Strategic Foresight Analysis voor een toekomstbestendige Defensie

Tom BURIN, Derrick-Philippe GOSSELIN, David MANUNTA, Pieter-Jan PARREIN & Koen TROCH

Dhr. Tom BURIN is *Global Security Intelligence Manager* voor Solvay. Hij heeft een achtergrond als jurist en medewerker van Defensie met een diverse operationele ervaring in inlichtingen en expertise op vlak van *Strategic Foresight*.

Prof. baron dr. ir. GOSSELIN is buitengewoon hoogleraar en directeur (oprichter) van het Institute for Futures Research aan de Universiteit Gent. Hij is lid van de Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten en van de Koninklijke Academie voor Overzeese Wetenschappen. Hij is voorzitter van het Studiecentrum voor Kernenergie SCK CEN, bestuurder van het Koninklijk Hoger Instituut voor Defensie, gewezen ondervoorzitter en bestuurder van het Von Karman Instituut en voorzitter van de European Corporate Security Association. Hij is tevens verbonden aan de universiteit van Oxford waar hij Associate Fellow is van Green Templeton College en de Oxford Martin School.

Le major David MANUNTA est officier 3D à COMOPSLAND, après avoir travaillé entre 2017 et 2021 pour la chaire *World Politics* du département *Conflict Studies* de l'École royale militaire et comme spécialiste *Strategic Foresight Analysis*. Il est titulaire d'un certificat interuniversitaire en analyse prospective (CIAP) de l'Université UCLouvain.

Majoor Pieter-Jan PARREIN is verantwoordelijk voor *Strategic Foresight Analysis* bij ACOS STRAT. Voordien werkte hij aan langetermijnplanning voor ACOS STRAT en aan de Strategische Visie voor Defensie voor de minister van Defensie.

Majoor Koen TROCH is wetenschappelijk medewerker aan de Koninklijke Militaire School, departement *Conflict Studies*, leerstoel *World Politics*. Hij is actief als docent in de basisvorming en aan het Defence College in het domein Internationale Veiligheid en Strategie. Hij geeft tevens les aan het Vesalius College, deel van de Brussels School of Governance.

Faire face à l'évolution rapide du monde dans lequel nous vivons doit rester une priorité pour des organisations robustes et à l'épreuve du temps telles que la Défense. La Strategic Foresight Analysis (SFA) est une méthode de prospective stratégique qui y contribue.[1] Cet article est basé sur le rapport final du premier projet de prospective stratégique de la Défense mené sur la période allant d'octobre 2020 à février 2021.[2] Ce projet a un horizon temporel de cinq ans et plaide pour des changements dans les orientations opérationnelles de la Défense. Les cinq auteurs ont contribué au développement de la méthode de ce premier projet de prospective stratégique de la Défense.

Wat is *Strategic Foresight Analysis*?

Bij *Strategic Foresight Analysis* (SFA) worden verschillende plausibele toekomstscenario's uitgewerkt om beter te begrijpen waarom en hoe de toekomst er anders zal uitzien dan vandaag. Dit gebeurt op basis van een weldoordachte beleidsvraag met mogelijk een grote impact op het toekomstige resultaat van het beleid. Vervolgens wordt de huidige strategie en/of het huidige beleid aan deze mogelijke toekomsten getoetst om na te gaan hoe toekomstbestendig of robuust deze is. SFA biedt geen glazen bol, maar verplicht een organisatie om na te denken over verschillende mogelijke toekomsten. Het uiteindelijke doel bestaat erin beleidsmakers toe te laten de strategie aan te passen om in die verschillende toekomstscenario's succesvol te zijn. Dankzij SFA kan een organisatie haar reactiesnelheid verhogen, verrassingen vermijden en sneller opportuniteiten ontdekken. SFA is een continu proces dat rekening houdt met de veranderende realiteit en terugkoppelt naar het topmanagement voor strategische of beleidsaanpassingen. Deze methode wordt toegepast door overheden, internationale organisaties (o.a. de NAVO en de EU) en ondernemingen.

[1] Dans un article précédent, le major David Manunta et le major Koen Troch ont déjà souligné l'importance de la SFA pour la Défense (Manunta, David en Troch, Koen, 'Sir, did you say Strategy? Our answer: foresight!', *Belgisch Militair Tijdschrift - Revue Militaire Belge*, Nr./N° 20, december 2020, p. 54-67).

[2] Chef Defensie – ACOS STRAT, 'Eindrapport Strategic Foresight Analysis X+5' en 'Aanbevelingen ACOS STRAT Operationele planning X+1/2', 5 mei 2021 (20210505 IU 'Eindrapport SFA X@5' en 'Aanbevelingen ACOS STRAT Operationele planning X@1-2.docx (21-50070310)).

SFA bij de Belgische Defensie

In het verleden had het operationele planningsproces een tijdshorizon van slechts één à twee jaar. ACOS Operaties en Training (ACOS O&T) heeft echter nood aan een planning op vijf jaar om zowel grote trainingsactiviteiten als de beschikbare capaciteiten beter af te stemmen op de te voorziene operationele noden. ACOS STRAT draagt hieraan bij door de aanbevelingen aan ACOS O&T omtrent de inzet, die al rekening hielden met een tijdshorizon van één à twee jaar, te kaderen in een *foresight* met een tijdshorizon van vijf jaar, een doelstelling van het Bedrijfsplan voor Defensie[3]. Daarnaast is SFA over een langere periode – tot wel twintig jaar – ook belangrijk om sturing aan de capacitaire planning te geven.

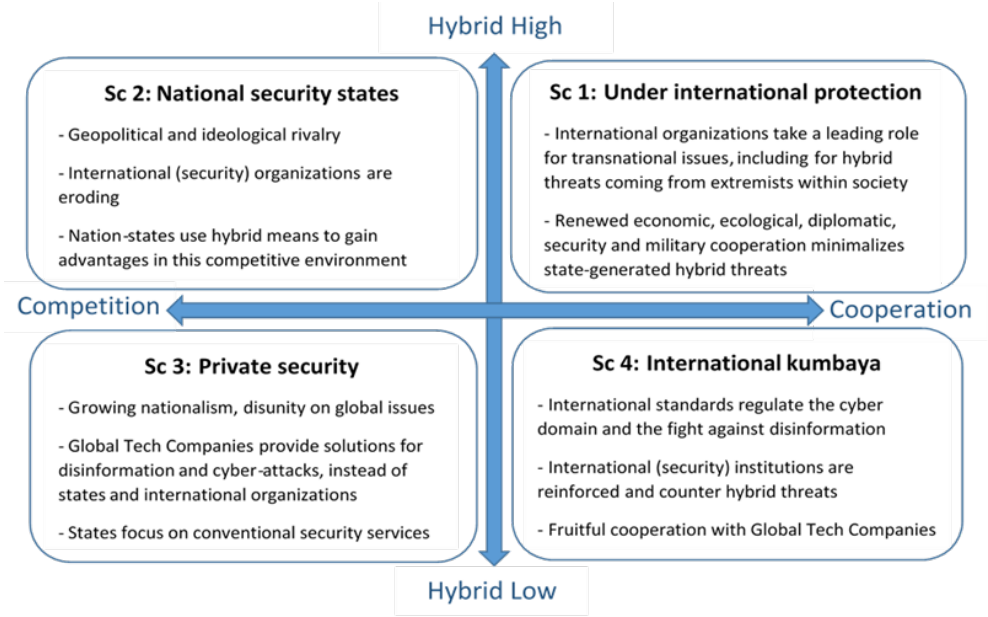
Opzet van de eerste SFA

De eerste SFA kreeg een heel brede insteek om tegemoet te komen aan het ontbreken van een overkoepelend strategisch kader – de Nationale Veiligheidsstrategie (NVS) was toen nog niet uitgewerkt. De onderzoeksvraag luidde als volgt: welke mogelijke toekomstscenario's voor België in de globale veiligheidsomgeving, met een tijdshorizon van vijf jaar? Vanwege deze brede onderzoeksvraag werden deelnemers met verschillende achtergronden betrokken: dertig vertegenwoordigers vanuit Defensie; de anderen waren tewerkgesteld bij de Civiele Bescherming, de Civiele Veiligheid, de industrie, het Centrum voor Cybersecurity België, de FOD Mobiliteit, het Nationaal Crisiscentrum, Justitie, Ontwikkelingssamenwerking, Staatsveiligheid, universiteiten, het Belgisch Instituut voor Postdiensten en Telecommunicatie, de FOD Buitenlandse Zaken, OCAD, EUMS en de FOD Financiën. Vanwege de coronacrisis werd er gebruik gemaakt van een digitale werkomgeving. De methodiek van de SFA werd ontwikkeld door de auteurs van dit artikel[4].

[3] Chef Defensie, *Bedrijfsplan voor Defensie 2021-2024*, Brussel, 9 maart 2021, p. 12 (https://dekast.mil.intra/Records/ArchiefLijn/132/CHOD/2021/20210309_IU_21-50046731_BedrijfsPlanDefensie21-24_N.pdf).

[4] Gebaseerd op de '4 Steps to the Future'-methode (Lum, Richard A. K., 4 *Steps to the Future: A Quick & Clean Guide to Creating Foresight*, Honolulu, Vision Foresight Strategy LLC, 2016) en de aanpak ontwikkeld door prof. D.P. Gosselin (Gosselin, Derrick & Tindemans, Bruno, Thinking Futures: Strategy at the Edge of Complexity and Uncertainty, Tielt, LannooCampus Publishers, 2016).

Tijdens een eerste workshop eind oktober 2020 werden drivers of change uit het verleden en het heden beoordeeld. De twee belangrijkste drivers of change 'hybride dreigingen'[5] en 'geopolitieke competitie' werden gebruikt om vier plausibele toekomstscenario's te ontwerpen die toch zo ver mogelijk uit elkaar liggen. In deze scenario's werden ook nog andere belangrijke drivers of change opgenomen, zoals polarisatie, klimaatverandering en cyber.[6]



Figuur 1: De vier toekomstscenario's: Welke mogelijke toekomsten voor België in de globale veiligheidsomgeving, met een tijdshorizon van vijf jaar

Er werd een bijkomende workshop 'hybride dreigingen' georganiseerd in samenwerking met het Crisiscentrum en expert Interdepartementale Samenwerking, majoor Maarten Verburg. Vervolgens werd een workshop *wind tunneling* opgezet samen met de cel Plans & Policy om na te gaan of de huidige strategie van Defensie

[5] Meer uitleg hierover in het eindrapport (zie voetnoot 2). Voor de definitie van het *European Centre of Excellence for Countering Hybrid Threats*: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
[6] Voor de uitgewerkte scenario's, zie het eindrapport (voetnoot 2).

(*Strategic Outcomes* van het Mission Statement van Defensie[7]) voor de verschillende toekomstscenario's overeind blijft. Deze workshop resulteerde in enkele strategische opties/aanbevelingen die hieronder worden uiteengezet.

Aanbevelingen vanuit de eerste SFA

De eerste vijf aanbevelingen voor Defensie gelden voor ieder scenario en de volgende vijf voor een aantal scenario's.

1. Onze nationale veiligheidsinstrumenten coördineren om de efficiëntie van het nationale veiligheidsbeleid te versterken

Een goede coördinatie vergt een duidelijke afbakening van verantwoordelijkheden, vastgelegd in een overkoepelende NVS. Het hele veiligheidsspectrum dient gedekt te worden, met enkel duplicatie waar nodig. Binnen de gebieden waar de capaciteiten van Defensie gelijkaardig zijn aan die van nationale veiligheidsactoren, zou er naar een intensievere samenwerking op vlak van investeringen en opleidingen gestreefd moeten worden. Complexe crisissen, zoals hybride acties in verschillende domeinen, vereisen verschillende veiligheidsactoren. Bijgevolg is er ook nood aan meer gecoördineerde training en oefeningen met vooral aandacht voor een overkoepelende *Command & Control*.

2. Het versterken van Europese samenwerking voor onze capaciteiten, in de eerste plaats met onze buurlanden

Onze Defensie is een trendsetter in Europa voor intensieve samenwerking op vlak van capaciteitsontwikkeling (marine, F-16, nieuwe gemotoriseerde capaciteit). Deze 'technische' samenwerking zou ook doorgetrokken moeten worden naar meer gezamenlijke operationele planning met onze partnerlanden.

3. De samenwerking met onze industrie en onderzoeksinstellingen verder versterken

Defensie moet meer dynamiek krijgen in de *triple helix* tussen Defensie, onze industrie en onze onderzoeksinstellingen om de weerbaarheid en strategische autonomie van België en Europa te versterken.

[7] Chef Defensie, *Mission statement Defensie: Opdrachtverklaring van Defensie en strategisch kader voor de paraatstelling*, Editie 2, Cab ChoD, Sep 2019, p. 17-18 (https://shpapps.mil.intra/sites/EDR/Publications/CHOD-APG-MISSION-001_N_E002_R002.pdf).

4. Het herkapitaliseren van het personeel van Defensie

Defensie heeft al belangrijke stappen gezet in het personeelsdomein. Daarnaast is er meer flexibiliteit nodig in ons personeelsbeleid om over alle nodige expertise binnen Defensie te beschikken, zeker in het kader van hybride conflicten die de nood aan cyber-/IT-specialisten en communicatie-/informatiespecialisten zeer groot maakt. Dit kan via een flexibelere verloning gekoppeld aan expertise en door meer deeltijdse militairen aan te werven.

5. Het versterken van strategische communicatie naar de maatschappij inzake de huidige veiligheidskwesties

Het is belangrijk dat onze maatschappij zich bewust is van de toenemende dreiging van hybride oorlogsvoering, informatieoperaties, cyberactiviteiten en de noodzaak om een geloofwaardige afschrikking te behouden via collectieve defensie.

6. Meer investeren in collectieve defensie

Collectieve defensie is heel relevant in de verschillende veiligheidstoekomsten met een tijdshorizon van vijf jaar, behalve, logischerwijze, in geval van het meest positieve toekomstscenario. Problematisch is wel dat in het meest negatieve toekomstscenario (scenario 2) er vanwege de moeilijke budgettaire en veiligheidssituatie en de prioritering van 'interne veiligheid'[8] en hybride dreigingen, geen bijkomend budget beschikbaar is voor deze kerntaak.

De NAVO dringt vandaag heel sterk aan op het verder uitbouwen van militaire capaciteiten die verbonden zijn aan collectieve defensie en ontrading, zoals bijkomende gevechtsvliegtuigen en gevechts- en vuurkracht voor de landstrijdkrachten, inclusief een adequate luchtverdediging. Binnen de beperkte tijdshorizon van vijf jaar van dit *foresight*-project kan de training en operationele inzet al sterker afgestemd worden op de kerntaak 'collectieve defensie'.

Nationale weerbaarheid (*resilience*) draagt eveneens bij aan deze kerntaak. Defensie zou daarom meer moeten trainen op het beveiligen van kritieke infrastructuur en belangrijke communicatielijnen op het nationale grondgebied en voor het ondersteunen van de militaire mobiliteit van troepen die via onze (lucht)havens ter

[8] Interne veiligheid omvat, naast nationale acties in het kader van collectieve defensie, iedere ontplooiing en actie van Defensie op het nationale grondgebied ten voordele van de maatschappelijke veiligheid.

versterking worden gestuurd. Een eveneens essentieel element van het verzekeren van collectieve defensie is het verzekeren van toptechnologie voor onze Defensie (zie de *triple helix*).

7. Meer aandacht besteden aan interne veiligheid

In het meest negatieve scenario 2 en in het meest positieve scenario 4 moet de Belgische Defensie meer inzetten op interne veiligheid. Dat de meeste veiligheidsexperten die deelnamen aan dit project scenario 2 als een heel plausibele toekomst beschouwen, is zorgwekkend. Mogelijke scenario's die meer nadruk op interne veiligheid vereisen zijn onder meer een grote cyberaanval, sabotage van kritische infrastructuur, terrorisme, een grote desinformatiecampagne, een CBRN-dreiging, beveiligen van militaire mobiliteit, crisisrespons na natuurrampen, een gezondheidscrisis.

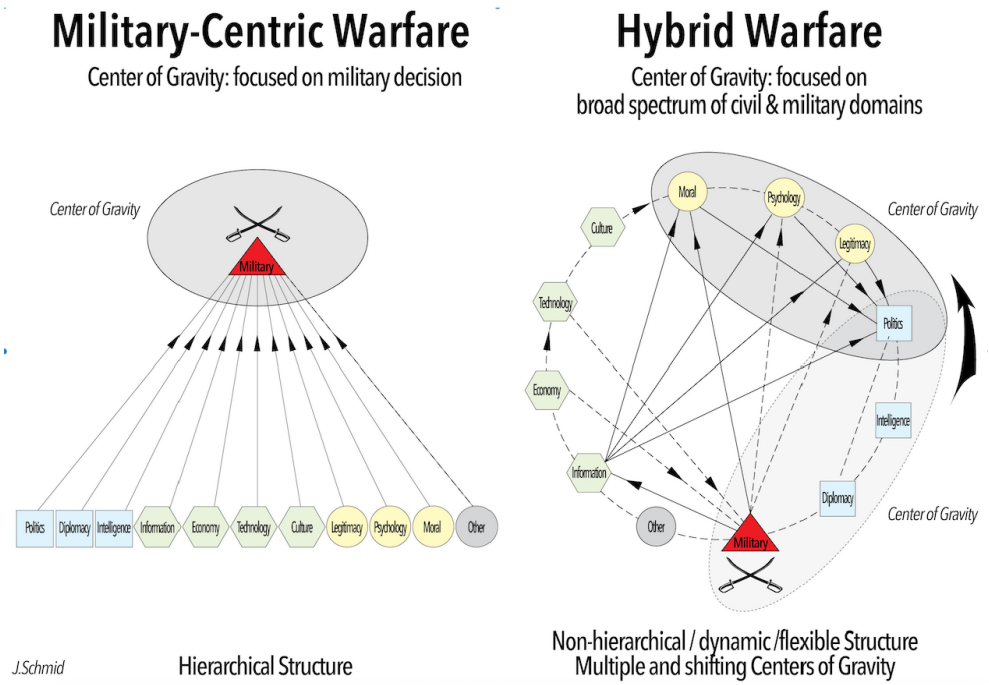
Een grotere rol voor Defensie op het gebied van interne veiligheid vergt heel wat voorbereidingswerk, zoals het uitwerken van scenario's en doctrines en het organiseren van training samen met de andere nationale veiligheidsactoren. Daarom zou Defensie zich de komende jaren zeker al moeten voorbereiden op een mogelijk versterkte rol in dit kader. In de Scandinavische landen neemt Defensie al een leidende rol op voor een grotere nationale coördinatie en voor de planning inzake nationale weerbaarheid via het *Total Defence concept*. In dit concept worden alle relevante overheids- en privésectoren van de hele maatschappij alsook de burgers zelf betrokken in het veiligheidsbeleid, met een wisselwerking tussen maatschappelijke weerbaarheid en militaire verdediging.

8. Meer aandacht besteden aan hybride dreigingen

Het is logisch dat wanneer hybride dreigingen worden geïdentificeerd als de belangrijkste *driver of change* voor de komende jaren, Defensie ook in dit domein een grotere rol zal moeten opnemen. Enkel in scenario 3 *Private security* is dit niet het geval omdat internationale technologiebedrijven deze taak overnemen.

Defensie heeft een bevoordeelde positie om hybride dreigingen te constateren. Het moeilijkste bij een hybride dreiging is het verbinden van alle signalen van een hybride actie, zoals onderstaande figuur weergeeft via het verschil tussen traditionele oorlogsvoering en hybride oorlogsvoering. De focus van hybride oorlogsvoering is veel onduidelijker en verspreid over domeinen die minder direct gelinkt worden aan veiligheid zoals informatie, moreel, psychologie, politiek, diplomatie en economie.

Defensie is natuurlijk dé specialist wat betreft het militaire domein, maar heeft ook nauwe linken met de andere domeinen via actoren zoals DG Stratcom, SGRS, KHID, DG MR, ACOS STRAT. Als Defensie erin slaagt de signalen van hybride dreigingen in al deze domeinen te detecteren en te verbinden, dan kan ze fungeren als de kanarie in de kolenmijn voor de Belgische veiligheid inzake hybride dreigingen. Detectie is slechts de eerste stap; het is belangrijk dat de daders van de hybride aanvallen worden geïdentificeerd (attributie) en dat er in competitie wordt gegaan met hybride actoren, om deze te ontraden.



Figuur 2: Military-centric warfare vs. hybrid warfare (Dr Johann Schmid, Hybrid CoE)

9. Een belangrijkere rol opnemen voor cyber en informatieoorlogvoering (*information warfare*)

In de twee scenario's met een hoge hybride dreiging wordt er van Defensie een bijkomende bijdrage verwacht in termen van cyber- en informatiecapaciteiten ter ondersteuning van de interne veiligheid.

10. Voldoende bijdragen aan collectieve veiligheid via crisismanagementoperaties

De zuidelijke Europese periferie (Noord-Afrika, Sahel, Midden-Oosten) blijft een belangrijke (potentiële) bron van internationaal terrorisme, piraterij, internationale misdaad en illegale immigratie, met een negatieve impact op de EU en België. Militaire inzet in het kader van collectieve veiligheid binnen een VN-, Europese en/of nationale integrale aanpak (*comprehensive approach*) zal er daarom noodzakelijk blijven. Het blijvende belang van collectieve veiligheid heeft ook te maken met de toenemende wereldwijde competitie om natuurlijke rijkdommen.

Momentum

De aanbevelingen van dit *Strategic Foresight Analysis*-project liggen in lijn met aanbevelingen in andere (buur)landen, de EU en de NAVO en de nieuwe nationale beleidsdocumenten rond veiligheid en defensie op strategisch-politiek niveau[9].

Wat betreft de toekomstige ontwikkeling van Defensie, worden twee mogelijke extreme rollen naar voren geschoven: Defensie als een centrale actor in een *Total Defence* van onze maatschappij of Defensie als louter de militaire specialist. Er zijn uiteraard nog veel grijze zones tussen beide visies. Beide kunnen een goede optie zijn als de NVS ervoor zorgt dat onze nationale veiligheidsactoren het volledige veiligheidsspectrum dekken. Dit *foresight*-project van Defensie neigt eerder naar de rol van centrale actor in een *Total Defence*-concept. De organisatie van een bijkomende workshop met het topmanagement van Defensie zou bijdragen aan een visie van Defensie op haar rol.

Tijdens dit eerste *foresight*-project van Defensie is gebleken dat Defensie geen duidelijke operationele strategie heeft, wat het aftoetsen van toekomstscenario's bemoeilijkte. Het uitwerken van een dergelijke strategie zal vergemakkelijkt worden met een NVS.

[9] Minister van Defensie, Beleidsverklaring Defensie, Brussel, 4 november 2020 (https://www.belspo.be/belspo/defra/doc/Policy%20Declaration%20Defence%202020.pdf); Ministerie van Defensie, Actualisering van de Strategische Visie 2030: Aanbevelingen, Brussel, juni 2021 (https://www.defence-institute.be/wp-content/uploads/2021/06/200622-Strategic-Vision-2021-NL.pdf).

De toekomst van foresight in de Belgische Defensie

De aanbevelingen van dit eerste *foresight*-project creëren het kader voor de jaarlijkse aanbevelingen vanuit ACOS STRAT voor het operationele planningsproces van ACOS O&T. Deze *foresight* zal verder geüpdatet en uitgewerkt worden door SFA-projecten met een specifiekere onderzoeksvraag. Samen met ACOS O&T werd er beslist dat een eerste uitwerking zal gebeuren over de mogelijke evolutie van de veiligheidssituatie in de Sahel en vervolgens deze in de regio van de Grote Meren. Het is belangrijk dat Defensie zelf ook nadenkt over de rol die het kan spelen en de meerwaarde die het kan hebben in de Sahel en de Grote Meren-regio en dit in de eerste plaats in samenwerking met de FOD Buitenlandse Zaken en de directie-generaal Ontwikkelingssamenwerking via een geïntegreerde aanpak. Zoals eerder vermeld, noopt de realiteit van meer veiligheidsdreigingen en de beperkte middelen en personeel van Defensie tot keuzes omtrent de inzet (regio's, types inzet) met het beste rendement voor de nationale veiligheid.

© Belgian Defence

In juni 2021 werd ook een SFA-project opgestart rond technologie met een tijdshorizon tot twintig jaar, ter ondersteuning van het proces van capaciteitsontwikkeling. Dit project omvat in een eerste fase een brede horizonscan van toekomstige technologie met een focus op *Emerging Disruptive Technologies* (EDT). Deze horizonscan zal nadien dienen als basis voor een discussie met Belgische stakeholders en technologie-experten die moet leiden tot voorstellen voor prioriteiten voor Defensie en opportuniteiten voor de technologische evolutie van Defensie vanuit het Belgische industriële en onderzoeksveld.

Besturen is vooruitzien

Een organisatie als Defensie moet voldoende aandacht blijven besteden aan het nadenken over de toekomst om betere beslissingen te kunnen maken in een steeds complexere, volatielere en onzekerdere omgeving. De vele uitdagingen vandaag en op korte termijn mogen geen excuus zijn om onvoldoende middelen te geven aan het voorbereiden van de toekomst. In een snel veranderende maatschappij is dit juist een prioriteit om onze Defensie relevant te houden. We kunnen dit ook niet enkel overlaten aan veiligheidsorganisaties zoals de NAVO en de EU, waarvan België een lidstaat is. De specificiteit van ons nationale veiligheidsbeleid en onze nationale veiligheidsactoren vereist ook een eigen nationale reflectie, die natuurlijk wordt gevoed door toekomstprojecten op andere niveaus. De verschillende tools en initiatieven, samengevat onder de noemer *foresight*, kunnen in dit kader een troef vormen als ze voldoende ingebed worden in onze organisatie en besluitvormers aanzetten om de nodige tijd te nemen om na te denken over de toekomst van onze Defensie.

Trefwoorden: *foresight, Strategic Foresight Analysis*