PNT & NAVWAR

POTENTIËLE BEDREIGING VAN HET INFORMATIEGESTUURD OPTREDEN

LTZ1 Ir. A. (Alex) Haasnoot,
PNT specialist Sectie Space CLSK

Een van de maatregelen in de Defensienota 2022 is het verbeteren van de IT-infrastructuur ten behoeve van het informatiegestuurd optreden (IGO). *Position, Navigation & Timing* (PNT) en *Navigation Warfare* (NAVWAR) zijn hierbij minder bekende onderwerpen die een grote rol spelen. In dit artikel wordt uitgelegd wat PNT en NAVWAR precies inhouden, waarom ze relevant zijn voor de operatie en waarom we hier aandacht aan moeten besteden. Daarnaast wordt inzicht gegeven in de roadmap voor PNT-ontwikkeling, waarvan de resultaten uiteindelijk via programma's als FOXTROT in de wapensystemen geïmplementeerd zullen worden. ➔

In december 2019 heeft NATO Space geformaliseerd als operationeel domein. PNT (Position, Navigation & aTiming) wordt hierbij gezien als een functiegebied onder Space. LTZ1 Alex Haasnoot is werkzaam als PNT-specialist binnen het Defensie Space Security Centre (DSSC) en geeft invulling aan dit functiegebied. Daarbij werkt hij onder andere samen met JIVC FOXTROT en KIXS aan een roadmap om de GPS-afhankelijkheden krijgsmachtbreed te verminderen.

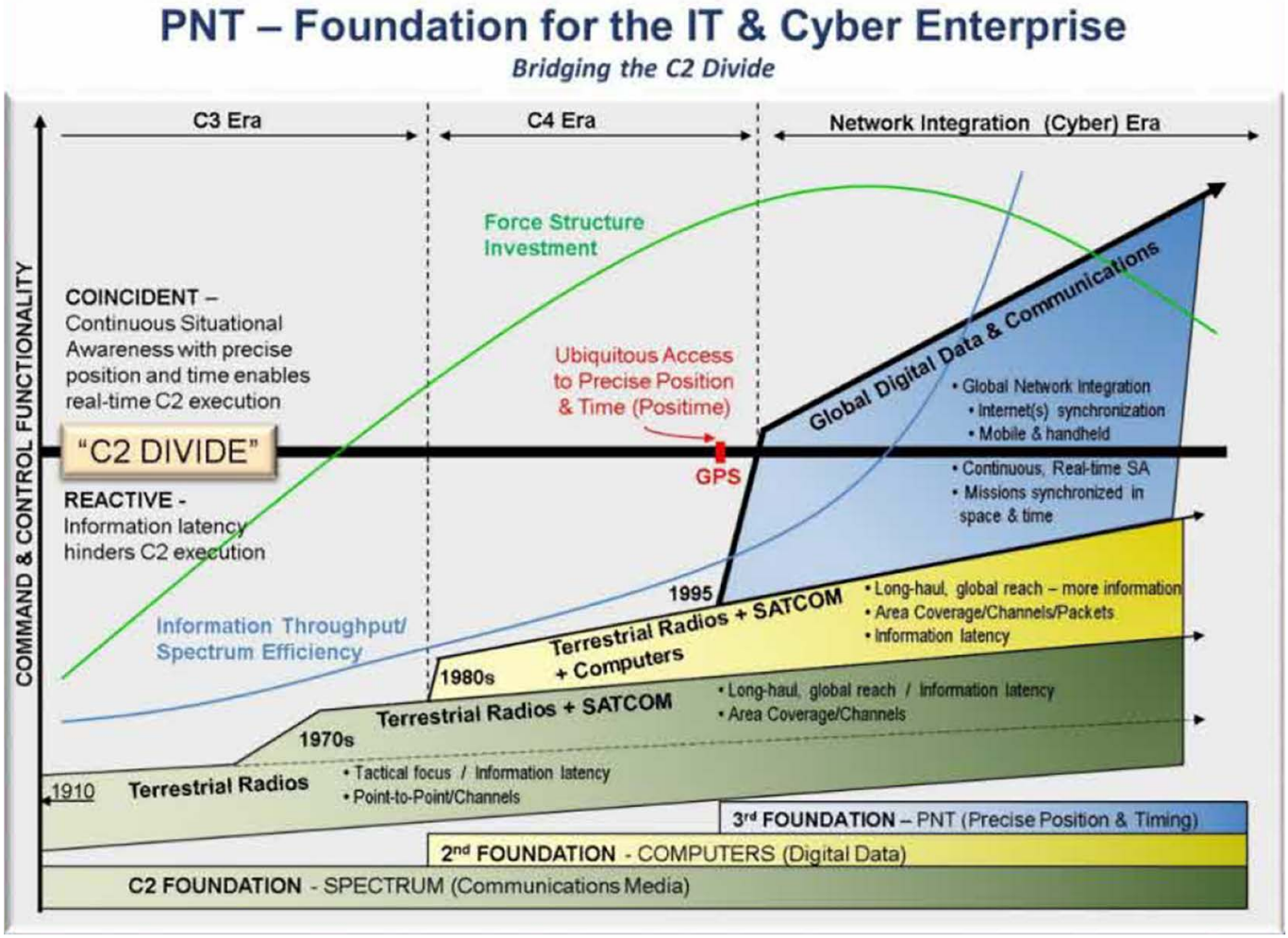
Position, Navigation & Timing

Positie-, Navigatie- en Tijdsinformatie (PNT) is essentiële informatie die sensor-, wapen- en communicatiesystemen gebruiken om zich te oriënteren en op te lijnen. Zo wordt positie-informatie gebruikt in navigatiesystemen en *blue* (en *red*) *force tracking* systemen, die essentieel zijn om te bepalen hoe en waar wapeninzet kan plaatsvinden om het beoogde militaire effect te bereiken. Navigatie-informatie is informatie over de beweging. Het bevat informatie over oriëntatie (richting) en de snelheid van een platform of een projectiel. Navigatie-informatie wordt bijvoorbeeld gebruikt om de loop van het kanon aan boord van een op de golven slingerend marinefregat op een bewegend doel te richten. Tijdsinformatie is essentieel voor het synchroniseren van operationele beeldopbouw (datalinks), maar bijvoorbeeld ook voor synchronisatie van (radio-)netwerken en voor het functioneren van *frequency hopping* systemen (zoals bijv. HaveQuick) voor communciatiebeveiliging.

Met de komst van het *Global Positioning System* (GPS) in de jaren '90 heeft PNT qua nauwkeurigheid en beschikbaarheid een revolutie ondergaan. Bij de introductie van dit systeem kwam nauwkeurige PNT-informatie voor veel gebruikers gratis en wereldwijd beschikbaar. Niet veel mensen zijn zich ervan bewust, maar door GPS heeft het informatiegestuurd optreden (IGO) zich kunnen ontwikkelen tot de vorm zoals we het nu kennen.

Figuur 1geeft dit duidelijk weer: de introductie van de radio heeft ervoor gezorgd dat we gebruik kunnen maken van het elektromagnetisch spectrum (EMS). De uitvinding van de computer heeft ervoor gezorgd dat we op een effectievere manier meer informatie kunnen processen. De introductie van GPS heeft ervoor gezorgd dat we informatie kunnen synchroniseren in ruimte en tijd. Nauwkeurige PNT is dus als het ware een 'nuts-product' voor IGO. Veel (wapen-, communicatie- en informatie-)systemen zijn ervan afhankelijk om goed te kunnen functioneren.

GPS is een strategische capaciteit. Om deze reden hebben Rusland, China en Europa ondertussen ook eigen wereldwijde *Global Navigation Satellite Systems* (GNSS), vergelijkbaar met GPS, ontwikkeld. Op deze manier zijn zij niet meer volledig afhankelijk van het Amerikaanse *Department of Defense* voor hun nauwkeurige PNT-informatie. Het Europese GNSS, Galileo, is echter in civiel beheer. Om deze reden is het door de Europese krijgsmachten in het algemeen nog niet in gebruik genomen.



Figuur-1: Electronic foundations of joint warfighting – bron: US DOD CIO PNT Strategy

Navigation Warfare (NAVWAR)

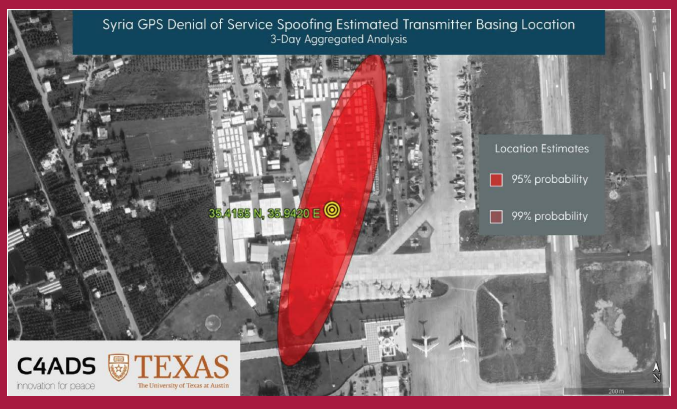
Omdat PNT-informatie een cruciale rol heeft in het functioneren van C4I-systemen is het een interessant *target* vanuit *information warfare* perspectief. Alle activiteiten die zich richten op het aanvallen of verdedigen van PNT-informatie vallen onder *Navigation Warfare* (cf. NATO definitie NAVWAR – NATO STANAG 4621).

Operationeel gezien kunnen NAVWAR-effecten op drie manieren worden bereikt: Ten eerste door middel van een *Electronic Attack* (EA) waarmee satellietnavigatiesignalen worden verstoord (*jamming*) of vervalst (*spoofing*). Een andere optie is een cyberaanval op de digitale PNT-informatie. Als laatste is het een optie om een kinetische aanval uit te voeren op kritische PNT-infrastructuur. Uiteraard zijn defensieve NAVWAR-maatregelen erop gericht om ervoor te zorgen dat bovenstaande activiteiten door een vijand zo min mogelijk impact hebben op de eigen systemen en missie. In het vervolg van dit artikel wordt vooral gefocust op de defensieve kant van NAVWAR. Het operationeel belang en de kansen van offensieve NAVWAR zijn opgenomen in het gedachtengoed van *Cyber and Electro Magnetic Activities* (CEMA) (zie ook 'CEMA' in Intercom 2021-3 en 2022-1).

Operationele relevantie

Afgelopen jaren is er een sterke toename van NAVWAR-activiteiten. De Russische Federatie zet op grote schaal *Zhitel Jammers* in tijdens de Oekraïnecrisis om d.m.v. *GPS-jamming* de effectiviteit van de Oekraïense strijdkrachten te verminderen.

Figuur-3: Russische Zithel EOV-truck in Oekraïne, waargenomen nabij de Krim]



Figuur-4: ISS Aggregratie analyse locatie Ru GPS denial spoofing capability bij Khmeimim Airbase in Syrie

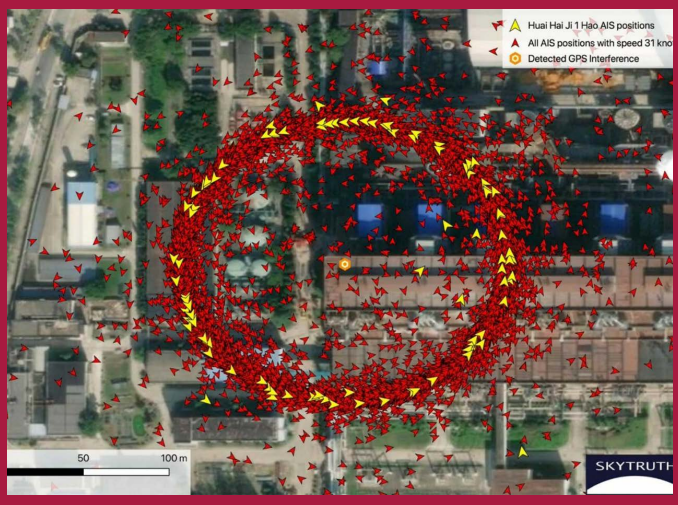
Figuur-2: NATO definitie van NAVWAR – bron: NATO PNT and NAVWAR policy

Daarnaast zijn er ook meerdere voorbeelden van *GPS-jamming* en *spoofing* door de Russische Federatie vanuit defensief oogpunt. Voorbeelden hiervan zijn de vaste *GPS denial spoofing* installatie op *Khmeimim Air Base* die waarschijnlijk gebruikt wordt als verdedigingsmiddel voor de op het vliegveld gestationeerde Russische eenheden tegen drones en GPS-geleide munitie (figuur-4) en de *GPS-spoofing* activiteiten die plaatsvinden op de locaties die president Poetin bezoekt.

Daarnaast zijn er ook voorbeelden van *GPS-spoofing* door China bij hun haveninstallaties.

In figuur-5 is te zien dat de GPS-posities van schepen om een vaste geografische positie op land heen cirkelen, wat zichtbaar wordt door uitlezing van het maritieme AIS (*Automatic Identification System*). Meerdere van dergelijke incidenten zijn gerapporteerd in China. Waarom dit wordt gedaan, is niet precies duidelijk. Wel is duidelijk dat dit om een meer geavanceerde vorm van *GPS-spoofing* gaat dan we tot nu toe hebben gezien.

Bovenstaande ontwikkelingen bevestigen dat NAVWAR makkelijk uitvoerbaar blijkt en een integraal onderdeel is van toekomstige oorlogsvoering.



Figuur-5: Chinese 'circle spoofing' nabij de haven van Sjanghai

Dit betekent dat wij hier als krijgsmacht de juiste aandacht aan moeten besteden want anders lopen wij het risico dat onze ver ontwikkelde *Tactics, Techniques & Procedures* (TTP) op basis van informatie niet blijken te werken zodra we blootgesteld worden aan een *GNSS denied environment*.

Kwetsbaarheid

Defensie gebruikt als primaire input voor PNT het militaire GPS-systeem. Het verschil tussen militaire GPS en civiele GPS is dat het militaire signaal encrypted is, waardoor het moeilijker te vervalsen is, het geeft dus een beveiliging tegen *spoofing* indien de crypto correct is ingeladen. Daarnaast maakt MilGPS onder andere gebruik van de L1 én de L2 frequentie, wat meer weerbaarheid geeft tegen jamming. De tegenstander moet immers twee frequenties *jammen* om MilGPS plat te leggen.

Figuur-6: DAGR MilGPS, de huidige handheld MilGPS in gebruik bij Defensie

Het militaire GPS-systeem geeft dus meer bescherming dan het civiele GPS-systeem, maar het blijft kwetsbaar. De signalen van GPS worden met ongeveer 50 W vermogen, het vermogen van een gloeilamp, uitgezonden vanuit satellieten op 20.000 km afstand van aarde. Het uiteindelijke vermogen dat je op aarde kan ontvangen is maar 0,0000000000000002 W. Als je dit beseft is het niet moeilijk voor te stellen dat deze signalen makkelijk te overstemmen zijn met laag vermogen *jammers* op aarde. Dit betekent tegelijkertijd dat een hoog vermogen *jammer* een zeer groot effectief bereik kan hebben.

Hoe kwetsbaar we precies zijn is niet in detail bekend. Bij gebruik van MilGPS zijn we in ieder geval beter weerbaar tegen *GPS-spoofing* en is het voor een vijand zeer moeilijk om tijd en positie te vervalsen. *GPS-denial* d.m.v. *jamming* blijft echter een realistisch scenario. Bij de grotere wapensystemen wordt dit in een aantal gevallen opgevangen door de integratie van *High Accuracy Clocks* (HAC) voor timing-informatie en *Inertial Navigation Systems* (INS) voor positie- en navigatie-informatie. De zorg zit vooral bij de systemen waarbij niet expliciet rekening is gehouden met de mate van GPS-afhankelijkheid. Zo zijn er gevallen bekend van SATCOM-installaties die gebruik maken van een door de fabrikant ingebouwde civiele GPS om de antenne te richten. Het is dus maar de vraag of een projectleider bij de aankoop van een nieuw systeem niet per ongeluk een GPS afhankelijkheid erbij heeft gekocht omdat de eisen voor GPS-onafhankelijkheid niet zijn meegenomen in het programma van eisen. Daarnaast zijn er ook diverse systemen in gebruik bij defensie die *commercial of the shelf* worden verworven. Zolang

Figuur-7: Simulatie van het effectief bereik van een 200W GPS jammer op 3m boven Mean Sea Level]

deze niet voor veiligheidskritische toepassingen worden ingezet is er niet veel aan de hand. Het is alleen de vraag of de juiste risicoanalyse wel altijd gemaakt wordt.

Naast de operationeel/tactische kwetsbaarheid zijn we op het gebied van PNT ook strategisch kwetsbaar. De rijksbrede Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie (IKUS) in 2016 en 2022 heeft aangetoond dat er een aantal kritische kwetsbaarheden in onze maatschappij aanwezig zijn in het geval van langdurige GPS-uitval. Dit is een nationaal veiligheidsprobleem dat ons als krijgsmacht ook raakt, want het is maar de vraag hoe effectief onze krijgsmacht nog kan opereren indien het thuisland in oorlogsomstandigheden te maken krijgt met falende IT-infrastructuur en stroomuitval door het wegvallen van tijdinformatie, maar ook met afnemende beschikbaarheid van hulpdiensten door het wegvallen van positie- en navigatie-informatie.

Complex dossier

Het PNT dossier is complex. In eerste instantie omdat het onderwerp niet past in de manier waarop de verantwoordelijkheden voor materieel in onze organisatie zijn verdeeld. Zoals al aangegeven raakt NAVWAR aan EOV, cyber en *space*, en er zal dus goed samengewerkt en afgestemd moeten worden om de dreiging op alle vlakken goed aan te pakken. De CEMA-initiatieven zijn hierbij een goede eerste stap, alleen daarbij ligt de focus bij de ontwikkeling van een (offensieve) operationele capaciteit en hierbij zijn niet altijd de partijen betrokken die verantwoordelijk zijn voor de robuustheid van de PNT-infrastructuur. De coördinatie moet dus breder.

Daarnaast is *GNSS-denial* slecht te trainen. Het verstoren van de satellietnavigatiesignalen van GNSS is verboden en Agentschap Telecom is zeer terughoudend met het verlenen van een vergun-

ning, omdat de impact op de civiele infrastructuur niet altijd duidelijk is. Als er al een vergunning wordt verleend, dan zijn de toegestane vermogens zodanig laag dat er geen sprake is van representatieve training van wat je op het slagveld zou kunnen verwachten. Dit is een groot risico, omdat we nu onze mensen trainen in een omgeving waar GNSS altijd beschikbaar is. Bijvoorbeeld Garmin horloges worden binnen defensie veelvuldig gebruikt vanwege de gunstige SWaP (*Size Weight and Power*) eigenschappen in vergelijking met de DAGR militaire handheld GPS. De vraag is alleen of de op Garmin gebaseerde TTP's *(Tactics, Techniques & Procedures*) standhouden in een *GNSS-denied* situatie en of de militair zijn vaardigheden nog op orde heeft om terug te vallen op de meer robuuste militaire GPS met minder functionaliteiten.

Figuur-8: GARMIN Fénix 5x, in gebruik bij defensie

Omdat *GNSS-denial* niet getraind kan worden is er ook gebrek aan *awareness*. We weten niet precies waar onze kwetsbaarheden zitten en moeten aannemen dat de technisch geïmplementeerde maatregelen, die nooit in het veld zijn getest, afdoende zijn om de gevraagde nauwkeurige PNT-informatie onder alle omstandigheden te leveren. Dit geldt op alle vlakken, in het mobiele domein, maar ook in onze vaste infrastructuur in Nederland. In het verleden is namelijk gebleken dat het vanuit kostenoverwegingen zeer aantrekkelijk is om netwerktiming, voor een militair netwerk, te coördineren met goedkope civiele GPS receivers. Als er dan niemand betrokken is bij het project die kan uitleggen dat dit niet verstandig is, omdat het netwerk ook in oorlogsomstandigheden moet functioneren, dan ontstaat er een kwetsbaarheid. Als het project is gegund is het zeer moeilijk om deze kwetsbaarheden tegen te gaan. Wij richten projecten namelijk zo (kosten) efficiënt mogelijk in, waarbij projectsucces voornamelijk wordt bepaald door de parameters tijd en geld omdat kwaliteit vaak een subjectieve discussie is met een vergroot risico op scope creep. In de praktijk zit dus niemand in een project te wachten op de inbreng van een complex onderwerp waarvan de tijd en kosten lastig zijn te overzien.

Ook technisch gezien is PNT een complex onderwerp. Allereerst is er maar één type systeem (GNSS) dat wereldwijd zowel *Position-, Navigation-* als *Timing-* informatie met hoge nauwkeurigheid levert. Alternatieve bronnen leveren vaak een deel van de oplossing, en in veel gevallen ook met een lagere nauwkeurigheid of met drift (verslechterende nauwkeurigheid na het verstrijken van tijd). Voorbeelden hiervan zijn klokken, traagheidsnavigatiesystemen, snelheidsmeters, LIDAR-systemen, radarsystemen, etc. Een alternatief voor GNSS is dus niet kant-en-klaar op de markt te koop en vereist integratie van verschillende sensoren: sensorfusie. Bij sensorfusie moeten keuzes gemaakt worden. Welke sensoren ga ik gebruiken (verschillende fabrikanten)? Wanneer is een sensor nog wel, en wanneer is hij niet meer te vertrouwen? Bij welke drempelwaarde nemen we een bepaalde sensor niet meer mee? Deze keuzes zouden in detail moeten worden afgestemd op de beoogde toepassing waarvoor de PNT-sensorsuite wordt ingezet. Daarbij is er altijd sprake van een dilemma, namelijk welke drempelwaarde geeft een aanvaardbaar risico? De vraag is of we dit soort kritische beslissingen aan de industrie willen delegeren.

Tenslotte is er ook geopolitiek rond PNT. Momenteel maken wij als NATO-krijgsmacht primair gebruik van het Amerikaanse militaire GPS-systeem. De gratis toegang tot dit encrypted systeem is geregeld in een MOU tussen de individuele NATO-krijgsmachten en het Amerikaanse *Department of Defense*. Sinds een paar jaar beschikt Europa ook over haar eigen Galileo GNSS, wat vergelijkbare capaciteiten heeft als het Amerikaanse GPS (inclusief een encrypted signaal). Amerika heeft toegang aangevraagd tot het encrypted deel van het Galileo systeem. Deze toegang is tot op heden nog niet door de Europese Commissie toegekend. Deze situatie roept meerdere vragen op die effect hebben op het PNT-dossier:

1. Moeten wij, vanuit het perspectief van dreiging en redundantie niet ook gebruik gaan maken van het Europese Galileo-systeem, waar wij als Nederland veel in hebben geïnvesteerd?
2. De Verenigde Staten wil voor dezelfde redundantie toegang tot het Galileo PRS Systeem. Is het niet ons belang om voor de Amerikanen deze toegang mogelijk te maken zodat we de samenwerking met betrekking tot deze strategische capaciteit in de toekomst versterken?

Momenteel is er nog geen antwoord op deze vragen. Wel is duidelijk dat Frankrijk, het land dat binnen Europa de minste afhankelijkheid heeft van de Verenigde Staten, activiteiten ontplooit om het Galileo-systeem te integreren in militaire toepassingen. Komende jaren zal Nederland beleidskeuzes moeten maken om ervoor te zorgen dat onze primaire PNT-input gegarandeerd blijft. Daarbij ontkomen we er niet aan om een meer concreet standpunt in te nemen met betrekking tot onze afhankelijkheid van de Verenigde Staten.

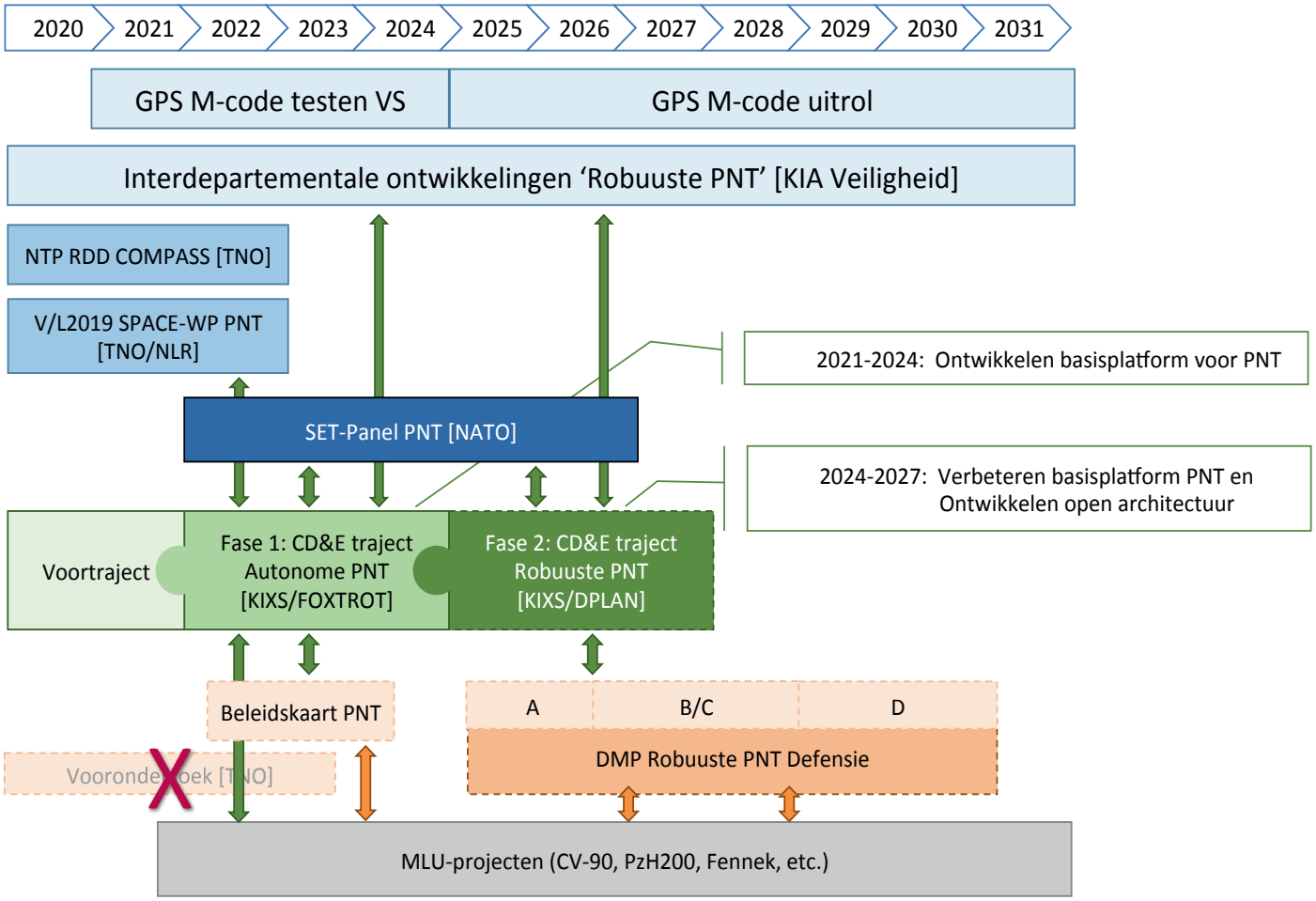
Galileo satellietnavigatiesysteem

Werken aan een oplossing

De toename van onze GPS-afhankelijkheid is niet een puur nationaal probleem. De meeste NATO-landen kampen met een vergelijkbare problematiek. Binnen de NATO C3-Board is er dan ook veel aandacht voor het onderwerp en wordt in samenwerking gekeken naar mogelijke oplossingen. Op 17 Augustus 2022 is de *NATO PNT and NAVWAR policy* formeel aangenomen. In deze *policy* wordt de NATO lidstaten opgedragen om de GNSS-afhankelijkheid te verminderen en oplossingen te zoeken door het integreren/fuseren van meerdere PNT-bronnen. De Verenigde Staten hebben dit al meer concreet gemaakt met de publicatie van hun nationale PNT-strategie in 2018. Uniek aan deze strategie is dat dit de eerste keer is dat de Amerikanen aangeven dat zij andere PNT-bronnen gaan gebruiken dan hun eigen GPS-systeem.

Sinds 2020 bouwen de kennisinstituten TNO en NLR gerichte PNT-kennis op binnen de contour *L/V2019 Space*. De opdracht hierbij is om vooral te focussen op sensorfusie en integriteit van PNT-data. Een nevenproduct van deze kennisopbouw is een defensie sensorfusie-algoritme, TOPS (*Timing, Oriëntation & Positioning Service*), dat ontwikkeld is door TNO. Om dit sensorfusie-algoritme naar een hoger *Technology Readiness Level* (TRL) te brengen wordt het algoritme toegepast binnen diverse nationale technologieprojecten binnen en buiten defensie, waarbij verschillende typen sensoren geïntegreerd worden. Bij deze projecten wordt nooit de sourcecode buiten defensie prijsgegeven, omdat inzicht in de exacte werking van het filter inzicht en kennis geeft over de keuzes die gemaakt zijn bij de sensorfusie. Dit wil je als defensie niet vrijgeven want deze kennis biedt de mogelijkheid om een gerichte cyber- of *electronic attack* te ontwikkelen die in de toekomst succesvol zou kunnen zijn. Civiele partijen mogen het algoritme dus gebruiken als ‘black box’.

Dit levert in de praktijk geen problemen op, want voor de civiele doelstelling gaat het om de *performance* en niet zo zeer om hoe deze *performance* wordt bereikt.
Dit jaar is in opdracht van het JIVC-programma FOXTROT gestart met het CD&E-traject Autonome PNT. Dit CD&E-traject, uitgevoerd door JIVC KIXS, is erop gericht om een antwoord te bieden op de meest urgente PNT-kwetsbaarheden binnen met name de landmacht. Daarnaast is in overleg met CDS DPLAN, het CD&E-programma uitgebreid met CD&E robuuste PNT, wat erop gericht is om een defensiebrede robuuste PNT-infrastructuur te ontwikkelen. Bij deze ontwikkeling zal o.a. samengewerkt worden met TNO om het concept van het TOPS-algoritme uit te werken in een Modulaire Open Systeem Architectuur (MOSA) voor PNT. Dit nationale CD&E-programma wordt parallel aangelopen met een *NATO Science, Experimentation and Technology panel*, NATO SET-309, waar een aantal NATO-landen onder leiding van de Verenigde Staten samen experimenteren met een dergelijke architectuur en de bijbehorende PNT-datastandaard die benodigd is om de industrie hierin mee te krijgen. Omdat Nederland hier een nationaal programma naast heeft lopen, geeft dat ons een goede uitgangspositie waarbij wij zelf kunnen kiezen waar wij kennis willen uitwisselen en waar niet.



Figuur-10: Roadmap Robuuste PNT

Daarnaast zorgt dit er ook voor dat we onafhankelijk zijn van de ontwikkelingen binnen het SET-panel, maar dat we wel goed aangesloten blijven bij de ontwikkelingen van onze partners binnen de NATO.
Het is de bedoeling dat het CD&E-traject Autonome/Robuuste PNT een prototype van een Modulaire Open Systeem Architectuur (MOSA) voor PNT oplevert. Dit prototype dient als basis voor de ontwikkeling van defensiebrede PNT-software door JIVC. Deze software is de PNT-basis voor alle wapensystemen, waarbij we zelf controle hebben over de keuzes in de sensorfusie. Uiteraard zal voor elk wapensysteem een eigen versie van deze software ingeregeld moeten worden op basis van de sensoren die beschikbaar zijn. Deze sensoren kunnen gewoon via het normale proces ingekocht worden bij de industrie, alleen wel onder de voorwaarden dat ze compatibel zijn met de PNT MOSA. Een ander voordeel van deze manier van werken is dat de sensoren onafhankelijk zijn van de partij die de sensorfusie uitvoert. Hierdoor ontstaat meer flexibiliteit bij de introductie van nieuwe sensoren en technieken en wordt een *vendor lock-in* situatie bij integratie voorkomen.

Samengevat

PNT is essentieel voor IGO en vormt de basis voor al onze militaire operaties en het functioneren van de civiele kritieke infrastructuur. NAVWAR is in opkomst en zal onderdeel zijn van het conflict van de toekomst. Om deze reden moeten we aandacht besteden aan het robuust maken van onze PNT-infrastructuren binnen de krijgsmacht en in Nederland, zodat operaties kunnen doorgaan onder *GNSS-denied* condities.

Dit is erg complex aangezien we onze kwetsbaarheden niet kennen en omdat we niet mogen testen. Daarbij komen de afhankelijkheden soms onbewust in onze organisatie binnen. Een mooi voorbeeld hierbij zijn drones. Heeft iemand al de vraag gesteld of onze drone-initiatieven binnen defensie nog wel functioneren als satellietnavigatiesystemen niet meer beschikbaar zijn? Met het CD&E-traject autonome PNT zetten we in ieder geval een goede eerste stap naar een constructieve oplossing. Mogelijk kunt u hier ook zelf aan bijdragen door mee te denken en scherp te blijven op eventuele kwetsbaarheden.