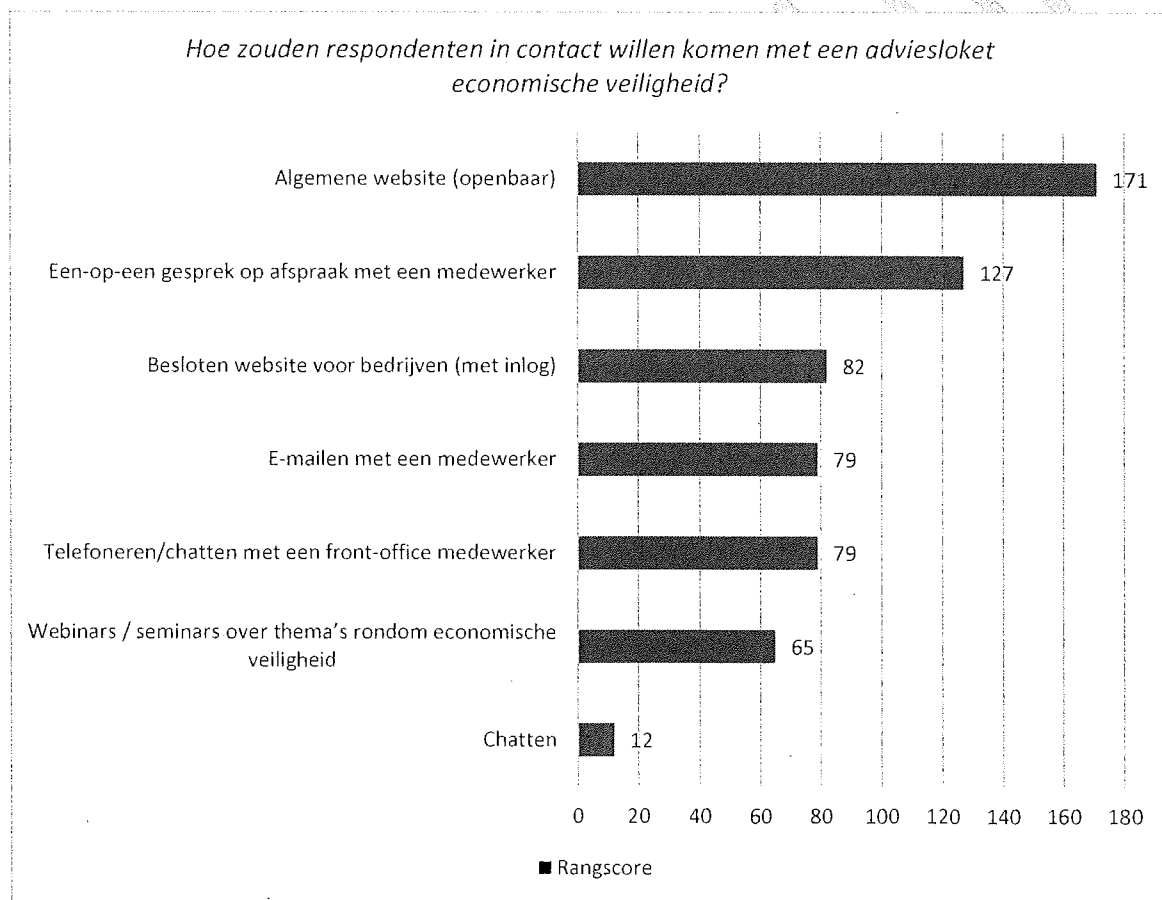
Nationaal Coördinator Terrorismedbestrijding en Veiligheid (NCTV, onderdeel van Min J&V)	Verschillende loketten op gebied van cybersecurity, met specifieke aandacht voor bedrijven in vitale processen. Verwijzingen onder meer naar Autoriteit Persoonsgegevens, de Nationale Politie en het Nationaal Cybersecurity Centrum (NCSC, onderdeel van Min J&V)	Ja	<p><u>Bedrijf of andere private organisatie Overzicht cyberloketten Nationaal Coördinator Terrorismedbestrijding en Veiligheid (nctv.nl)</u></p> <p><u>Home Nationaal Cyber Security Centrum (ncsc.nl)</u></p> <p><i>Wij zijn het Nationaal Cyber Security Centrum (NCSC). Als expert werken wij aan een digitaal veilig Nederland. De digitale infrastructuur is van levensbelang: voor het betalingsverkeer, schoon water uit de kraan en om de voeten droog te houden.</i></p> <p><i>Wij begrijpen de kwetsbaarheden en dreigingen in het digitale domein. We identificeren en duiden risico's en trends. De kennis die we verzamelen is breed toegankelijk.</i></p> <p><i>Wij verbinden partijen, kennis en informatie. Als overheidsorganisatie zijn we de verbindende schakel in een netwerk van nationale en internationale partners.</i></p> <p><i>Wij voorkomen maatschappelijke schade en beperken dreigingen. We geven vakkundige ondersteuning en advies. Met onze onderzoeken, analyses en producten geven we direct handelingsperspectief. In het geval van een crisis staan we 24/7 paraat.</i></p>
Digital Trust Center (DTC, onderdeel van Min EZK)	Cybersecurity	Nee	<p>https://www.digitaltrustcenter.nl/</p> <p><i>Digital Trust Center helpt jouw organisatie met advies en tools om veilig digitaal te ondernemen.</i></p>
Centrale Dienst In- en Uitvoer (CDIU) / Douane	Vergunningen voor in-, uit- en doorvoer strategische goederen	Nee	<p><i>Centrale Dienst voor In- en Uitvoer (CDIU) behandelt in- en uitvoervergunningen. Andere douanevragen? Kijk op douane.nl, of bel 0800 - 0143. De CDIU is alléén verantwoordelijk voor (de informatievoorziening over en de afgifte van) vergunningen voor in- en uitvoer. In- en uitvoervergunningen zijn in een zeer beperkt aantal gevallen nodig. Denk aan 'strategische goederen en diensten, cultuurgoederen, wapens en munitie (consenten), dual use goederen (goederen die ook voor zaken kunnen worden gebruikt die slechts beperkt of niet zijn toegestaan), en dergelijke'.</i></p>

Hoofdstuk 4. Praktische inregeling van het loket economische veiligheid

Voorkeur contactmogelijkheden

Aan respondenten is de vraag gesteld hoe zij in contact zouden willen komen met een adviesloket economische veiligheid. Hierbij is de mogelijkheid gegeven om drie antwoorsoorten te rangschikken. In figuur 12 zijn de rangscores te zien van de verschillende contactmogelijkheden. Hieruit komt naar voren er een voorkeur is voor een combinatie van directe, individuele contactmogelijkheden (via één-op-één gesprekken, emailwisselingen en telefoneren/chatten met medewerkers) en het beschikbaar stellen van informatie op een website.

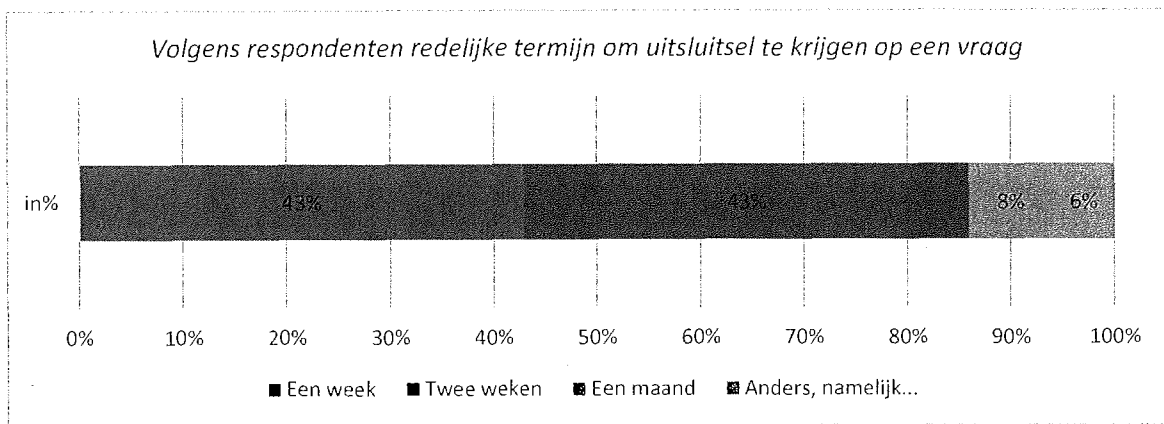
Uit de diepte-interviews komt een soortgelijk beeld naar voren. Binnen een aantal dagen kunnen sparren met een medewerker wordt bijvoorbeeld gewaardeerd, zeker als het nodig is in geval van een crisis.



Figuur 12

Redelijke termijn van beantwoording van vragen

Respondenten geven aan dat één of twee weken een redelijke termijn is om uitsluitsel te krijgen op een gestelde vraag (figuur 13). Daarbij werd wel door een aantal respondenten opgemerkt dat het afhankelijk is van het soort vraag wat een redelijke termijn zou zijn. Twee van de 119 respondenten gaven daarnaast aan dat een antwoordtermijn korter dan een week redelijk zou zijn.



Figuur 13

Gebruik van input vragen loket economische veiligheid voor beleidsontwikkeling
 93% van de respondenten staat positief tegenover het gebruik van de input in het loket voor beleidsontwikkeling, een aantal respondenten die hier negatief tegenover staan, geeft als reden het risico van het delen van bedrijfsgeheimen en een gebrek aan vertrouwen in de overheid.

Hoofdstuk 5. Conclusies en aanbevelingen

Conclusies

In de voorgaande hoofdstukken zijn de resultaten van het kortlopende onderzoek ('quick scan') 'adviesloket economische veiligheid' besproken. Hierbij is gekeken naar de vraagstukken rondom economische veiligheid die spelen bij bedrijven en de behoeften die bedrijven hebben ten aanzien van het opzetten van een loket op gebied van economische veiligheid. In het onderzoek zijn bedrijven benaderd bedrijven die actief zijn in vitale sectoren, en/of beschikken over sensitieve technologie en internationaal actief zijn of willen worden, vanuit de aanname dat bij deze bedrijven een breed scala aan vragen leeft rondom verschillende aspecten op gebied van economische veiligheid. Met het oog op de resultaten van dit onderzoek kunnen een aantal conclusies worden getrokken.

Uit het onderzoek komt naar voren dat er een indirecte behoefte is aan een adviesloket economische veiligheid. De behoefte is indirect omdat het onderwerp '**economische veiligheid**' als **overkoepelend begrip** niet erg bekend is bij bedrijven. Dit bleek uit de diepte-interviews, maar dit zou ook een reden kunnen zijn dat van de enquête een grote meerderheid van de respondenten nog geen contact met de Rijksoverheid heeft gehad ten aanzien van 'economische veiligheid' en meer dan de helft van de respondenten niet zou weten met wie ze bij de Rijksoverheid contact zouden moeten opnemen. Dit beeld wordt ondersteund door het feit dat de onderdelen bij de Rijksoverheid waarmee bedrijven wel contact hebben sterk versnipperd zijn. Daarnaast laat een 'quick scan' van bestaande, aan economische veiligheid gerelateerde loketten zien dat er vooral op verschillende economische veiligheidsthema's informatie en advies te vinden is, maar bijna niet op het onderwerp in zijn geheel.

Dat betekent dat bedrijven eerst moeten weten waar een loket economische veiligheid over gaat voordat ze kunnen aangeven of ze hier behoefte aan hebben. Dat de behoefte er is blijkt allereerst uit het feit dat er wel degelijk een aantal **economische veiligheidsthema's** kunnen worden gedestilleerd waar bedrijven vragen over hebben en onderwerpen waar bij bedrijven een adviesbehoefte van de Rijksoverheid bestaat. Deze twee categorieën zijn gedeeltelijk overlappend en daarbij valt op dat het om een vrij breed scala aan onderwerpen gaat die te maken hebben met verschillende aspecten van het ondernemerschap.

Onderwerpen waar bedrijven vragen over hebben	Onderwerpen waar bij bedrijven een adviesbehoefte van de Rijksoverheid bestaat
<ul style="list-style-type: none">• Intellectueel eigendom;• Buitenlandse reizen door medewerkers;• Export;• Dual-use of andere sensitieve technologieën;• Aannemen/screenen van medewerkers	<ul style="list-style-type: none">• Export;• Intellectueel eigendom;• Vermoedens van beïnvloeding/spionage;• Opzetten van een buitenlands verkoopkantoor of een buitenlandse dochter;• Buitenlandse reizen door medewerkers.

En ten tweede blijkt dat er een behoefte bestaat aan een contactpunt dat verschillende adviesfuncties kan vervullen op deze thema's, welke bij uitstek in een loket kunnen worden samengebracht. Het loket is met name nuttig voor het kennisintensieve, internationaal actieve MKB. Een adviesloket economische veiligheid zou wel aan een aantal randvoorwaarden moeten voldoen om voor bedrijven nuttig te zijn:

- **Proactief en reactief:** het loket moet bedrijven stimuleren om over economische veiligheid na te denken en moet hen helpen met de juiste vraagformulering. Dit moet via een algemene website en door middel van één-op-één gesprekken met medewerkers;
- **Algemene en specifieke informatie:** bedrijven hebben zowel behoefte aan algemene informatie zoals tools, checklists en updates, maar zoeken ook advies op maat;
- **Deskundigheid:** medewerkers van het loket dienen of zelf deskundig genoeg te zijn voor vraagbeantwoording of moeten efficiënt kunnen doorverwijzen naar een ander onderdeel van de Rijksoverheid wanneer dit geschikter is om de vraag te beantwoorden.
- **Vindbaarheid, bereikbaarheid en responsiviteit:** het loket moet goed vindbaar en bereikbaar zijn. Bedrijven verwachten een reactie binnen één of twee weken.

Aanbevelingen

Op basis van de resultaten van het kortlopende onderzoek 'adviesloket economische veiligheid', te weten de antwoorden op de vragenlijst alsook de diepte-interviews in Hoofdstuk 2 t/m 4 en de conclusies zoals besproken in Hoofdstuk 5, worden hier een aantal aanbevelingen gedaan ten aanzien van de reikwijdte en praktische inrichting van een adviesloket economische veiligheid, alsook hoe het huidige Loket Kennisveiligheid kan worden uitgebouwd.

1. Maak het onderwerp '**economische veiligheid**' in zijn **integraliteit** zichtbaarder bij bedrijven. Het loket moet hiervoor actief bedrijven gaan benaderen en voorlichten. Daarbij is het van belang om uit te leggen aan bedrijven waarom het onderwerp in zijn integraliteit moet worden gezien. Zoek hierbij de synergiën op met lokale en regionale overheden, andere overheidsinstanties, alsook met brancheorganisaties. Beperkingen van de onderwerpen waarop geadviseerd wordt.
2. Gebruik de behoefte-inventarisatie op gebied van thema's als leidraad voor welke informatie er beschikbaar moet worden gesteld door het loket. Zorg er daarbij voor dat het loket optimaal gebruik maakt van **reeds bestaande adviesmogelijkheden** bij de Rijksoverheid zodat het loket een efficiëntieslag betekent voor bedrijven. Dat betekent extra inzet om informatie beschikbaar te stellen op prioriteitsthema's waar nog weinig advies over beschikbaar is, maar met name verwijzen naar andere aanspreekpunten indien deze er al zijn. Breid het overzicht in Hoofdstuk 4 uit als onderdeel van het opzetten van het loket en zoek daarbij ook de synergiën op met lokale en regionale overheden, alsook met brancheorganisaties.
3. Richt het loket in eerste instantie op **kennisintensieve, internationaal actieve bedrijven binnen het MKB**, waar de behoefte ligt. Hierdoor kunnen inhoud en expertise scherper worden afgesteld dan wanneer de doelgroep bedrijven van alle groottes beslaat.
4. Zorg voor een **efficiënte en effectieve vraagafhandeling**, waarbij de duur van de beantwoording maximaal twee weken is en het streven is om vragen binnen één week te beantwoorden.
5. Zorg voor voldoende **deskundigheid** bij medewerkers van het adviesloket zodat zij vragen zelf kunnen beantwoorden of bedrijven kunnen doorverwijzen.
6. Gebruik een website voor **algemene informatie** en biedt tegelijkertijd de mogelijkheid om **maatwerk** te leveren. Dit is voor bedrijven van grote meerwaarde.
7. Het **Loket Kennisveiligheid** biedt op een deel van de thema's die in dit onderzoek naar voren komen aanknopingspunten. Het is dan ook te verwachten dat vragen van kennisinstellingen en bedrijven voor een deel overlappen. Indien de wens bestaat om beide loketten samen te voegen dan dient niet alleen goed te worden bekeken naar het aanvullen van het Loket Kennisveiligheid met de juiste informatie en expertise, maar moet ook vooral worden gelet

op naamgeving en communicatie zodat het thema 'economische veiligheid' als zodanig goed onder de aandacht kan worden gebracht.

8. Tot slot: start met een **pilot** van het loket en evalueer deze na een periode van 6-12 maanden. Deze 'quickscan' schetst een goed eerste beeld, maar gezien de breedte van het onderwerp en de grootte van de doelgroep is het verstandig om te werken met een eerste aanloopfase. Wees hier als Rijksoverheid transparant over naar bedrijven toe en vraag aan hen om mee te denken en te helpen evalueren.

VERTROUWELIJK

Bijlage A. Vragenlijst enquête

Welkomsttekst

Definitie

Ten behoeve van dit onderzoek wordt onder economische veiligheid verstaan 'het ongestoord functioneren van Nederland als een effectieve en efficiënte economie' (Nationale Veiligheid Strategie, 2019). Bedreigingen van economische veiligheid kunnen uiteenlopend van aard zijn; het kan gaan om risico's voor vitale processen, risico's op de vertrouwelijkheid en integriteit van gevoelige kennis en informatie of over ongewenste strategische afhankelijkheden. Voor bedrijven kunnen die risico's zich bijvoorbeeld voordoen bij het opzetten van een dochter in het buitenland of bij een investering door een ongewenst bedrijf.

I Algemeen

1. Namens wie vult u deze enquête in (u hoeft hierbij niet de naam van uw bedrijf te noemen)?
 - a. *Namens mijn bedrijf*
 - b. *Namens het bedrijfsonderdeel waaraan ik verbonden ben*
 - c. *Anders, namelijk..*
2. In welke branche is uw bedrijf actief?
 - a. *Agrosector*
 - b. *Infrastructuur*
 - c. *Energie*
 - d. *Transport*
 - e. *Life sciences & health en biotechnologie*
 - f. *ICT/Telecom (o.m. micro- en nanoelectronica, robotica, photonica)*
 - g. *High-tech maakindustrie*
 - h. *Lucht- en ruimtevaart*
 - i. *Anders, namelijk..*
3. Hoeveel personen zijn bij uw bedrijf werkzaam? *Antwoorden worden geanonimiseerd verwerkt. Deze vraag wordt gebruikt voor de statistieken en om algemene conclusies te kunnen trekken.*
 - a. *1 werkzaam persoon*
 - b. *2 – 50 werkzame personen*
 - c. *50 – 250 werkzame personen*
 - d. *250 – 500 werkzame personen*
 - e. *Meer dan 500 werkzame personen*
4. In welk bedrijfsonderdeel bent u werkzaam?
 - a. *Financieel*
 - b. *Informatietechnologie*
 - c. *Juridisch*
 - d. *Onderzoek en ontwikkeling*
 - e. *Sales en marketing*
 - f. *Operations en logistiek*
 - g. *Anders, namelijk..*

II Situatie binnen uw organisatie

5. In welke landen doet u op dit moment zaken? *Hier kunt u zowel regio's als specifieke landen noemen.*
6. Bij welke aspecten spelen er bij uw bedrijf vragen omtrent eventuele risico's voor economische veiligheid? *Matrixvraag 'nooit' 'zelden' 'soms' 'vaak' 'heel vaak'*
 - a. *Import*
 - b. *Export*
 - c. *Opzetten van een buitenlands verkoopkantoor of een buitenlandse dochter*

- d. *Toelevering, uitbesteding of aanbesteding*
 - e. *Fusie, overname of het verkrijgen van een belang in de aandelen van een bedrijf (participatie)*
 - f. *Licentieverlening of franchiseverlening*
 - g. *Joint-venture*
 - h. *Aannemen/screenen van medewerkers*
 - i. *Intellectueel eigendom*
 - j. *Vermoedens van beïnvloeding/spionage*
 - k. *Buitenlandse reizen door medewerkers*
 - l. *Dual-use of andere sensitieve technologieën*
 - m. *Anders, namelijk..*
 - n. *N.v.t.*
7. Bij welke aspecten heeft u behoefte aan advies van de Rijksoverheid ten aanzien van risico's voor economische veiligheid? *Matrixvraag 'geen behoefte' 'behoefte' 'sterke behoefte'*
- a. *Import*
 - b. *Export*
 - c. *Opzetten van een buitenlands verkoopkantoor of een buitenlandse dochter*
 - d. *Toelevering, uitbesteding of aanbesteding*
 - e. *Fusie, overname of het verkrijgen van een belang in de aandelen van een bedrijf (participatie)*
 - f. *Licentieverlening of franchiseverlening*
 - g. *Joint-venture*
 - h. *Aannemen/screenen van medewerkers*
 - i. *Intellectueel eigendom*
 - j. *Vermoedens van beïnvloeding/spionage*
 - k. *Buitenlandse reizen door medewerkers*
 - l. *Dual-use of andere sensitieve technologieën*
 - m. *Anders, namelijk..*
 - n. *N.v.t.*
8. Zijn er onderwerpen gerelateerd aan economische veiligheid die in voorgaande vraag niet genoemd staan, maar waar u wel vragen over zou hebben?
- a. *Ja*
 - i. *Welke onderwerpen? Meerdere antwoorden mogelijk.*
 - b. *Nee*
9. In hoeverre zijn eventuele risico's rondom economische veiligheid voldoende in beeld binnen uw organisatie? *Slider vraag*
- a. *Zeer goed in beeld*
 - b. *Goed in beeld*
 - c. *Noch slecht noch goed in beeld*
 - d. *Slecht in beeld*
 - e. *Zeer slecht in beeld*
 - f. *Weet ik niet*

III Inrichting van een adviesloket

10. Weet u waar u terecht kunt bij de Rijksoverheid met vragen omtrent economische veiligheid?
- a. *Ja*
 - b. *Nee*
 - i. *Waar loopt u tegenaan?*
11. Heeft u weleens contact gehad met onderdelen van de Rijksoverheid over vragen omtrent economische veiligheid?
- a. *Ja*

- i. Welk onderdeel was dit?
 - b. Nee **[ga naar vraag 13]**
- 12. Hoe ervaart u de contactmogelijkheden met de Rijksoverheid over dit soort (veiligheids)kwesties? *Slider mogelijkheid*
 - a. Zeer goed
 - b. Goed
 - c. Neutraal
 - i. Waar loopt u tegenaan?
 - d. Slecht
 - ii. Waar loopt u tegenaan?
 - e. Zeer slecht
 - iii. Waar loopt u tegenaan?
- 13. Wanneer heeft een adviesloket economische veiligheid voor uw organisatie echt een meerwaarde? Met andere woorden, hoe kunnen wij, de Rijksoverheid, u met een adviesloket het beste helpen om afwegingen te maken over aan economische veiligheid gerelateerde risico's?
- 14. Wat voor informatie zou u graag willen ontvangen van een adviesloket economische veiligheid?
 - a. Juridisch (bijvoorbeeld hulp bij het opstellen van contracten);
 - i. Hoe zou u graag in contact willen komen met een adviesloket economische veiligheid voor deze vraag?
 - o Algemene website (openbaar)
 - o Besloten website voor bedrijven (met inlog)
 - o Telefoneren/chatten met een front-office medewerker
 - o Een-op-een gesprek op afspraak met een medewerker
 - o E-mailen met een medewerker
 - o Chatten
 - o Webinars / seminars over thema's rondom economische veiligheid
 - o Anders, namelijk..
 - b. Landen-specifieke informatie (bijvoorbeeld expertise over mogelijk samenwerkingspartners);
 - i. Hoe zou u graag in contact willen komen met een adviesloket economische veiligheid voor deze vraag?
 - o Algemene website (openbaar)
 - o Besloten website voor bedrijven (met inlog)
 - o Telefoneren/chatten met een front-office medewerker
 - o Een-op-een gesprek op afspraak met een medewerker
 - o E-mailen met een medewerker
 - o Chatten
 - o Webinars / seminars over thema's rondom economische veiligheid
 - o Anders, namelijk..
 - c. Technische expertise (bijvoorbeeld over de (sensitieve) toepassingen van een product);
 - i. Hoe zou u graag in contact willen komen met een adviesloket economische veiligheid voor deze vraag?
 - o Algemene website (openbaar)
 - o Besloten website voor bedrijven (met inlog)
 - o Telefoneren/chatten met een front-office medewerker
 - o Een-op-een gesprek op afspraak met een medewerker
 - o E-mailen met een medewerker
 - o Chatten
 - o Webinars / seminars over thema's rondom economische veiligheid
 - o Anders, namelijk..

- d. *Anders, namelijk...*
- i. *Hoe zou u graag in contact willen komen met een adviesloket economische veiligheid voor deze vraag?*
 - o *Algemene website (openbaar)*
 - o *Besloten website voor bedrijven (met inlog)*
 - o *Telefoneren/chatten met een front-office medewerker*
 - o *Een-op-een gesprek op afspraak met een medewerker*
 - o *E-mailen met een medewerker*
 - o *Chatten*
 - o *Webinars / seminars over thema's rondom economische veiligheid*
 - o *Anders, namelijk..*
- e. *N.v.t.*
15. Wat is volgens u een redelijke termijn om uitsluitel op uw vraag te krijgen?
- a. *Een week*
 - b. *Twee weken*
 - c. *Een maand*
 - d. *Anders, namelijk...*
 - e. *N.v.t.*
16. Stel, er komt een adviesloket economische veiligheid. Hoe staat u tegenover het gebruik van uw input voor beleidsontwikkeling? De vragen die u aan het loket stelt, zullen in dat geval (anoniem) worden verzameld en geanalyseerd ten behoeve van beleidsontwikkeling.
- a. *Positief*
 - b. *Negatief*
 - i. *Kunt u hier een toelichting op geven?*
 - c. *N.v.t.*
17. Heeft u nog overige opmerkingen en/of suggesties, dan kunt u die hier kwijt.

Hartelijk dank voor uw deelname.



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Z1

Dep. **VERTROUWELIJK**

Contactpersoon

[REDACTED]

[REDACTED]

5.1.2e

Datum

21 juni 2022

agenda

TFEV

Omschrijving	TFEV
Vergaderdatum en -tijd	28 juni 2022, 12:00-13:30 uur
Vergaderplaats	Turfmarkt 147, NCTV, ICCb/MCCb (7 ^e etage)

1. Opening en mededelingen

2. Verslag TFEV 10 mei 2022

Bijlage 1. Verslag TFEV 10052022 [REDACTED]

5.1.2i

3. Technologisch leiderschap (EZK)

Bijlage 2. Oplegnota technologisch leiderschap

Bijlage 2a. Raamwerk toegang en capaciteiten technologie

Bijlage 2b. [REDACTED]

5.1.1b

4. Opvolging conferentie Economische Weerbaarheid Tokyo (BZ)

5. Opvolging motie Rajkowski-van Weerdenburg (BZK)

6. Kader nationale veiligheid inkoop en gebruik producten en diensten (NCTV)

Bijlage 3. Kader nationale veiligheid inkoop en gebruik producten en diensten

7. Internationaal/Europees

8. Parlementair

9. Rondvraag en sluiting

Dep. **VERTROUWELIJK**

Ministerie van Economische Zaken
en Klimaat

TER BESLUITVORMING

Aan
TFEV

Directoraat-generaal
Bedrijfsleven & Innovatie

Auteur

5.1.2e

Datum
15 juni 2022

Kenmerk
DGBI / 22260791

nota

Technologisch leiderschap

Kopie aan

Bijlage(n)

Parafenroute

Aanleiding

In de TFEV van 10 februari zijn criteria voor technologisch leiderschap besproken. Hierop is door de TFEV verzocht een aantal aspecten verder uit te diepen. U wordt gevraagd in te stemmen met de inhoud van de voorliggende notities waarin uitvoering is gegeven aan het uitwerken van criteria voor *toegang* tot technologieën, *capaciteiten* en de relatie tot *kritieke grondstoffen*. Daarnaast wordt u gevraagd in te stemmen met de voorgestelde vervolgstappen.

Voorgenomen besluiten

- Akkoord op raamwerk, met inachtneming van eventuele opmerkingen van de TFEV-leden.
- Akkoord op de vervolgstappen:
 - Ten eerste het stuk bespreken in een Catshuissessie – mede afhankelijk van de agenda van AZ.
 - Een interdepartementaal team levert eind van de zomer een voorstel op bij de TFEV met daarin de benodigde capaciteits- en kennisopbouw over technologie binnen de Rijksoverheid.
 - Het gebruiken van het raamwerk om technologieën door te lichten en te selecteren om technologisch leiderschapsbeleid te kunnen voeren.
 - Steun voor het opnemen van de op pagina 4-5 genoemde elementen van de notitie in de aangekondigde grondstoffenstrategie (toegezegd aan de TK). Deze leggen de nadruk op het perspectief van open strategische autonomie (w.o. EV en technologisch leiderschap).
 - Het laten landen van het raamwerk in beleid, zoals bijvoorbeeld in het sleuteltechnologieënbeleid.
 - Inzetten van dit raamwerk als basis voor Europese en internationale inzet.

Kernpunten

- De notitie bouwt voort op het conceptueel kader (besproken in TFEV van 16 december 2021) en criteria en handelingsrichtingen technologisch leiderschap (besproken in TFEV van 10 februari 2022).

Kenmerk
DGBI / 22260791

- Het biedt een richtinggevend raamwerk over wanneer en hoe we inzetten op toegang, capaciteiten en/of leiderschap.
- Het raamwerk kijkt naar het belang van een technologie voor de nationale veiligheid, het verdienvermogen in brede zin en/of maatschappelijke uitdagingen.
- Vervolgens wordt nagegaan of er strategische afhankelijkheden zijn of dreigen te ontstaan voor een technologie.
- Daarnaast wordt ingegaan op de rol van kritieke grondstoffen.
- [REDACTED]
- [REDACTED]
- [REDACTED]
- Met deze uitwerkingen wordt dit richtinggevende traject afgerond (behoudens verwerkingen opmerkingen TFEV). Het voorstel is om het raamwerk te gaan gebruiken voor toekomstig beleid dat raakt aan technologie en de NLse inzet in EU en internationaal verband.
- In de Industriebrief wordt hier al uitvoering aan gegeven, door technologisch leiderschap als onderdeel van strategische autonomie een plek te geven. Daarnaast wordt dit traject meegenomen in een mogelijke technologiestrategie en een herziening van het sleuteltechnologieënbeleid.

5.1.2i

Raamwerk toegang en capaciteiten technologie

Inleiding

Nederland streeft in Europees verband naar 'open strategische autonomie'. Dat houdt in dat we nu en in de toekomst onze publieke belangen kunnen borgen en weerbaar zijn in een onderling verbonden wereld. In de huidige verschuivende geopolitieke orde worden Nederland en de EU geconfronteerd met geopolitieke concurrentie, die zowel ons verdienvermogen, maatschappelijke uitdagingen en de nationale veiligheid raakt. Om ook in de toekomst onze publieke belangen – op het vlak van veiligheid, verdienvermogen en maatschappelijke uitdagingen (zie bijlage 1 voor toelichting) – te kunnen borgen, is het belangrijk om beschikking te hebben en houden over enkele cruciale technologieën. Het bewaken en stimuleren van de ontwikkeling van technologie en standaarden conform Europese normen en waarden is hierbij tevens een belangrijke overweging. Nederland kan dit als klein land in beginsel niet eigenstandig. Daarom bezien we de inzet primair vanuit het Europese speelveld. Zo zal bijvoorbeeld inzet op technologisch leiderschap voor Nederland vaak samengaan met inzet op capaciteiten in de EU en samenwerking met gelijkgezinde landen. Er zal nader moeten worden bezien waarop we primair nationaal willen inzetten, waarop in EU-verband en waarop met gelijkgezinde landen.

Tegen die achtergrond schetst het conceptueel kader dat het in veel gevallen voldoende is om via andere (derde) landen¹ toegang te hebben tot een bepaalde technologie, maar niet altijd. Soms is toegang tot technologie elders te kwetsbaar en wil de EU over eigen technologische capaciteiten beschikken. In specifieke gevallen zal Nederland over een eigen technologische capaciteit willen beschikken, bijvoorbeeld ter bescherming van staatsgeheimen.² Daarbovenop is het voor onze open strategische autonomie belangrijk dat de EU op enkele technologieën een leiderschapspositie inneemt. Dat stelt ons in staat om toegang te houden tot technologie elders, maar ook om ons te kunnen verdedigen, spelregels en standaarden internationaal af te dwingen en de koers van technologische ontwikkeling mede te bepalen langs onze normen en waarden (bijvoorbeeld met betrekking tot privacy en ethiek).

Voor de technologieën die de komende jaren belangrijk zijn voor onze open strategische autonomie en waarvoor we technologisch leidend willen zijn, kan de overheid gericht knelpunten wegnemen die Europese technologieclusters belemmeren bij het verwerven van een leiderschapspositie. Het gericht wegnemen van knelpunten vereist een probleemanalyse, een verantwoordelijkheidsverdeling tussen markt en overheid en maatwerk per technologiecluster. Bovendien vraagt dit om een geïntegreerde aanpak waarin oog is voor zowel *promote*- als *protect*-maatregelen³. Schaarste op zowel de arbeidsmarkt als grondstoffenmarkt onderstrepen dat alleen extra geld niet genoeg is om technologische capaciteiten op te bouwen. Scherpe keuzes zijn nodig, aangezien de benodigde factoren (kennis, kunde, mensen, materiaal) beperkt beschikbaar zijn. Daarbij dient ook rekening gehouden te worden met de risico's die inzet op toegang, capaciteiten en leiderschap met zich mee brengen.

Raamwerk

Open strategische autonomie via technologie⁴ vraagt om een slim samenspel tussen het behoud van zo goed mogelijke toegang tot technologie wereldwijd enerzijds en – in een beperkt aantal gevallen – een keuze voor inzet op technologisch leiderschap dan wel technologische capaciteiten anderzijds. Hierbij is er zowel een EU- als een nationale dimensie. Zo zal bijvoorbeeld inzet op Nederlands leiderschap vaak samengaan met inzet op capaciteiten in de EU en samenwerking met like-minded landen. We stellen de volgende richtinggevende principes voor:⁵

¹ Het betreft hier landen buiten de EU. Hierbij kan een onderscheid gemaakt worden tussen bondgenoten en gelijkgezinde derde landen enerzijds en andere derde landen die onze normen en waarden niet delen.

² Voorbeelden hiervan zijn zogenaamde *High Assurance* en *Cryptoproducten* waarmee Nederland staatsgeheimen tot en met staatsgeheim zeer geheim beschermen. Nederland is bijvoorbeeld een *cryptoproducing nation*, van wetenschappelijk onderzoek (lage TRL) tot en met productie van cryptoproducten (hoge TRL) heeft Nederland alle kennis en kunde in huis. Het is voor Nederland van strategisch belang deze kennis en technologie in eigen huis te hebben en houden.

³ Onder *protect*-maatregelen vallen in het bijzonder maatregelen op het terrein van economische veiligheid.

⁴ De term technologie verwijst naar de kennis en vaardigheden om een bepaald product (goed of dienst) te kunnen vervaardigen, waarbij we het in deze notitie hebben over hoogwaardige technologie en niet over alom beschikbare technologieën. Technologie kan duiden op een overkoepelend kennisgebied, een onderdeel daarvan en/of een toepassing (zie ook het conceptueel kader van de TFEV van 16 december).

⁵ Hierbij verdient opmerking dat elke technologie uniek is en er bij uitzondering gevallen kunnen zijn waarbij niet aan alle voorwaarden voor inzet op toegang, capaciteiten of leiderschap voldaan is, maar extra inzet toch wenselijk is.

- We zetten in beginsel (hoofdzakelijk op EU-niveau) in op zo goed mogelijke **toegang tot technologie wereldwijd**. Deze toegang zal niet onbelemmerd zijn, we zijn zelf immers ook beschermend waar moet.
- Als uitgangspunt willen we, gezien in beginsel op EU-niveau als uitgangspunt, ongehinderde toegang tot alle technologieën. Hierbij zijn voor dit raamwerk in het bijzonder technologieën relevant die nodig zijn voor een van de volgende drie publieke belangen:^{6 7}
 - de nationale veiligheid of;
 - het verdienvermogen in brede zin of;
 - het vinden van oplossingen voor maatschappelijke uitdagingen⁸
- Er kunnen risico's bestaan voor het borgen van bovenstaande publieke belangen door uit te gaan van toegang tot een technologie elders. Dan kan de overheid overwegen de **toegang te verbeteren of technologische capaciteiten** te versterken^{9 10}, indien er voor een technologie:
 - (i) sprake is van een afhankelijkheid van een niet-EU land of een klein aantal niet-EU landen (bijvoorbeeld wanneer een chokepoint binnen de waardeketen in een land geconcentreerd is) (of in de toekomst een afhankelijkheid dreigt te ontstaan) en;
 - (ii) er geen technologische alternatieven voor handen zijn en;
 - (iii-a) de verwachte impact van het wegvallen van de technologie op het publieke belang groot is, waardoor het Nederland gevoelig maakt voor geopolitieke druk of protectionisme, of;
 - (iii-b) de technologie in Nederland een opening biedt naar gevoelige informatie (bijv. via 5G, opslag, software) of vitale processen kan ondermijnen, of;
 - (iii-c) sprake is van een inrichting of benutting elders die strijdig is met de Nederlandse en Europese normen en waarden.
- Maatregelen om de toegang te verbeteren (bv. via handelsdiversificatie) zijn over het algemeen minder vergaand dan inzet op technologische capaciteiten en hebben daarom in beginsel de voorkeur. Enkel als door dergelijke maatregelen het risico voor onze publieke belangen niet voldoende gemitigeerd wordt, dan wel is te voorzien dat deze niet voldoende gemitigeerd kunnen worden, is inzet op technologische capaciteiten wenselijk.
- Bij de inschatting van de grootte van het risico zijn vragen relevant zoals of de technologie gemakkelijk te imiteren of substitueren is, welke capaciteiten Nederland en de EU reeds hebben m.b.t. de technologie, hoe de relatie met het derde land (of de derde landen) waar we afhankelijk van zijn is en of handelsdiversificatie op korte termijn mogelijk is.¹¹
- Net als toegang, gezien we capaciteiten in beginsel op EU-niveau. Dat betekent dat Nederland in beginsel gebruik maakt van Europese capaciteiten en andersom. Waar Nederland een comparatief voordeel heeft, nemen we onze verantwoordelijkheid in capaciteitsversterking. In specifieke gevallen waar het een nationaal veiligheidsbelang betreft, bijvoorbeeld bij staatsgeheimen, of de krijgsmacht (zie ook defensie-industriestrategie), zullen we over *ationale* capaciteiten moeten beschikken.
- Vanuit open strategische autonomie gezien is het ook goed om in een aantal technologieën de beste te zijn. Met andere woorden, om een **leiderschapspositie** te hebben op (knel)punten binnen een technologieketen. Dat versterkt onze balans van wederzijdse afhankelijkheden en maakt ons zowel economisch als geopolitiek minder kwetsbaar. Hierbij is zowel de nationale als EU-component belangrijk.¹² We stellen¹³ voor om te streven naar een of enkele leiderschapsposities binnen een technologieketen wanneer¹⁴:

⁶ Zie pagina 3 van deze notitie voor een toelichting op de publieke belangen.

⁷ Dit neemt niet weg dat er ook andere publieke belangen kunnen zijn die belangrijk zijn in relatie tot technologieën. Gegeven dat dit traject wordt aangevlogen vanuit 'open strategische autonomie' en de focus op hoogwaardige technologieën ligt, zijn deze drie publieke belangen echter geïdentificeerd als meest relevant.

⁸ In het bijzonder de drie grote transitiegebieden klimaat en energie, digitalisering en de circulaire economie, deze worden in het coalitieakkoord genoemd als prioritaire missies van het missiegedreven innovatiebeleid.

⁹ Zie pagina 6-7 voor handelingsperspectieven voor toegang en capaciteiten.

¹⁰ Eigen capaciteiten zijn niet kosteloos en ook niet altijd haalbaar. Deze oplossingsrichting zal afgewogen moeten worden tegen andere oplossingsrichtingen.

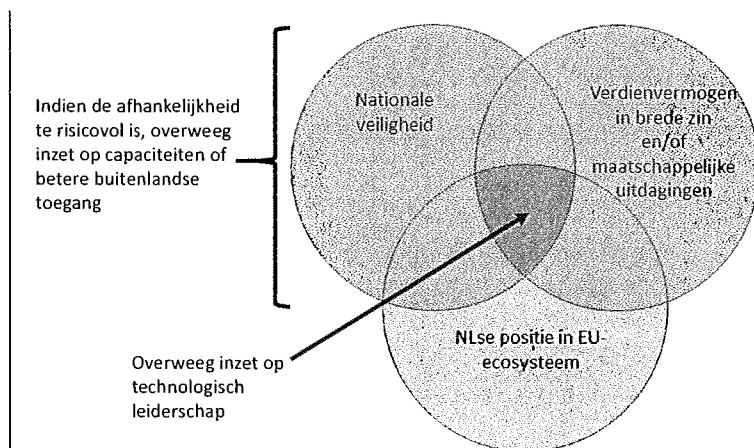
¹¹ Zie hiervoor ook de Basisvragen voor het bepalen van mogelijke risico's voor publieke belangen.

¹² Zo zou een gedeeld beeld op EU-niveau van op welke technologieën ingezet moet worden behulpzaam zijn, waarbij dan aan de hand van de Nederlandse positie in een ecosysteem bepaald kan worden op welke van de technologieën wij nationaal op leiderschap willen inzetten (in samenhang met EU-beleid).

¹³ Conform de notitie Criteria en handelingsrichtingen technologisch leiderschap (TFEV 10 februari 2022).

¹⁴ Voor een uitgebreide toelichting op deze criteria (incl. voorbeelden van op welke technologieën de criteria van toepassing zouden kunnen zijn), kan de notitie criteria en handelingsrichtingen technologisch leiderschap (besproken in TFEV van 10 februari 2022) geraadpleegd worden.

- (i) deze een aanzienlijke potentiële impact heeft op onze nationale veiligheid (waaronder militaire veiligheid, sensitieve technologie¹⁵ en vitale processen); en
 - (ii) een leidende positie haalbaar is, doordat er al een ecosysteem in de EU bestaat waarbinnen Nederland een positie van betekenis heeft; en
 - (iii-a) deze nodig is voor ons verdienvermogen in brede zin (omdat de technologie meerdere economische processen en sectoren dient); of
 - (iii-b) deze nodig is voor een of meer van de door het kabinet vastgestelde maatschappelijke uitdagingen.
- Net als toegang en capaciteiten, bezien we leiderschap op in beginsel EU-niveau. Nederland zet zich in daar waar onze positie sterk is, maar bij voorkeur in samenwerking met andere EU-landen. Waar we zelf geen goede positie in hebben, maar andere EU-landen wel, zetten we zelf niet actief op in maar ondersteunen we de EU-inzet.



Vragenlijst:

Bovenstaande leidt tot de vragenlijst in het kader hieronder. Deze vragen zijn bedoeld om te helpen bij beleidsdiscussies omtrent inzet op technologieën, niet als strak omlijnd stappenplan. Elke technologie is uniek en vergt maatwerk. Dit geldt in het bijzonder voor in ontwikkeling zijnde technologieën. Bij toepassing van de vragenlijst is het niet altijd noodzakelijk om alle vragen te doorlopen. Als bijvoorbeeld de impact van het wegvallen van de toegang tot de technologie beperkt is en er geen veiligheidsredenen zijn waarom we niet afhankelijk willen zijn van een buitenlandse partij, hoeven de resterende vragen niet worden doorlopen. Bij alle mogelijke handelingsopties is het daarbij van belang te bezien in hoeverre de handelingsoptie een oplossing voor het probleem is.

1. Aan welk publiek belang raakt de technologie?
2. Is er sprake van een afhankelijkheid of dreigt in de toekomst een afhankelijkheid te ontstaan m.b.t. de technologie? Zijn er cruciale knooppunten in waardeketens gevestigd in een klein aantal niet-EU landen? Geeft de technologie toegang tot gevoelige informatie? Of is er een andere veiligheidsreden waarom we niet afhankelijk willen zijn van een buitenlandse partij?¹⁶ Wat is de impact voor onze publieke belangen als de toegang tot de technologie wegvalt?
3. Hoe betrouwbaar is de toegang tot de technologie? Van welke landen zijn we afhankelijk? Zijn er mogelijke risico's voor onze geopolitieke positie?¹⁷
4. Zijn er diversificatie-mogelijkheden m.b.t. de toegang? Zo ja, waar en tegen welke kosten?
5. Is de technologie te imiteren of substitueren? Zo ja, tegen welke kosten en hoe veel tijd kost dit?

¹⁵ Zie het rapport Sensitieve technologie [REDACTED] voor een definitie van sensitieve technologie.

¹⁶ Hiervoor relevante vragen zijn : Is de partij die de dienst of product levert (1) een staatsbedrijf of staat het onder controle van een staat (2) afkomstig uit een land met een inlichtingenprogramma gericht op Nederland of waarmee Nederland een gespannen relatie heeft? (3) Krijgt deze partij uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of vitale infrastructuur, waarbij misbruik een nationaal veiligheidsrisico kan vormen? (4) Zijn er beheersmaatregelen mogelijk die de nationale veiligheidsrisico's voldoende beschermen?

¹⁷ In deze afweging worden tevens (voor zo ver mogelijk) de intenties en capaciteiten van andere landen of machtsblokken in relatie tot technologie meegenomen.

6. Is een leidende NL of EU een positie binnen een (EU-)ecosysteem haalbaar? Hebben we controle over een cruciaal knooppunt in de technologische waardeketen?
7. Is er sprake van Nederlandse of Europese capaciteiten die kunnen worden uitgebreid of aangepast? Zo ja, tegen welke kosten, hoe veel tijd kost dit en hoe ontwikkeld is de technologie (TRL)? Zo nee, zijn er andere mogelijkheden die overwogen kunnen worden?

Kritieke grondstoffen

Kritieke grondstoffen zijn van cruciaal belang voor technologie en de publieke belangen die daarmee gepaard gaan. Grondstoffen staan nationaal en internationaal, in het bijzonder in EU-verband, steeds hoger op de agenda. In het coalitieakkoord wordt ingezet op vermindering van de afhankelijkheid voor strategische goederen en grondstoffen. Tevens wil het kabinet 'in de transitie naar een groene economie tot de kopgroep in Europa behoren'.

Voor kritieke grondstoffen zijn NL en de EU in grote mate afhankelijk van derde landen. In veel gevallen is hierbij de productie van kritieke grondstoffen voor een groot deel geconcentreerd in een enkel land of beperkt aantal landen. In enkele gevallen hebben deze landen ook investeringen in en/of afspraken met derde landen gemaakt over kritieke grondstoffenwinning en/of raffinage, waardoor landen in sommige gevallen een dominante positie hebben verworven. Zo heeft China via raffinage sleutelposities ingenomen in waardeketens van kritieke grondstoffen die China niet of in beperkte mate mijnt. Daar komt bij dat statelijke actoren in toenemende mate bereid zijn om handel in te zetten voor politieke doeleinden. Economische afhankelijkheden van kritieke grondstoffen krijgen hierdoor een strategische dimensie.

Hoewel voor veel kritieke grondstoffen geldt dat deze in overvloed beschikbaar zijn in de aardkorst, is winning in verschillende landen te kostbaar om winstgevend te zijn. Bovendien kan winning milieuschade met zich meebrengen, waardoor kritieke grondstofprojecten maatschappelijk vaak niet populair zijn. Daar komt bij dat de winning van kritieke grondstoffen niet van de een op andere dag opgeschaald kan worden. Het kost zo'n 15 jaar om een mijn te exploiteren en openen. Daarom moet vooruitgekeken en geanticipeerd worden op aanstaande tekorten, dan wel strategische afhankelijkheden. Grondstoffen waarvoor schaarste ontstaat zullen duurder worden, wat de technologie waarvoor ze worden gebruikt ook duur en minder rendabel maakt.

Op dit moment wordt het nationale beleid omtrent (kritieke) grondstoffen in NL voornamelijk vanuit de thema's circulaire economie, mensenrechten, ontwikkelingssamenwerking en duurzaamheid aangevlogen. Veiligheidsaspecten in relatie tot kritieke grondstoffen komen beperkt terug. Met het oog op het mitigeren van de risico's van strategische afhankelijkheden van kritieke grondstoffen is het wenselijk om in te zetten op het vergroten van de voorzieningszekerheid van kritieke grondstoffen op EU niveau. Momenteel volgt Nederland de beginnende beleidsontwikkelingen in de EU, maar speelt een beperkte rol bij de vorming hiervan.

Inmiddels is er een grondstoffenstrategie toegezegd aan de Kamer waarin wordt ingegaan op de concrete handelingsperspectieven die er zijn. Gegeven de ambities in het coalitieakkoord en de positie van bepaalde landen in de waardeketens van kritieke grondstoffen en de afhankelijkheden die dat voor NL en de EU met zich meebrengt is het wenselijk om in deze grondstoffenstrategie in te zetten op het onderstaande:

- Het vaststellen van criteria op basis waarvan kan worden besloten welke grondstoffen voor NL 'kritiek' zijn voor behalen van de ambities op het terrein van klimaat- en digitale transitie, vermogen en/of nationale veiligheid, in aanvulling op de EU-lijst met kritieke grondstoffen;
- Het in kaart brengen van nationale kritieke grondstofafhankelijkheden;
- Toetsen of bestaande EU en nationale instrumenten voldoen voor het verhogen van de voorzieningszekerheid (o.a. diversificatie/winning elders, duurzaamheid, circulariteit en substitutie) m.b.t. kritieke grondstoffen en nagaan of aanvullende beleidsinzet nodig is;
- Haalbaarheid onderzoeken voor opwerking (raffinage) van kritieke grondstoffen in EU verband;

- In kaart brengen van mogelijkheden van circulaire strategieën;
- Het financieel borgen en indien mogelijk uitbreiden van de grondstoffenscanner.
- Het bezien van de mogelijkheden van het aangaan van partnerschappen om toegang tot kritieke grondstoffen te vergroten¹⁸, daarbij ook kijkende naar de beschikbaarheid van kritieke grondstoffen in Europa;
- Inzicht krijgen in geopolitieke intenties en strategieën van tegenstrevers op het gebied van technologie en grondstoffen.

Bijlage 1: Toelichting op publieke belangen

Technologieën die nodig zijn voor onze (1) nationale veiligheid (2) ons verdienvermogen in brede zin of (3) het vinden van oplossingen voor maatschappelijke uitdagingen, dienen een publiek belang. Alle drie lichten we hieronder toe.

Nationale veiligheid

De nationale veiligheid is in het geding wanneer een of meerdere nationale veiligheidsbelangen zodanig bedreigd worden, dat er sprake is van (potentiële) maatschappelijke ontwrichting. In de zomer van 2019 zag de Nationale Veiligheid Strategie (NVS 2019) het licht. Het uitbrengen van de NVS markeerde de start van een meerjarige cyclus. In de NVS 2019 zijn zes nationale veiligheidsbelangen geïdentificeerd:

1. Territoriale veiligheid
2. Fysieke veiligheid
3. Economische veiligheid
4. Ecologische veiligheid
5. Sociale en politieke stabiliteit
6. Internationale rechtsorde

Wanneer in dit document onze nationale veiligheid wordt benoemd dan betreft dat deze zes belangen en de mate waarin zij geraakt worden, met een mogelijke maatschappelijke ontwrichting tot gevolg. Er wordt momenteel gewerkt aan een Rijksbrede Veiligheidsstrategie die eind 2022 zal worden gepresenteerd waarin tevens de strategische inzet op het gebied van interne en externe veiligheid en de optimale verbinding tussen beide wordt geschetst.

Verdienvermogen in brede zin

Een technologie is nodig voor ons verdienvermogen in brede zin wanneer het nodig is voor een substantieel deel van ons verdienvermogen, dat wil zeggen dat het nodig is in meerdere sectoren en waardeketens. Dan hebben we het bijvoorbeeld over breed toepasbare technologie zoals energie-technologie of digitale technologieën. Belangen van één bedrijf of sector zijn in beginsel geen publiek belang. Vanuit macro-economisch perspectief zal het verdwijnen van een bedrijf of groep bedrijven namelijk opgevangen worden door nieuwe bedrijven.

Maatschappelijke uitdagingen

Nederland en de EU staan voor een aantal forse maatschappelijke uitdagingen, waarbij bij het vinden van oplossingen technologie een rol speelt. Het begrip maatschappelijke uitdagingen is zeer breed. De uitdagingen waaraan in de context van technologie in ieder geval gedacht kan worden, zijn de klimaat- en energietransities, de digitalisering van economie en maatschappij en de gezondheidszorg.¹⁹ Het coalitieakkoord spreekt van drie grote transitie: klimaat en energie, digitalisering en sleuteltechnologieën, en de circulaire economie. Voor het aangaan van veel van deze uitdagingen zijn toepassingen van technologie nodig. Die variëren van volwassen technologie (e.g. de huidige generatie zonnepanelen) tot cutting edge toepassingen (e.g. zelfrijdende auto's of de nieuwste medische technologie).

Een rol voor de overheid?

Nederland en de EU menen dat op termijn de economische kernwaarden van openheid, concurrentie en een gelijk speelveld de beste voedingsbodem zijn voor technologisch leiderschap. Een sterke technologische positie is gebaat bij stimulerende randvoorwaarden zoals een goed opgeleide beroepsbevolking, een goed vestigingsklimaat, duidelijke regelgeving en een dynamische, diverse en innovatieve economie. Daarbij is het belangrijk dat gegeven de snelheid en complexiteit van technologische ontwikkelingen, de private sector niet alleen hulp van de overheid vraagt maar ook relevante informatie aanlevert en zelf naar oplossingen zoekt. Omgekeerd heeft ook de overheid een proactieve signaleringsfunctie richting het bedrijfsleven met betrekking tot zowel kansen als bedreigingen.

Bedrijven hebben over het algemeen een prikkel om te zorgen voor toegang tot technologie die zij nodig hebben voor het uitoefenen van hun commerciële belangen, maar niet altijd om de toegang tot technologie voor de Nederlandse samenleving te borgen. Ook kunnen zij soms de (private en publieke) risico's van technologische afhankelijkheden van buitenlandse (staats)bedrijven

¹⁹ De verklaring van de EU-leiders in Versailles van 11 maart 2022 noemt onder het kopje 'reducing our strategic dependencies': kritieke grondstoffen, semicon, gezondheid, digitaal en voedsel.

onderschatten. Daarnaast hebben bedrijven vaak onvoldoende handelingsvermogen om weerstand te bieden tegen geopolitieke druk of protectionisme. Hier ligt dus mogelijk een rol voor de overheid. Daarbij is er zowel een EU- als een nationale dimensie. Inzet op leiderschap voor Nederland zal vaak samengaan met inzet op capaciteiten in de EU en samenwerking met like-minded landen. Er zal per technologie nader moeten worden bezien waarop we primair nationaal willen inzetten, waarop in EU-verband en waarop met like-minded landen.

Bijlage 2: Handelingsperspectieven

Handelingsperspectief toegang elders

Voor ons verdienvermogen, het vinden van oplossingen voor maatschappelijke uitdagingen en de nationale veiligheid is toegang tot technologie elders cruciaal. Door internationale handel hebben Nederlandse bedrijven toegang tot voor productie benodigde grondstoffen, halffabricaten en intellectueel eigendom, alsook technologische eindproducten. Internationale handel speelt daarmee een centrale rol in de toegang tot technologie (en andere goederen/diensten) elders. Deze toegang is van groot belang voor kennisuitwisseling en innovatie. Daarbij is relevant dat toegang tot technologie elders niet alleen belangrijk is voor technologieën waarbij NL geen rol van betekenis speelt in de waardeketen, maar juist ook voor technologische gebieden waarin Nederland leidend is of capaciteiten heeft of hierop inzet. Het stimuleren van kennisuitwisseling en innovatie is hiervoor belangrijk.

Bij toegang tot technologie elders kan onderscheid gemaakt worden tussen het brede handelspolitieke beleid ter bevordering van markttoegang in derde landen en beleid op het gebied van specifieke technologieën. De hieronder beschreven inzet op handelspolitiek beleid is grotendeels staand beleid. Voor beleid op het gebied van specifieke technologieën zou een intensivering van de inzet mogelijk kunnen zijn.

Het op regels gebaseerde multilateraal handelssysteem, waarbij het WTO-recht centraal staat, vormt de basis voor toegang tot (onderdelen van) technologie elders.²⁰ Daarbij is binnen de EU toegang tot technologie vrijwel onbeperkt (op basis van de EU-verdragen), terwijl de handels- en investeringsakkoorden die de EU sluit met derde landen een rol kunnen spelen in het verdiepen van toegang tot technologie in derde landen. Handelsakkoorden verlagen tarifaire en non-tarifaire handelsbarrières, wat het makkelijker kan maken voor bedrijven om grondstoffen, halffabricaten en technologische eindproducten uit het buitenland te halen.²¹ Ook het faciliteren van dienstenhandel binnen een akkoord kan bijdragen aan de uitwisseling van (technologische) expertise. Verder kan een handelsakkoord ruimte bieden voor een bredere dialoog over gedeelde prioriteiten op bijvoorbeeld het gebied van toegang tot technologie. Investeringsbeschermingsakkoorden kunnen het aantrekkelijker maken voor Nederlandse bedrijven om in derde landen te investeren en voor bedrijven uit derde landen om in NL te investeren. Niet in alle gevallen zal het mogelijk zijn om een handelsakkoord af te sluiten over verbeterde markttoegang voor een specifieke technologie, omdat handelsakkoorden moeten voldoen aan *'substantially all the trade between the parties'*-verplichtingen in de verschillende WTO akkoorden. Binnen bredere onderhandelingen voor handelsakkoorden met een land dat een belangrijke rol speelt op het gebied van hoogwaardige technologieën kan wel aandacht uit gaan naar het verbeteren van de toegang tot technologie. Men kan bijvoorbeeld inzetten op het verlagen van handelsbarrières voor specifieke goederen die een cruciale schakel zijn in technologische waardeketens.

Technologie-specifiek draagt economische diplomatie reeds bij aan (behoud van) toegang tot technologie elders. Ook de EU-VS Trade and Technology Council kan hieraan een bijdrage leveren. Wat verder zou kunnen worden overwogen is het gebruik van handelsakkoorden als platform of basis voor het opzetten van strategische partnerschappen op het gebied van technologie. Dergelijke partnerschappen zijn op technologie-gebied nog niet opgezet door de EU, maar bestaan wel reeds op het gebied van grondstoffen. Zo vergemakkelijkt CETA de totstandkoming van het EU-Canada Strategic Partnership on Raw Materials. Verder is standaardisatie belangrijk. Als landen dezelfde technologische standaarden hanteren, maakt dit het makkelijker om technologie uit derde landen te importeren. Dit is niet alleen voor toegang relevant; ook voor het behoud en inzetten op technologisch leiderschap is de EU standaardisatiestrategie van belang.

²⁰ Hierbij moet worden aangetekend dat het op regels gebaseerde multilateraal handelssysteem onder druk staat.

²¹ Non-tarifaire barrières kunnen ook verlaagd worden via specifieke afspraken, bijvoorbeeld via de wederzijdse herkenning van *conformity assessment procedures*.

Een andere handelingsoptie die onder toegang tot technologie elders valt is het inzetten op handelsdiversificatie. Dit is in het bijzonder relevant als er sprake is van strategische afhankelijkheid. Het brede handelspolitieke beleid draagt hier reeds aan bij; handels- en investeringsakkoorden faciliteren diversificatie van handelsstromen. Hoogwaardige technologie is lastiger te diversifiëren dan traditionele goederenstromen, omdat hoogwaardige kennis en kunde vaak geconcentreerd is in een klein aantal landen in de wereld. Diversificatie kan bijvoorbeeld gefaciliteerd worden door bij te sluiten handelsakkoorden in te zetten op ruimhartige oorsprongsregels waarbij toegevoegde waarde uit verschillende landen gecumuleerd kan worden. Dit zou een positieve uitwerking kunnen hebben op de grensoverschrijdende technologiesamenwerking tussen bedrijven gevestigd in verschillende landen, wat belangrijk is gegeven de fragmentatie van de gehele technologiewaardeketen en clustering van specifieke delen van deze waardeketens. Ook het handelsbevorderings-instrumentarium zou gericht kunnen worden ingezet om handelsdiversificatie op het gebied van specifieke technologieën te bevorderen. Uiteindelijk kiezen bedrijven zelf hoe zij hun waardeketens inrichten en welke producten of diensten zij importeren. Deze keuzes kunnen in beperkte mate gestuurd worden door de overheid. Zo kan een WTO-conforme heffing geïntroduceerd worden als er bijvoorbeeld sprake is van dumping of ongeoorloofde staatssteun aan bedrijven door een derde land. Ook exportcontrolemaatregelen hebben invloed op mate waarin bedrijven hun waardeketens kunnen inrichten. Bewustmaken van bedrijven van de risico's van bepaalde bedrijfskeuzes voor publieke belangen kan ook een bijdrage leveren.

Handelingsperspectief capaciteiten

NL en de EU kunnen vanuit het oogpunt van de bovengenoemde publieke belangen inzetten op de opbouw van eigen capaciteiten om minder afhankelijk te worden van toegang tot technologie vanuit derde landen. We kunnen ervan uitgaan dat daar publieke kosten aan zijn verbonden, aangezien deze capaciteiten nog niet aanwezig zijn. Er zou dus bezien moeten worden voor welke (delen van) technologische toepassingen er behoefte is aan eigen Europese of Nederlandse capaciteit en wat er voor nodig is om die capaciteit op te bouwen of uit te breiden. Dit is industriepolitiek met de bekende risico's van dien. Belangrijke overwegingen hierbij zijn de mate van volwassenheid van een technologie waarin we capaciteiten willen opbouwen, tegen welke prijs in Europa kan worden geproduceerd en wat de voornaamste afnemers worden. Dit raakt aan staatssteunregels en het op regels gebaseerde handelssysteem: subsidies zijn mogelijk onder voorwaarden, maar je kunt bedrijven of sectoren niet zomaar subsidiëren, dwingen primair voor de eigen markt te produceren of primair van eigen producenten af te nemen. Enerzijds kan het politiek als onwenselijk worden gezien als gesubsidieerde productie plaatsvindt die vervolgens aan derde landen wordt verkocht, terwijl dergelijke productie anderzijds noodzakelijk kan zijn omdat de EU en/of NL eigen capaciteiten willen opbouwen.²² Tot slot is ook denkbaar dat de EU en/of NL bewust beleid voeren om een positie op te bouwen in technologieketens, zodat invloed uitgeoefend kan worden op de richting waarin deze technologieën zich ontwikkelen. Maar ook daar zit wel een kostenplaatje aan.

Naast de overwegingen in relatie tot een proactief technologiebeleid, kunnen we alvast enkele uitgangspunten formuleren:

- We kunnen als klein land niet alles. Meer capaciteit voor de ene technologie betekent minder capaciteit op een andere technologie.
- We stimuleren bij voorkeur een ecosysteem. Ecosystemen zijn krachtig doordat samenwerking gebaat is bij (fysieke) nabijheid. De aantrekkingskracht van ecosystemen maakt ze toekomstbestendig; ze zijn een voedingsbodem voor niet alleen de technologieën van vandaag, maar ook van die van morgen.
- Vanuit strategisch oogpunt is controle over cruciale knooppunten binnen de technologiewaardeketen het meest gunstig. Die geven geopolitiek gewicht.
- Het ligt voor de hand om een hoogwaardig deel van de technologieketen te versterken, die zijn namelijk moeilijk te diversifiëren of te substitueren en vormen daarmee eerder een risicovolle strategische afhankelijkheid.
- Investeren in capaciteiten betekent niet alleen investeringen in bedrijven, maar ook in scholing en opleiding van arbeidskrachten én toegang tot grondstoffen.
- Afhankelijkheden volledig afbouwen is onmogelijk dat zou leiden tot fors welvaartsverlies en minder slagkracht in het aangaan van maatschappelijke uitdagingen.
- We houden ruimte voor adaptief beleid, om dat technologische en economische ontwikkelingen niet goed voorspelbaar zijn.

²² Bij het verlenen van subsidies is het streven dat bedrijven op termijn concurrerend worden op de wereldmarkt, zodat subsidiering niet blijvend nodig is.

- Een (neven)voordeel van binnenlandse capaciteiten is dat het ons in staat stelt de richting van innovatie te beïnvloeden naar onze normen en waarden (bijvoorbeeld via standaarden).

Handelingsperspectief technologisch leiderschap

Hiervoor zijn drie handelingsrichtingen te onderscheiden: (1) kennisopbouw, (2) beleidsontwikkeling en (3) middelen.

Handelingsrichting 1: Kennisopbouw over technologie

Voorstel is om (verder) te werken aan kennisopbouw over technologie als machtsfactor. Bijvoorbeeld door onderzoek naar technologie(deel)gebieden die raken aan de nationale veiligheid (sensitieve technologie), zoals al gebeurt in het kader van de Wet vifo en de het toetsingskader voor ongewenste kennis- en technologieoverdracht. Een voorbeeld van een concrete maatregel is om te onderzoeken bij welke sensitieve technologieën een technologische positie bestaat die een voorsprong mogelijk zou maken op andere machtsblokken, of op welke technologieën we juist kwetsbaar zijn. Ook een intensivering van de kennisopbouw over internationale technologieontwikkelingen ligt in de rede en is in de maak.

Handelingsrichting 2: Beleidsontwikkeling voor technologisch leiderschap

Voorstel is om de kennisopbouw doorlopend te benutten voor verdere beleidsontwikkeling. Een voorbeeld van beleidsontwikkeling is om de hierboven genoemde criteria te operationaliseren: hoe verhouden de genoemde criteria zich tot onze huidige inzet op een aantal technologieën, zoals semicon? Op welke technologie(ën) of onderdelen ervan wil Nederland leiderschap nastreven, zelf of met de EU? Bij de beleidsontwikkeling zal ook rekening moeten worden gehouden met de belangen en keuzes van partners (bondgenoten en/of samenwerkingsverbanden). Nederland moet enerzijds bereid moet zijn mee te bewegen met beleidsprincipes van de gewenste partner omwille van de samenwerking en anderzijds in staat zijn de partner te overtuigen van de eigen belangen en keuzes. Een voorbeeld van beleidsontwikkeling op gebied van semicon is de Nederlandse input op de EU Chips Act, de dialoog met de VS en de input in de relevante werkgroep van de EU-VS TTC.

Handelingsrichting 3: Middelen beschikbaar stellen voor technologisch leiderschap

Voorstel is om bovenop de huidige middelen voor generiek technologiebeleid, middelen in te zetten voor het behalen of behouden van technologisch leiderschap bij een gericht aantal kennis(deel)gebieden. Bijvoorbeeld door het inrichten van middelen voor deelname aan technologie-, innovatie- en industriesamenwerking in grensoverschrijdend, bilateraal en Europees verband. De middelen zijn dan gericht op voor-en co-financiering van PPS. Daarbij dient eerst geïdentificeerd te worden voor welke (sleutel)technologieën technologisch leiderschap wenselijk en haalbaar is. Vervolgens dient in kaart gebracht te worden wat de knelpunten zijn en waar specifiek behoefte aan is, in aanvulling op middelen die reeds beschikbaar zijn vanuit bijvoorbeeld het Missiegedreven topsectoren en innovatiebeleid (MTIB) en het Nationaal Groeifonds (NGF). Het best en meest toekomstbestendig is om middelen beschikbaar te stellen die een bestaand ecosysteem²³ versterken. Daarbij investeren we niet in één poot van de technologie, maar versterken we het hele ecosysteem, bijvoorbeeld door een stapje bij te zetten op zwakke punten. Bijvoorbeeld de beschikbaarheid van talent, risicodragend kapitaal, onderzoeksfaciliteiten of valorisatieactiviteiten. Ecosystemen zijn krachtig doordat samenwerking gebaat is bij (fysieke) nabijheid. De aantrekkingskracht van ecosystemen maakt ze toekomstbestendig; ze zijn een voedingsbodem voor niet alleen de technieken van vandaag, maar ook van die van morgen. Een concreet voorbeeld is de IPCEI ME2, waar EU-lidstaten investeren in de productie van chips die niet cutting-edge zijn. Die productie kan toch waardevol zijn om het ecosysteem te versterken en daarmee de productie van cutting-edge chips en/of andere toepassingen in de toekomst wel mogelijk te maken.

²³ Zie ook Kabinetsstrategie van onderzoeks- en innovatie-ecosystemen.



Dep. ~~VERTROUWELIJK~~
TFEV

Datum
22 maart 2022

nota

Kader nationale veiligheid: inkoop en gebruik van producten en diensten

Van
BZK (DG00), NCTV
Datum/eindparaaf

Doel nota

- TFEV informeren over de huidige inzet om risico's voor de nationale veiligheid te identificeren en mitigeren bij de inkoop en het gebruik van producten en diensten bij de (rijks- en lokale) overheid en vitale aanbieders.

Aanleiding

- TFEV van 10 februari jl. heeft aangegeven behoefte te hebben aan een breder kader waarbinnen casuïstiek gericht op de inkoop en het gebruik van (met name buitenlandse) producten en diensten kan worden geplaatst/opgepakt. Dit kader wordt geschetst in deze nota.

Toelichting

- Met enige regelmaat worden vragen gesteld vanuit de bewindspersonen, parlement of media over het (mogelijke) gebruik van producten en diensten door de Nederlandse (rijks)overheid of binnen de vitale infrastructuur en mogelijke risico's die hieraan verbonden zijn, bijvoorbeeld het risico op spionage of sabotage.
- Denk aan vragen over de DJI-drones van de Politie en Rijkswaterstaat, het gebruik van █████ camera's door de Rijksoverheid en gemeenten, de scan- en detectieapparatuur bij de Douane en Schiphol en antivirussoftware van █████
- Het is van belang om bij de aanschaf en in gebruik name maar ook daarna te monitoren op risico's en deze te beheersen. Hier is, en wordt, via diverse trajecten op ingezet. Deze nota schetst de huidige stand van zaken en inzet hierop.
- De inzet komt tot uiting in verschillende beleidskaders. Vanuit nationale veiligheid o.a. in de aanpak Tegengaan Statelijke Dreigingen (specifiek Economische Veiligheid), beleid op Cybersecurity en beleid voor de vitale infrastructuur. Vanuit Rijksinkoopbeleid/BZK krijgt dit vorm via onder

5.1.2i

5.1.2i

meer de regelgeving/kaders voor inkoop, Baseline Informatiebeveiliging Overheid, het CIO-stelsel Rijksdienst. De komende ABRO wordt een aanvullend nieuw instrument in dit geheel.

Datum
22 maart 2022

Inkoop en aanbesteding

Juridisch kader

Voor aanbestedende diensten en speciale sectorbedrijven is het verplicht om bij de inkoop van producten en diensten, indien deze boven een bepaald drempelbedrag uitkomen, volgens voorgeschreven Europese procedures aan te besteden. Het Rijk, evenals een aantal aanbieders van de vitale infrastructuur vallen onder deze aanbestedingsplicht. Hieronder geschetst juridisch kader is hierbij van toepassing.

- Voor het inrichten van het aanbestedingsrechtelijke proces, moet eerst worden vastgesteld welk juridisch kader op de opdracht van toepassing is. Hierbij wordt uitgegaan van de volgende kaders:
 1. Aanbestedingswet 2012 (AW 2012)
 2. Aanbestedingswet op defensie- en veiligheidsgebied (ADV)
- In uitzonderlijke gevallen kan een opdracht geheim worden verklaard op grond van artikel 346 VWEU, waarbij er geen aanbestedingsprocedure hoeft te worden gevolgd.
- Vervolgens zijn er diverse mogelijkheden voor het opnemen van uitsluitingsgronden, geschiktheidseisen, selectiecriteria, gunningscriteria en contractvoorwaarden die risico's voor de nationale veiligheid kunnen beheersen bij toepassing van de AW 2012 of de ADV.

1. *Aanbestedingswet 2012*

- Voor overheidsopdrachten en een deel van de opdrachten van vitale aanbieders geldt dat ze vallen onder de AW 2012.
- De AW 2012 biedt geen directe uitsluitingsgrond om een ondernemer te weren als deze een risico vormt voor de nationale veiligheid.
- De casus [REDACTED] onderschrijft dit. Onlangs heeft de Landsadvocaat bevestigd dat de AW 2012 geen directe uitsluitingsgrond biedt om de ondernemer in deze casus te weren. [REDACTED]
- Wel kunnen eisen en criteria zo worden vormgegeven dat dit de facto leidt tot uitsluit of niet-gunning aan partijen waarbij risico's voor de nationale en economische veiligheid worden vermoed. Daarvoor is wel vereist dat de aanbestedende dienst zich bewust is van deze risico's bij het ontwerp van de aanbesteding en dat de eisen en criteria voldoende verband houden met de opdracht. Zo kan een aanbestedende dienst voor de inkoop van potloden geen strenge beveiligingseisen stellen, omdat het functioneren van de potloden niet afhangt van die beveiliging.
- Inzet: EZK en NCTV doen momenteel navraag bij Europese lidstaten hoe zij de Europese aanbestedingsrichtlijn hebben geïnterpreteerd en doorgevoerd in nationale wetgeving om te kijken of er meer ruimte nodig is om nationale veiligheid mee te nemen. Mogelijk moet toegewerkt

5.1.2i

5.1.2i

worden naar een aanpassing/actualisering van de AW 2012. Dit zal in overleg met EZK als eerste ondertekenaar van de wet worden verkend.

Datum
22 maart 2022

2. *Aanbestedingswet Defensie en Veiligheid (ADV)*

- De ADV biedt, meer dan de AW 2012, opdrachtgevers de mogelijkheid om in het kader van nationale veiligheid bij aanbestedingen de juiste randvoorwaarden te stellen. Als de ADV van toepassing is, wordt er vanuit de wet al vanuit gegaan dat er eisen gesteld moeten worden aan een product of dienst die risico's voor de nationale (en economische) veiligheid tegengaan. Voor een aanbestedende dienst is het dan makkelijker gerichte eisen ten aanzien van o.a. beveiliging, screening, en de herkomst van het product te stellen. De ADV is momenteel toepasbaar voor maar een selecte groep aan aanbestedingen.

Inzet:

- In september jl. ging de ACEV (opnieuw) akkoord met het breder toepasbaar maken van de ADV zodat ook bepaalde aanbestedingen van vitale aanbieders hieronder vallen. Dit draagt bij aan het stellen van de juiste randvoorwaarden in het kader van de nationale veiligheid. Departementen zijn zelf verantwoordelijk voor het uitvoeren van deze opdracht, onder coördinatie van de NCTV en EZK. De CDINEV wordt regelmatig geïnformeerd over de voortgang van dit traject.
- Tegelijk wordt geconstateerd dat in veel gevallen de ADV niet ten volle wordt gebruikt door aanbestedende diensten om risico's voor nationale en economische veiligheid te mitigeren. Dit is een kwestie van bewustwording van de risico's en instrumentarium bij aanbestedende diensten. EZK en NCTV kijken samen naar verdere voorlichting hierover.

Bewustwording en instrumentarium nationale veiligheid bij inkoop en aanbesteding, waaronder ICO

- Het staande Rijksinkoopbeleid is dat per inkoopopdracht moet worden bezien of er mogelijk risico's zijn voor de nationale veiligheid.
- Als er mogelijke risico's kleven aan een inkoopopdracht wordt geadviseerd een risicoanalyse te doen en waar nodig en mogelijk, mitigerende maatregelen te treffen. Organisaties zijn zelf verantwoordelijk voor het treffen van risicomitigerende maatregelen. Dit kunnen technische of organisatorische maatregelen zijn, maar ook aanbestedingsrechtelijke maatregelen.
- Inkopers kunnen voor het bezien van deze risico's gebruik maken van het instrumentarium nationale veiligheidsrisico's bij inkoop en aanbesteding dat eind 2018 door BZK en NCTV is ontwikkeld. Dit bestaat uit een quickscan, een handleiding risicoanalyse en handvatten risicomitigatie.
- Als onderdeel van de Roadmap Digitaal Veilige Hard- en Software, het programma NL DIGibeter en het Rijksinkoopbeleid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is in 2021 het instrument Inkoop-eisen Cybersecurity Overheid (ICO) opgeleverd. Met dit instrument, kunnen (overheids)opdrachtgevers ten behoeve van ICT-

inkopen en -aanbestedingen specifieke informatiebeveiligingseisen formuleren.¹ Deze eisen worden vervolgens meegestuurd bij een aanbesteding en kunnen later in een contract met een leverancier worden opgenomen. Door de open toegang is het daarnaast mogelijk voor marktpartijen om gebruik te maken van de mogelijke eisen die de inkopende overheden hanteren. Sinds de start van de ontwikkeling hebben er hebben pilots plaats gevonden met de cybersecurity inkoopseisen bij 35 inkooptrajecten binnen alle overheidslagen inclusief uitvoeringsinstanties.

- ICO bestaat inmiddels uit tien inkoopsegmenten waaronder clouddiensten en serverplatformen. Tegelijkertijd worden ook nieuwe invalshoeken toegevoegd. Zo zijn dit jaar de informatieveiligheidseisen aangevuld met privacy-eisen. Deze aanvulling wordt nu in de praktijk getest. Het beeld dat uit de pilots kwam is dat ICO door de informatiebeveiligingsfunctionarissen als een belangrijk inkoop hulpmiddel wordt gezien. Daarmee verdient ICO een vaste plek in het inkoopproces van de overheid. Tegelijkertijd werd geconstateerd dat inkopers en opdrachtgevers het complex vinden om informatiebeveiligingseisen mee te nemen bij inkooptrajecten omdat ze moeite hebben om een programma van functionele eisen te vertalen naar specifieke ICT-gerelateerde beveiligingseisen. Betere samenwerking tussen ICT-specialisten, opdrachtgevers en inkopers kan dit vraagstuk oplossen.
- Inzet: Er wordt verder in gezet op bewustwording op dit thema en de borging van de instrumenten binnen het Rijksinkoopstelsel. Daarnaast zijn de instrumenten gericht op nationale veiligheid bij inkoop en aanbesteding ook beschikbaar gesteld voor vitale aanbieders en lokale overheden en wordt met enige regelmatig voorlichting gegeven over dit onderwerp bij de vitale aanbieders. Eind 2022 zal het gebruik van ICO worden geëvalueerd.

ABRO (Algemene Beveiligingseisen Rijksoverheid Opdrachten)

- De komende tijd wordt gewerkt aan het ontwikkelen van de ABRO: het nationale veiligheidsraamwerk voor alle gerubriceerde en gevoelige aanbestedingen bij het Rijk en het ministerie van Defensie.
- De huidige Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) dient als basis voor de ABRO waarbij de ABRO de ABDO zal vervangen.
- Het ABRO sluit niets uit, maar biedt een toetsingskader voor aanbestedingen.
- De ABRO kent 3 fasen:
 - I Opzetten projectorganisatie en randvoorwaarden creëren;
 - II Uitvoering geven aan ABRO voor de Rijksoverheid;
 - III Doorontwikkeling en eventueel uitbreiden richting decentrale overheden en vitale sectoren (middellange termijn)
- BZK/DGOO/IFHR, AIVD, MIVD en NCTV zijn betrokken bij uitwerken ABRO.

¹ ICO Wizard - bio-overheid

- Het ABRO-traject zal zich focussen op: bewustwording, regelgeving, toetsing en controle.

Datum
22 maart 2022

Overheid: stelsel en kaders

De (rijks)overheid zet structureel en continu in op de veiligheid en weerbaarheid van zijn digitale systemen. Dit gebeurt onder meer via het CIO-stelsel Rijksdienst en de Baseline Informatieveiligheid Overheid (BIO), waarop hier beneden nader wordt ingegaan. Regels rondom het omgaan met gerubriceerde informatie en bijvoorbeeld de advisering over kwetsbaarheden vanuit het NCSC aan rijksoverheidsorganisaties spelen een rol bij het beheersen van risico's, maar wordt hier niet nader op ingegaan. De inzet op inkoop en aanbesteding, zoals hierboven geschetst, past ook binnen deze structurele inzet.

Besluit CIO-stelsel Rijksdienst 2021

Eind 2020 is het Besluit CIO-stelsel Rijksdienst vastgesteld. Hierin zijn onder meer de positie van de departementale CIO's versterkt, en is de positie van de CIO Rijk verzaamd en geherpositioneerd. Informatiebeveiliging is een integraal onderdeel van het stelsel, waartoe ook de nieuwe positie CISO Rijk is gecreëerd. Binnen dit stelsel zijn onder andere rapportagecycli ingericht, waarin risico's en dreigingen worden geïdentificeerd en een reactie op wordt geformuleerd, waarbij de primaire verantwoordelijkheid binnen de bestaande lijnorganisaties blijft. Zo is er structureel op alle lagen aandacht voor risicomanagement. Ook de ADR kan concrete onderzoeken uitvoeren, en tot aanbevelingen komen.

Baseline informatieveiligheid overheid (BIO)

Voor de gehele overheid geldt de Baseline Informatiebeveiliging Overheid (BIO). De BIO kent een risicogebaseerde aanpak, en is gebaseerd op de internationale standaarden ISO27001 en ISO27002. Dat betekent dat overheidsorganisaties op basis van risicoafweging (nieuwe) dreigingen onderkennen en daarop passende en proportionele beveiligingsmaatregelen treffen. Dit jaar wordt de BIO geëvalueerd. Onderdeel van die evaluatie is de herijking van de dreigingen die richting geven aan de concrete overheidsmaatregelen in de BIO. De BIO bevat ook richtlijnen voor inkoop.

Wet Digitale Overheid

Veel specifieke informatieprocessen van de overheid kennen informatieveiligheidswet- en regelgeving die onderling vergelijkbare algemene informatieveiligheidseisen stellen, die min of meer overeenkomen met de BIO. Voor een aantal van deze processen is verticaal interbestuurlijk toezicht op de naleving van deze regels opgezet. Vooral bij de medeoverheden komen deze regels in de uitvoering weer samen waardoor zij zich geconfronteerd zien met een grote hoeveelheid gelijksoortige toezicht- en verantwoordingsprocessen. Om de lastendruk bij overheden te verminderen en de BIO als juridisch uitgangspunt te hanteren voor informatieveiligheid, bereidt het ministerie van BZK de wettelijke grondslag voor de BIO gaan voor in de volgende tranche van de Wet Digitale Overheid.

In het Commissiedebat met VKC Digitalisering op 22 maart is op verzoek van de VVD door de staatssecretaris voor Koninkrijksrelaties en Digitalisering toegezegd dat er een onderzoek komt naar inkoopbeisen en –richtlijnen over cyberveiligheid in het overheidsapparaat, voor wat betreft producten uit (voornamelijk) landen met een offensief cyberprogramma tegen Nederlands en diens belangen. Over de opzet/uitwerking van dit onderzoek, en samenhang met andere lopende trajecten, waaronder trajecten geschetst in deze nota, wordt de volgende TFEV geïnformeerd.

Expertise teams

Op het moment dat er sprake is van complexe risico's bij inkoop of gebruik van producten en diensten die meerdere departementen raken kan er een interdepartementaal expertiseteam worden opgericht. In de structuur van een expertiseteam wordt een technische analyse gemaakt van NV-risico's en een apart beleidsadvies met beheersmaatregelen, die afhankelijk van de situatie, bij de inkoop (voorkant) of tijdens gebruik (achterkant) kunnen worden geïmplementeerd.

Er zijn op dit moment verschillende expertise teams, gericht op Rijk en diverse vitale processen:

- | | |
|--|-----------------|
| - Expertiseteam Veilige Digitale Overheid ([REDACTED]) | 5.1.1b + 5.1.2i |
| - Expertiseteam Telecom | |
| - Expertiseteam Scan ([REDACTED]) | 5.1.2i |
| - Expertiseteam Electro | |

Vervolg

Deze nota schetst het bredere kader waarbinnen casuïstiek rondom de inkoop en het gebruik van producten en diensten kan worden geplaatst. De TFEV wordt apart geïnformeerd over de ontwikkelingen binnen de verschillende dossiers/onderdelen genoemd in deze nota.