OT & CYBERSECURITY CONFERENTIE

Geopolitiek risico als vraagstuk voor de procesbesturing

22 April 2026 • Amersfoort

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

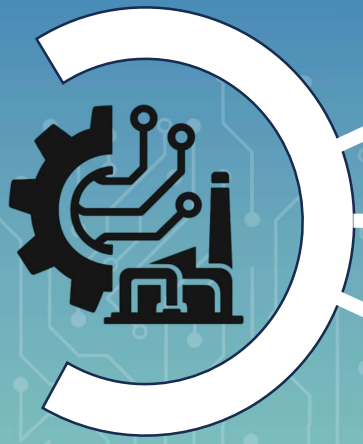
OT & CYBERSECURITY CONFERENTIE

Wat is geopolitiek risico?

OT & CYBERSECURITY CONFERENTIE

Geopolitiek risico procesbesturing

Mijn focus: chemie, raffinage, offshore, pijpleidingtransport



Strategische druk

(Intentie, sancties, exportcontrole, review-eisen en broncode-inzage, licentiebeperkingen, beleidsescalatie)

Afhankelijkheid

(Leveranciers, licenties, support en specialistische kennis, externe infrastructuur, digitale besturingsfuncties)

Operationele blootstelling

(Uitval van levering, licenties, updates, lokale support of support op afstand en reserveonderdelen)

OT & CYBERSECURITY CONFERENTIE

Geopolitieke actoren en beïnvloedingskanalen

Staten / statelijke actoren

- Inlichtingen en strategische cyberoperaties
- Sancties, export- en licentiecontrole
- Nationale regels, vendor controle en markttoegang

Staatsgesteunde of statelijk gelieerde proxies

- Offensieve cyberoperaties
- Malware, exploits, phishing en sabotage
- Ontkenbare operaties

Leveranciersketen- en serviceactoren onder geopolitieke invloed

- Levering, support en onderhoud
- Updates, tools, credentials en remote access
- Logistiek, beschikbaarheid en componentintegriteit

Geopolitiek risico

De oorzaken kunnen we meestal niet voorkomen

Sancties, exportrestricties, beleidsescalatie of terugtrekkende leveranciers zijn externe feiten.

Wat we wél kunnen beheersen:

- Afhankelijkheid verminderen
- Doorwerking beperken
- Uitwijk en herstel organiseren
- Operationele weerbaarheid vergroten

OT & CYBERSECURITY CONFERENTIE

Hoe kun je het analyseren?

OT & CYBERSECURITY CONFERENTIE

Het analyseproces in 3 stappen

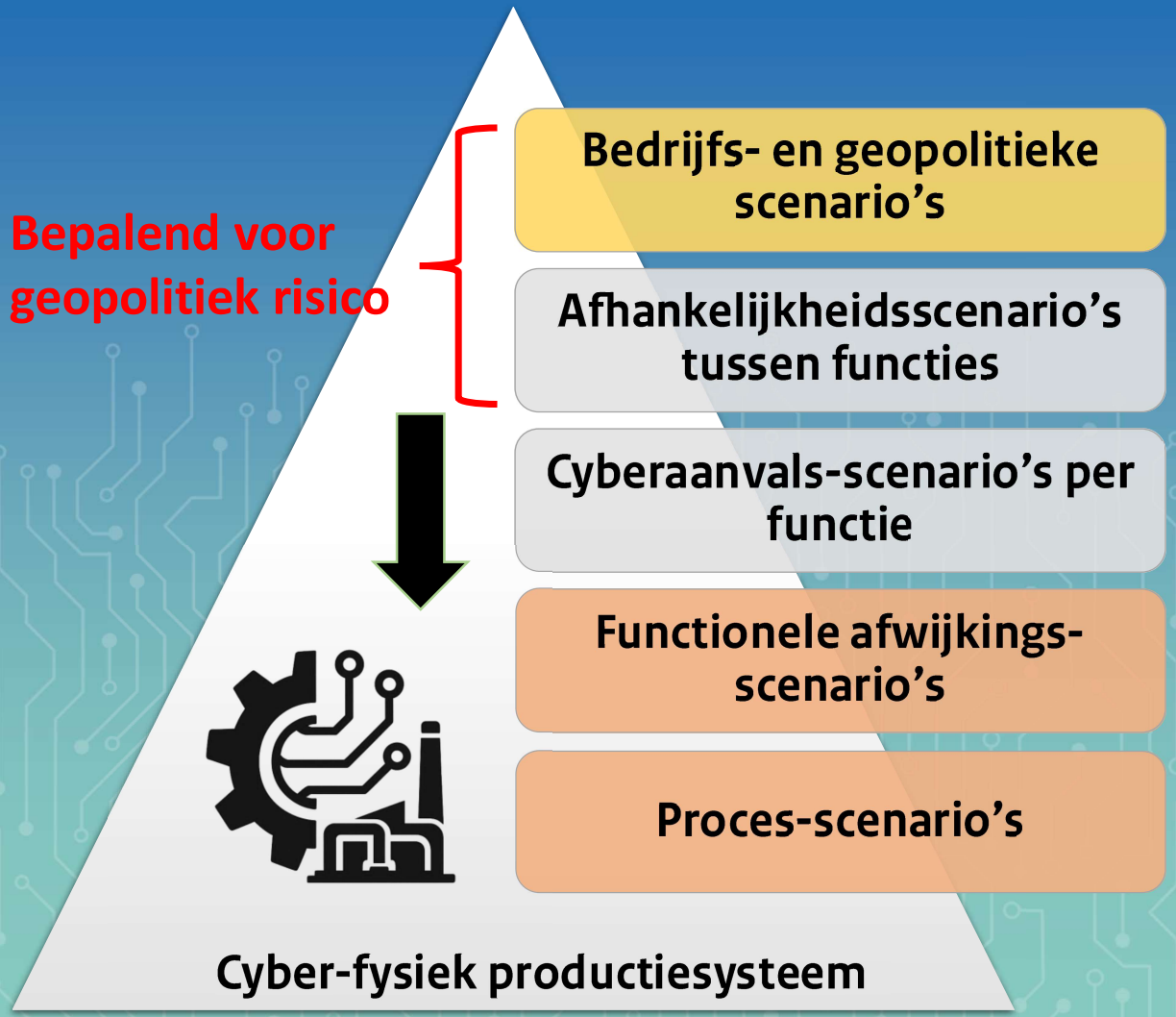
Cyclisch risicomanagementproces voor geopolitieke dreigingen

Identificatie van scenario's waarin strategische druk via afhankelijkheden en operationele blootstelling leidt tot verlies van proces besturing, veiligheid, ondersteuning, bescherming of herstel.

OT & CYBERSECURITY CONFERENTIE

Doorwerking binnen scenarioketens

Bepalend voor geopolitiek risico



Propagatieketen:

Externe en organisatorische verstoringen werken meestal niet direct in op het proces.

Zij werken via afhankelijkheden, cyberaanvallen en functionele afwijkingen door naar processcenario's.

Van boven naar beneden neemt de directe relatie met het fysieke proces toe.

OT & CYBERSECURITY CONFERENTIE

Van proces naar oorzaak

Cyber-fysiek productiesysteem

- Proces-scenario's
- Functionele afwijkings-scenario's
- Cyberaanvals-scenario's per functie
- Aanvalspad scenarios via functieafhankelijkheden
- Bedrijfs- en geopolitieke scenario's

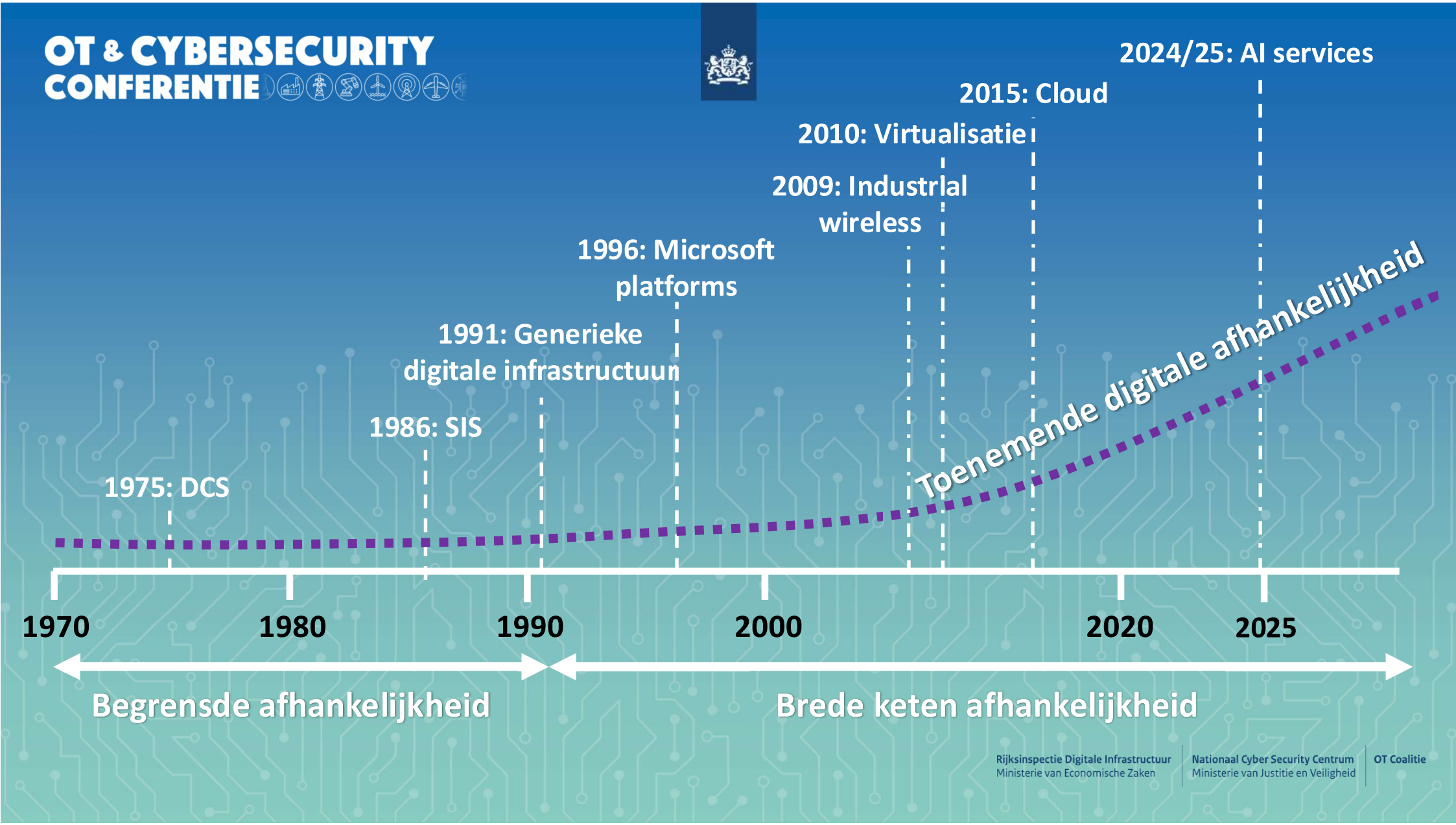
Risico analyse keten:

- Bepaal de processcenario's
- Bepaal de initiërende functionele afwijkingen
- Bepaal per functie de cyberaanvalscenario's
- Bepaal via functieafhankelijkheden de aanvalspaden
- Bepaal externe invloeden die het scenario versterken of tot een zelfde resultaat leiden

OT & CYBERSECURITY CONFERENTIE

Hoe is het zo gekomen?

OT & CYBERSECURITY CONFERENTIE



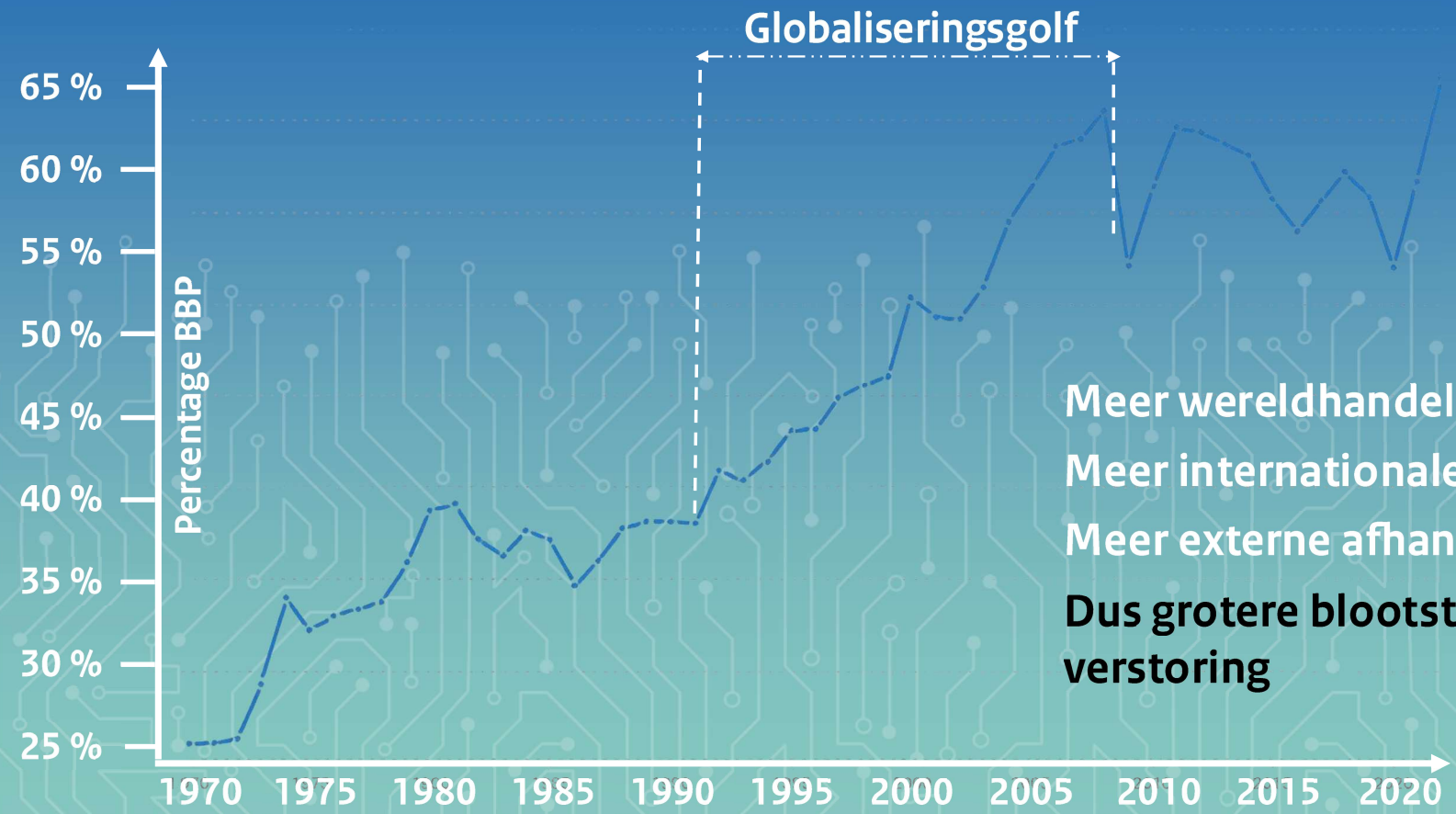
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

OT & CYBERSECURITY CONFERENTIE

Wereldhandel als % van mondiaal BBP



Meer wereldhandel ->

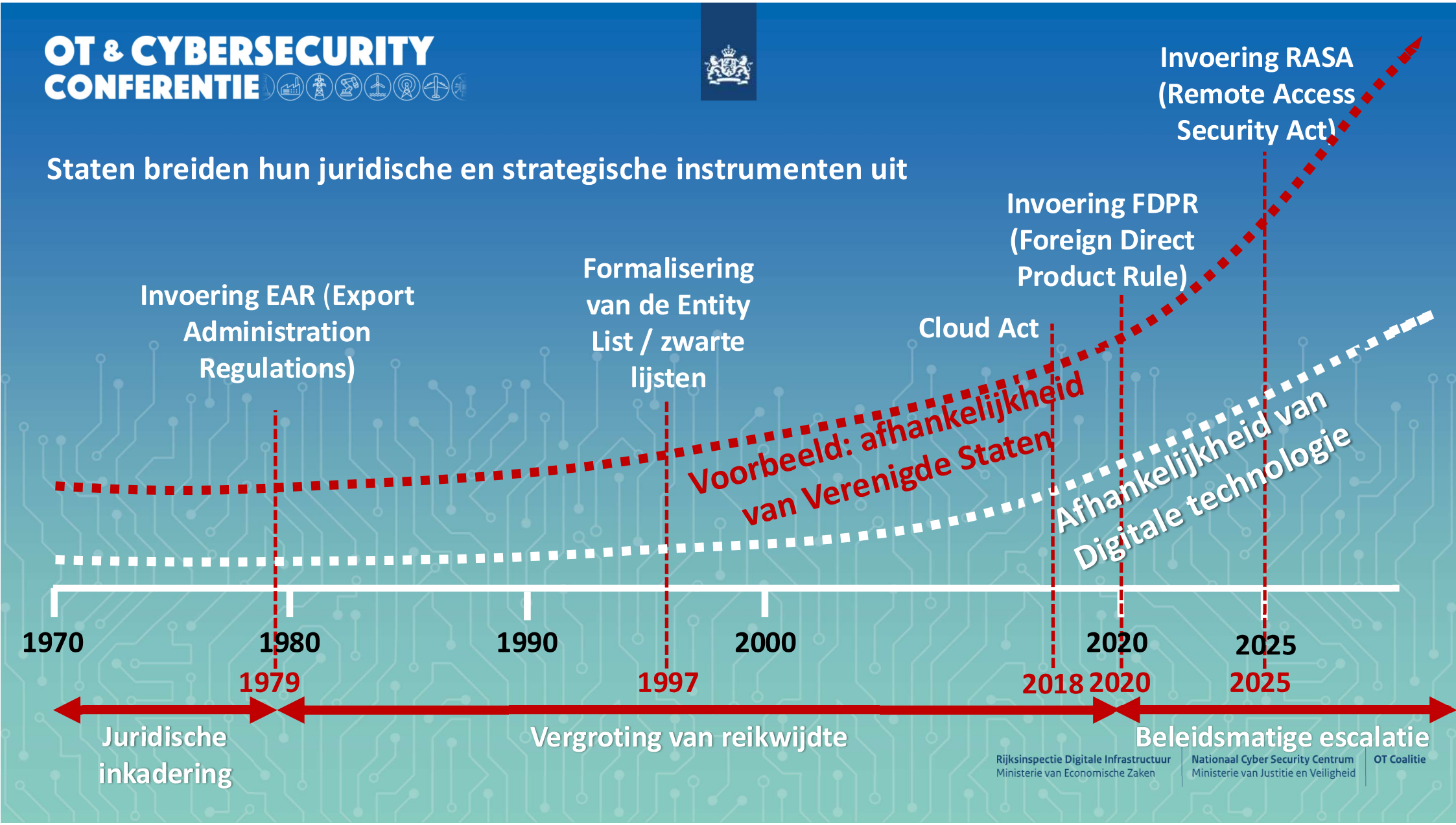
Meer internationale ketens ->

Meer externe afhankelijkheden ->

Dus grotere blootstelling aan geopolitieke verstoring

OT & CYBERSECURITY CONFERENTIE

Staten breiden hun juridische en strategische instrumenten uit



OT & CYBERSECURITY CONFERENTIE

Wat doet het met ons?

OT & CYBERSECURITY CONFERENTIE

1. Trigger-scenario's (bedrijfs- en geopolitiek) :

a. Sancties
b. Verstoring van financiële transacties en betalingsverkeer
c. Exportrestricties
d. Handelsbeperkingen
e. Jurisdictie-conflicten
f. Leverancier trekt zich terug uit een regio
g. Conflict-escalatie, inclusief hybride aanvallen

2A. Operationele doorwerking (digitaal) :

a. Licentieserver niet bereikbaar
b. Reserveonderdelen niet leverbaar
c. Patches of firmware-updates niet meer verkrijgbaar
d. Cloudactivatie valt weg
e. Ondersteuning op afstand niet meer beschikbaar
f. Tijdsynchronisatie of positionering via GPS valt weg

2B. Operationele doorwerking (logistiek & fysiek)

Dit zijn de operationele doorwerkingsscenario's van die geopolitieke context:

a. Aanvoer van grondstoffen via pijpleidingen raakt verstoord

b. Grensoverschrijdende aanvoer, tussenstromen of afvoer worden belast, vertraagd of beperkt

c. Externe energievoorziening raakt verstoord

d. Specialistische interventie of veldondersteuning niet beschikbaar

e. Remote procesdiensten of specialistische procesdiagnostiek vallen weg

OT & CYBERSECURITY CONFERENTIE

Typologie van geopolitieke afhankelijkheden van de fysieke procesinstallatie

Grondstoffen en procesinput

- Energiegebonden feedstocks: aardgas, nafta, LPG, waterstof
- Monomeren en tussenproducten voor polymeren en vezels
- Procesreagentia: zuren, logen, oplosmiddelen
- Waterbehandelingschemicaliën, filtermedia en harsen
- Katalysatoren: metaal-, zeoliet-, hydrotreating- en polymerisatiekatalysatoren

Kritieke industriële apparatuur

- Transformatoren (hoog- en middenspanning)
- Grote compressoren
- Industriële gasturbines of stoomturbines
- Grote elektromotoren en aandrijvingen
- Specialistische reactorvaten of hogedrukapparatuur

OT & CYBERSECURITY CONFERENTIE

Scenario's kunnen afhankelijkheden blootleggen, uitbuiten of verstoren.

Risico-register

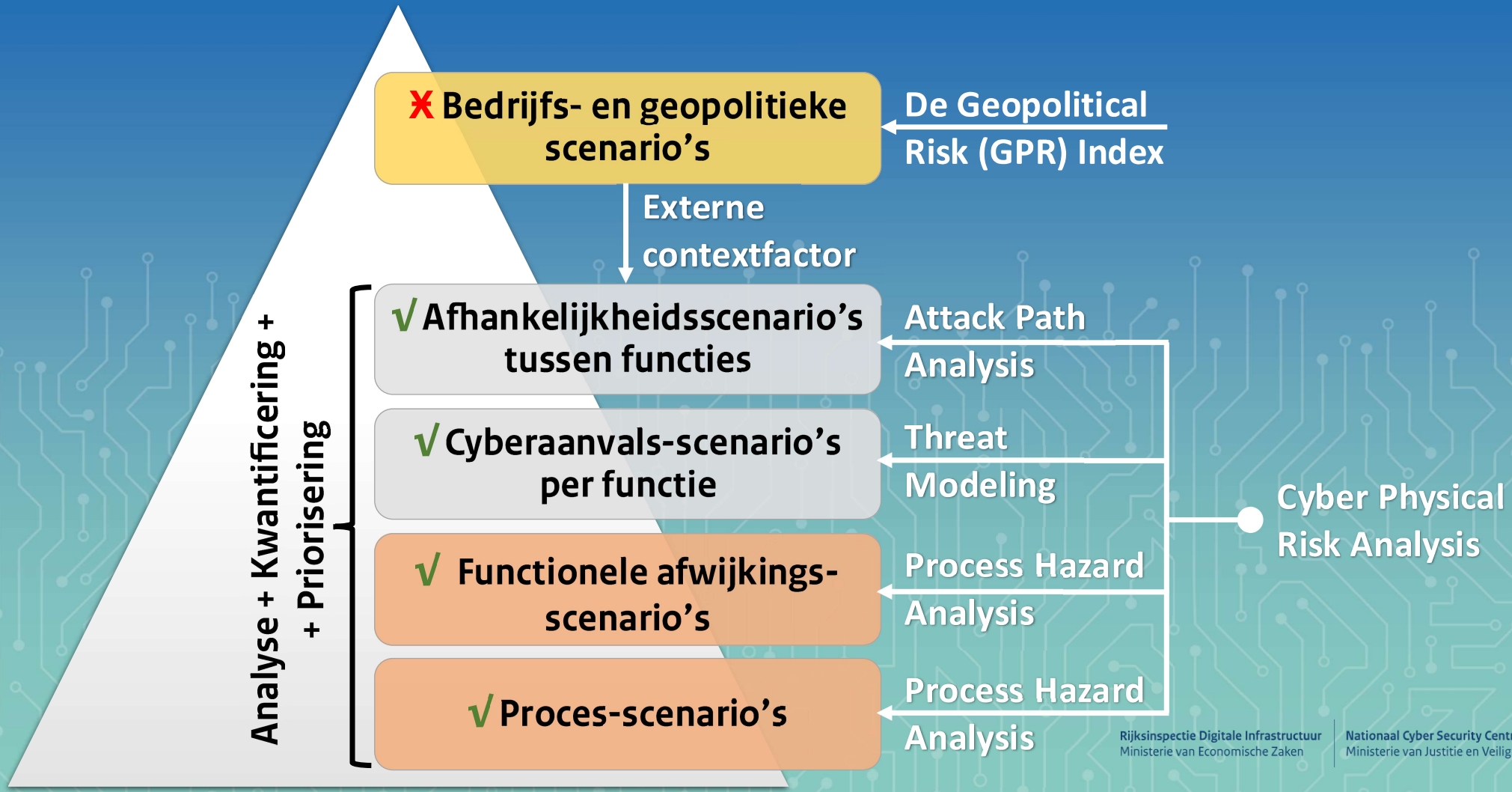
- Digitale bestuurbaarheids-afhankelijkheden
- Grondstoffen en procesinput afhankelijkheden
- Leveranciers- en kennisafhankelijkheden
- Materiële en logistieke afhankelijkheden
- Kritieke industriële apparatuur afhankelijkheden
- Externe infrastructuurafhankelijkheden

OT & CYBERSECURITY CONFERENTIE

Hoe groot is het?

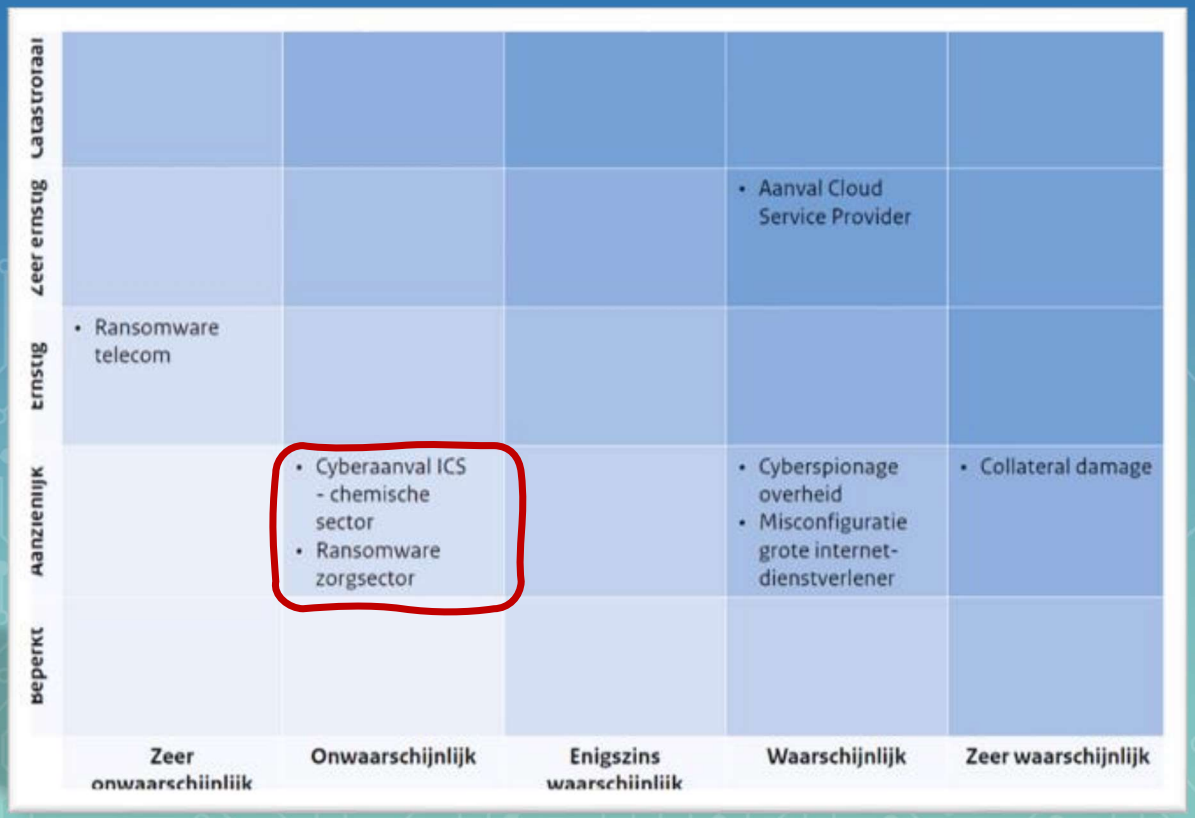
OT & CYBERSECURITY CONFERENTIE

Doorwerking binnen scenarioketens



OT & CYBERSECURITY CONFERENTIE

Rijksbrede Risicoanalyse Nationale Veiligheid (2022)



M5
M4
M3
M2
M1

W1 W2 W3 W4 W5

W2 0,05 – 0,5 % per 5 jaar
→ ± 1×10^{-4} tot 1×10^{-3} events per jaar

M2 10 – 100 doden, of < 500 miljoen euro

OT & CYBERSECURITY CONFERENTIE

Risico versus norm – en de nuance

De wettelijke norm voor de procesindustrie (Bevi / VROM-richtlijn) is veel strenger:

Brownfield installaties: maximaal 1×10^{-5} doden per jaar (Plaatsgebonden risico)
Greenfield installaties: maximaal 1×10^{-6} doden per jaar (Sinds 1 januari 2004)

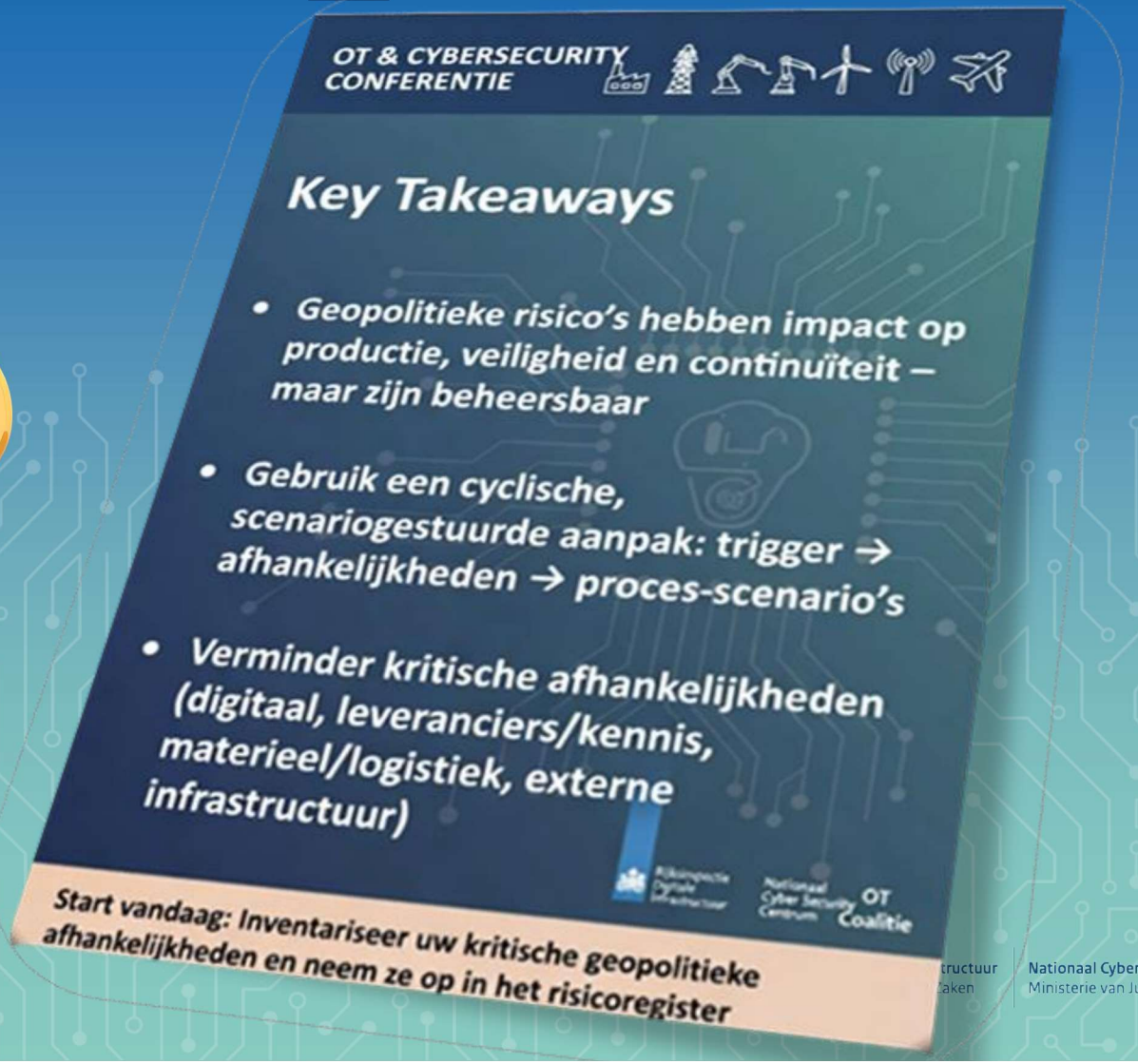
Dit NRB risico, ligt 10 tot 1000 keer hoger dan wat de industrie als acceptabel beschouwt.

De nuance:

Bij geopolitieke dreigingen ontstaat falen vooral doordat onze eigen verdediging onvoldoende sterk is. Daarom gebruiken we de Bevi-norm niet als harde juridische grens, maar als referentiekader.

OT & CYBERSECURITY CONFERENTIE

Vragen?



OT & CYBERSECURITY CONFERENTIE

Reserve slides

Hoe benader je geopolitiek risico voor de procesbesturing?

Door **scenario's** te identificeren waarin **strategische druk** via **afhankelijkheden** en **operationele blootstelling** kan leiden tot verlies van besturing, ondersteuning, bescherming of herstel.

OT & CYBERSECURITY CONFERENTIE

WAARSCHIJNLIJKHEID PER 5 JAAR

W1	< 0.05%	$<10^{-4}$ EPA *)
W2	0.05 – 0.5%	10^{-4} - 10^{-3} EPA
W3	0.5 – 5%	10^{-3} - 10^{-2} EPA
W4	5 – 50%	10^{-2} – 1.4 x 10^{-1} EPA
W5	50 – 100%	>1.4 x 10^{-1} EPA

*) Events per jaar (EPA) = $-\ln(1 - W_{5j}) / 5$

IMPACT MAGNITUDE

M1	<10 doden, of <50 miljoen euro
M2	10 – 100 doden, of <500 miljoen euro
M3	100 – 1000 doden, of <5 miljard euro
M4	1000 – 10.000 doden, of <50 miljard euro
M5	>10.000 doden, of >50 miljard

Volgens de NRB 2022 valt “Cyberaanval ICS – chemische sector” in:

W2: Kans per 5 jaar: 0,05% – 0,5%
Omgerekend naar EPA: ± 1×10^{-4} tot 1×10^{-3} (events per jaar)

De keerzijde van digitale afhankelijkheid

Terwijl onze digitale en operationele afhankelijkheid van buitenlandse technologie en leveranciers exponentieel groeide
…… begonnen geopolitieke actoren deze afhankelijkheid strategisch te benutten.

Belangrijkste actoren:

- **Verenigde Staten – meest dominant via exportcontroles, sancties en wetgeving**
- **China en Rusland – actieve tegenstanders, vaak via andere kanalen (cyberoperaties, supply-chain druk, intellectueel eigendom)**

Gevolg:

Een ooit puur transactionele relatie werd een geopolitiek machtsmiddel.

OT & CYBERSECURITY CONFERENTIE

Typologie van afhankelijkheden van cyber-fysieke productiesystemen

Digitale bestuurbaarheid (vermogen om het systeem te besturen en te vertrouwen)

- Afhankelijkheid van toegangs- en rechtenbeheer
- Afhankelijkheid van updates en patchbeheer
- Afhankelijkheid van communicatie- en positioneringsdiensten
- Afhankelijkheid van productintegriteit

Leveranciers- en kennisafhankelijkheden (externe expertise en governance)

- Afhankelijkheid van leveranciers en kennis
- Afhankelijkheid van herstel en reconstitutie
- Afhankelijkheid van ketenzichtbaarheid en regie

Materiële en logistieke afhankelijkheden (fysieke instandhouding van het systeem)

- Afhankelijkheid van reserveonderdelen en vervangbaarheid
- Afhankelijkheid van continuïteit van de aanvoerketen

Externe infrastructuurafhankelijkheden (onderliggende nationale infrastructuur)

- Externe infrastructuurafhankelijkheden

(Telecom, satelliet/PNT, energievoorziening, datanetwerken, logistieke corridors)

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie