Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2021 R10943-v2

Op weg naar een gezamenlijke cyber foresight capaciteit (P2108)

Datum	Mei 2022
Auteur(s)	B.D.S. Cadet D. Lassche D. Molema M. Neef Y.N. Kamphuis
Rubricering rapport	TNO Publiek | ONGERUBRICEERD Releasable to the public
Vastgesteld door	R. van Dijk, MA
Vastgesteld d.d.	2 november 2021
Titel	TNO Publiek | ONGERUBRICEERD releasable to the public
Samenvatting	TNO Publiek | ONGERUBRICEERD releasable to the public
Rapporttekst	TNO Publiek | ONGERUBRICEERD releasable to the public
Bijlagen	TNO Publiek | ONGERUBRICEERD releasable to the public
Aantal pagina's	39 (incl. bijlagen, excl. distributielijst)
Aantal bijlagen	5
Opdrachtgever	NCSC
Projectnaam	Cyber Foresight
Projectnummer	060.46708

Samenvatting

Dit rapport is geschreven in het kader van het project ‘Cyber Foresight’. Dit project wordt uitgevoerd in opdracht van het Nationaal Cyber Security Centrum (NCSC). Doel van het project is het verkennen van de mogelijkheden voor een gezamenlijk cyber foresight platform door het NCSC en haar partners. Met dit rapport wordt de eerste fase van dit project, de verkenning, afgesloten. Het bevat allereerst een conceptueel raamwerk wat alle (theoretische) aspecten van foresight vanuit diverse wetenschappelijke disciplines belicht. Het bevat daarnaast de resultaten van de interviews die zijn gehouden met het NCSC en de beoogde partners voor een gezamenlijk cyber foresight platform. Het rapport sluit af met een schets van de aspecten die nog een verdere discussie tussen de partners behoeven en geeft een voorzet voor de mogelijke inrichting van het platform door vier voorbeeldvariaties te geven. De volgende fase van het project zal zich aan de hand van dit rapport richten op het verder uitwerken van het beoogde platform.

Inhoudsopgave

Bijlage(n)

1 Inleiding

1.1 Inleiding project

Nieuwe technologieën, met name binnen het cyberdomein, zorgen voor grote veranderingen in de samenleving. Het in kaart brengen van technische, sociale, en politieke ontwikkelingen die met deze technologieën samenhangen, is cruciaal voor de overheid en haar partners om te kunnen anticiperen en zo onze nationale veiligheid te bewaken. Het cybersecurityveld kenmerkt zich daarbij door een hoge dynamiek, veranderlijkheid en onvoorspelbaarheid, zowel qua technologie maar ook wat betreft spelers en motieven. Er zijn kwaadwillende actoren die het bijvoorbeeld gemunt hebben op het illegaal verkrijgen van waardevolle kennis, maar ook nietsvermoedende gebruikers die niet doorhebben aan welke kwetsbaarheden ze zichzelf en anderen blootstellen. Daarnaast ontwikkelen offensieve en defensieve technieken zich in een rap tempo. Om hier zo goed mogelijk op voorbereid te zijn, is het belangrijk om na te denken over welke ontwikkelingen er op ons af komen. Dit is niet makkelijk, maar wel noodzakelijk.[1] Het project 'Cyber Foresight' onderzoekt de mogelijkheden hiertoe in samenwerkingsverbanden en heeft als doel om te verkennen welke soorten platformen zouden kunnen bijdragen aan een gezamenlijke foresight capaciteit. Het project is onderdeel van het kennisopbouwprogramma Cyber Weerbaarheid dat TNO uitvoert in opdracht van het Nationaal Cyber Security Centrum (NCSC).

1.2 Aanleiding en probleemstelling

Het nadenken over toekomstige ontwikkelingen is de kern van *foresight*: het vermogen om tijdig veranderingen waar te nemen en een beeld van de toekomst te kunnen schetsen. Hierop lopen er binnen Nederland al reeds diverse initiatieven. Echter, er zijn nog enkele onvervulde behoeftes.

Bestaande foresight initiatieven

Bestaande initiatieven op het gebied van verkenningen voor het cyber domein zijn het Cyber Security Beeld Nederland (CSBN) en het Cyber Kompas. Het CSBN is een jaarlijks door de NCTV uitgebracht rapport dat inzicht biedt in de huidige digitale dreigingen en aangeeft welke belangen daardoor kunnen worden aangetast[2]. Het CSBN doet geen voorspellingen en heeft daarmee eerder het karakter van een trendanalyse dan een foresightanalyse (zie H2 voor een uiteenzetting van deze begrippen). Door het NCSC wordt jaarlijks het Cyberkompas uitgegeven. Dit is een jaarlijkse toekomstverkenning die belanghebbenden inzicht geeft op verandering of fenomenen die de komende jaren verwacht worden. Het Cyberkompas kijkt met een cybersecurity bril naar thema's zoals digitalisering, internet (gekoppelde) producten, nieuwe aanvalspaden en aanvallers, en monopolisering van het digitale domein. Elk van deze thema's wordt beoordeeld op verwachte impact en relevantie voor stakeholders. Het Cyberkompas geeft verwachtingen op de korte tot middellange termijn (2-4 jaar).

---

[1] Bestedingsplan JenV Programmering 2021-P2108 Cyber Weerbaarheid v.1.1. van 30-09-2020, p. 14.

[2] NCTV (2021). Cybersecuritybeeld Nederland 2021. Online: Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

Tabel 1 Producten op het gebied van verkenningen voor cybersecurity.

Initiatief	Opdrachtgever	Inhoud	Horizon	Verschijnings-ritme
Cyber Security Beeld Nederland	NCTV	Trendanalyse		Jaarlijks
Cyberkompas	NCSC	Veranderingen of fenomenen die verwacht worden	2-4 jaar	Jaarlijks

Naast deze producten is er ook het Analistennetwerk Nationale Veiligheid (ANV). Het ANV is in 2011 opgericht als consortium met als doel analyses te verzorgen die gebruikt konden worden als input voor het vaststellen van prioriteiten voor budgettering en capaciteiten binnen het (interdepartementale) nationale veiligheidsdomein (als onderdeel van de Strategie Nationale Veiligheid). Het consortium bestaat uit het Rijksinstituut voor Volksgezondheid en Milieu (RIVM), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), TNO, het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie en Veiligheid, Clingendael, het Institute for Social Studies van de Erasmus Universiteit Rotterdam en de Stichting Economisch Onderzoek (SEO). Het ANV is de hofleverancier voor input voor de Nationale Veiligheidsstrategie en verzorgt jaarlijks een uitgebreide Horizon Scan en om de twee jaar een grote integrale risicoanalyse. De risicoanalyse en de Horizon Scan geven veelal trends aan die op middellange termijn een invloed gaan hebben (0-5 jaar), waarbij de Horizon Scan ook nog wat verder kijkt mochten ontwikkelingen daar aanleiding toe geven. Cyber is hier één van de vele onderwerpen. Incidenteel worden er ook andere verkennende of verdiepende vragen rondom nationale veiligheid bij het netwerk neergelegd. Of hieraan tegemoet gekomen kan worden is afhankelijk van de ruimte in het jaarlijks beschikbare budget en de instemming van de NCTV als opdrachtgever.

Naast deze initiatieven zijn er verschillende departementale interne activiteiten die kijken naar fenomeen- en dreigingsontwikkeling die verband houden met het digitale domein – zowel op strategisch als operationeel niveau. Dit zijn echter vaak sterk verkokerde processen. Dit soort dreigingsmonitors worden intern opgebouwd, kennen een korte tijdshorizon en richten zich op specifieke thema's.
Binnen sectorale samenwerkingsverbanden zoals Information Sharing and Analysis Centres (ISACs), de Digital Trust Centers en andere coalities wordt ook gesproken over toekomstverwachtingen en inzichten. Echter, deze verkenningen zijn veelal gericht op de actualiteit, beperkt onderbouwd en vaak, logischerwijs, gekleurd door sectorale belangen.
Tot slot heeft The Hague Security Delta (HSD) onlangs een nieuw platform gelanceerd, getiteld 'Security Insight'. Deze website brengt heel veel informatie over cyber security samen. Het is een grote, doorzoekbare database, waarop diverse informatiebronnen te vinden zijn zoals live-events, podcasts, blogs, video's of rapportages van externe bronnen. Als informatiebron zeker van grote waarde, maar de analist moet vervolgens nog wel het antwoord op zijn eigen vraag destilleren uit het omvangrijke aanbod.

Training
In het verleden zijn er meerdere gezamenlijke initiatieven geweest op het gebied van foresight en het ontwikkelen van foresight-vaardigheden, zoals het Cyber Forecasting Toernooi georganiseerd door het NCSC, Sybilink en TNO (Joseph,

Klaver, van de Kuijt, & van Luijk, 2019). Ook het Ministerie van Buitenlandse Zaken organiseert op regelmatige basis foresight-cursussen. Deze initiatieven worden telkens met enthousiasme ontvangen en als zeer positief beoordeeld. Echter, er is geen sprake van een continu karakter.

Probleemstelling
Kortom: er zijn diverse initiatieven maar geen enkel initiatief kijkt breed – dus departement overstijgend – naar specifiek het cyberdomein. Dit is wel de juiste mate van scope die nodig is om relevante relaties tussen fenomenen op waarde te kunnen schatten en voorspellingen te kunnen doen. De onderbouwing van de bestaande producten kan nog versterkt worden door krachten te bundelen, informatie-uitwisseling te verbeteren en methodieken verder aan te scherpen. Ook is er een behoefte aan een mogelijkheid om op doorlopende basis te werken aan het aanscherpen van de vaardigheden van de analisten en het verbeteren van gebruikte methoden en technieken.
Kortom, de probleemstelling is dat er twee onvervulde behoeften zijn: het eerste is een meer gezamenlijke en gestructureerde aanpak van toekomstverkenning rondom digitale fenomenen en dreigingen. Het tweede is een plek om (continu) te trainen in foresight-methoden en elkaar helpen te ontwikkelen en scherp te houden.

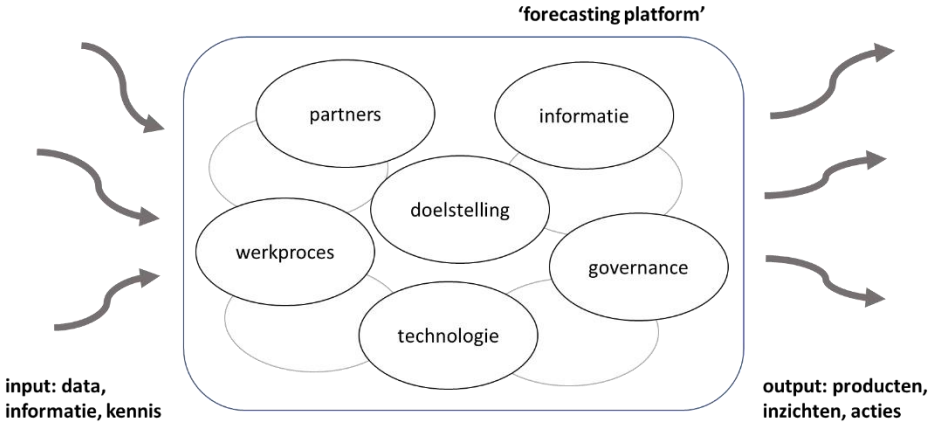
1.3 Onderzoeksvraag

De onderzoeksvraag die hieruit volgt is:
Op welke manier kunnen het NCSC en haar overheidspartners het beste gezamenlijk foresight-activiteiten uitvoeren om zo foresight in het cyber domein binnen de Nederlandse overheid te verbeteren?

1.4 Definities

Het hoofddoel van het project ‘Cyber Foresight is het ontwerpen van een ‘platform’ ten behoeve van (gezamenlijke) foresight door het NCSC en geïnteresseerde partners.

Het woord ‘platform’ verdient allereerst enige toelichting in deze context. Gewoonlijk wordt bij het woord ‘platform’ vaak gedacht aan digitale omgevingen, zoals bijvoorbeeld social media platformen, of online fora. In dit project gebruiken we de term platform in bredere zin: een samenwerkingsverband, met inbegrip van de organisatorische, technologische, informatie-technische en *teamwork*-gerelateerde elementen. Hoe zo’n platform werkt en wat het doet, wordt bepaald door een werkproces, de informatie waarmee het werkt, de afspraken die er tussen partners gemaakt worden en de technologie die de samenwerking ondersteunt. Figuur 1 laat een aantal belangrijke elementen zien van het soort platform dat we hier onderzoeken, zoals de werkvorm, het proces, de doelstelling, de partners die deelnemen en de ondersteunende technologie.



Figuur 1 Belangrijke onderdelen van een foresight platform.

In dit rapport verkennen we verschillende facetten van zo'n platform, om antwoord te kunnen geven op de onderzoeksvraag.
Ten tweede verdient het begrip 'foresight' een nadere toelichting. De begrippen foresight en forecasting worden vaak verwisselbaar gebruikt, maar hebben in de kern wel een verschillende betekenis. Foresight richt zich op het tijdig identificeren van ontwikkelingen in den breedte en heeft een langere tijdshorizon. Forecasting richt zich op het voorspellen van specifieke gebeurtenissen en richt zich op een kortere termijn. Het verschil tussen deze begrippen en andere gerelateerde begrippen wordt verder uitgewerkt in hoofdstuk 2. Omdat het begrip foresight een bredere focus heeft en kan worden gezien als parapluterm voor allerlei toekomstverkennende activiteiten, wordt er in dit rapport gekozen voor het gebruik van het begrip foresight.

1.5 Onderzoeksopzet

Het beantwoorden van de onderzoeksvraag vindt plaats in drie fases. Dit rapport behandelt de eerste fase. In deze eerste fase zijn er door het TNO-projectteam interviews uitgevoerd met het NCSC en potentiële partners. Omdat het gezamenlijk uitvoeren van foresight op vele manieren vorm kan krijgen, is het van belang om te inventariseren welke partners hier interesse in hebben, wat hun behoeften en wensen zijn, en hoe de samenwerking het beste ingericht kan worden. De te interviewen partijen zijn in overleg met de projectbegeleider van het NCSC vastgesteld. Het resultaat van deze interviews is samengebracht in dit rapport, waarbij op basis van de interviews op hoofdlijnen een algemeen beeld is geschetst van de huidige stand van zaken. Er zijn ook enkele interviews geweest met partijen die al ervaring hebben met een gezamenlijk platform en/of gezamenlijke foresight om *tips and tricks* op te halen en gevormde ideeën te toetsen. Daarnaast heeft er een korte literatuurstudie plaatsgevonden om relevante inzichten uit de literatuur mee te kunnen nemen in het ontwerpen van een gezamenlijk foresight-proces voor het NCSC en haar partners. Dit is naast de resultaten van de interviews gelegd. Op basis van de interviews en de literatuurstudie doet dit rapport een voorzet voor hoe een gezamenlijk platform voor foresight in het cyberdomein door het NCSC en haar partners eruit kan zien en welke zaken nog verdere discussie behoeven.

Een volgend rapport gaat in op het toetsen van deze resultaten uit de eerste fase bij de potentiële deelnemers. De in dit rapport gedane voorzet zal in de tweede fase

van het project worden bediscussieerd en aangescherpt in een brainstormsessie met het NCSC en haar partners, waarna het proces verder zal worden uitgewerkt in een eerste blauwdruk. In de derde, laatste fase, is het de bedoeling het gekozen en uitgewerkte gezamenlijke foresight-proces te beproeven door deze gezamenlijk te doorlopen in enkele experimentele sessies.

1.6 Opzet rapport

Het rapport is als volgt opgebouwd: na deze inleiding (hoofdstuk 1) begint hoofdstuk 2 met een theoretische uiteenzetting van het begrip foresight en daaraan gerelateerde concepten en methoden. Hoofdstuk 3 zet de resultaten van de interviews uiteen en presenteert een overkoepelende analyse van deze resultaten, gericht op wat zij betekenen voor een toekomstig gezamenlijk foresight-proces. Hoofdstuk 4 bevat de conclusies. Het hoofdstuk schetst de punten waarop er nog verschillende visies zijn en geeft een viertal voorbeelden voor mogelijke inrichtingen van het platform. Hoofdstuk 5 bevat de referenties. Tot slot vindt men in de bijlages verdere toelichtingen op diverse onderwerpen zoals terminologie en foresightmethodieken.

2 Verkenning foresight

2.1 Inleiding

Dit hoofdstuk bevat de verkenning van diverse concepten en methoden rondom foresight en enkele theoretische achtergronden die hieraan ten grondslag liggen. Deze verkenning biedt handvatten voor het schetsen van de mogelijkheden met betrekking tot de inrichting van het platform door het belichten van alle aspecten van foresight. Dit omvat bijvoorbeeld kaders voor organisatorische inpassingsvraagstukken, maar ook de diversiteit aan methodieken en inzichten rondom het cognitieve deel van het analyseproces. Hiermee geeft het de bouwblokken aan voor het cyber foresight platform.

2.2 Begrippen

Wanneer men spreekt over foresight zijn er diverse termen die vaak de revue passeren. Om een eenduidig beeld te bevorderen, worden hier de belangrijkste begrippen toegelicht in de onderstaande tabel. Van elk begrip is er ook een uitgebreidere toelichting te vinden in bijlage A. De bedoeling is vooral om grofweg het verschil tussen deze begrippen te duiden en niet om een sluitende definitie van elk begrip te geven. Van elk begrip bestaan er namelijk uiteenlopende definities en opvattingen, onder andere afhankelijk van de gebruikte wetenschappelijke discipline.

Tabel 2 De relevante begrippen rondom foresight vergeleken.

Begrip	Typisch gebruik	Typisch termijn	Voorbeeldvraag
Trend watching	Monitoren van bekende ontwikkelingen. Prioriteren van trends.	Kortere termijn	Zal het gebruik van drones door veiligheidsdiensten toe of afnemen?
Horizon Scanning	Gericht op identificeren van onbekende trends, onbekende ontwikkelingen	Kortere termijn	Welke nieuwe verschijnselen zien we op dit moment wat betreft doelen of aanvalspaden in cybersecurity?
Foresight	Systematische scenario generatie en analyse op basis van data, kennis, duiding.	Langere termijn	Welke dreigingen komen er op de lange termijn af op de Nederlandse energiesector?
Forecasting	Voorspellen.	Korte termijn, middellange termijn	Gaat Nederland binnen drie jaar een doelbewuste verstoring van het betalingsverkeer meemaken?
Intelligence	Vergaren relevante informatie voor besluitvorming	Korte termijn, real time	Welke malafide actoren zijn op dit moment actief met de verkoop van phishing platformen op DarkWeb?

De hierboven genoemde termen zijn nauw aan elkaar verwant, maar kennen ook duidelijke verschillen. Forecasting en foresight verschillen van elkaar omdat foresight breder is: het kan ook gaan over het in kaart brengen van een domein met

ontwikkelingen in brede zin in plaats van specifieke gebeurtenissen. Horizon scanning kan worden gezien als het begin van het proces (oppikken van signalen), waar forecasting meer gaat om het doen van te controleren voorspellingen.
Het verschil tussen intelligence en foresight is dat foresight kan worden gezien als onderdeel van een intelligence proces: het verkennen van mogelijke (toekomstige) ontwikkelingen. Tegelijkertijd gaat intelligence vaak weer verder dan alleen de verkenning van mogelijke toekomstige ontwikkelingen, want men moet voldoende concreetheid bereiken om de besluitvorming te kunnen ondersteunen. Omgekeerd is foresight niet altijd gericht op het ondersteunen van concrete besluitvorming. Beide begrippen hebben dus overlap maar zijn niet hetzelfde.

Het verschil tussen intelligence en forecasting zit erin dat bij forecasting er specifieke uitspraken worden gedaan of gebeurtenissen wel of niet gaan plaatsvinden, terwijl bij intelligence vaak wordt gewerkt met kansen en waarschijnlijkheden. Ook doet men vaak meer overkoepelende analyses dan specifiek één gebeurtenis. Tot slot geeft intelligence veelal een antwoord over een toestand in het huidige tijd, terwijl forecasting zich altijd richt op de toekomst.

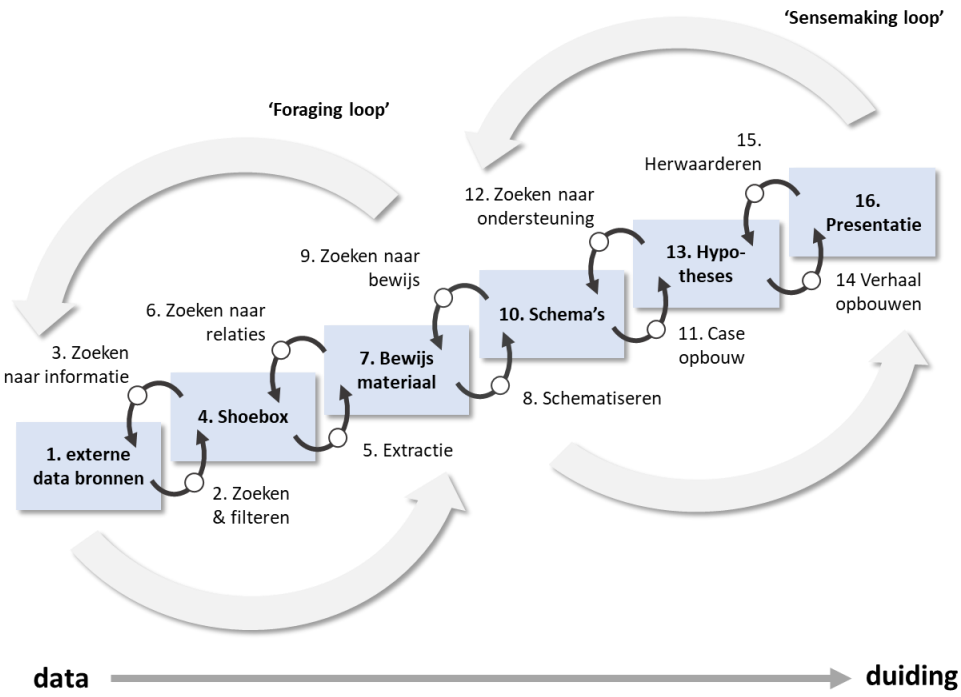
In de dagelijkse praktijk zullen deze termen vaak door elkaar gebruikt worden. Ze zijn dan ook nauw verwant en soms is er ook sprake van een activiteit die onder meerdere termen geschaard kan worden. Het is echter wel van belang om bij de ontwikkeling van het platform hierbij stil te staan. Immers, een *foresightplatform* heeft een andere intentie dan een *forecastingsplatform,* of een *horizon scanning platform.*

2.3 Foresight als een cognitief proces

Het opbouwen en trainen van competenties is een belangrijk onderdeel binnen het werkveld van intelligence. Zo kunnen biases vroegtijdig worden onderkend en voorkomen. Biases zijn een “onvolledige weergave” door irrationele besluitvormingsprocessen (Valk, 2005). Ze gebeuren elke dag en door iedereen. Belton en Dhami (2020) identificeren acht mogelijke biases in de inlichtingencyclus, zoals overmoedigheid, tunnel visie, belief bias en confirmation bias. De moeilijkheid bij analyse voor intelligence is om creatief te zijn in een gestandaardiseerd en zeer rationeel proces, wat analisten kwetsbaar maakt voor die vooroordelen.

Analisten herkennen de toegevoegde waarde van aangeleerde vaardigheden om biases tegen te gaan. Het rapport van het Cyber-Forecasting Toernooi benoemt dat de analisten aangaven te profiteren van de confrontatie met andere opvattingen en achtergronden. Het hielp ze om het grotere geheel te zien en creatiever te zijn (Klaver, van de Kuijt, Joseph, van Luijk, 2019).

In de literatuur is er veel te vinden over hoe deze competenties ontwikkeld kunnen worden, zogenaamde ‘learning path ways’ (Belton & Dhami, 2020). Het model van Pirolli en Card kan hier ook een mooie kapstok voor zijn. Pirolli en Card (2005) hebben, na uitvoerig onderzoek van de werkwijze van diverse intelligence analisten, een gedetailleerd model opgebouwd van hoe een typisch inlichtingenproces verloopt, waarbij zij hebben gefocust op het cognitieve aspect. Zie figuur 2.



Figuur 2 Een typisch inlichtingenproces (naar Pirolli & Card, 2005).

Dit model laat verschillende interacterende processen zien, met twee kernprocessen: 'foraging' en 'sensemaking'. Foraging gaat over het verzamelen en ordenen van data en informatie. 'Sensemaking' gaat over het interpreteren van informatie, en bepalen of en hoe relevant informatie is voor een te nemen besluit. Dit model is vanwege haar opbouw ook geschikt om te gebruiken als startpunt voor discussie over competentieontwikkeling, bijvoorbeeld voor het vaststellen van de relevante competenties.[3]

2.4 Methodes

Naast de vele termen die er zijn rondom foresight, zijn er ook meerdere methodes die gebruikt kunnen worden. Sommige lenen zich meer voor bijvoorbeeld horizon scanning en anderen meer voor forecasting. Welke methode het meest geschikt is om toe te passen door het cyber foresight platform, hangt af van de gewenste output, de beschikbare tijd en de voorkeur van de deelnemers. Een combinatie van verschillende methodes is ook mogelijk.

[3] Forecasting en foresight draaien in essentie grotendeels om de juiste analyse van data. Hiervoor zijn diverse vaardigheden nodig, zowel op individuele basis als binnen teamverband. Op individuele basis zijn er een aantal vaardigheden die essentieel kunnen worden genoemd. Een intelligence analist moet detailgericht, analytisch en vasthoudend zijn om signalen te kunnen identificeren en begrijpen. Bovendien heeft het vakgebied van cognitieve psychologie de nadruk gelegd op kernvaardigheden om het niveau van zingeving te verhogen. Het toevoegen van de capaciteit om kritisch te denken, om een breed perspectief aan te kunnen nemen en diverse hypotheses te kunnen overwegen zorgt ervoor dat er minder fouten worden gemaakt en dat analyses scherper worden (Pirolli & Card, 2005). Door te werken in een team kunnen deze individuele vaardigheden versterkt en ondersteund worden. Bijvoorbeeld door het delen van diverse meningen en perspectieven, die het kritisch denkvermogen aanscherpen. Of door het feit dat er meerdere disciplines ingebracht worden die kunnen helpen om diverse stukken informatie aan elkaar te koppelen (connecting the dots) (Wiener, Gattringer & Strehl, 2018).

Hieronder worden als startpunt voor discussie de methodes genoemd die benoemd zijn tijdens de interviews en methodes die in gebruik zijn bij TNO. Daarmee is deze lijst zeker niet uitputtend.

We richten ons hiermee met name op de kwalitatieve methodes. Uiteraard zijn er ook vele kwantitatieve methodes.[4] We zijn ons hier bewust van maar in eerste instantie lijken die minder te passen bij het beoogde cyber foresight platform, afgaande op de interviews.

- SHIFTER;
- Superforecasting;
- DESTEP;
- 'Clingendael/ANV' Horizon Scanning methode;
- Futures Wheel;
- Teach the Future;
- SMART Futures.

In bijlage B is een tabel te vinden waarin van elke methode een korte beschrijving staat, aangegeven wordt door welke organisatie het gebruikt wordt of genoemd tijdens de interviews, in welke literatuur er meer informatie over gevonden kan worden en tot slot bij welke activiteit uit paragraaf 2.2 de methode het beste past.

2.5 Foresight als onderdeel van het bedrijfsproces

Foresight als onderdeel van het bedrijfsproces kent twee aspecten: de manier waarop de foresight georganiseerd is en het niveau binnen de organisatie de foresight gericht is. Hieronder worden beide aspecten uiteengezet.

2.5.1 De variaties in het organiseren van foresight in het bedrijfsproces

Afhankelijk van de beschikbare resources, capaciteiten, behoeften, functies en cultuur van een organisatie, kan foresight op verschillende manieren georganiseerd worden. Slaughter (1997) identificeert drie opties, die ook met elkaar gecombineerd kunnen worden:

1 **In een bestaande capaciteit.** In deze variant komt foresight terug in bestaande expertises zoals planning, strategische analyses of informatieverzamelende functies of statistiek. Dit kan inhouden dat bepaald personeel foresight capaciteiten bezit. In deze vorm kan foresight dan ook een wat implicietere taak betreffen (zoals onderdeel van het opstellen van rapportages of visiestukken). Het is dan ook goed mogelijk dat verschillende onderdelen van het foresight proces op verschillende plekken in de organisatie belegd zijn.
2 **In een separaat team.** Deze variant betreft een aparte afdeling of unit met gespecialiseerd personeel die specifiek in het leven geroepen is om zich bezig te houden met forecasts. Het gaat dan om de eigen unieke foresight capaciteit van een organisatie en betreft dan ook vaak een expliciete taakvermelding.
3 **Als externe expertise**. Er kan ook voor worden gekozen om externe expertise aan te trekken op het gebied van foresight in het betreffende domein van de organisatie. Dit kan een goede optie zijn wanneer het een kleine organisatie betreft. Externe expertise kan inhouden dat bijvoorbeeld individuele consultants

[4] Voorbeelden zijn systeem dynamica methoden zoals causal loop modellen, stock and flow modelling, simulatie, of statistische methoden zoals regressieanalyse en tijdsreeksanalyses.

worden ingehuurd of dat foresight producten en publicaties vanuit andere instanties worden benut.

Voor alle drie de varianten geldt dat dit ook gedaan zou kunnen worden door een geautomatiseerd systeem in plaats van door personeel. Meer informatie hierover staat in bijlage E.

2.5.2 De focus van het foresightproces

2.5.2.1 Foresight als strategisch proces

Foresight als een strategisch proces omhelst het proces van het creëren en onderhouden van een kwalitatieve en samenhangende vooruitblik, en de inzichten hieruit toepassen in het strategisch management van de organisatie. Denk aan het uitwerken van visie, scenario's, strategie en beleid. Het is daarmee een combinatie van toekomstverkenningsmethoden en strategisch management. Foresight op strategisch niveau betreft dan ook het verder vooruitkijken met een brede blik. Het doel is daarbij vaak het herkennen van brede trends en ontwikkelingen die van invloed kunnen zijn op de betreffende organisatie en haar stakeholders. Hierbij wordt vaak ook data gebruikt die over een langere periode strekt in het verleden om iets te zeggen over een toekomst die over een langere termijn vooruit strekt. Om die reden wordt foresight als strategisch proces over het algemeen ook met een lage frequentie uitgevoerd (Slaughter, 1997).

2.5.2.2 Foresight als operationeel proces

In tegenstelling tot foresight als strategisch proces draait foresight als operationeel proces om het extrapoleren van operationele data (uit een relatief kort verleden) naar verwachte gebeurtenissen op de korte termijn, dus met een korte tijdshorizon. Echter, doordat het wel gaat om het formuleren van concrete verwachtingen of scenario's, bestempelen we dit proces hier als forecasting, en niet als horizon scanning (zie ook het begrippenkader). Dit soort forecasting dient dan ook vaak als input voor operationele besluitvorming voor acute vraagstukken. De frequentie van operationele foresight analyses is relatief hoog aangezien het ook een link heeft met het verkrijgen en behouden van situational awareness: het kunnen projecteren van de toekomstige status van de huidige situatie (Endsley, 2017). Hoewel foresight als operationeel proces nauw gelinkt is aan informatiemanagement en het gebruik van operationele data, kan dit soort informatie uiteraard ook dienen als input voor foresight op een strategisch niveau.

De keuze waar iets wordt belegd in de organisatie bepaalt welke methodes, competenties en technieken het best passend zijn. Maar dit is ook sterk afhankelijk van de daadwerkelijke implementatie.

2.6 Foresight als een gezamenlijk proces

Foresight kan een activiteit zijn van een individu, een team, een organisatie of een netwerk. Het kan zelfs zo open zijn dat het publiek erbij betrokken wordt. De kern zal vaak hetzelfde zijn (*inzicht opbouwen over de toekomst*), maar er zullen, afhankelijk van de vorm, andere zaken meespelen om het proces goed te laten verlopen. In deze sectie worden een aantal vormen van samenwerken verkend, inclusief de factoren die daarbij meespelen.

Vorm en doelstelling
Samenwerken kan in allerlei vormen, van een hecht team tot een open sociaal mediakanaal. Wenger en Snyder (2000) schetsen de volgende typische netwerkstructuren:

- Projectteam,
- Working group,
- Community of practice,
- Community of interest,
- Informal network/ social network/media network.

Al deze varianten kunnen gepositioneerd worden binnen een organisatie, tussen organisaties en in een open vorm. Welke vorm gewenst is, is afhankelijk van het doel.

In bijlage C is een tabel te vinden waarin van elke vorm een typische doelstelling wordt genoemd, de voorziene bestaansduur en een voorbeeld van toepassing in een foresight proces.

Teamwork en taskwork
Foresight is een *proces* dat bestaat uit een reeks van activiteiten die leidt tot een bepaalde gewenste uitkomst. Als we foresight neerzetten als een gezamenlijk proces, dan kunnen we de activiteiten op verschillende manieren verdelen over de betrokken actoren. Als het team groot genoeg is, dan zou een deel van het team zich bijvoorbeeld voornamelijk bezig kunnen houden met data verwerken, terwijl een ander deel zich bezighoudt met conclusies trekken. Anderzijds zou je ook alle actoren eenzelfde foresight proces kunnen laten doorlopen, en dan onderling de resultaten vergelijken om verschillen en overeenkomsten te identificeren.

Het verdelen van de inhoudelijke activiteiten die horen bij foresight valt onder **taskwork**. In teamverband spelen er echter ook andere zaken mee, zoals onderlinge interactie, rolverdeling, leiderschap, onderlinge feedback, motivatie en onderling begrip. Dit zijn voorbeelden van **teamwork** factoren en activiteiten. Deze zijn essentieel om een team goed te laten functioneren (Shuffer, Diaz Granados & Salas, 2011; Salas, Cooke & Rosen, 2008).

In bijlage D is er een tabel te vinden met diverse combinaties van team- en taskwork, zogenaamde werkwijzen. Bij elke werkwijze staat een beschrijving en een voorbeeld van toepassing binnen een foresight proces.

De meest passende werkwijze hangt af van de doelstelling van de samenwerking, en de context waarin deze samenwerking geplaatst wordt. Teams zijn veelal doelgericht, en hebben daarom een meer uitgewerkte structuur (taskwork, teamwork). *Communities* hebben meestal de doelstelling om kennis en ervaringen te delen, en kunnen daarom af met minder structuur, meer nadruk op informele communicatie en meer opportunistische houding. Open netwerken kennen nog minder structuur en coördinatie, en zijn vooral sterk als medium voor spontane interactie en het vastleggen van de ‘wisdom of the crowd’.

De vorm van de samenwerking moet passen bij de behoeftes. Als er behoefte is voor doelgericht resultaat, zoals een specifieke forecast op een bepaald onderwerp, dan zal een team-vorm gekozen moeten worden – met alle aandacht voor de

benodigde teamfactoren. Andersom, als er meer behoefte is aan netwerken en delen van ervaringen tussen organisaties, dan hoeft er geen team opgezet te worden, en is een community-vorm een meer geschiktere variant.

2.7 Foresight voor het cyber security domein

Aangezien het domein waarvoor men foresight activiteiten onderneemt bepalend is voor zowel de methode als het proces van foresight, is het van belang stil te staan bij de specifieke kenmerken van het cybersecurity domein in relatie tot foresight.

Ten eerste is het cybersecurity domein een snel veranderend landschap. Zo zijn kwaadwillenden steeds op zoek naar nieuwe modus operandi en onontdekte kwetsbaarheden voor cyberaanvallen. Trenddetectie over de modus operandi van aanvallers gaat dan ook eerder over een tijdsbestek van maanden dan jaren. Hieruit volgt dat adequaat vooruitkijken en anticiperen op mogelijke verstoringen, dreigingen en kansen of veranderende operationele omstandigheden een essentieel onderdeel is van cyberweerbaarheid. Om het dynamische cyberlandschap niet alleen bij te kunnen blijven, maar ook op een vooruitziende manier te kunnen aanvliegen is het nodig om foresight activiteiten eveneens dynamisch, proactief en met een snelle doorlooptijd uit te voeren.

Ten tweede kent het cyberdomein een bijzonder data- en informatielandschap. Een groot deel van relevante data over dreigingen, aanvallen of aanvalstechnieken is niet openbaar. Cybersecurityinformatie is vaak bedrijfs- of staatsgevoelig van aard, en kan niet breed gedeeld worden. Hierdoor kan bijvoorbeeld het tracken van soorten aanvallen of de ontwikkelingen van bepaalde fenomenen lastig zijn en moet er genoegen genomen worden met incomplete informatie om een forecast te maken.

Er zijn veel initiatieven opgezet om datadeling te stimuleren. Zo ontwikkelt het NCSC zich als een knooppunt om incidentdata te verzamelen en te aggregeren. Dit is een logische stap, aangezien cybersecurity incidenten reeds aan de NCSC gerapporteerd dienen te worden. Daarnaast bestaan er ook sectoren die een gezamenlijk opgebouwd cyber threat landscape rapport opstellen, zoals de financiële sector.

Naast incidentdata zijn er echter nog andere bronnen die relevant kunnen zijn voor cyber foresight activiteiten. Informatie betreffende de omstandigheden van cyberincidenten en/of specifieke kwetsbaarheden (zgn. *circumstantial information*) kan ook waardevolle inzichten bieden voor cyber foresights. Dit type informatie is, in tegenstelling tot cyber-incidentdata, vaker uit open bronnen te halen. Zo is het bijvoorbeeld mogelijk om Twitter te scrapen op *circumstantial information* of nieuwe cybersecuritytools.

Tot slot is het ook voor het cyberdomein goed om onderscheid te maken tussen operationeel en strategisch foresighten (zie ook 2.5.2.1 en 2.5.2.1). Onder de categorie operationeel foresighten vallen in het geval van het cyber domein met name activiteiten als *operational threat intelligence*. Dit betreft o.a. de detectie van een hack, de analyse ervan en de respons. Hierbij wordt bijvoorbeeld ook gekeken naar soortgelijke incidenten in het verleden waarna middels dataextrapolatie gekeken wordt hoe een hieruit afgeleide mogelijke trend zich in de toekomst zou

kunnen ontwikkelen. Echter, door het snel veranderende landschap en de werkwijze van hackers om te zoeken naar onontdekte kwetsbaarheden om uit te buiten is het zelfs voor de korte termijn moeilijk om voorspellingen te doen over bijvoorbeeld welke type aanvallen in te toekomst vaker of juist minder vaak zullen voorkomen. Daarnaast kunnen deze nieuwe soorten aanvallen of kwetsbaarheden moeilijk gedetecteerd worden aangezien er nog geen indicatoren van bekend zijn die op een incident zouden kunnen wijzen. In het geval van strategisch foresighten valt eerder te denken aan activiteiten als *cyber threat landscaping*. In deze rapporten over het dreigingslandschap wordt Chief Information Security Officers (CISO's) gemeld wat er de komende jaren kan worden verwacht op het gebied van cyberaanvallen. Deze analyses worden veelal gebaseerd op expert-based judgment en de ervaringen uit de cybersecurity community.

2.8 Technologische ondersteuning voor Foresight

Technologieën kunnen op verschillende manieren het foresight proces ondersteunen, bijvoorbeeld door data sneller te verwerken middels automatisering of door datadeling te faciliteren. Het is belangrijk op te merken dat hierbij technologie bedoeld wordt in de brede zin van het woord, inclusief softe technologieën, methodieken en werkwijzen. In de context van deze rapportage onderscheiden we drie rollen die technologie kan spelen in het ondersteunen van foresight-activiteiten, te weten 1) procesondersteuning; 2) kennisondersteuning; en 3) teamworkondersteuning (Neef, van Berlo, Molema, & Govers, 2021).

In bijlage E staat een verdere uitleg van deze rollen en worden er enkele specifieke voorbeelden gegeven van ondersteunende tools.

2.9 Samenvatting

In dit hoofdstuk hebben we diverse elementen van een succesvol foresight proces geschetst, zowel op het niveau van de inhoud (methodes, cognitief proces, biases etc.), als op het niveau van het proces (teamwerk, tooling). Het toont de complexiteit van cyber foresight vanwege de relatief jonge staat van de methode en de toepassing ervan op het relatief nieuwe terrein van cyber. Daarnaast zijn er vele verschillende elementen waarmee rekening moet worden gehouden. In het volgende hoofdstuk wordt er beschreven welke behoeftes er leven bij de beoogde deelnemers aan het gezamenlijk cyber foresight platform.

3 Analyse

3.1 Aanpak en methode

Om inzicht te krijgen in welke behoeften er leven rondom cyber foresight bij de geïnteresseerde partijen en aan welke eisen een samenwerkingsverband zou moeten voldoen, zijn er interviews gehouden met vertegenwoordigers van geïnteresseerde organisaties. Er zijn ook twee interviews geweest met partijen die al ervaring hebben met een gezamenlijk platform en/of het uitvoeren van gezamenlijke foresight om *tips and tricks* op te halen en gevormde ideeën te toetsen (de onderste twee organisaties in tabel 3). Alle geïnterviewde organisaties zijn geïdentificeerd in samenwerking met de projectbegeleider vanuit het NCSC. Er is met de volgende organisaties gesproken:

Tabel 3 Geïnterviewde organisaties voor dit project.

Organisatie	**Reden interview**
Nederlands Cybersecurity Center (NCSC)	Beoogd deelnemer gezamenlijke foresight
Cyber Warfare Training Centre – Defensie Cyber Commando	Beoogd deelnemer gezamenlijke foresight
Digital Trust Centre van het Ministerie van Economische Zaken	Beoogd deelnemer gezamenlijke foresight
Rijkswaterstaat	Beoogd deelnemer gezamenlijke foresight
DICTU, Beheerderseenheid Ministerie van Economische Zaken (Security Operation Centre)	Beoogd deelnemer gezamenlijke foresight
NCTV	Beoogd deelnemer gezamenlijke foresight
Nationale Politie	Beoogd deelnemer gezamenlijke foresight
Foresight Analysis Network Koninklijke Luchtmacht	Ervaring met gezamenlijke foresight door diverse overheidspartijen
Cyber Warfare Training Centre – Defensie Cyber Commando	Verkennende studie foresight methodes

De interviews zijn aangepakt volgens de semigestructureerde methode. Er is een interviewguide opgesteld die in elk interview is toegepast. Hierbij is er geen exact vraag-antwoord format toegepast maar werd er wel zorg voor gedragen dat steeds dezelfde vragen werden gesteld en dat alle onderwerpen aan bod kwamen.

De vragen waren verdeeld over vier blokken:
1 Terminologie en de plaats van foresight in het werk van de organisatie,
2 Inventarisatie van huidige werkwijzen,
3 Toekomstvisie,
4 Foresight in samenwerkingsverband.

De volledige interviewguide is te vinden in bijlage I. Van elk interview is er een verslag opgesteld, dat is goedgekeurd door de geïnterviewde. Deze zijn vertrouwelijk, tenzij anders wordt bepaald door het NCSC en de geïnterviewde gezamenlijk.

3.2 Observaties

Uit de interviews zijn diverse observaties gedestilleerd. Hieronder staan allereerst de algemene observaties, gevolgd door observaties over de diversiteit van de beoogde partners, de huidige werkwijzen en de zienswijzen op samenwerking.

3.2.1 Algemene observaties

De observaties die volgen zijn gebaseerd op de gehouden interviews en wijzen op specifieke aspecten die verder uitgekristalliseerd moeten worden tijdens de volgende stap in het project, de brainstorm, om zo ieders positie helderder te krijgen.

Bijna alle geïnterviewde partijen voeren al enkele foresight activiteiten uit of zouden deze kant op willen. Sommigen van hen namen eerder al deel aan het Cyber Forecasting Toernooi dat in 2019 georganiseerd werd door onder andere het Ministerie van Buitenlandse Zaken en TNO. Dit evenement heeft bij de geïnterviewden een positieve indruk achtergelaten en het enthousiasme voor foresight versterkt.

Op het gebied van methoden is er niet één duidelijke methode die door alle partners gedeeld wordt. Er zijn dan ook veel verschillende methoden in omloop. Dit komt waarschijnlijk door het relatief jonge veld van cyber security en de recente toepassing van foresight door de deelnemende organisaties. Ook wordt er nog weinig gebruik gemaakt van technologische ondersteuning. Vaardigheden die men graag wil ontwikkelen komen sterk overeen met vaardigheden die van belang zijn in het inlichtingenveld. Een andere vaardigheid die werd benoemd is het kunnen formuleren van de juiste vragen aan de hand waarvan de foresight te verrichten. Hierbij is de scope qua onderwerp ook nog niet helemaal afgebakend. De organisaties gaven hier verschillende antwoorden op. Qua tijdshorizon lijken de organisaties redelijk op dezelfde lijn te zitten: de foresight zou zich moeten richten op de komende 3 tot 5 jaar.

De geïnterviewde partijen zien heil in samenwerking, maar verschillen in wat ze er precies uit willen halen. Iedereen spreekt over de toegevoegde waarde van een multidisciplinair perspectief. Anderen geven aan dat er van elkaar geleerd kan worden met betrekking tot methoden. Ook wordt aangegeven dat een ‘advocaat van de duivel’ altijd welkom is, om zo tunnelvisie te voorkomen. Deze voordelen werden duidelijk tijdens de deelname aan het eerdergenoemde Cyber Forecasting Toernooi. Hierin waren door de variëteit in achtergronden van de deelnemers verschillende visies op scenario’s, wat interessante discussies opleverde.

Een mogelijke belemmering voor samenwerking kan zijn dat bijna alle geïnterviewde partijen aangeven dat ze graag input willen geven en krijgen, maar dat ze het eigenaarschap willen houden over hun eigen eindproduct (bijv. de forecast). Uiteindelijk ligt de focus op de eigen organisatie en het eigen landschap. Een andere mogelijke belemmering is dat niet bij alle beoogde partners evenveel capaciteit beschikbaar is en dat vanwege de nog bestaande onduidelijkheid over het rendement van foresight activiteiten, het moeilijk zou kunnen worden om de investering hiertoe in gang te zetten.

Als beoogd resultaat van het gezamenlijke foresighten noemen de organisaties het delen van (openbare) data en het gezamenlijk schrijven van rapporten op huidige ontwikkelingen in verschillende aangrenzend gebieden (technologie, maatschappij, geopolitiek) die van belang zijn voor het cyber domein. Deze resultaten kunnen op verschillende manieren landen in de organisatie. Daarbij wordt wel aangegeven dat foresight meer is dan scenario's genereren en deze verspreiden. Sommige geïnterviewden geven aan dat scenario's hen inzicht verschaffen maar te weinig impact in de praktijk genereren. Men is zoekende naar manieren om meer resultaten uit het foresighten te halen, resultaten beter te communiceren en het werk beter strategisch te kunnen positioneren en inzetten. Wellicht dat het platform hierin kan ondersteunen.

Naast het gezamenlijk ontwikkelen van scenario's noemt men ook nadrukkelijk het gezamenlijk investeren in training als mogelijk resultaat van de samenwerking. Hiermee bedoelt men zowel het trainen on-the-job, bijvoorbeeld door elkaar aan te scherpen door elkaar bewust tegenspraak te geven over bepaalde assumpties of analyses (aangeduid door de geïnterviewden als advocaat van de duivel spelen, een bekende methode om tunnelvisie en *groupthink* te voorkomen), als specifieke formele training.

Met betrekking tot het netwerk waarbinnen de gezamenlijke foresight zou plaatsvinden is men nog zoekend. Een sterk hiërarchische opzet lijkt niet voor de hand te liggen. Het interview met iemand van het vergelijkbare Foresight Analysis Network van de Koninklijke Luchtmacht bevestigt dit.

3.2.2 Diversiteit van de beoogde partners

Wat opvalt tijdens de interviews, is de diversiteit van de beoogde partners. Dit uit zich allereerst in verschillende posities en functies van de geïnterviewden binnen de organisaties zelf. Eén geïnterviewde bijvoorbeeld, beschrijft zijn werk als heel operationeel, met activiteiten die dagelijks terugkomen. Anderen werken op strategisch niveau en van hen wordt een brede blik op de gehele organisatie gevraagd. Ten tweede is het verschil zichtbaar tussen de organisaties onderling, bijvoorbeeld het doel en functioneren van de organisaties. Ten derde is er een verschil in ervaring met foresight. Twee organisaties zijn al drie jaar bezig met het onderwerp, drie zijn net begonnen en anderen moeten er nog mee beginnen. Dit verschil ziet men ook vaak terug in de beschikbare capaciteit: soms zijn er speciale teams voor, en soms komt het neer op personen die het naast hun reguliere functie moeten doen. Vier organisaties hebben speciale capaciteit voor foresight. Voor de anderen is foresight een extra activiteit naast de reguliere werkzaamheden. Wat opvalt is dat er ondanks deze verschillen door de meesten wel is deelgenomen aan het Cyber Forecasting Toernooi. Dit zorgt voor enige nivellering in kennis en ervaring. Ook erkent iedereen het nut van foresight en het ontwikkelen van omgevingsbewustzijn.

3.2.3 Huidige foresight praktijken

Het valt op dat er uiteenlopende termen door de beoogde partners gebruikt worden, waarbij niet iedereen altijd hetzelfde verstaat onder een term. De beoogde partners zijn zich bewust van deze ambiguïteit.

Er is uit de interviews nog geen eenduidige methodologie te onderscheiden die de beoogde partners gemeen hebben. Foresight is ook redelijk nieuw voor de

overheid, dus concrete ervaringen zijn nog schaars. Vijf organisaties laten zich voeden door experts en twee organisaties richten zich op de eigen verkenning van ontwikkelingen van dreigingen en specifieke signalen. Een van de geïnterviewden is nu bezig met een onderzoek over methodieken, om het eigen team verder te ontwikkelen. Het verschil in methode door organisaties wordt niet verklaard door de relatieve nieuwigheid van het foresighten binnen de organisatie en de inbedding ervan in de werkzaamheden. Ook maken sommige partijen al gebruik van technische (basis) tools en anderen nog helemaal niet. Er zijn ook partijen die nog geen processen ingeregeld hebben en/of producten hebben opgeleverd. Wat betreft termijn voor de foresight is er één partner die drie jaar vooruitkijkt. De andere partners waren minder specifiek in hun horizon. Voor de meeste beoogde partners vindt het foresighten plaats op het strategische niveau maar is het nog niet verankerd in de organisatie. Een enkeling doet het foresighten juist op operationeel niveau.

3.2.4 Visie op toekomstige samenwerking voor foresight

Er is een sterke consensus dat het voor een succesvolle samenwerking belangrijk is om een gedeeld begrip te hebben van wat met elke term bedoeld wordt. Het is daarbij niet nodig om te komen tot dé definitie, maar wel tot een werkbare definitie waarin alle partners zich kunnen vinden.

Naast een gedeeld begrippenkader (bijvoorbeeld over wat er precies verstaan wordt onder termen zoals foresight en forecasting) wordt een gedeeld belang en een gedeeld doel genoemd als voorwaarde voor samenwerking. Daarnaast noemt men als voorwaarde dat iedereen een zekere mate van betrokkenheid moet tonen.

Men wil graag het eigenaarschap over het eigen eindproduct behouden, maar het samenwerkingsverband gebruiken voor het aanscherpen van methodes, het verbeteren van resultaten en het verkrijgen van multidisciplinaire input. Daarnaast geven bijna alle geïnterviewden aan dat er een behoefte is om de vaardigheden te verbeteren. Hierbij noemt men zaken als *critical thinking*, *out-of-the-box*, biases herkennen en slimme dataverzameling.

Sommige partijen geven aan dat niet alle informatie met alle deelnemers gedeeld kan worden. Een eventueel platform zou het dan moeten kunnen faciliteren dat informatie slechts met enkelen gedeeld wordt. Het is de vraag of zoiets wenselijk en/of haalbaar is. Uit het interview met het Foresight Analysis Network van de Koninklijke Luchtmacht (FAN) kwam de aanbeveling om hier geen onderscheid in te maken en alleen informatie uit open bronnen met elkaar te delen.

3.2.5 Lessen van het FAN

Naast gesprekken met de potentiële deelnemers aan het platform is er ook gesproken met het Foresight Analysis Network, een initiatief vanuit de staf van de Nederlandse Koninklijke Luchtmacht. Zij brengen al een aantal jaren geïnteresseerden vanuit diverse hoeken van de Defensieorganisatie - maar ook daarbuiten - samen om na te denken over vraagstukken gerelateerd aan foresight. Uit dit gesprek kwamen er een aantal aanbevelingen naar voren om mee te nemen in het ontwerp van een platform voor foresight in cybersecurity.

Allereerst over het opzetten van het netwerk. Het advies was om zoveel mogelijk te werken met openbare bronnen. Dit houdt het proces voor iedereen toegankelijk en

werkbaar. Daarnaast is het van belang om met enige regelmaat ook ruimte te maken voor fysieke ontmoeting. Het bouwen aan de onderlinge relatie is een belangrijk aspect van de samenwerking. Consistentie in het onderhouden van de contacten is essentieel om de inspanningen niet te laten verwateren. Een belangrijk bouwblok hierin zijn het regelmatig organiseren van gezamenlijke (foresight)activiteiten. Tot slot werd er aangegeven dat de ontwikkeling van het netwerk niet lineair hoeft te verlopen: zij ervaren dat sommige deelnemers er altijd zijn en anderen alleen als het past qua inhoud en werkdruk. Maar, men sluit bijna altijd wel weer aan op een gegeven moment. Schrik dus niet van absentie en ga uit van de behoefte van de deelnemers.

Ten tweede werden er enkele tips gegeven over de inhoud. Een scope bepalen is en blijft moeilijk. Dat blijft een continu proces. Thema's worden bij het FAN gekozen op basis van wat de trekkers van het netwerk observeren 'in de buitenwereld' en op basis van de bekende interesses van de deelnemers. Als ondersteunende software wordt er bij het FAN gebruik gemaakt van Petlet en Miro. Maar men gebruikt verder niet veel technische hulpmiddelen in het proces.

Tot slot gaf ook deze geïnterviewde aan dat er veel waarde zit in het gezamenlijk opbouwen van omgevingsbewustzijn. Het bijeenbrengen van diverse perspectieven is zeer waardevol.

3.3 Conclusies

De interviews hebben aangetoond dat het vormen van een samenwerkingsverband geen sinecure is. Foresight in cyber security is een relatief nieuw fenomeen voor de Nederlandse overheid. Eenduidigheid in gebruik van definities en een open, flexibele structuur van het platform zal van belang zijn om potentiële deelnemers te binden en te behouden. De gedeelde behoefte aan het ontwikkelen en trainen van vaardigheden is daarin iets wat kan samenbinden als gezamenlijk doel. Gebaseerd op de interviews lijkt dit de voornaamste behoefte die het platform kan vervullen: competentie-ontwikkeling, wellicht meer nog dan de behoefte aan het gezamenlijk uitvoeren van foresight op het gebied van cybersecurity. Maar uiteraard hoeft het één het ander niet uit te sluiten, want in veel interviews werd ook de toegevoegde waarde van verschillende perspectieven en databronnen voor het uitvoeren van foresight genoemd. Het platform kan ook daar een mooie rol vervullen, bijvoorbeeld door te helpen in het voorkomen van tunnelvisie.

De interviews hebben zodoende een paar belangrijke inzichten opgeleverd. Ten eerste verschilt de opvatting van wat foresight inhoudt per deelnemer wat betreft interesse, huidige gebruik, middelen en ambities. Men deelt echter een gemeenschappelijke interesse in het delen van data en het belang van multidisciplinair werken. Ook is iedereen geïnteresseerd in het ontwikkelen van competenties en heeft men dezelfde visie over het behoud van autonomie, bijvoorbeeld over (de doorontwikkeling van) eigen scenario's. De interviews wijzen daarmee uit dat er zeker een grond is voor samenwerking, maar dat het goed is om met elkaar in gesprek te gaan over de precieze details en werkwijze. Daarbij is het niet ondenkbaar dat de opzet er één moet zijn die ruimte biedt voor *pick-and-choose*: niet elke deelnemer hoeft aan elke activiteit deel te nemen, maar kan kiezen wat past bij de behoefte van zijn of haar organisatie.

Gebaseerd op de inzichten die zijn opgedaan in de literatuurstudie, de analyse van de interviews en de lessen die het FAN met ons gedeeld heeft, hebben we enkele dimensies gekozen die leidend zullen zijn voor het verder uitwerken van de opzet van het platform. De presentatie hiervan in het volgende hoofdstuk zal de basis zijn voor een brainstorm met alle potentiële deelnemers aan het platform.

4 Suggesties en aanbevelingen

We kunnen concluderen dat er zeker interesse is bij de geïnterviewde partijen om een samenwerking op te zetten op het gebied van foresight in het cyber domein. Er zijn wel verschillen in het belang dat men hieraan hecht voor de eigen organisatie, hoeveel vertrouwen men heeft in samenwerking op dit gebied en hoeveel men wil investeren qua personeelsinzet. Dit betekent dat er, ondanks de positieve vooruitzichten voor een gezamenlijk foresight platform, nog veel uitgewerkt moet worden qua methodiek, doelstelling en opzet.

In dit hoofdstuk schetsen we enkele opties voor een gezamenlijke foresight proces. Dit doen we aan de hand van vier kenmerken. Deze kenmerken representeren de kernonderwerpen die uit de interviews gedestilleerd zijn als belangrijke thema's, en waarop veel variatie zat tussen de geïnterviewde partijen.

4.1 Denkrichtingen voor een foresight platform

Uit interviews kwamen vier belangrijke kenmerken terug die bepalend gaan zijn voor de komende discussie: **vraagvorm, samenwerkingsvorm, informatiedelingsniveau en ontwikkeling van het platform**.

Over elk van deze kenmerken blijken er tussen de deelnemers verschillende opvattingen te bestaan. Het zijn de kernmerken waar het verschil tussen de organisaties en hun behoeften tot uiting komt, en waar er gezocht moet worden naar overeenstemming. Hoewel er meer kenmerken te identificeren zijn uit de interviews die van belang zijn voor het platform, is er op deze andere onderwerpen dusdanige overeenstemming tussen de bevraagde partijen dat deze buiten beschouwing kunnen worden gelaten.

Bij sommige van de vier kenmerken zit er opbouw in de varianten (ordinaal) – bijvoorbeeld van laag naar hoog – maar soms zijn het van elkaar losstaande opties (nominaal). Hieronder wordt elk kenmerk toegelicht samen met een voorbeeld relevant voor de context van foresight in het cyberdomein.

4.1.1 Vraagvorm

Het eerste kenmerk, de vraagvorm, gaat over de aansturing van de activiteiten in het platform: wat is de aard van de foresight-vraag? Een platform zou verschillende soorten vragen aankunnen. Behandelt het team een open vraag ('hoe ziet de wereld er over een aantal jaar uit?'), of een gesloten vraag ('gaat er een grootschalige aanval op de Nederlandse financiële sector plaatsvinden'?), of iets er tussenin, bijvoorbeeld op basis van een thema ('verken toekomstige dreigingen op de financiële sector'). Naarmate meer afbakening en doel gegeven wordt aan de vraag, zal het proces verschuiven van toekomstverkenning (foresight) naar voorspelling (forecasting).

Tabel 4 Ontwerpdimensie 'Vraagvorm'.

Dimensie: Vraagvorm		
Open vraag	**Thematische vraag**	**Gesloten vraag**
Verkenning, scanning, zoektocht naar interessante ontwikkelingen, zonder specifieke vraag.	Toekomstverkenning van een bepaald gesteld thematisch gebied, of fenomeen.	Opdracht om een bepaalde vraag te beantwoorden.
Bouw een lange-termijn toekomstbeeld op van cybersecurity in Nederland. Identificeer de belangrijkste actoren die over 5 jaar een rol gaan spelen in het cybersecuritybeeld Nederland.	*Verkenning van de impact van AI op de cybersecurity in de Nederlandse logistieke sector. Welke cybersecurity dreigingen gaan er de komende 5 jaar plaatsvinden op de landelijke en regionale verkiezingen?*	*Gaan we binnen een 2 jaar doelbewuste digitale aanvallen zien op Nederlandse kabinetsleden?*

4.1.2 Samenwerkingsvorm

Het tweede kenmerk, de samenwerkingsvorm, gaat over de intensiteit van de samenwerking. Moet deze gezien worden als het vormen van een team (zoals besproken in hoofdstuk 2), of gaat het meer richting een community of een netwerk. Beperkt men zich tot een vrijblijvende bijeenkomst één à twee keer per jaar? Of komt men regelmatiger samen en heeft men ook daadwerkelijk gezamenlijke werksessies en producten?

Tabel 5 Ontwerpdimensie ‘Samenwerkingsvorm’.

Dimensie: Samenwerkingsvorm		
Open netwerk	**Werkgroep**	**Team**
Een open groep waar partners van verschillende achtergronden zich vrij bij kunnen aansluiten. Geen vaste taken. Vrijelijke delen van materiaal en interesses.	Een groep met een gelijkwaardige achtergrond en interesses, en een gezamenlijke doelstelling om informatie en kennis te delen.	Een geselecteerde groep die een specifieke opdracht uitvoert.

4.1.3 Informatiedelingsniveau

Het derde kenmerk, het niveau van informatiedeling, gaat over het niveau en de mate waarin (bewerkte) informatie gedeeld wordt. Dit kan zich beperken tot ‘ruwe’ data als signalen en open bronnen tot uitgewerkte duidingen van specifieke onderwerpen. Een tussenvariant kan hier zijn ruwe data plus eerste aantekeningen. Tevens speelt ook de vertrouwelijkheid van de informatie een rol, hoe hoger het informatiedelingsniveau, hoe makkelijker ook vertrouwelijke informatie gedeeld wordt binnen het platform.

Tabel 6 Ontwerpdimensie ‘Informatiedelingsniveau’.

Informatiedeling		
Laag: **Delen van data en signalen.**	**Middel:** **Delen van patronen en interpretaties.**	**Hoog:** **Delen van voorspellingen**
De deelnemers van de groep delen data en interessante signalen, maar geen interpretaties, of voorspellingen.	De deelnemers van de groep delen, naast data en signalen, ook interpretaties en analyses daarvan. Er worden geen voorspellingen gedeeld.	De deelnemers werken samen in het gehele foresight proces waarbij data, patronen, interpretaties en voorspellingen gedeeld worden.
De groep deelt in het reguliere overleg relevante signalen uit media, en informatie uit bronnen.	*De groep bespreekt hoe bepaalde signalen tot patronen leiden, en delen inzichten hoe patronen op elkaar inwerken. Toekomstbeelden en voorspellingen worden niet gedeeld of samen opgebouwd.*	*De groep bouwt samen aan gedetailleerde toekomstbeelden en voorspellingen, die als (aanvullende) input dienen voor de organisatie specifieke voorspellingen.*

4.1.4 Platformontwikkeling

Het vierde en laatste kenmerk, de ontwikkeling van het platform, gaat over de doorontwikkeling van het platform en haar deelnemers. Aan de ene kant kan het platform zich limiteren tot een simpel verzamelingsplatform, aan de andere kant kan het platform ook het coördineren of zelfs verzorgen van trainingen op zich nemen. Hierbij kan men denken aan een continue variant van het Cyber Forecasting Toernooi. Een tussenvariant is hier ‘learning-on-the-job’, waarbij er zowel samen gewerkt wordt aan foresight producten als wel er gezamenlijk getraind wordt.

Tabel 7 Ontwerpdimensie ‘Platformontwikkeling’.

Ontwikkeling van het platform		
Vaste doelstelling	**Lerend**	**Verbredend**
Het platform heeft een vaste vorm, en gebruikt vaststaande methodes.	Het platform heeft een bepaalde manier van werken bij aanvang, maar leert van ervaringen en past daarop werkwijzen aan.	Het platform verbreedt gedurende de looptijd haar takenpakket, bouwend op ervaringen en nieuwe inzichten.
Het platform gebruikt methode XYZ voor foresight generatie.	*Het platform gebruikt methode XYZ als start, maar past de methode steeds verder aan de omstandigheden, capaciteiten en gestelde vragen.*	*Het platform begint als groep die toekomstverkenningen uitvoert, maar verbreedt haar taken ook naar gezamenlijke training, publieke informatievoorziening en denk- tank voor urgente vragen.*

4.2 Vier voorbeeldvarianten

Om te illustreren hoe het combineren van de gradaties in kenmerken eruit zou komen te zien in platformvarianten, zijn hieronder vier voorbeelden opgenomen. Deze vier varianten zijn niet de enige opties, maar zijn bedoeld als inspiratie voor een discussie over de uiteindelijke vorm van het platform. We hebben deze varianten de volgende namen gegeven: High Performance Team, Special Interest Group, Joint Learning Group en Horizon Scanning Network.

Er is geen noodzakelijk verband tussen de vorm van het platform en de methodes die ingezet worden. Binnen elke variant kunnen verschillende methodes relevant zijn, afhankelijk van de doelstelling van het platform. In de praktijk zullen methodes specifiek aangepast moeten worden aan de omstandigheden van het platform, zoals beschikbare capaciteiten, competenties, vraagsturing, rubricering van informatie en wensen van partners.

4.2.1 High performance team

Een high performance team laat zich kenmerken door een specifiek mandaat, gezamenlijk belang en gezamenlijk uitgevoerde opdrachten waarbij ook de interpretatie van de voorspellingen gezamenlijk uitgevoerd wordt. Dit omvat veelal ook een opleveringsverplichting van een foresight product zoals bijvoorbeeld een rapport. Om dit in een team te kunnen bereiken, is er een hoge mate van informatiedeling: ze delen veel data, interpretaties en analyses. Alle deelnemende organisaties dragen personeel bij en bieden ruimte om als een team te werken. Hoewel het team in een hechte vorm werkt, gaan ze niet verder dan hun opdracht. Het samenbrengen van visies en expertises binnen een toegewijd team maakt dat het kan functioneren als een *high performance* team.

4.2.2 Special interest group

Een special interest group is een verband voor partners met een gezamenlijke interesse in methodes of bepaalde onderwerpen. Binnen de groep worden ervaringen en informatie op de betreffende thematische interesse gedeeld. Deze thema- of interessegeoriënteerde insteek van het verband laat verder vrij hoe de intensiteit van de informatiedeling of het gezamenlijk leren eruitziet. Tevens kan het type vragen die binnen de groep behandeld worden ook verschillende vormen aannemen. Dit kunnen bijvoorbeeld open of gesloten vragen zijn, hetgeen afhankelijk is van het onderwerp dat binnen het verband wordt aangekaart. Het thema of het besproken onderwerp blijft dan ook leidend in de verdere opzet van het verband, dat zich meer als community laat kenmerken. Daarmee is deze variant ook vrijblijvender en vrijwilliger opgezet dan het hiervoor uiteengezette high performance team. Er is in dit geval dus geen sprake van directe of verplichte output.

4.2.3 Joint learning group

De joint learning group is enkel gericht op het delen van methoden en nieuwe inzichten ten behoeve van het ontwikkelen van vaardigheden en kennis omtrent het foresight proces. Dit omvat activiteiten die gericht zijn op bijvoorbeeld het delen van best practices en het trainen of verkennen van analysemethodes. De vraagvorm is daarbij wederom afhankelijk van de onderwerpen die daarbij aan bod komen. Ook de informatiedeling heeft te maken met het verder ontwikkelen en versterken van de gebruikte methodologieën. Daarbij ligt de samenwerkingsfocus naast het delen van ervaringen en informatie over methodes op het gezamenlijk trainen en oefenen zodat er als platform verder kan worden ontwikkeld op de foresight processen. Het onderscheid met een special interest group is dat daarbinnen slechts informatie wordt gedeeld omtrent een bepaald thema, en er niet samen getraind wordt ten behoeve van platformontwikkeling.

4.2.4 Horizon scanning network

Tot slot is het horizon scanning network een platformvariant waarin bredere vragen worden behandeld in een open setting. Het gaat hierbij om het verkennen van

algemene trends in het cybersecuritydomein met een open, naar buiten gerichte blik om zo te scannen naar de ontwikkelingen waar in de (nabije) toekomst mogelijk rekening mee moet worden gehouden. Doordat er vooral naar signalen gezocht wordt in open bronnen is er sprake van een laag informatiedelingsniveau. Om dit proces af te bakenen is er wel een thema of opdracht dat men wil verkennen. Toch betreffen de gestelde vragen in het horizon scanning netwerk vragen van een hoger abstractieniveau en een bredere insteek dan bij de special interest group het geval is. Ook is er in deze variant wel de insteek om samen output te produceren, hoewel de vorm daarvan niet vastligt. Daarnaast is het netwerk ook opener dan een high performance team en is er geen sprake van een lerende component zoals bij de joint learning group.

4.3 Aanbevelingen en verdere stappen

Zoals aangegeven in de inleiding, behandelt dit rapport de eerste fase van het beantwoorden van de onderzoeksvraag:
Op welke manier kunnen het NCSC en haar overheidspartners het beste gezamenlijk foresight-activiteiten uitvoeren om zo foresight in het cyber domein binnen de Nederlandse overheid te verbeteren?

Er zijn vele manieren om een foresight platform vorm te geven. De ideale vorm hangt onder andere af van de wensen, capaciteiten en belangen van de betrokken partners. Dit rapport geeft op basis van literatuurstudie en interviews inzicht in de behoeften van de potentiële partners, de overeenkomsten en verschillen hierin en mogelijke varianten voor de opzet van de samenwerking.

De aanbeveling op basis van dit rapport is om met de beoogde partners gezamenlijk in discussie te gaan over de kenmerken die geschetst zijn in paragraaf 4.1 en om de daaruit voortvloeiende voorbeeldvarianten uit paragraaf 4.2 te bespreken. Het is belangrijk om te komen tot een gedeeld begrippenkader (hebben de betrokken partijen het over hetzelfde wanneer bepaalde terminologie gehanteerd wordt), wederzijds getoetste verwachtingen en een organisatievorm die werkbaar is op zowel inhoud als proces.

De volgende stap in het project zal dan ook zijn om een (digitale) sessie te organiseren die deze discussie faciliteert. Daarbij is het niet alleen de bedoeling om te komen tot een gedeeld begrip en de keuze voor de beste vorm, maar ook om voorkeuren, posities en varianten nog scherper te krijgen. Vervolgens zal de uitkomst kunnen leiden tot een gezamenlijk gedragen organisatievorm, die getoetst kan worden in een of meerdere dry-runs.

5 Referenties

Belton, I. K., & Dhami, M. K. (2020). Cognitive biases and debiasing in intelligence analysis. In Routledge Handbook of Bounded Rationality (pp. 548-560). Routledge.

Competence Center on Foresight. (n.d.). Knowledge4policy.Ec.Europa.Eu. https://knowledge4policy.ec.europa.eu/foresight_en

Endsley, M. R. (2017). Toward a theory of situation awareness in dynamic systems. In Situational awareness (pp. 9-42). Routledge.

Tetlock, P. E., & Gardner, D. (2015). Sharpening Your Forecasting Skills.

Hulnick, A. S. (2014). 5 The future of the intelligence process. The Future of Intelligence: Challenges in the 21st century, 47.

Klaver, M., van de Kuijt, J., Joseph, R., van Luijk, E., (2019), Opzet en resultaten van het cyber forecasting toernooi, TNO Rapport,

Krzysztofowicz, M., Goudeseune, L., Bontoux, L., Balian, E., 2018. JRC CONFERENCE AND WORKSHOP REPORTS: Workshop on Horizon Scanning: from Interesting to Useful, from Practice to Impact. European Commission.

Neef, M., Veenendaal, M., Smulders, A., van der Ven, J., Cadet, B., (2018) SHIFTER: Scanning the Horizon for Future Technologies and Emerging Risks. A Horizon Scanning and Narrative Generation Method for Long-term Outlook Development in the Cybersecurity Domain, TNO Report.

Neef, M., van Berlo, M. P., Molema, D., & Govers, B. W. (2021). Een technologieverkenning naar het versterken van informatieduiding in de Nederlandse crisisbeheersing. Den Haag: TNO.

OECD. (2009). Horizons. OECD Publications. https://www.oecd.org/sti/futures/42332642.pdf

Pearson, T. (2015, June 29). DEFINING “HORIZON SCANNING”? Simplexity Analysis. https://www.simplexityanalysis.com/blog/2015/6/23/defining-horizon-scanning#:%7E:text=The%20Department%20for%20Environment%20Food,of%20current%20thinking%20and%20plannin

Pirolli, P., & Card, S. (2005, May). The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. In Proceedings of international conference on intelligence analysis (Vol. 5, pp. 2-4).

Salas, E., Cooke, N.J., & Rosen, M.A. (2008). On teams, teamwork, and team performance: Discoveries and developments. Human Factors: The Journal of the Human Factors and Ergonomics Society, 50, 540. doi:10.1518/001872008X288457

Slaughter, R. A. (1997). Developing and applying strategic foresight. ABN Report, 5(10), 13-27.

Shuffler, M. L., DiazGranados, D., & Salas, E. (2011). There’sa science for that: Team development interventions in organizations. Current Directions in Psychological Science, 20(6), 365-372

Valk, G. G. D. (2005), Dutch Intelligence- towards a qualitative framework for analysis: with case studies on the Shipping Research Bureau and the National Security Service (BVD). s.n.

Wenger, E. C., & Snyder, W. M. (2000). Communities of practice: The organizational frontier. Harvard business review, 78(1), 139-146.

Wiener, M., Gattringer, R., & Strehl, F. (2018). Participation in inter-organisational collaborative open foresight A matter of culture. Technology Analysis & Strategic Management, 30(6), 684-700.

6 Ondertekening

Den Haag, januari 2022

Ir. H.J. Fitski
Plv. research manager

TNO
Military Operations

B.D.S. Cadet
Auteur

A Verdere toelichting termen rondom Foresight

Trendverkenning
Trendverkenning kijkt naar patronen uit het verleden die zich in de toekomst zouden kunnen herhalen. Hoewel het waardevolle inzichten kan geven, richt trendverkenning zich niet op het identificeren van potentiële onverwachte gebeurtenissen. Daarom zijn er andere voorspellingsmethodieken ontwikkeld.

Foresight
Het woord “Foresight” omvat alle activiteiten op het gebied van de verkenning van de toekomst. Het Competence Center on Foresight van de Europese Commissie definieert Foresight als volgt:

“Foresight explores the future of scientific and technological achievements and their potential impacts on society. It aims to identify the areas of scientific research and technological development most likely to bring about change and drive economic, environmental and social benefits for the future”.

Het proces om Foresight te generen omvat veel stappen, van horizon scanning (zie hieronder) tot lange-termijn scenario generatie, en wordt vaak als een overkoepelende term gebruikt. Een Foresight proces bestaat typisch uit een dataverzamelings- en inzichtproces, en een duidingsproces waarin signalen en patronen worden verwerkt tot toekomstscenario’s. Afhankelijk van data- en expertise-beschikbaarheid kan een foresightproces meer data- of juist expert-judgement gedreven zijn. Afhankelijk daarvan bevatten de ontwikkelde toekomstscenario’s meer of minder aannames of voorspellingen.

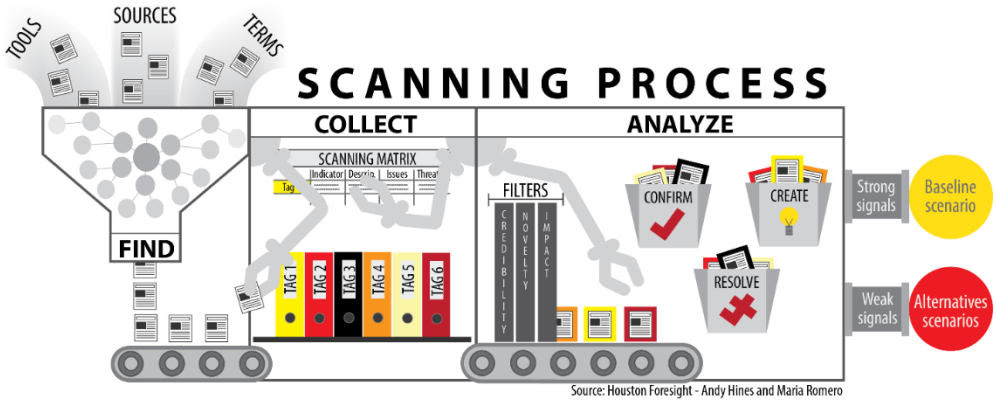
Horizon Scanning
Horizon scanning gaat over het analyseren van data om trends te herkennen. Hierbij wordt vaak gebruik gemaakt van historische data en nieuwsbronnen. In deze bronnen wordt gezocht naar ‘weak signals’: signaaldata die indicatief is voor een bepaalde ontwikkeling door de tijd heen maar nog niet overduidelijk alom aanwezig is. Denk bijvoorbeeld aan het signaleren van geopolitieke verandering (nieuwe machthebbers, nieuwe geopolitieke verhoudingen) en technologische veranderingen die op termijn zouden kunnen leiden tot nieuwe digitale aanvallen. Deze signalen kunnen opgepikt worden uit nieuwsbronnen, databases, interviews of andere bronnen.

De Organisation for Economic Co-operation and Development (OECD) definieert horizon scanning als volgt:

“Horizon scanning is a technique for detecting early signs of potentially important developments through a systematic examination of potential threats and opportunities, with emphasis on new technology and its effects on the issue at hand”.

De UK’s Department for Environment Food and Rural Affairs (DEFRA), stelt: dat horizon scanning

".. is the systematic examination of potential hazards, opportunities and likely future developments which are at the margins of current thinking and planning. Broadly speaking, it is a scientific way of exploring what is happening in the world around us, including unexpected issues, emerging trends, early signals, persistent problems, etc."



Figuur A.1 Scanning process by Andy Hines and Maria Romero (Houston Foresight).

Omdat horizon scanning in de kern gaat over het extrapoleren van trends uit data, is de tijdshorizon relatief kort.

Forecasting

Forecasting gaat over het voorspellen dat een bepaalde situatie zich gaat voordoen binnen een bepaalde tijd. Het is veel concreter dan foresight. Vaak wordt hierbij een gesloten keuze gebruikt (het event gaat zich wel of niet voordoen), of wordt er gesteld dat een bepaalde kwantitatieve waarde behaald wordt (hoeveel digitale aanvallen op een bepaalde organisatie er verwacht worden, of hoe groot het tekort aan cybersecuritypersoneel zal zijn in 2025). Meestal is een forecastvraag opgesteld in een vraagvorm waarop het antwoord achteraf beoordeeld kan worden op zijn juistheid.

Naarmate er meer data voorhanden is, en deze data consistent en logisch van aard is, heeft forecasting meer gemeen met statistische analyse dan 'trendwatching' (bv. horizon scanning). Als er naar fenomenen gekeken wordt waarover er weinig bruikbare data voorhanden is, of waar niet duidelijk is welke data relevant is, dan heeft forecasting meer gemeen met horizon scanning en foresight.

Een bekend begrip is 'superforecasting' (Gardner, Tetlock, 2015). Superforcasting is een techniek voor analisten om beter lange-termijn voorspellingen te kunnen doen door gevoeliger te worden voor weak signals, en beter in staat te zijn om eigen biases uit te schakelen. Deze techniek is toegepast in het NCTV/TNO project 'Cyber Forecasting Tournament' (Klaver, 2019)

Intelligence

Informatie wordt 'intelligence' genoemd als het relevant is voor het nemen van een bepaald besluit. Dit betekent dat er een waardering is gedaan van de data, een zogenaamde analyse. Daarmee is dus niet alle data of informatie meteen 'intelligence'. Data of informatie is pas intelligence zodra het is verwerkt. Het is dan geduid zodat het direct toepasbaar is in het besluitvormingsproces. Een voorbeeld:

Informatie over nieuwe soorten digitale kwetsbaarheden is generiek van aard, maar kan intelligence vormen voor instanties die daarop moeten reageren of juist gebruik van willen maken indien er een waardering aan wordt gegeven. Een intelligenceproces is dus het proces om van basisinformatie een analyse te maken die een bepaald besluit kan ondersteunen.

De traditionele manier om het intelligenceproces weer te geven is door middel van de zogenaamde intelligence cycle, bestaande uit vier fases: direction, collection, analysis en dissemination. Direction gaat over het uitzetten van de intelligence vraag en het bepalen wie wat gaat doen om de vraag te beantwoorden. Collection is de fase waarin de informatie verzameld wordt. In de analysefase wordt deze informatie verwerkt. In de laatste fase van disseminatie wordt het resultaat van de analyse verspreid naar diegenen voor wie het van belang is.

Inmiddels is er vanuit meerdere hoeken kritiek gekomen op dit model. Onder andere (Hulnick, 2014) vat deze kritiek samen. De kern van de kritiek richt zich voornamelijk op de volgordelijkheid van de stappen: dit zou niet stroken met de realiteit. Deze zouden vaker niet dan wel volgordelijk zijn. Tussen de diverse fasen gaat men soms weer terug naar de vorige fase of slaat men een stap over.

Intelligenceprocessen hebben veel gemeen met ‘forecasting’ processen. Ze doorlopen min of meer dezelfde stappen van bijvoorbeeld het zoeken en beoordelen van bronnen. Ze dragen beide bij aan een scherper handelingsperspectief.

B Verdere toelichting methodes

Methode	Focus	Genoemd of gebruikt door	Literatuur	Type activiteit
SHIFTER: Scanning the Horizon for Future Technologies and Emerging Risks. A Horizon Scanning and Narrative Generation Method for Long-term Outlook Development in the Cyber-security Domain	Expert-based judgment. Een foresight methode, gericht op het opbouwen van een toekomst narratief.	TNO; CWTC	Neef, Veenendaal, Smulders, van de Ven, Cadet, 2018.	Foresight
Super-forecasting	Forecasting methode, gebaseerd op versterken vermogen om weak signals te observeren.	TNO; DICTU. Gebruikt in het Cyber Forecasting Tournament	Tetlock, Philip E, and Dan Gardner. Superforecasting: The Art and Science of Prediction. 2015. (Klaver, 2018)	Forecasting
DESTEP	Methode afkomstig uit de strategische marketing. Methode ter ondersteuning van het bouwen van scenario's of horizon scanning. Methodiek bestaat uit de analyse van maatschappelijke ontwikkelingen aan de hand van de letters DESTEP: Demografie; Economie; Sociaal-Cultureel; Technologie; Ecologie; Politiek-Juridisch.	TNO; Foresight Analysis Network van de Koninklijke Luchtmacht	(Marijs & Hulleman, 2013)	Trend analysis (scenario generatie)
'Clingendael/ANV' Horizon Scanning methode	Een rapid horizon scanning methode, gecentreerd rond het identificeren van trends, megatrends voor nationale veiligheid.	TNO. Gebruik in het Analisten Netwerk Nationale Veiligheid (ANV) ANV/Clingendael methode	Horizon Scan Nationale Veiligheid, 2020.	Horizon Scanning
Futures Wheel	Methode om systematisch toekomstontwikkelingen van complexe	TNO.	The Futures Wheel: A Method for Exploring the Implications of	Trend analysis (generieke methode)

Methode	Focus	Genoemd of gebruikt door	Literatuur	Type activiteit
	systemen in kaart te brengen.		Social–Ecological Change, Bengston (2015)	
MARVEL. Method to Analyse Relations between Variables using Enriched Loops	Methode om systeem-dynamische afhankelijkheden in kaart te brengen. Basis voor het opbouwen van toekomstscenario's	TNO	Veldhuis et al., 2015	Trend analysis (generieke methode)
Teach the Future (Peter Bishop)	Een algemene foresight aanpak, ontwikkeld door Hines en Bishop en gepubliceerd in het boek 'Thinking about the Future: Guidelines for Strategic Foresight'. De aanpak bestaat uit zes stappen: framing, scanning, forecasting, visioning, planning en acting.	CWTC	Hines, A., & Slaughter, R. A. (2006). *Thinking about the future: Guidelines for strategic foresight*. P. J. Bishop (Ed.). Washington, DC: Social Technologies.	Foresight
SMART Futures (Rafael Popper)	Methodologie ontwikkeld door Rafael Popper in het kader van het European Foresight Platform. Deze aanpak bestaat grofweg uit vijf fases: scoping futures, mobilising futures, anticipating futures, transforming futures	CWTC	Popper, R., Amanatidou, E., Jones, B., & Teichler, T. (2012). FLA mapping. http://www.foresight-platform.eu/wp-content/uploads/2011/01/EFP-FLA-mapping-report.pdf	Foresight

C Samenwerkingsvormen

Tabel C.1 Typische samenwerkingsvormen en een voorbeeldtoepassing op een forecasting proces (Wenger & Snyder, 2002).

Vorm	**Typische doelstelling**	**Bestaansduur**	**Voorbeeld toepassing op een forecasting proces**
Project-team	Afronding van een taak	Totdat het de taak afgerond is	*Een project om een cybersecurity forecast 2050 rapport op te leveren in 2021*
Working group	Een dienst leveren	Totdat er geen behoefte meer is aan de dienst	*Een multi-organisatie forecast team dat elk half jaar een horizon scanning report oplevert.*
Community of practice	Kennis uitwisselen, capaciteiten opbouwen op specifieke onderwerpen	Zolang er voldoende animo is bij professionals om samen op te trekken	*De Netherlands Cybersecurity Forecasting Expert Network (NL-CYFEN) is een professional-only netwerk van analisten en foresight expert uit overheid en vitale sectoren.*
Community of interest	Informatie uitwisselen, samenkomen op een breed terrein	Zolang er voldoende interesse is om aan te sluiten, en de community levend te houden	*De Cybersecurity Future Interest Group brengt experts, bedrijven, publiek en overheid samen om samen de toekomst van cybersecurity vorm te geven. De CFIG organiseert jaarlijks een 'Future Roundtable' sessie waar deelnemers samen aan toekomstscenario's werken.*
Informal network, social network, media network	Informatie uitwisselen, netwerken op open kanalen. Emergent, zelf-organiserend.	Zolang er voldoende actoren zijn die actief zijn en bijdragen leveren.	*Het online magazine 'Cyber Future NOW' is een open magazine waar bijdrages gedeeld worden over nieuwe dreigingen, toekomstvoorspellingen en relevante ontwikkelingen. Tevens worden er spontane discussies gevoerd en vragen gesteld aan het lezende publiek.*

D Werkwijzen taskwork en teamwork

Tabel D.1 Teamwork factoren (naar Salas, et.al, 2008) en toepassing op een forecasting proces.

Werkwijze	**Beschrijving**	***Voorbeeld positieve toepassing in een foresight proces***
Team leadership	Duidelijk erkende leiderschapsrol	*Er is een aangewezen coördinator van het foresight team. Deze coördinator is het aanspreekpunt voor het team bij vragen en problemen, en fungeert als projectleider.*
Mutual Performance Monitoring	Transparantie in elkaars activiteiten en resultaat	*Er wordt in het foresight team gewerkt met een gezamenlijke virtuele werkruimte, en er zijn wekelijkse synchronisatiemeetings waar voortgang besproken wordt.*
Team orientation	Gedeeld beeld van aanpak en doelstelling	*Er is bij aanvang van het foresight team besproken wat een ieders belang is, en hoe er samengewerkt zou worden. Bij team meetings wordt standaard besproken of er zaken spelen bij de achterban organisaties die besproken moeten worden.*
Backup behaviour	Motivatie en competentie om elkaars taken over te nemen als dat nodig is.	*Er is een duidelijk beeld van actuele taken (bv. zoekopdrachten, analyses, updaten van hypotheses, voorbereiden presentaties), en het team pakt deze op als een gezamenlijke verantwoordelijkheid. Bij uitval van een teamlid worden taken vanzelfsprekend herverdeeld zodat het eindresultaat niet in geding komt.*
Adaptability	Aanpassend vermogen als er zaken veranderen	*Het foresight team heeft nauw contact met de opdrachtgevers, en toetst regelmatig of de basisopdracht nog actueel is. Als dit niet zo is, of als er relevante actuele ontwikkelingen zijn, dan wordt er een nieuw teamplan opgesteld, en werkzaamheden opnieuw ingedeeld.*
Shared Mental Models	Opbouw van een gezamenlijk gedeeld beeld	*Het team benadert het analyse proces en het trekken van conclusies over foresights als een gezamenlijk proces. In dit proces worden meningen en beelden gecontrasteerd, en wordt er gewerkt aan een beeld waar het team als geheel achter kan staat bij presentatie aan opdrachtgevers.*
Mutual Trust	Vertrouwen in elkaars competenties en motivatie om bij te dragen	*Het foresight team werkt al gedurende langere tijd samen in een stabiele samenstellingen, en kent elkaar goed. Door samen te werken aan de basisopdracht, en daarbij ook nog speciale opdrachten met urgentie uit te voeren hebben ze vertrouwen in elkaars vaardigheden en motivatie voor deelname in het team.*
Closed Loop communication	Gesloten communicatielijnen binnen team	*Inhoudelijke en projectmatige informatie wordt door iedereen in het team gedeeld, of toegankelijk gemaakt. Teamleden stellen elkaar op de hoogte van relevante communicatie met anderen. De teamleider is transparant over zijn interactie met de opdrachtgever en financierende instantie.*

E Verdere toelichting rondom technologische procesondersteuning

1 **Procesondersteuning**. Dit betreffen technologieën die helpen het proces van datavergaring tot voorspellingen te verbeteren en/of te versnellen. Deze tools zijn vooral gericht op het organiseren van de informatieruimte en het standaardiseren van dataformaten en informatieprocessen. In de praktijk gaat het hierbij vooral om kantoorapplicaties (zoals Office, databases, workflow-applicaties). Daarnaast worden er ook eerste stappen gezet in het automatiseren van (delen van) het foresightsproces op basis van AI en Big Data Analytics technologieën. Dit betreffen bijvoorbeeld geavanceerde webscrapers en horizon scanning tools die data uit openbare bronnen kunnen scrapen, clusteren en visualiseren.

2 **Kennisondersteuning**. De hierboven genoemde ‘OSINT-tools’ (tools die helpen om data uit openbare bronnen te vergaren en te analyseren) zijn tevens een voorbeeld van een technologie dat kennisondersteuning biedt. Onder dit type technologieën vallen systemen die kennis hebben van een bepaald domein of een thema, of die met behulp van achtergrondkennis kunnen assisteren in het duiden van informatie of signalen. Gebruikmakend van onderliggende kennismodellen kunnen dit type tools ondersteuning bieden in de kennisvorming en de duiding voorafgaand aan het kunnen doen van een voorspelling. Een ander voorbeeld hiervan zijn ‘social media mining’ tools die helpen om trends en patronen te herkennen uit content op social media-kanalen.

3 **Teamworkondersteuning**. Tot slot kan technologie ook ondersteunen in het verbeteren van de samenwerking in het foresightsproces. Dit betreft technologie die het delen van data, informatie en informatieproducten faciliteert of die helpen verschillende beelden bij elkaar te brengen om samen te werken aan informatieproducten. Bij dit laatste gaat het vaak om het creëren van ‘team situational awareness’: een gezamenlijk gedeeld beeld. Voorbeelden van dit type ondersteunende technologieën zijn ICT, waaronder standaard-kantoorapplicaties (bv. Microsoft Teams), social media platformen (Whatsapp) en commerciële applicaties.

De tabel geeft enkele specifieke voorbeelden van ondersteunende tools en de rol die zij kunnen vervullen:

Tabel E.1 Voorbeelden van ondersteunende technologie en hun rol in het proces.

Voorbeeld	**Betreft:**	**Proces ondersteuning**	**Kennis ondersteuning**	**Teamwork ondersteuning**
Itonics Radar	Horizon scanning tool dat geautomatiseerde ondersteuning biedt in het verzamelen, extraheren, clusteren en visualiseren van OSINT data	X	X	
Buzzsumo	Social media signaal monitor, biedt ondersteuning in het verzamelen en analyseren van content uit social media platforms	X	X	
COBRA	Software dat alle relevante (overheids)instanties met elkaar verbindt in noodsituaties.	X		X

Distributielijst TNO 2021 R10943-v2 (P2108)

JenV

Programmabegeleider NCSC Rik van Dijk r.van.dijk@minjenv.nl en Rik.vanDijk@ncsc.nl	pdf
Co-referent NCSC Martin Pekárek m.e.pekarek@minjenv.nl	pdf
Directie X	
- x@minjenv.nl	pdf
- h.hanoeman@minjenv.nl	pdf
- b.ter.luun@minjenv.nl	pdf

Politie

Directie Strategie en Innovatie	
- Innovatie@politie.nl	pdf
- onderzoekscoordinatie@politie.nl	pdf
- sven.hamelink@politie.nl	pdf
- kirsten.hehemann@politie.nl	pdf

TNO

Referent, Directeur Roadmap National Security Drs. R.A.J.M. Pellemans	email-alert
VP-manager VPVM Dr. T.W.J. van Ruijven	email-alert
VP-manager KOP T.H.E.E.A. Krabbendam MSc	email-alert
PMC cluster trekker Esther van der Weide	email-alert
Projectleider Deborah Lassche	email-alert
Programmaleider	
Allard Kernkamp	email-alert
Tom van Schie	email-alert
Gwen Ferdinandus	email-alert
Research manager projectleider Ingrid van Bemmel	email-alert
Yori Kamphuis	email-alert
Beatrice Cadet	email-alert
Dolinda Molema	email-alert
TNO Bibliotheek locatie Den Haag	hard copy & cd