NOTE 3

Rapport n° 193/FRS/CONFLITS2035
du 13 mai 2022

[Mise à jour partielle en Janvier 2024]

Marché n° 2021 – 1050 056 262 / Année 2
EJ court 180 006 47 00
notifié le 29 juin 2021

Navigation Warfare et positionnement, navigation, synchronisation (PNT)

PHILIPPE GROS

En partenariat avec

Liste des abréviations

AED	Arme à énergie dirigée	M2MC	Multimilieux / multichamps
BDS	*BeiDou Sytem*	MEMS	*Microelectromechanical systems*
CEP	Cercle d'erreur probable	NAVMAG	Navigation magnétique
CRPA	*Controlled Reception Pattern Antenna*	NAVWAR	Navigation Warfare
dB	Decibel	OMEGA	Opération de Modernisation des Équipements GNSS des Armées
DSMAC	*Digital Scene Matching Area Correlator*	P3TS	*Plug and Play Positioning and Timing System*
EMSO	*Electro Magnetic Spectrum Operation*	PNT	Positionnement, navigation & timing
GBAS	*Ground-Based Augmentation System*	PVT	Position vélocité, temps
GEO	*Geosynchronous Equatorial Orbit*	ROEM	Renseignement d'origine électromagnétique
GEOINT	*Geospatial Intelligence*	RPO	Rendez-vous and Proximity Operations
GNSS	*Global Navigation Satellite System*	SBAS	*Satellite-based Augmentation Systems*
GPS	*Global Positionning System*	SDB	*Smalll Diameter Bomb*
HEL	*High Energy Laser*	SNR	*Signal-to-Noise Ratio*
HOJ	*Home on Jam*	SWaP-C	*Size, Weight, and Power - Cost*
HPEM	*High Power Electromagnetic*	TERCOM	*TERrain COntour Matching*
IGAS	*Integrated GPS Anti-Jam System*	USV	*Unmanned Surface Vehicle*
IMU	*Inertial Measurement Unit*	UTC	*Coordinated Universal Time*
INS	*Inertial Navigation System*	UUV	*Unmanned Unsersea Vehicle*
JASSM	*Joint air-to-surface standoff missile*	VLF	*Very Low Frequency*
JDAM	*Joint Direct Attack Munition*	WGS	*World Geodetic Survey*
LEO	*Low Earth orbit*		
LIO	Lutte informatique offensive		

SOMMAIRE

FIGURES

Navigation Warfare et positionnement, navigation, synchronisation (PNT)

Résumé

La guerre de la navigation (*Navigation Warfare*, NAVWAR) désigne « [l'] *action défensive et offensive délibérée visant à assurer et à empêcher la transmission d'informations sur le positionnement, la navigation et la synchronisation grâce à l'emploi coordonné d'opérations de guerre spatiale, cybernétique et électronique* »[1].

L'information de PNT a toujours été nécessaire, sinon vitale, à l'action des forces militaires, dans l'ensemble de leurs fonctions opérationnelles. Le *Global Positioning System* (GPS) américain a néanmoins provoqué une rupture en fournissant une source de données de positionnement, de vélocité et de temps (PVT) tout à la fois absolue, d'une précision croissante (avec l'évolution continue des techniques de traitement du signal), plus polyvalente et en général moins coûteuse à exploiter que les techniques et équipements précédents. Ce saut capacitaire a en retour démultiplié les attentes en matière de PNT et de capacités en résultant : suivi en temps réel de la position des unités, frappe de précision bas coût à toutes les portées, synchronisation des systèmes de communication à l'échelle globale, etc. La rupture s'est aussi produite à l'échelle des sociétés, affectant nombre de ses secteurs : communication, finance, transport, agriculture, etc. Les États-Unis ont donc été suivis par les grandes puissances dans la maîtrise de cette manne informationnelle : Galileo européen, Glonass russe, BeiDou chinois, QZSS japonais, NavIC indien, en attendant les systèmes sud-coréen ou encore turc.

Or, ces systèmes de navigation satellitaires globaux (*Global Navigation Satellite Systems* – GNSS) ou régionaux (RNSS) fournissent chacun un signal de très faible puissance qu'il apparaît assez simple de brouiller et même maintenant d'usurper, comme en attestent de multiples exemples. Ce type de capacité est, à des degrés divers, à la disposition d'un nombre croissant d'acteurs allant du club restreint des grandes puissances militaires maîtrisant la guerre électronique aux opérateurs privés dans nos sociétés. De là émerge donc cette notion de NAVWAR consistant précisément à sécuriser la fourniture de cette information de PNT et à pouvoir entraver celle de l'adversaire. De cette vulnérabilité critique émerge l'impression qu'une épée de Damoclès plane non seulement sur le fonctionnement des forces armées, voire sur la supériorité militaire occidentale, mais aussi sur le fonctionnement de nos sociétés.

[1] « *Deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare operations* ».

En réalité, il convient de nuancer fortement cette menace. Tout d'abord, force est de constater qu'en 20 ans, ces actions de NAVWAR offensives, bien que nombreuses, n'ont pas généré d'effets de rupture sur les plans tant civil que militaire, même au niveau tactique. Les raisons sont largement techniques. Le chiffrement des signaux militaires réduit les potentialités d'usurpation. Les investissements réalisés depuis 30 ans, non seulement dans la constellation elle-même, mais aussi en matière de techniques antibrouillages (le couplage étroit entre réception GPS et unités de mesures inertielles dans les centrales inertielles et plus encore les techniques de réjection d'interférence) sont de nature à durcir considérablement le GPS. De multiples systèmes d'amplification de ces signaux, tant spatiaux que terrestres, tout en améliorant les performances des GNSS, réduisent eux aussi les risques. Toutes ces techniques contribuent également à améliorer la détectabilité des attaques, qui constitue un enjeu permanent. Ce n'est donc pas tant le manque de technologies disponibles que leur traduction capacitaire effective, particulièrement lente, qui maintient cette vulnérabilité des utilisateurs à ces attaques électroniques. À plus long terme se pose toutefois la question des menaces pesant sur les constellations proprement dites, principalement à base de capacités co-orbitales et bien sûr de lutte informatique offensive. Les perspectives de concrétisation de ces menaces restent cependant encore incertaines.

Dans ce contexte, les GNSS restent au cœur des stratégies capacitaires en matière de PNT aux États-Unis, en Chine et de toute évidence en Europe. Cependant, pour améliorer la résilience de cette fonction, émergent de véritables visions d'écosystèmes visant à intégrer de multiples solutions de complément. Il s'agit également de doter les futurs éléments du champ de bataille (robots, drones, munitions de précision et réseaux associés) de sources de PNT suffisamment précises tout en restant à coût abordable. Ces efforts se manifestent par un investissement important dans de multiples technologies voire un réinvestissement dans des technologies anciennes de PNT, souvent relatif, transitoirement délaissées. Cet écosystème inclut d'autres systèmes spatiaux de PNT, notamment positionnés en orbite basse d'où ils émettent des signaux plus puissants avec un temps de latence réduit, les centrales inertielles à microsystèmes électromécaniques, les horloges atomiques de plus en plus miniaturisées, les nouvelles techniques de navigation aidée par capteurs notamment par la corrélation d'image, la navigation astronomique, la navigation gravimétrique, la navigation magnétique, la transmission de ces données via les réseaux, etc. Il faut également ajouter à cet ensemble les techniques de navigation acoustique permettant de soutenir le développement de capacités de « *seabed warfare* ». Les travaux portent également sur les architectures devant intégrer ces différentes sources, presque de façon « *plug-and-play* », ainsi que sur l'évolution des modèles de référence et des techniques de renseignement géospatial. Cependant, là encore, la traduction de ce foisonnement d'efforts de recherche / développement en transformations capacitaires se heurte, notamment aux États-Unis, à de multiples obstacles, principalement bureaucratiques et culturels. Ils sont avant tout liés au contexte de primat du GPS, à la difficulté de faire prendre en compte, pour des raisons de résilience, des technologies restant de niche, parfois coûteuses, quand elles ne sont pas moins performantes.

Dans ce contexte, nos armées sont confrontées aux mêmes problèmes de résilience que les autres. Ces problèmes se posent de façon différente pour les forces terrestres, aériennes et navales. Ces dernières ne sont cependant pas dépourvues de solutions, bien au contraire. Peut-être moins avancées que les forces américaines en matière de durcissement de l'exploitation GPS, elles tirent cependant mieux parti de la combinaison de ce système et du Galileo européen. Ensuite, elles bénéficient d'une base industrielle et technologique de défense parmi

les plus avancées au monde en matière de source de PNT autonomes, notamment de centrales inertielles mais aussi de techniques innovantes comme les navigations astronomique ou gravimétrique. L'étude propose pour chaque armée plusieurs recommandations, qui tentent de répondre aux mêmes défis : poursuivre la résorption à court-moyen terme des vulnérabilités, plus ou moins résiduelles, au brouillage et à l'usurpation des GNSS, trouver à plus long terme le mix adéquat de sources de PNT en mesure de parer aux menaces, encore hypothétiques, d'un « *day without space* ».

Introduction

Le GPS est partout. Certaines manifestations de son ubiquité sont évidentes : trouver sa pizzeria, éviter les encombrements sur la route des vacances, etc. D'autres le sont moins : faire du trading haute fréquence, mais aussi réaliser une frappe sur coordonnées ou encore synchroniser son réseau radio tactique. Le GPS est le substrat positionnel, spatial et temporel, du monde contemporain, même de l'Internet. Cet outil « *made in US Air Force* » est aussi l'un des facteurs de supériorité des forces armées occidentales. Mais il serait en même temps terriblement vulnérable… au point d'être interdit localement par des brouilleurs grands comme une canette de soda. La Chine, la Russie et l'Iran peuvent faire largement mieux et l'ont pour partie déjà démontré. Voici, un peu caricaturé, le discours classique tenu depuis de nombreuses années par une large partie des observateurs. Il n'est certes pas faux mais, en réalité, les choses sont beaucoup plus complexes et donc nuancées.

Plus que de GPS, il faut en réalité parler plus largement d'information de positionnement, navigation et synchronisation (PNT), dont l'impératif existe… depuis toujours. Il n'en reste pas moins que la « guerre de la navigation » (*Navigation Warfare* – NAVWAR) n'émerge comme discipline spécifique de la confrontation armée que ces dernières décennies et trouve bien, elle, ses racines dans la dialectique entre ces émissions électromagnétiques de PNT et la capacité à les neutraliser.

L'observatoire des conflits futurs se devait donc de réaliser une note sur ce sujet crucial. S'inscrivant dans le cadre capacitaire et prospectif propre à ce programme, cette note est sans surprise l'une des plus techniques réalisées depuis le début de l'observatoire. Elle n'en est pas moins organisée, comme la plupart autour de la méthode CIIP :

- Cadrer le sujet avec ses définitions et ses typologies, relatives d'une part à la notion d'information de PNT et ses multiples sources, d'autre part à la NAVWAR (première partie) ;
- Informer sur les développements capacitaires des autres puissances ou sur l'évolution des thèmes d'intérêt (seconde partie). En l'occurrence, cette partie décline les capacités NAVWAR offensives et défensives et surtout l'extrême diversité des solutions alternatives aux GPS et autres GNSS. La stratégie américaine en matière de PNT récemment publiée nous servira de fil rouge en la matière, sans pour autant restreindre le propos aux États-Unis ;
- Enfin, inférer et recommander (troisième partie). Après une synthèse des menaces relativisées à l'aune des développements technico-opérationnels en cours et envisageables, la partie expose des implications et quelques recommandations pour les milieux terrestre, aérien et spatial, enfin maritime, sans oublier les considérations par essence multimilieux.

Précisons enfin que, si la NAVWAR et la résilience de l'information de PNT sont, à l'instar du cyber par exemple, devenues des enjeux concernant l'ensemble des activités de nos sociétés, cette note se concentre avant tout sur la problématique intéressant les forces armées.

Partie 1 – NAVWAR et PNT : De quoi parle-t-on ?

La *Navigation Warfare* est un terme à l'usage encore assez confidentiel. Cela étant, il est rapidement associé au brouillage ou à la préservation du GPS, ce qui n'est pas faux mais reste bien réducteur. Cette partie propose donc de développer les définitions et typologies relatives à ce domaine de confrontation et plus largement au monde du Positionnement, Navigation, Synchronisation ou *timing* (PNT), dont il est indissociable.

1. Introduction : définition de la *Navigation Warfare*

La « *Navigation Warfare* » (NAVWAR) est actuellement définie par les Américains comme « [l'] *action défensive et offensive délibérée visant à assurer et à empêcher la transmission d'informations sur le positionnement, la navigation et la synchronisation grâce à l'emploi coordonné d'opérations de guerre spatiale, cybernétique et électronique* »[2].

Si on se limite au sens le plus étroit de la technique, la NAVWAR en soi n'offre pas d'intérêt conceptuel particulier. Elle ne désigne en effet qu'un type de cible donné dans les domaines de la guerre électronique, de la lutte informatique et des opérations dans le milieu spatial. Là où elle devient critique voire vitale pour les forces armées, c'est dans ses conséquences fonctionnelles. La NAVWAR est donc inséparable de la fonction PNT elle-même, des activités et capacités permettant de générer et d'exploiter ces informations de PNT, donc de la résilience de cette fonction.

2. L'information de PNT et ses sources

Il convient donc de préciser ce que l'on entend par « information de PNT ». Empiriquement, pour beaucoup, elle s'apparente au GPS. Si ces systèmes spatiaux sont certes au cœur de la problématique actuelle, le PNT est en réalité bien plus large.

[2] « *Deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare operations* ».

2.1. L'information de PNT : un « enabler » indispensable

Globalement, on peut qualifier l'information PNT comme l'information relative au cadre spatio-temporel de l'action. Le besoin pour cette information est donc un intangible. Depuis toujours, les armées ont besoin de savoir et de se figurer où elles, l'adversaire et d'autres éléments d'intérêts se situent, dans quelles directions les unités se déplacent, enfin de synchroniser leurs actions.

Les données de PNT permettent actuellement des services bien connus, qu'il est néanmoins important de rappeler succinctement :

- En matière de renseignement, le positionnement précis **des moyens et cibles adverses** ;
- En matière de mouvement et manœuvre, **la position** et **l'aide à la navigation** des unités et plateformes terrestres et des combattants débarqués, des plateformes navales, aériennes et spatiales permettant leurs **actions tactiques** ;
- En matière de feux, **la position** ainsi que **l'aide à la navigation** des **munitions de précision** permettant **la frappe de précision sur coordonnées** à toutes les portées ;
- En matière de soutien, les informations de positionnement et de navigation permettent également, comme dans l'industrie et le commerce, de disposer d'une **meilleure appréciation des soutiens** et de mieux **organiser les flux logistiques** ;
- Lorsque ces informations sont correctement relayées, le développement et le suivie de la **tenue de situation tactique** aux différents échelons, à différentes échelles de temps et d'espace, et le **commandement et le contrôle** des forces ;
- La **synchronisation** des émissions/réceptions des réseaux de **télécommunication,** des **radars et des systèmes de guerre électronique,** dont l'exigence en précision s'accroit au fur et à mesure que les fréquences augmentent.

De ces éléments, découle enfin la faculté à **mieux coordonner, synchroniser, voire intégrer les effets et les actions jusqu'au niveau tactique**. De multiples évolutions technico-opérationnelles viennent encore accroître le besoin pour une information PNT extrêmement précise : le combat collaboratif, les systèmes autonomes, la guerre électronique « cognitive » et la convergence croissante des différentes opérations dans le spectre électromagnétique, et de ces dernières avec le milieu cyber.

2.2. Précision et référencement au cœur du PNT

Le PNT est réalisé selon des techniques diverses mais qui reposent toutes sur la même logique que Jacques F. Raquet présente comme un cycle « prédire – observer – comparer » mettant en interaction un « état de navigation » de l'acteur (son positionnement, etc.), les capteurs lui permettant de mesurer son environnement et un modèle du monde réel permettant de réaliser des prédictions[3].

[3] Jacques F. Raquet, « Integrated Technologies and Implications » in Frank van Diggelen, Y. Jade Morton, James J. Spilker, Jr., Bradford W. Parkinson (dir), *Position, Navigation, and Timing Technologies in the 21st Century*, Wiley, 2021, pp. 1117-1118.

Une façon d'appréhender la question consiste à distinguer le **caractère relatif ou absolu de l'information PNT obtenue**. À la base, la localisation d'un élément et/ou la détermination de son mouvement peuvent être :

- Relatives, donc s'effectuer par rapport à une référence locale, parfois en mouvement, subjective, déterminées par rapport à un autre élément ;
- Absolues, donc exprimées sous forme de données objectives (coordonnées) sur un référentiel partageable par tous.

Bien évidemment, le degré de précision et même le besoin pour un référentiel absolu ont varié avec le temps et continuent de varier, selon les usages ou les activités, et selon les échelles de temps et d'espace considérées. Le « grenadier-voltigeur au coin du bois », s'il n'y a qu'un seul bois dans sa ligne de vue, n'a besoin que de la référence de ce bois pour manœuvrer et coordonner sa manœuvre avec les autres grenadiers. Le général commandant des milliers de grenadiers-voltigeurs et sur un espace comprenant de multiples bois aura besoin de basculer sur un référentiel absolu pour y situer l'ennemi, concevoir la situation et la manœuvre de ces grenadiers-voltigeurs de bois en bois, plus encore coordonner cette manœuvre, organiser leur soutien, etc.

La question du référentiel absolu renvoie plus globalement à la problématique de la cartographie à des fins militaires, dont la présente note ne nécessite pas de retracer l'histoire passionnante. Qu'il suffise ici de rappeler que ce référentiel cartographique est devenu, avec l'émergence de la science topographique à partir du XVIIème siècle, de plus en plus précis et diversifié (cartes, raster, etc.) et que les enjeux ne concernent plus tant cette précision que l'emploi de plusieurs référentiels concurrents, la prise en compte d'une masse croissante d'informations et du facteur de temporalité. C'est toute la problématique du renseignement géospatial (GEOINT) qui évolue à grande vitesse à l'aune des évolutions technologiques. Aujourd'hui, le seul milieu encore mal cartographié reste le milieu sous-marin mais on peut anticiper qu'avec son exploitation croissante et l'émergence de la « *seabed warfare* », cette lacune pourrait finir à son tour par être comblée dans les prochaines décennies.

En dépit de la diffusion de ces référentiels absolus, jusqu'à ces trois dernières décennies, l'information de PNT est, quant à elle, restée surtout relative et souvent déterminée de façon approximative, en raison soit des ressources intrinsèques de l'acteur cherchant à se situer, soit de méthodes et moyens techniques différents relatifs à une situation donnée et ne se recoupant qu'imparfaitement (par exemple, deux radars rapportant un même objet de façon différente).

2.3. Les sources de données de position, vélocité, timing

Techniquement, cette information PNT se fonde sur des **données de PVT (Position** – latitude, longitude et altitude –, **Vélocité, *Timing* (heure))** délivrées par de multiples types de moyens, initialement propres à l'opérateur cherchant à se situer et à naviguer, et depuis le XXème siècle reposant essentiellement sur des émissions électromagnétiques, dont les plus importantes depuis 30 ans sont les systèmes satellitaires.

2.3.1. Les systèmes de navigation satellitaire

A. Les Global Navigation Satellite Systems (GNSS)

Les systèmes de navigation par satellite (GNSS)[4] comprennent le ***Global Positioning System* (GPS) américain, le Galileo européen, le Glonass russe et le BeiDou (*BeiDou* Sytem – BDS) chinois**. Leur segment spatial est situé en tout ou partie sur les orbites médianes (MEO, soit environ 20 000 km d'altitude) mais le BDS comprend aussi des satellites en orbite géostationnaire et en orbite géosynchrone inclinée. Ces constellations comptent (ou compteront) un minimum de 24 satellites (30 pour BDS-3, 31 pour le GPS) permettant le positionnement de n'importe quel récepteur sur la surface du globe par tri-latéralisation (un quatrième satellite étant utilisé pour renforcer la précision). Les signaux GNSS sont émis sur trois ou quatre fréquences UHF (sur la bande L, de 1176.45 à 1610 MHz). Plusieurs de ces fréquences sont d'ailleurs identiques d'un GNSS à l'autre. Chaque signal comprend, outre l'onde porteuse analogique, des « codes d'étalement » binaires permettant d'authentifier le signal et les données opérationnelles numériques, principalement l'heure permettant la synchronisation et les éphémérides du satellite (*Clock and Ephemeris Data* – CED).

De façon plus spécifique :

- Le système américain GPS propose historiquement deux codes : un code d'acquisition grossière (*Coarse/Acquisition* ou C/A) qui est le principal code civil et un code P précis, chiffré et désigné P(Y), pour les utilisateurs militaires. À ce jour, 57 pays bénéficient du code P(Y). La majorité des satellites actuels émettent également trois codes civils supplémentaires dédiés respectivement aux besoins commerciaux, à la sûreté des transports et à l'interopérabilité avec les autres GNSS, ainsi qu'un nouveau M-code militaire ;

- Le Glonass russe représente chronologiquement la seconde constellation GNSS. Typique du parcours chaotique des capacités de défense russes durant ces dernières décennies, il a atteint une première capacité opérationnelle au milieu des années 1990, n'a pas été maintenu jusqu'à la fin des années 2000 puis est revenu à une pleine capacité en 2011 avec une nouvelle génération de satellites Glonass-M puis Glonass-K. Le Glonass diffuse des codes C/A et P analogues à ceux du GPS et a adopté sur les derniers satellites la même technique de diffusion en « répartition de code » que le système américain. À noter que les satellites Glonass K-2 plus lourds vont également embarquer une charge ROEM de surveillance maritime Ruveta destinée au ciblage antinavire, pour accroître une capacité dédiée devenue très insuffisante ;

- Le système européen Galileo, de conception plus récente, pleinement opérationnel depuis 2020, propose également plusieurs codes correspondant à une palette de services plus importante que celle offerte par le GPS : l'*Open Service* (OS), le *High Accuracy Service* (HAS) qui peut être chiffré, le *Public Regulated Service* (PRS) chiffré explicitement pour les forces de l'ordre, et un *Search and Rescue Service* (SAR) ;

[4] Voir une « bible » en la matière : Y. T. Jade Morton, Frank van Diggelen, James J. Spilker, Jr., Bradford W. Parkinson, (dir), *Position, Navigation, and Timing Technologies in the 21st Century, Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, Institute of Electrical and Electronics Engineers, Inc., John Wiley & Sons, Inc., (Hoboken, New Jersey), 2021,deux volumes.

- Le BDS chinois, lui aussi pleinement opérationnel depuis 2020, est un peu plus complexe que les autres GNSS : outre un service de diffusion analogue aux autres systèmes (*Radio Navigation Satellite Service*), il inclut également un *Radio Determination Satellite Service*, dans lequel c'est une station au sol qui calcule la position d'un utilisateur à partir d'une émission de son équipement. Le BDS comprend également un service de messagerie limité qui serait largement utilisé par les militaires chinois.

Chaque NSS emploie un repère de référence spécifique : *World Geodetic Survey 1984* (WGS84) pour GPS, GTRF pour Galileo, PZ-90 pour Glonass, CGCS2000 pour BDS, JGS2010 pour GZSS. Chacun de ces repères est cependant aligné sur le Repère International de Référence Terrestre (ITRF) géré par le Service international de la rotation terrestre et des systèmes de référence. L'IRTF atteint une précision inférieure au millimètre. Il est alimenté par un dispositif complexe de centaines de stations géodésiques couvrant la planète et des techniques de mesures (laser, interférométrie, etc.) s'affinant sans cesse et auxquelles contribuent au demeurant les GNSS[5]. Il fournit donc la base fondamentale du positionnement.

B. Les Regional Navigation Satellite Systems (RNSS)

Plusieurs puissances régionales se sont dotées ou entendent se doter de systèmes souverains de navigation par satellites couvrant leurs espaces nationaux :

- Le *Quasi-Zenith Satellite System* (QZSS) japonais, opérationnel depuis 2018. Il est composé de quatre satellites en orbite elliptique géosynchrone sur un plan orbital incliné de 40°, ce qui permet de bien couvrir l'archipel nippon. Le QZSS est explicitement un complément au GPS dont il relaie les signaux civils ;

- La dégradation du signal GPS par Washington en 1999 lors de la guerre de Kargil avec le Pakistan a incité l'Inde à développer aussi son propre RNSS autonome, l'*Indian Regional Navigation Satellite System* (IRNSS) ou NavIC. Il est lui aussi complètement déployé depuis 2018. Il est composé de huit satellites en orbites géostationnaire ou géosynchrone couvrant l'Inde et une zone s'étendant à 1 500 / 2 000 km de ses frontières avec une précision allant de dix à vingt mètres. La première génération de satellites a connu des vicissitudes entre échecs de lancement, de fonctionnement des horloges (etc.) ne laissant qu'un minimum de quatre satellites opérationnels. Une seconde génération de satellites a commencé sa mise à poste depuis 2023[6] ;

- La Corée du Sud a décidé à son tour en 2018 de développer un *Korean Positioning System* (KPS) régional du même ordre que le NavIC. Le système sera apparemment développé avec un appui américain. La date de pleine capacité était initialement fixée à 2039 mais il est prévu maintenant que les lancements s'étalent de 2027 à 2035[7].

---

[5] Zuheir Altamimi, Xavier Collilieux, Laurent Métivier, « Le Repère International de Référence Terrestre (ITRF) : état actuel et perspectives », *Revue XYZ*, N° 133 – 4e trimestre 2012, pp. 36-40 – https://www.aftopo.org/download.php?type=pdf&matricule=aHR0cHM6Ly93d3cuYWZ0b3BvLm9yZy93cC1jb250ZW50L3VwbG9hZHMvYXJ0aWNsZXMvcGRmL2FydGljbGU0MTMzMTEucGRm

[6] Anonna Dutt, « New NavIC satellite launching today: why a regional navigation system matters to India », *The Indian Express*, 29 May 2023.

[7] Byung-Kyu Choi et alii, « Performance Analysis of the Korean Positioning System Using Observation Simulation », *Remote Sensing*, 2020, 12(20), 3365 & Lim Chang-won, « Some $2.8 billion earmarked for development of independent satellite-navigation system by 2035, » *Aju Business Daily*, July 18, 2022.

- Dans le cadre de la montée en puissance de son programme spatial et de sa BITD, la Turquie a également décidé de développer son système régional de navigation et de synchronisation (*Bölgesel Konumlama ve Zamanlama Sistem* – BKZS). La stratégie spatiale publiée par Ankara en 2022 prévoit de commencer par des satellites de renforcement des signaux GNSS existants, puis de déployer les services PNT nationaux à partir du quatrième satellites, ce qui laisse penser à des satellites géostationnaires/géosynchrones comme dans les autres RNSS. Le calendrier prévoit le lancement du premier satellite en 2031[8].

2.3.2. Les techniques et systèmes de renforcement de ces signaux GNSS

Un signal GNSS n'est en soi pas d'une fiabilité à toute épreuve. Il est de faible puissance ce qui le rend vulnérable aux menaces associées à la NAVWAR (nous y reviendrons). De surcroît, il est régulièrement entaché d'erreurs : celles résiduelles concernant l'orbite et la synchronisation du satellite, celles plus conséquentes résultant des aléas de la propagation des signaux dans l'ionosphère puis la troposphère. Cet environnement géomagnétique est constamment affecté par les productions solaires. Ces dernières provoquent sur une base courante des phénomènes de scintillation qui peuvent fausser le positionnement de plusieurs dizaines de mètres[9]. De façon plus exceptionnelle, les orages magnétiques générés par les « éjections coronales de masse » (ECM), c'est-à-dire les bulles de plasma ionisé expédiées par les éruptions solaires, peuvent dégrader non seulement les signaux mais aussi les satellites eux-mêmes (ces risques sont cependant pris en compte dans leur conception depuis longtemps). Enfin, en bout de chaîne, il existe les erreurs liées aux récepteurs.

Il est donc apparu rapidement le besoin de renforcer les signaux et d'améliorer les techniques de réception et de traitement par le récepteur au profit des utilisations les plus exigeantes. À la base, le positionnement se limitait à la corrélation du code binaire envoyé par le satellite avec celui en mémoire dans le récepteur, ce qui offrait une précision de positionnement réduite, de l'ordre de 5 à 30 mètres. Le premier axe a été de développer d'autres relais spatiaux, aériens ou terrestres du même signal ce qui permet aussi d'améliorer sa puissance et de prolonger son accessibilité dans des zones masquées aux satellites. Plusieurs architectures de renforcement ont donc vu le jour :

- Les systèmes GNSS peuvent être relayés au sol par des amplificateurs, ou ***Ground-Based Augmentation System*** **(GBAS)**. Il existe aussi de multiples projets **de « pseudolites » (pseudo-satellites)** terrestres ou aéroportées locaux, civils comme militaires. Les relais terrestres fixes à la position précisément géoréférencée permettent une **« correction différentielle » (DGNSS)** avec les signaux des constellations satellitaires ;

- Existent aussi des systèmes spatiaux de renforcement satellitaires, les ***Space-Based Augmentation System*** **(SBAS)**, recourant aux systèmes de communications par satellite (SATCOM) en **orbite géostationnaire** donc fixes par rapport à des régions données : les WAAS sur l'Amérique du Nord (dès 2003), EGNOS en Europe, MSAS japonais, GAGAN indien sont opérationnels depuis plusieurs années. Les BDSBAAS chinois (les satellites GEO du système Beidou déjà évoqués), SDCM russe, KASS sud-coréen, A-BAS pour l'Afrique sub-saharienne et SPAN australien et néo-zélandais rentrent ou vont rentrer en service à leur tour dans

[8] Turkish Space Agency, *2022-2030 National Space Program Strategy Document*, 2022, p. 30.

[9] Joe Comberiate et alii, *Space Weather Effects on GPS Systems*, presentation, Applied Physics Laboratory, Johns Hopkins University, 17 Sep. 2012 – www.gps.gov/cgsic/meetings/2012/comberiate.pdf

les prochaines années. Il existe également des SBAS spécifiquement militaires comme le Talon NAMATH de l'US Air Force. Le PNT commence enfin lui aussi à bénéficier **des caractéristiques inhérentes à l'orbite basse** (*Low Earth Orbit* – LEO), qui est l'un des traits fondamentaux du « *New Space* » : un signal beaucoup plus puissant, un temps de latence réduit. Nous y reviendrons dans la partie suivante.

D'autres techniques de traitement ont depuis vu le jour. L'une d'elles revient à calculer les biais d'erreurs dans le signal à partir des données du réseau de contrôle du GNSS (le PPP pour Positionnement Ponctuel Précis) mais cette technique gourmande en calcul peut nécessiter plusieurs dizaines de minutes de calage. Elle représente cependant la base du service GPS militaire. BeiDou l'utilise également. L'autre technique est de recaler le positionnement, non plus simplement avec les codes binaires numériques (qui sont émis selon une fréquence basse), mais avec la phase de l'onde porteuse elle-même du signal GNSS (technique de la cinématique temps réel, RTK[10]). La précision de positionnement atteint alors le centimètre en ce qui concerne le GPS. L'optimal est de combiner ces deux techniques pour parer aux différents types d'erreurs. Le BDS reste un peu moins précis que le GPS ou Galileo (environ 10 m pour le signal civil au niveau mondial) mais les performances se rapprochent beaucoup entre ces différents systèmes. Sur le plan de l'horlogerie, un système comme le GPS distribue l'*Universal Coordinated Time* (UTC) déterminé par l'*US Naval Laboratory* avec une précision de moins de 30 nanosecondes la plupart du temps.

2.3.3. Les systèmes PNT alternatifs

Il existe de multiples autres systèmes de PNT fournissant **des signaux et services distincts des GNSS** (même s'ils sont maintenant calés eux-mêmes sur les GNSS pour leur propre P/T)**, de précision et portée variables**. Ces services sont souvent dédiés à une fonction particulière.

Les systèmes PNT terrestres (*Ground-Based PNT System* – GBPS) sont extrêmement variés et précèdent historiquement les GNSS. Il s'agit par exemple des **multiples radiobalises** d'aide à la navigation comme **VOR**[11] dans le milieu aérien, ou le **LORAN**[12] avant tout utile pour le milieu maritime de surface. Ce dernier est un vaste réseau de positionnement régional en HF de plusieurs milliers de kilomètres de portée, d'une précision de quelques centaines de mètres, couvrant l'ensemble des mers. Sa conception remonte à la Seconde Guerre mondiale. L'investissement dans le maintien de beaucoup de ces systèmes a décliné à l'ère des GNSS mais il est maintenant partiellement rétabli pour améliorer la résilience de la fonction PNT.

Les données PVT peuvent aussi être transmises par des systèmes ou des réseaux occupant d'autres fonctions, notamment les réseaux de communication. Il peut s'agir de PNT fournies par diverses constellations, notamment les SATCOM. Sur le plan du *timing*, il existe plusieurs techniques pour synchroniser le temps et les fréquences des émetteurs récepteurs. Par exemple, un réseau de liaison de données tactique comme la L16 inclut sa propre horlogerie.

Cette catégorie de moyens de PNT alternatif va en s'élargissant. De nouvelles techniques émergent comme **l'exploitation des signaux radio d'opportunité** émis par les réseaux GSM,

[10] *Real Time Kinematic*.

[11] VHF Omnidirectional Range, dont les applications militaires utilisent l'UHF comme son nom ne l'indique pas.

[12] *LOng RAnge Navigation*.

de télévision ou encore de Wi-Fi. Le positionnement peut s'effectuer alors avec les multiples techniques de géolocalisation (puissance du signal reçu, angle d'arrivée, différence de temps ou de fréquence d'arrivée entre plusieurs émetteurs, etc.). En d'autres termes, il ne s'agit pas ici de géolocaliser un émetteur, comme en surveillance électronique, mais de se géolocaliser par rapport à cet émetteur. **Les réseaux 5G** qui intègrent nativement des données de positionnement nécessaires pour les applications mobiles de l'internet des objets (comme les voiture autonomes), devraient à cet égard fournir une source de PNT très importantes à l'avenir.

Les développements technologiques associés au New Space, notamment **l'investissement de la LEO** par des constellations de plus en plus diversifiées, plus généralement la flexibilisation et la polyvalence dans l'exploitation du spectre électromagnétique renforcent considérablement les sources envisageables de PNT et les possibilités d'hybridation de ces services avec les autres fonctions d'émissions de radiofréquences. Pour fournir une information de PNT distincte des GNSS, ces systèmes doivent cependant eux-mêmes exploiter d'autres techniques et sources, notamment des systèmes de PNT autonomes.

2.3.4. Les systèmes autonomes

Ils recouvrent évidemment les sources historiques de données PVT, bien avant les systèmes à réception de signaux électromagnétiques externes. L'information de ces systèmes est déterminée grâce aux équipements mécaniques ou électroniques :

- **Les équipements de navigation astronomique** (à commencer par le sextant), déterminant la position du mobile par rapport au soleil ou aux étoiles. Ce sont historiquement les premiers moyens de positionnement et de navigation. Ils sont toujours employés en dernier recours (en cas de dégradation majeure de l'environnement électromagnétique par exemple) voire font l'objet d'investissement nouveaux (voir seconde partie) ;

- **Les centrales à inertielle *(Inertial Navigation System* – INS)** dotant les plateformes et munitions complexes de portée étendant, ce dans tous les milieux**.** Elles sont équipées d'une unité de mesure inertielle (*Inertial Measurement Unit* – IMU) combinant gyromètres, accéléromètres et magnétomètres afin de déterminer l'orientation, la position, la vitesse et le cap du mobile. En raison des multiples sources d'erreurs (frictions mécaniques, erreurs de mesures, etc.), les données PNT produites par toute centrale restent affectées d'une plus ou moins grande dérive dans l'espace et le temps. On distingue usuellement plusieurs niveaux de qualité de performances (*grades*) de ces INS : *Automotive, Industrial, Tactical et Navigation*, le plus élevé. En ce qui concerne les biais de navigation, la limite entre les niveaux *Tactical* et *Navigation* est en général présentée comme se situant, par heure, à 0,01° et 25 micro-g pour un mobile en virage (aboutissant à une dérive de l'ordre de 1 mille nautique pour un avion évoluant à Mach 0,8). En fait, dans la plupart des mobiles, le PNT est assuré par un système hybride dans lequel cette centrale est régulièrement recalée par les signaux GNSS et/ou d'autres sources externes ;

- **Les capteurs** fournissent également des données PNT. On mentionnera en particulier les systèmes de P/N par corrélation topographique, photographique par imagerie optronique ou radar. Cela étant, la première navigation par capteur est historiquement la navigation magnétique (NAVMAG), grâce à la boussole. La recherche d'exploitation des caractéristiques du champ magnétique terrestre connaît elle aussi un renouveau ;

- **Les systèmes d'horlogerie.** Les horloges atomiques fournissent la référence absolue en matière de timing, qu'elles soient embarquées dans les GNSS ou de multiples autres systèmes. Elles restent toutefois volumineuses. Cela étant, des horloges atomiques miniaturisées ont été mises au point et commercialisées depuis 10 ans.

Plusieurs capacités militaires continuent de reposer en priorité sur ces systèmes autonomes, dans les cas où il n'est pas souhaitable ou possible de s'en remettre à des émissions externes. On mentionnera par exemple les missiles à charge nucléaire de la dissuasion ou encore la navigation sous-marine.

2.4. Classification de synthèse

Mark Johnson de Collins Aerospace[13] et Justin Wymore de BAE Systems[14] résument la situation par quatre ensembles d'informations PNT en fonction du degré de précision et du caractère absolu/relatif de l'information PVT. Par « précision », les auteurs retiennent moins de 10 mètres en positionnement et moins d'une milliseconde en temps. Le terme « absolu » renvoie au WGS-84 du GPS et au *Coordinated Universal Time* (UTC). Ces catégories sont :

- **Les informations relatives et peu précises**. Elles sont suffisantes pour la mise en œuvre d'armes à tir direct, la manœuvre en combat débarqué, la communication au sein d'une unité ou encore la navigation en route. Elles sont fournies par exemple par le chronomètre, la navigation séquentielle ou encore un point de référence visible ;

- **Les informations absolues restant peu précises**. Elles sont suffisantes pour concevoir et conduire une stratégie ou une manœuvre aux échelles opérative ou tactique haute, pour la mise en œuvre des feux non précis comme les tirs d'artillerie classiques, celle d'armes à effet de zone, pour la communication point à point, etc. Ce sont historiquement les informations fournies par la carte, la navigation astronomique, la montre, plus récemment les radiobalises, etc. ;

- **Les informations relatives de précision** : elles sont requises pour les actions tactiques de précision en ligne de vue et les opérations en réseau locales. Dans le domaine du positionnement et de la navigation, ces données sont fournies par les systèmes de navigation inertiels précis, les capteurs ou encore les systèmes de guidage terminaux (optroniques, laser, etc.). Dans le domaine de la synchronisation, une horlogerie de précision est indispensable aux systèmes modernes d'émission/réception électromagnétique car elle est inséparable de la mesure de la fréquence. De multiples cas d'usage requièrent des précisions de timing allant de l'échelle de la microseconde à celle de la nanoseconde et une forte stabilité de la mesure (en particulier sur des plateformes soumises à de fortes vibrations). Citons notamment la synchronisation dans l'utilisation du spectre électromagnétique entre de nombreux opérateurs, en particulier celle des communications numériques, celle des sauts de fréquence ainsi que la localisation précise des émetteurs adverses en guerre électronique, la vitesse d'acquisition des signaux par l'utilisateur d'un réseau de

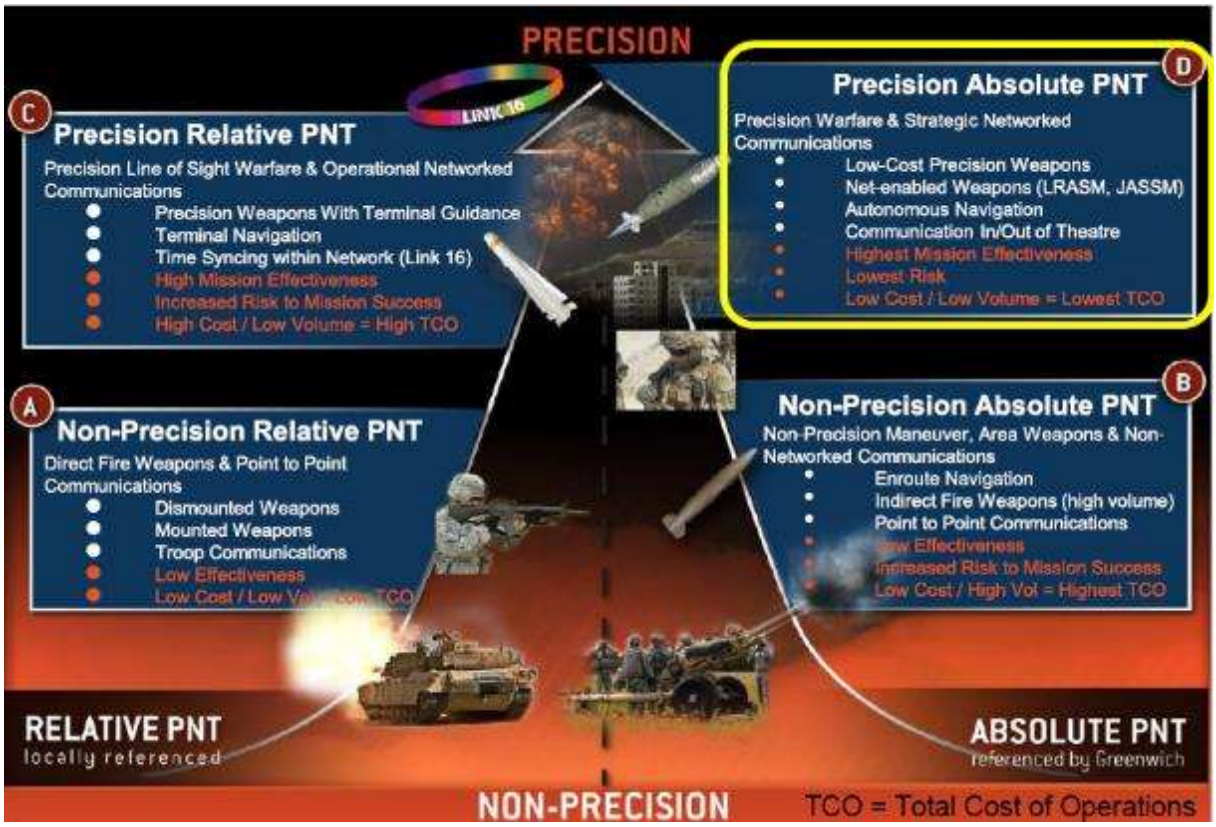
[13] Mark W. Johnson, APNT Campaign Lead, *Collins Aerospace, A Positioning Navigation and Timing (PNT) Threat Environment Model for Military and Civilian Use*, June 6, 2019 – https://www.gps.gov/governance/advisory/meetings/2019-06/johnson.pdf

[14] Justin Wymore, BAE Systems, « Preserving operational capabilities by hardening GPS », *Military Embedded Systems*, December 02, 2021 – https://militaryembedded.com/comms/gps/preserving-operational-capabilities-by-hardening-gps

transmission, l'analyse des échos radars doppler faibles, la synchronisation des radars multistatiques, etc. ;

- Enfin, **les informations absolues de précision** : elles sont requises pour toutes les activités exigeant la même précision que la catégorie précédente mais s'étendant au-delà de la ligne de vue ou nécessitant un partage de ces données PNT entre de nombreux acteurs distants. Citons par exemple la synchronisation des SIC aux échelles tactiques hautes, du théâtre ou stratégique, les cas d'usage nécessitant un géoréférencement précis comme la tenue de situation tactique, le renseignement de ciblage et en partie le renseignement géospatial, la frappe de précision sur coordonnées exigeant des *Target Location Error* (TLE) de catégorie 1 ou 2 (de 0 à 15 m), la navigation autonome sur de grandes distances, etc. Seuls les GNSS peuvent en l'état les fournir.

Figure n° 1 : « CLASSIFICATION DES BESOINS EN PNT »



Source : Mark W Johnson, APNT Campaign Lead, Collins Aerospace, *A Positioning Navigation and Timing (PNT) Threat Environment Model for Military and Civilian Use*, June 6, 2019

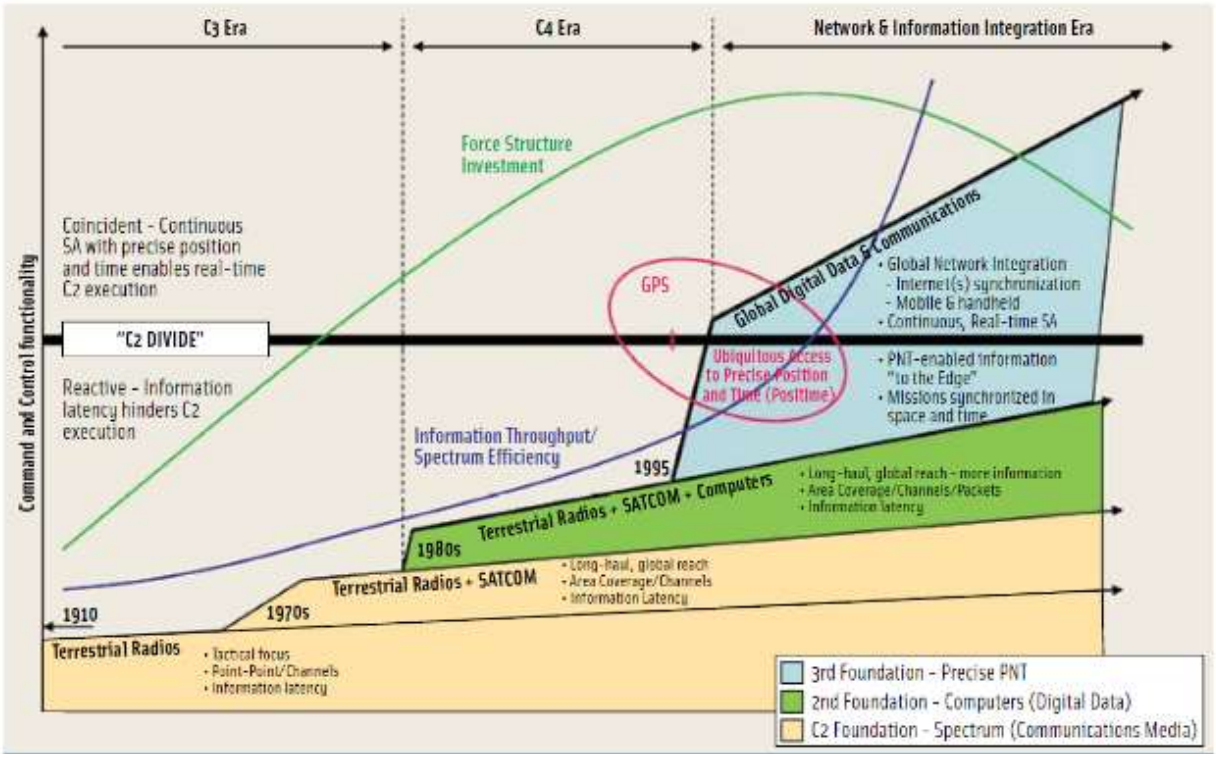
2.5. Les GNSS : l'avènement d'une information PNT absolue de précision

À bien des égards, comme le conçoivent les Américains**, les GNSS, à commencer par le GPS, ont donc donné lieu à une véritable révolution**. En découlent le *Blue Force Tracking* et plus généralement la démultiplication de la conscience situationnelle en temps réel, l'effondrement du coût de la frappe de précision et donc sa massification, la synchronisation des réseaux sur de larges échelles comme évoqués ci-dessus, etc. À bien des égards, **le GPS représente**

donc un substrat de la guerre en réseau et de nombre de capacités qui ont contribué à affirmer la supériorité militaire occidentale ces dernières décennies.

Ils ont aussi constitué un **élément fondateur de l'ensemble du tissu des systèmes d'information et de communication contemporain** bien au-delà des considérations militaires.

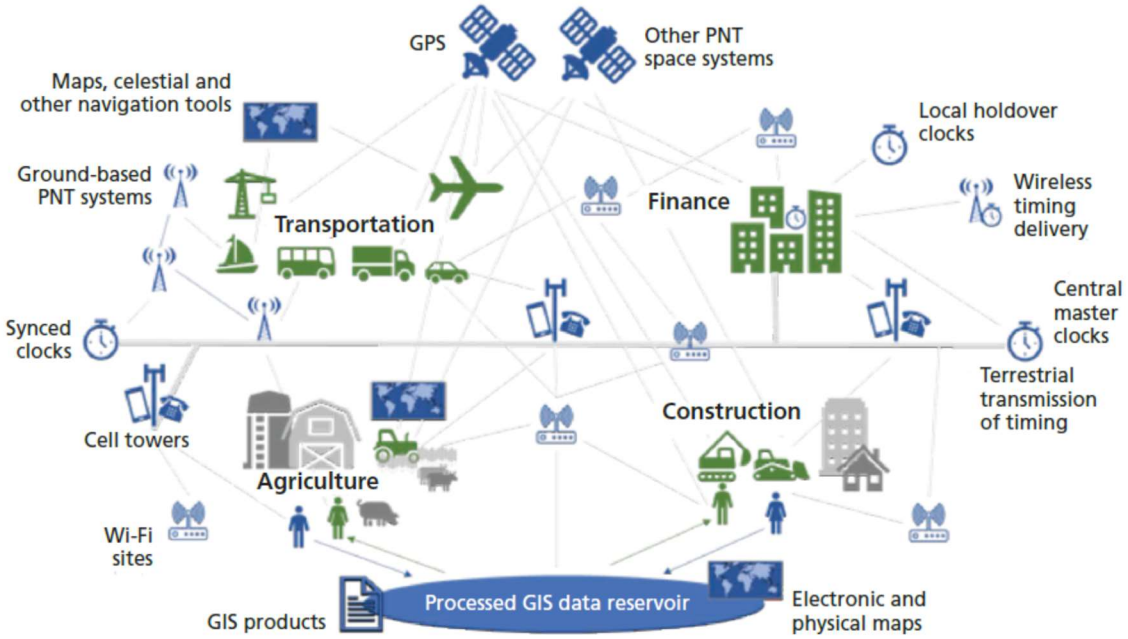
Figure n° 2 : LE PNT DE PRÉCISION, UN « *GAME CHANGER* » DES ARMÉES



Source : Jules McNeff, « Changing the Game Changer: The Way Ahead for Military PNT », *Inside GNSS*, November/December 2020, p. 46.

Ces GNSS occupent donc une place centrale, quoique non exclusive, dans ce qu'il est maintenant convenu d'appeler **un « écosystème de PNT »** conditionnant les activités de la plupart des secteurs de la société : télécommunication, transport, finance, construction, agriculture, énergie (cadencement des réseaux de transport et de distribution d'électricité), etc. Un rapport de la Rand l'a résumé dans le schéma ci-dessous pour les États-Unis mais cette représentation est valable pour l'ensemble des pays développés.

Figure n° 3 : L'ÉCOSYSTÈME DE PNT AUX ÉTATS-UNIS SELON LA RAND CO.



Source : Richard Mason et alii, *Analyzing a More Resilient National Positioning, Navigation, and Timing Capability*, Rand Corporation, 2021, p. 3.

Les GNSS n'offrent pas simplement une information situationnelle de PNT absolue et en générale très précise. Ils fournissent également **une ressource bien plus facile et moins coûteuse à exploiter que la plupart des autres moyens**. Par exemple, un radar ou un réseau de communication, qui existait bien avant le GPS, n'a *a priori* pas besoin de son horlogerie pour synchroniser ses émissions/réceptions mais la diffusion de cette technologie a rendu la tâche beaucoup plus facile. De même, une centrale inertielle recalée par GNSS est bien moins onéreuse qu'une centrale purement autonome. Le recours à ces GNSS a donc été généralisé dans la conception de l'ensemble des systèmes pour des raisons de coûts et de simplicité. Cela étant, les redondances sont, comme nous l'avons vu, multiples en ce qui concerne les systèmes critiques, en particulier ceux dont la mise en échec mettrait en danger des vies, comme les systèmes de guidage à l'atterrissage.

Le développement des RNSS des puissances régionales témoigne de ce caractère stratégique des données PNT fournies par ces systèmes satellitaires et de l'enjeu de souveraineté qu'elles constituent ; ceci compte tenu des risques pesant sur la diffusion des GNSS en cas de crise, longtemps associés à la politique américaine d'accessibilité aux signaux GPS mais exacerbés ces dernières années par le renforcement de la compétition stratégique.

3. Des menaces plurielles, constitutives de la NAVWAR

Comme la plupart des autres domaines de *warfare* (c'est-à-dire désignant la façon de faire la guerre, sur le plan des types d'activités et de capacités), la NAVWAR repose sur un **triptyque surveillance / attaque / défense** avec comme objectif le contrôle de l'environnement donné et de son exploitation. Il nous apparaît d'emblée utile de proposer une définition instanciée de ce triptyque que nous n'avons pas trouvée dans les glossaires institutionnels :

- Surveillance : l'entretien de la conscience situationnelle de l'information de PNT, de sa transmission et sa réception dans l'environnement électromagnétique (EME) ou cybernétique. Il comprend en particulier la capacité à détecter, caractériser, localiser, cartographier et diffuser les sources d'interférence avec cette transmission ;
- Attaque : les mesures offensives permettant d'affecter les informations de PNT de l'adversaire, de détruire, interdire, interrompre, décevoir ou dégrader cette information ;
- Défense : les mesures de protection ou les contre-contre-mesures garantissant la disponibilité et l'intégrité de ces informations face aux attaques adverses.

En matière de NAVWAR offensive, **les GNSS et les systèmes de renforcement font face de l'avis de tous à des menaces potentielles croissantes**. L'ensemble des modes d'action relève à bien des égards de la guerre électronique et du *counterspace*. Le *Joint Navigation Warfare Center* (JNWC) américain, situé à Kirtland Air Force Base (NM), chargé de ces missions afin d'appuyer des commandements opérationnels dans l'obtention d'une *PNT superiority*, dépend d'ailleurs de l'*US Space Command*.

Ces menaces s'exercent tout d'abord sur **le « segment utilisateur »** de ces systèmes, donc le signal et sa réception par l'opérateur, selon **les deux approches de guerre électronique** déjà bien connues :

- **Le brouillage classique (*jamming*)** de puissance. Il consiste à augmenter le niveau de bruit électromagnétique de façon à empêcher l'acquisition du signal ou à le faire décrocher. Ces GNSS utilisent des émissions UHF de puissance faible, donc à la base très vulnérables, comme de multiples évènements l'ont déjà démontré. Précisons que ce brouillage s'effectue dans la ligne de vue du récepteur visé ;
- **L'usurpation (*spoofing*)**. Elle consiste à substituer un faux signal à l'original. Elle se fait elle aussi en ligne de vue. Il existe plusieurs techniques d'usurpation. La plus simple est le « *meaconing* », qui consiste, grâce à une balise, à répercuter en décalage, avec un surcroît de puissance, le signal GNSS sans en changer les paramètres. Les modes d'action plus avancés consistent à fabriquer un faux signal PVT. Le défi est alors de concevoir un signal précisément adapté aux antennes et à la posture de la cible. Le but peut être de détourner la plateforme, de la détruire ou de s'en emparer. L'usurpation est certes plus sophistiquée que le brouillage mais elle est aussi plus complexe à réaliser et dépend de multiples paramètres : qualité du renseignement, écart de puissance avec le signal satellitaire, angle d'arrivée sur le récepteur visé, etc.[15]

[15] Shah Zahid Khan, Mujahid Mohsin, Waseem Iqbal, « On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions », *PeerJ Comput. Sci.* 7:e507 6 May 2021 – http://doi.org/10.7717/peerj-cs.507

Il est ensuite théoriquement possible de **s'attaquer au segment de contrôle** de ces constellations ainsi qu'aux stations terrestres type GBAS ou GBPS. Le mode d'action peut alors relever :

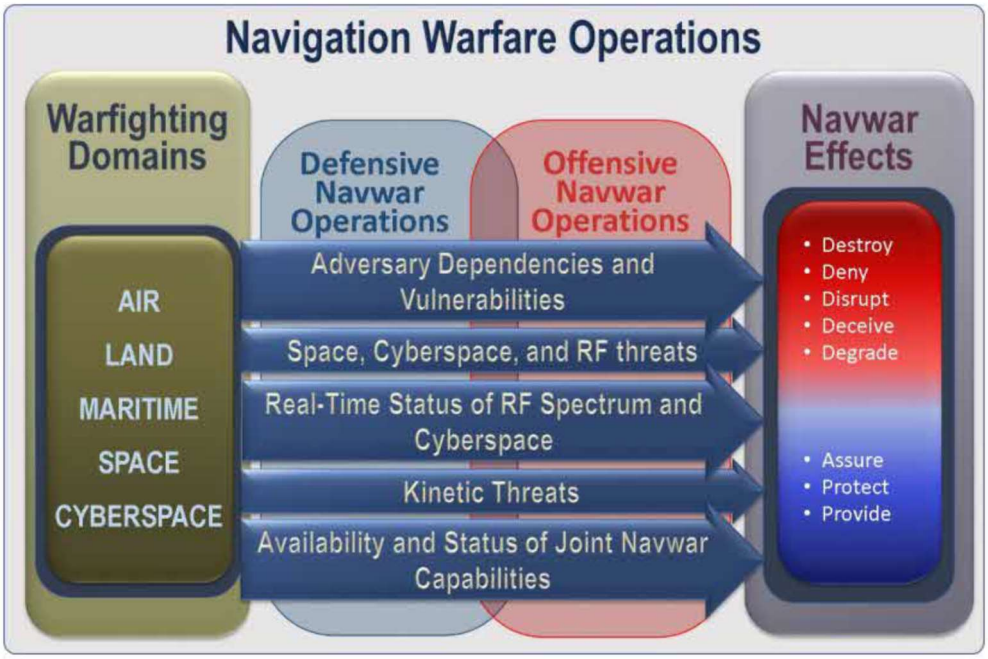
- De **l'attaque cinétique ou électronique** si des stations de contrôle sont à portée des moyens adverses ;
- Ou de la **lutte informatique offensive,** à condition de pouvoir accéder aux systèmes d'information du segment contrôle.

La dernière option théorique est de **s'en prendre directement au segment spatial**, aux satellites proprement dit. Plusieurs modes d'action sont alors à prendre en compte :

- **Les attaques de proximité et de rendez-vous co-orbitaux (RPO).** Elles peuvent être entreprises soit sous forme d'attaque électronique à effets physiques (laser, armes à micro-ondes de forte puissance) sur les satellites, de brouillage de la liaison montante à proximité des SATCOM opérant comme SBAS en géostationnaire. Elles recouvrent également l'exploitation des technologies duales d'inspection et de réparation de satellites ou de suppression de débris ;
- Peut-être les armes à énergie dirigée depuis la surface, en l'occurrence **les lasers de forte puissance (HEL)**.

Enfin, il ne faut pas exclure à l'horizon de l'étude la capacité à **attaquer les sites de lancement** eux-mêmes des satellites GNSS.

Figure n° 4 : SCHÉMA DE SYNTHÈSE DES OPÉRATIONS DE *NAVIGATION WARFARE*



Source : DoD Chief Information Officer, Principal Staff Assistant for PNT Policy, *Strategy for the Departement of Defense Positioning, Navigation and Timing Enterprise*, Unclassified Version, November 2018, p. 37.

C'est le croisement de la dépendance critique des armées modernes (notamment occidentales) aux systèmes GNSS et de leur vulnérabilité qui donne surtout corps à la notion actuelle de NAVWAR, même si cette dernière s'étend également aux autres moyens de PNT exploitant

les environnements électromagnétiques et cyber. La problématique essentielle de la NAVWAR reste donc avant tout celle du devenir de ces GNSS à l'aune de ces menaces et de l'émergence ou de la réémergence d'autres options, notamment de moyens d'information de PNT relatifs de précision.

À cet égard, comme la typologie de Mark Johnson le montre, une des questions clés de la NAVWAR, qu'il s'agisse de ciblage offensif ou de protection et d'investissement à des fins de résilience, reste donc de **distinguer les fonctions pour lesquelles ces données GNSS constituent une dépendance critique,** un « *enabler* » dont elles ne peuvent se passer, **ou alors un « *enhancer* », un élément améliorant l'efficacité ou la rentabilité** de la fonction considérée, mais dont elles peuvent se passer, même moyennant une dégradation de leurs performances.

Partie 2 – Développements technologiques et capacitaires

Le débat sur la vulnérabilité de la fonction PNT remonte aux années 1990. Il est depuis régulièrement alimenté par des cas concrets de brouillage et d'usurpation du GPS. L'appréhension de la vulnérabilité à ces menaces de plus en plus présentes se double de celle des constellations elles-mêmes. Cependant, les états-majors, comme les industriels, ne sont pas restés les bras croisés. Dans le domaine militaire, aux États-Unis en particulier mais pas uniquement, les armées ont développé de multiples moyens de renforcer ces GNSS face au continuum de menaces cyber-électroniques. Aujourd'hui, la place centrale des GNSS dans la fourniture de l'information de PNT n'est pas remise en cause. Émerge cependant la volonté de créer de véritables écosystèmes PNT militaires mobilisant l'essentiel des techniques présentées en première partie pour parvenir à une fonction plus résiliente. Si les projets de R&D abondent, leur traduction capacitaire prend du temps car elle se heurte à de multiples obstacles.

1. La NAVWAR offensive : menaces affirmées et putatives

1.1. Des menaces de brouillage et d'usurpation de plus en plus courantes

De multiples cas d'attaque électronique sur la réception du GPS ont défrayé la chronique depuis 20 ans, participant à la diffusion d'un sentiment d'insécurité croissant, d'appels au réveil des gouvernements pour se prémunir contre ces menaces. Ces cas sont bien documentés, voire cités à satiété, donc nous en rappellerons les principaux ici pour mémoire. Il s'agit tout particulièrement d'actions de brouillage :

- Les forces irakiennes ont recouru à ce mode d'action contre les Américains en 2003 avec une demi-douzaine de brouilleurs russes Aviaconversia à 40 000 $ pièce. Leur efficacité a toutefois été nulle, puisque la puissance aérienne les a détruit en 48h, parfois même avec des munitions guidées par GPS[16] ;
- La Corée du Nord en a réalisé de façon répétée à partir de 2010 affectant la partie septentrionale de la Corée du Sud, avec des brouilleurs du même fabricant ou un dérivé indigène. Là encore, cependant, l'impact a été très limité sur les activités tant civiles que militaires[17] ;

[16] Frank Vizard, « Safeguarding GPS ».*Scientific American*, April 14, 2003 – https://www.scientificamerican.com/article/safeguarding-gps/

[17] *North Korean Jamming of GPS Systems*, June 2012, TRADOC G-2 Intelligence Support Activity – https://community.apan.org/wg/tradoc-g2/operational-environment-and-threat-analysis-directorate/m/documents/213288/download, « North Korea jams South's guided missiles » Blog Defence Forum India – http://defenceforumindia.com/forum/threads/north-korea-

- La Russie brouille le GPS de plus en plus couramment. Ce fut notamment le cas en Ukraine depuis 2014, puis en zone Méditerranée orientale et en Syrie comme s'en était plaint le commandant des opérations spéciales américaines[18] et plus récemment les Israéliens. Les Russes ont également brouillé le système GPS lors de l'exercice de l'OTAN Trident Juncture 2018 en Norvège. Dans la confrontation actuelle, les activités de guerre électronique de Moscou se sont nettement accentuées. Bien évidemment, le brouillage du GPS sur lequel repose largement les forces ukrainiennes est une constante de cette guerre depuis 2022 mais au-delà de ce théâtre et de ses zones proches comme la mer Noire, les Russes sont aussi accusés d'être à l'origine – c'est un euphémisme – de perturbations devenues presque systématiques en Méditerranée orientale, dans nord de la Norvège, en zone Baltique, des activités s'étendant de plus en plus en ce début 2024, sur le nord de l'Allemagne et de la Pologne[19] ;
- Il existe aussi de nombreux cas de brouillage accidentel, comme celui de l'*US Navy* sur la réception du GPS à San Diego en 2007[20].

Le brouillage du GPS s'est donc installé comme mode d'action courant non seulement dans les conflits armés, mais aussi en phase de « contestation », comme mode d'action non létale de pression ou de manifestation de tension diplomatique.

Il se diffuse également dans le domaine de la sécurité intérieure, s'inscrivant dans la veine des nombreuses initiatives entendant protéger la vie privée contre l'industrie de la surveillance, illustré par exemple par la multiplication des dispositifs permettant d'éviter le pistage des véhicules. À cet égard, la menace ne concerne pas uniquement les GNSS mais aussi par incidence les systèmes d'amplification comme ce fut le cas en 2012 avec le GBAS installé à l'aéroport de Newark.

Ces systèmes de brouillage sont extrêmement variés. À un bout du spectre figurent les dispositifs portables (PDD) d'une puissance de quelques watts, de la taille d'un paquet de cigarette et même maintenant d'une clé USB, déjà largement commercialisés en dépit de leur caractère illégal dans la plupart des pays. À l'autre bout, certaines armées modernes déploient des brouilleurs de plusieurs kW voire dizaines de kW. Parmi leurs nombreux moyens de guerre électronique[21], les forces russes alignent par exemple au moins deux types de système de brouillage UHF affectant entre autres, les GNSS : le R-330ZH Zhitel d'une puissance d'au moins 6 kW[22] au sein des compagnies de guerre électronique enrégimentées et le R-340RP Pole-21,

---

jams-souths-guided-missiles.19963/, Kyle Mizokami, « North Korea Is Jamming GPS Signals », *Popular Mechanics*, Apr 5, 2016

[18] Joseph Trevithick, « The Russians Are Jamming US Drones in Syria Because They Have Every Reason To Be », Blog *The War Zone, The Drive*, April 10, 2018 ; Alex Hollings, « SOCOM Commander: Russia is using electronic warfare to 'disable' SOCOM aircraft over Syria SOFREP Original Content », *Foreign Policy*, accessible sur le site SOFREP, 27 avril 2018 – https://sofrep.com/102518/socom-commander-russia-is-using-electronic-warfare-to-disable-socom-aircraft-over-syria/

[19] Voir le site : https://gpsjam.org/ & « Airlines report GPS signal jamming: Russia gets the blame », *Politico*, March 28, 2024, https://www.politico.eu/article/airlines-flying-baltic-region-report-gps-signal-russia-gets-blame/

BY TOMMASO LECCA

[20] Randy Dotinga, « Fact Check: Mysterious Outage Unleashes S.D. Chaos? », Voice of San Diego, June 10, 2011 – https://voiceofsandiego.org/2011/06/10/fact-check-mysterious-outage-unleashes-s-d-chaos/

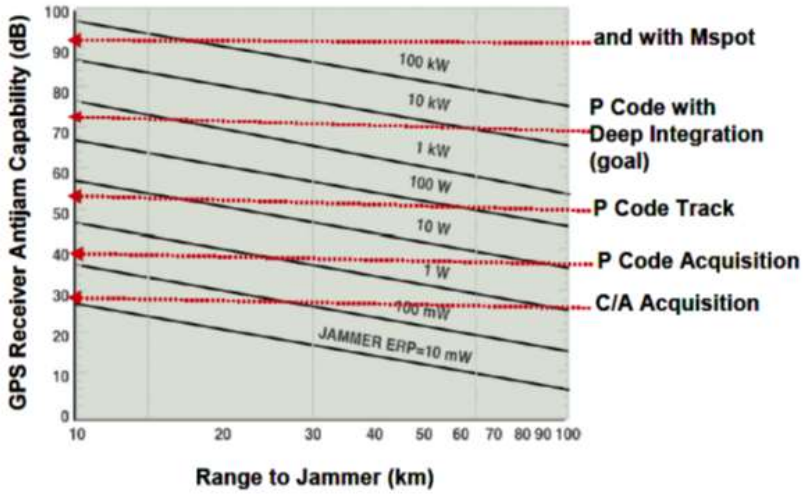
[21] Voir note 1 de l'Observatoire des conflits futurs, Philippe Gros, « Les opérations en environnement électromagnétique dégradé », FRS, 2018.

[22] « R-330ZH », Fiche Rosobobonexport, http://roe.ru/eng/catalog/air-defence-systems/elint-and-ew-equipment/r-33ozh/

un dispositif de protection des sites fixes composé d'antennes de 20 W, au sein de la brigade de GE que compte chaque grand district militaire.

De fait, comme évoqué en première partie, **le signal du GPS est faible.** Sans sa modulation, il se perd même dans le bruit EM ambiant. Après traitement et amplification, le rapport « signal sur bruit » (SNR) du code C/A, le plus utilisé, est de moins de 30 décibels (dB). Dans ce contexte, bien entendu, de multiples paramètres conditionnent la portée du brouillage : angle de réception par la cible, condition de propagation, etc. En condition optimale, un simple PDD d'un Watt peut prévenir l'acquisition du code C/A à des distances de près de 100 km. Le code P(Y), plus étalé sur la bande de fréquence, est, à la base, encore moins puissant mais son traitement permet au final un SNR sensiblement supérieur, d'environ 10 dB. Le même brouilleur basse puissance pourra empêcher son acquisition à plusieurs dizaines de kilomètres et même le faire décrocher à environ 20 km. Ceci place l'essentiel d'une zone d'action tactique et même en partie la profondeur tactique ou la zone des soutiens, à portée de ces systèmes. De même, ils peuvent dérouter les armes de précision guidées par GPS en phase de guidage terminale, comme l'ont démontré les échecs de bon nombre de frappes de précision des forces ukrainiennes, réalisées à base de JDAM – ce que confirment les fuites de documents classifiés américains du début de l'année 2023[23] – voire de roquettes GMLRS. Entre autres effets, le brouillage russe, s'il est en ligne de vue, entrave également le raccordement des stations-sol avec les satellites du système Starlink[24].

Figure n° 5 : CAPACITÉ DE BROUILLAGE GPS
EN FONCTION DE LA PORTÉE ET DU RAPPORT SIGNAL / BRUIT DU RÉCEPTEUR



Source : George T. Schmidt, *Navigation Sensors and Systems in GNSS Degraded and Denied Environments* STO-EN-SET-197, NATO STO, 2013, pp. 1-6. Note : dB= décibel.

[23] Lara Seligman, « Russia jamming U.S. smart bombs in Ukraine, leaked docs say », *Politico*, 4 décembre 2023.

[24] Sam Skove, « Using Starlink Paints a Target on Ukrainian Troops », *Defense One*, 23 mars 2023.

L'usurpation, démontrée par l'expérimentation réalisée sur un drone puis un Yacht par le *Radionavigation Laboratory* de l'Université du Texas en 2012-2013, est moins courante mais les cas se multiplient également :

- Elle a été réalisée en 2017 sur plusieurs navires commerciaux en mer Noire, probablement là encore par la Russie. La question a été bien investiguée par le *Center for Advanced Defense Studies* (C4ADS) de Washington en lien avec l'Université du Texas[25] ;
- En juillet 2019, plusieurs centaines de navires mais aussi des riverains ont été affectés par une vaste entreprise d'usurpation dans le port de Shanghai, plus sophistiquée encore qu'en mer Noire[26] ;
- L'Iran a peut-être aussi démontré des capacités en la matière : même si les circonstances restent sujettes à caution, la fameuse capture du drone furtif RQ-170 américain en décembre 2011 en serait, selon certains, la démonstration. L'incident a en effet donné lieu à bien des spéculations dont l'une des principales est celle de l'usurpation de son signal GPS par les Iraniens. Certains ont émis l'hypothèse d'un emploi combiné de stations type Avtobaza et 1L125M APUR, mais il n'est fait mention nulle part de l'acquisition par l'Iran de ce système[27]. De sorte qu'il n'y a à ce jour aucune preuve que les Iraniens soient effectivement parvenus à leurrer le GPS du drone. Cependant, les Gardiens de la Révolution sont peut-être également parvenus depuis à usurper à plusieurs reprises les signaux de bâtiments dans le Golfe Persique. C'est une forte probabilité en ce qui concerne la capture du pétrolier britannique *Stena Impero* en 2019[28]. L'usurpation est aussi suspectée dans l'affaire de la saisie du navire de patrouille de l'US Navy en 2016[29].

Si ces attaques ne se sont pas traduites par des dommages, le risque est néanmoins considéré comme élevé, ce d'autant que 50% des accidents maritimes résultent d'erreurs de positionnement et de navigation.

L'un des défis majeurs de ces attaques est leur **détectabilité**. Un brouillage peut être difficilement discernable d'une perturbation accidentelle, mais il est détectable. L'usurpation, si elle est bien menée, ne pourra parfois être appréhendée qu'à l'aune des erreurs de navigation constatées.

Le passage à l'ère de la radio logicielle (*Software-Defined Radio* – SDR) et les perfectionnements croissants de l'intelligence artificielle démultiplient ces capacités de leurrage, comme c'est d'ailleurs le cas pour l'ensemble de la guerre électronique. Cela étant, le chiffrement du code P(Y) continuerait de prémunir les utilisateurs militaires jusqu'à présent des techniques de fabrication de signaux. Le chiffrement de plusieurs services de Galileo va renforcer cette résilience. Cependant, les techniques de « *meaconing* » ne sont pas affectées par ce chiffrement

---

[25] Auteur non mentionné, *Above Us Only Sky, Exposing GPS Spoofing in Russia and Syria*, Center for Advanced Defense Studies, 2019 – https://www.c4reports.org/aboveusonlystars

[26] Mark Harrisarchive, « Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai », *MIT Technology Review*, November 15, 2019 – https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

[27] Voir sur cette affaire, les articles de David Cenciotti, blog the Aviationist – https://theaviationist.com/tag/lockheed-martin-rq-170-sentinel/page/7/

[28] Michelle Wiese Bockmann, « Seized UK tanker likely 'spoofed' by Iran », Lloyd's List, 16 août 2019 – https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

[29] Nick Adde, « Calls Grow to Find Back Up Systems for GPS », *National Defense*, 11 février 2021, https://www.nationaldefensemagazine.org/articles/2021/2/11/calls-grow-to-find-back-up-systems-for-gps

et peuvent réaliser des effets de dénis de service mais la manipulation est alors beaucoup moins sophistiquée. En outre, reste à savoir si le *meaconing* peut répliquer plusieurs signaux à la fois. La plupart des récepteurs GNSS sont maintenant multi-constellations, surtout dans le milieu civil, ce qui limite d'autant plus les risques[30].

1.2. Quels risques pour « A Day without space » à l'avenir ?

Sur le plan militaire, le débat se décale progressivement sur la neutralisation des constellations GNSS elles-mêmes et les enjeux du « *counterspace* »[31]. Beaucoup plus grave que le brouillage et l'usurpation, de portée locale, elle aurait pour conséquence une perturbation, une dégradation et même une interruption totale des services sur l'ensemble du globe. Une constellation comme le GPS avec ses 31 satellites semble toutefois relativement résiliente dans le sens où le minimum requis de quatre satellites en ligne de vue serait encore atteint même avec la perte de six satellites. Si les pertes dépassaient ce seuil en revanche, se produirait alors un effet d'interruption de service d'ampleur croissante dans le temps et l'espace.

Actuellement, pour neutraliser une constellation en MEO, la seule capacité envisageable est la **lutte informatique offensive** contre les segments spatiaux et de contrôle. Une fois rappelées les évidences, à savoir que ces systèmes sont théoriquement bien protégés, en particulier le GPS de la *Space Force*, mais que les vulnérabilités restent toujours possibles, on ne spéculera pas plus sur cette menace faute de disposer de la moindre information tangible en la matière.

Pour l'avenir, **les armes à énergie dirigée (AED)** pourraient (avec beaucoup de réserves) constituer une menace. Un premier candidat serait le **laser sol-espace**. À ces portées (environ 20 000 km), pointer précisément un laser sur une cible en défilement à 2 km/sec représente sans doute un défi mais dès lors que la technologie devient mature pour les communications entre satellites en orbite basse et vers la surface, on peut penser qu'à l'avenir, la performance ne serait pas insurmontable. Le plus grand défi reste sans doute la question de la puissance déposée sur la cible à ces distances. Tout faisceau laser obéit à la loi de la diffraction qui conditionne la surface de la tâche laser sur la cible, donc l'irradiance en watt/cm^2. Elle dépend non seulement de la puissance mais aussi de la longueur d'onde, de la portée de la focalisation et du diamètre du télescope de pointage. Pour donner un ordre de grandeur, génériquement, à 20 000 km, un laser solide d'une longueur d'onde d'un peu plus d'un micromètre, devrait atteindre des puissances de sortie de l'ordre de 10 MW pour réaliser un effet de perforation équivalent (1,5 à 2 cm d'aluminium par seconde) à celui que devraient afficher, à 20 km de portée, les lasers de 300 kW développés par les Américains pour le moyen terme[32].

Il existe déjà, ce depuis les années 1990, des prototypes d'arme laser de plusieurs Mégawatt (comme le MIRACL américain). Ce sont des lasers à milieu chimique, des solutions abandonnées depuis pour leur toxicité et les difficultés de ravitaillement. Les militaires leur préfèrent aujourd'hui des lasers à milieu solide (fibre optique, dalles refroidies par liquide, etc.). Il serait

[30] Opinion d'un ingénieur industriel spécialiste de ces technologies, 2018.

[31] Voir par exemple : Brian G. Chow et Brandon W. Kelley, « Op-ed | Peace in the Era of Weaponized Space », *Space News*, July 28, 2021.

[32] Exemples et calcul rapide de l'auteur développé à partir des équations proposées par « LWW: Laser Weapon Web », *ThoughSF*, 13 April 2016 – http://toughsf.blogspot.com/2016/04/lww-laser-weapon-web.html.

possible en théorie d'atteindre ces niveaux de puissance à l'avenir mais, pour éviter une diffraction trop importante, il faudrait des télescopes de l'ordre de 10 mètres, donc de vastes infrastructures fixes type laboratoire. Pour autant, selon la *Defense Intelligence Agency*, un laser sensiblement moins puissant, de l'ordre de quelques MW, s'il est en mesure de pointer son faisceau pendant plusieurs minutes, serait capable d'échauffer le satellite, de déstabiliser son subtil équilibre thermique, d'endommager certaines de ses composantes (câbles, etc.) précipitant sa mise hors service[33]. On peut cependant s'interroger sur la faisabilité d'une arme laser en mesure d'effectuer un tir dépassant les quelques dizaines de secondes. Il faudra de toute façon attendre encore bien des années pour que de tels niveaux de puissance soient atteints par les lasers solides. Cela étant, cette capacité pourrait être à la portée des Américains et probablement des Chinois, dans les deux prochaines décennies.

Intéressons-nous maintenant aux perspectives de neutralisation par **opérations co-orbitales, d'ores et déjà plus crédibles que le laser sol-espace** contre ce type de constellation. Il est possible d'envisager l'embarquement sur satellites d'AED, laser mais aussi d'armes à micro-ondes/électromagnétiques de forte puissance (HPEM) opérant par perturbation ou dégradation des composantes électriques de la cible. En ce qui concerne les lasers, le positionnement spatial s'affranchirait des contraintes de la perturbation atmosphérique. Un laser d'une puissance de sortie de quelques kW à dizaines de kW, posté à quelques centaines de mètres voire quelques kilomètres de sa cible, pourrait tout à fait cibler ses panneaux solaires. Les armes HPEM sont également des effecteurs à prendre en compte pour l'avenir dans la mesure où leur efficience progresse, rendant possible leur embarquement sur satellite, à condition d'être utilisées à très courte portée de leur cible. Il est également possible d'envisager des satellites de brouillage qui devraient alors être précisément positionnés pour affecter la liaison ascendante de contrôle du satellite GNSS ou du satellite SATCOM en GEO opérant comme SBAS. Les opérations ASAT reposant sur les opérations de rendez-vous et de proximité (RPO) sont plus crédibles encore en ce qu'elles utiliseraient des techniques duales, déjà pleinement matures, d'accostage du satellite cible à des fins de maintenance ou de ravitaillement. Il s'agit même d'ailleurs de la principale menace envisagée dans les wargames de guerre spatiale chinoise contre les États-Unis et leurs alliés, organisés par le *Nonproliferation Policy Education Center* (NPEC)[34].

Cependant, ces techniques co-orbitales nous semblent partager les mêmes contraintes en termes de phénoménologie spatiale. Il faudrait en effet déployer des constellations de satellites ASAT pour espérer neutraliser celles des GNSS, avec un satellite effecteur par satellite GNSS ciblé. La manœuvre d'un satellite est prédictible mais elle est lente et peut se compter en jours voire semaines dans le cas qui nous occupe. Elle resterait de plus très limitée par la consommation de carburant nécessaire pour se rapprocher des satellites cibles[35]. N'oublions pas enfin qu'un satellite GNSS dispose lui aussi d'une capacité de manœuvre, comme démontré

[33] Defense Intelligence Agency, *State of the Art and Evolution of High-Energy Laser Weapons*, Defense Intelligence Reference Document, Acquisition Threat Support, 31 March 2010, pp. 22-23 – https://documents2.theblackvault.com/documents/dird/state-of-art-and-evolution-of-high-energy-laser-weapons.pdf

[34] Henry Sokolski (dir), *China Waging War in Space: An After-Action Report*, Occasional Paper 2104, August 2021.

[35] Lire Rebecca Reesman, James R. Wilson, *The Physics of the Space War: How Orbital Dynamics Constrain Space-to-Space Engagement*, Center for Space Policy and Strategy, The Aerospace Corporation, Oct 16, 2020 – https://csps.aerospace.org/papers/physics-war-space-how-orbital-dynamics-constrain-space-space-engagements

récemment par la manœuvre d'évitement de collision effectuée par un des véhicules Galileo[36]. Elle le place temporairement hors fonction mais peut lui permettre d'éviter la neutralisation en cas de conflit. Ces contraintes posent évidemment des limites à la capacité de neutralisation d'une constellation sur court préavis par exemple pour les modes d'action préemptifs prêtés à la stratégie de défense active chinoise, ce d'autant que ces déploiements interviendraient probablement au vu et au su des capacités de *Space Situational Awareness* (SSA) de leurs opposants qui s'accroissent elles aussi significativement.

Pour limiter ces contraintes et garantir un effet en temps opportun, la seule solution serait de déployer ces constellations offensives en marquage de chaque satellite GNSS ciblé dès le temps de paix (ou de contestation). C'est d'ailleurs ce qu'envisagent les participants au wargame du NPEC et d'autres spécialistes. Les estimations du nombre de mini-satellites RPO que la Chine pourrait potentiellement déployer à la fin de la décennie ont ainsi doublé de 100 à 200, ce qui permettrait à Pékin d'attaquer l'ensemble des constellations américaines en même temps[37]. Cela étant, de tels déploiements signifieraient assumer un niveau d'agressivité et de dissuasion inédit. Il laisserait de plus le temps à l'opposant de préparer des contre-mesures. Néanmoins un mode d'action ASAT impliquant un déploiement plus progressif, en cas de conflit dans le cadre d'une démarche d'escalade calculée, est tout à fait envisageable et rend crédible ces menaces.

1.3. Conscience situationnelle et NAVWAR défensive

1.3.1. La conscience situationnelle : élément central de la NAVWAR

Le premier défi à relever en NAVWAR fondée sur la guerre électronique est celui de la conscience situationnelle, au même titre d'ailleurs que dans tous les autres domaines de la GE. Ces techniques de NAVWAR relèvent typiquement des disciplines de surveillance et de défense électronique d'une part, de surveillance et de lutte informatique défensive d'autre part. Par exemple, l'identification et la localisation des sources d'interférence à la réception des GNSS ou d'autres émissions de PVT relèvent classiquement des mesures de soutien électronique ou encore de l'élaboration du renseignement d'origine électromagnétique (ROEM), notamment de l'ordre de bataille électronique. La détection d'usurpation est quant à elle typiquement au croisement de la guerre cyber et électronique. Sur le plan technique, nous peinons à distinguer des approches spécifiques à ce volet de la NAVWAR. On ne les détaillera donc pas ici[38]. Qu'il suffise ici de rappeler qu'il s'agit d'un champ en pleine mutation, marqué par une flexibilisation croissante des opérations dans le spectre électromagnétique à l'ère du « *software-defined* » (les technologies de traitement logiciel des signaux) et de la polyvalence et la miniaturisation toujours accrues des équipements, par la convergence avec la lutte informatique (illustrée par le processus de synchronisation des *Cyber Electromagnetic Activities* dans les armées

[36] Tracy Cozzens, « Galileo satellite performs collision avoidance maneuver », *GPS World*, March 25, 2021 – https://www.gpsworld.com/galileo-satellite-performs-collision-avoidance-maneuver/

[37] Brian G. Chow, Brandon Kelley, « China's Anti-Satellite Weapons Could Conquer Taiwan—Or Start a War », *The National Interest*, August 21, 2021.

[38] Nous renvoyons donc le lecteur à la première note de cet observatoire sur les opérations en environnement électromagnétique dégradé.

occidentales). Une bonne illustration de cette polyvalence réside en ce que plusieurs des solutions PNT qui suivent sont en mesure de servir non seulement la résilience, le volet défensif mais aussi cette conscience situationnelle.

1.3.2. La « défense active » : la neutralisation des capacités d'attaque électronique adverses

Il est intéressant de mentionner plus spécifiquement les développements dans le domaine de l'attaque cinétique à des fins de GE défensives. Sur ce plan, en effet, les Américains mettent au point activement depuis quelques années les capacités dites de **« guidage sur brouillage » (*Home-on-Jam*)**, dans la pratique, « guidage sur signal », dérivées de celles de frappe antiradar faisant historiquement partie de la neutralisation des défense antiaériennes (SEAD). Depuis dix ans, l'*Air Force* travaille ainsi au développement de technologies à bas coût à intégrer sur ses principales familles de munitions guidées, la *Joint Direct Attack Munition* (JDAM) et la *Small-Diameter Bomb* (SDB), permettant à ces variantes de géolocaliser et de se guider sur les sources de contre-mesures électroniques adverses, notamment les brouilleurs de GPS[39]. Il n'est pas impossible que la destruction d'un Pole 21 russe par une JDAM ukrainienne en octobre 2023 ait relevé de ce mode d'action[40]. La technique devient plus sophistiquée à l'ère du combat collaboratif et des armes guidées par réseau (*Network-Enabled Weapons* – NEW*)*. C'est ainsi sur ce mode d'action qu'a porté la première étape de l'initiative *Golden Horde*, l'un des grands projets R&D de l'*US Air Force*, visant à développer les munitions *Networked Collaborative and Autonomous* (NCA). Les *Collaborative Small Diameter Bombs* ont ainsi détecté un brouilleur d'opportunité et se sont coordonnées entre elles pour le frapper de façon synchronisée[41]. En matière d'acquisition, cette technologie de NCA a plutôt vocation à être incorporée sur les missiles de croisière AGM-158 *Joint Air-to-Surface Standoff Missile* (JASSM) et/ou les leurres ADM-160 *Miniature Air-Launched Decoy* (MALD), aux avant-postes de l'action *stand-off* de contre-déni d'accès[42].

2. Les mesures incrémentales pour neutraliser ces menaces

2.1. La stratégie américaine comme feuille de route

Pour parer à ces menaces pesant sur la fonction PNT, **plusieurs techniques ont été développées et sont incorporées de façon incrémentale depuis des années, tant dans le monde militaire que civil**.

---

[39] John Keller, « Air Force to enable smart weapons to track and kill sources of electronic warfare (EW) jamming », *Military Aerospace Electronics*, Nov. 13, 2014 – https://www.militaryaerospace.com/rf-analog/article/16718805/air-force-to-enable-smart-weapons-to-track-and-kill-sources-of-electronic-warfare-ew-jamming

[40] David Axe, « Ukraine's GPS-Guided Bombs Work Even When You Jam Their GPS », *Forbes*, Nov 1, 2023.

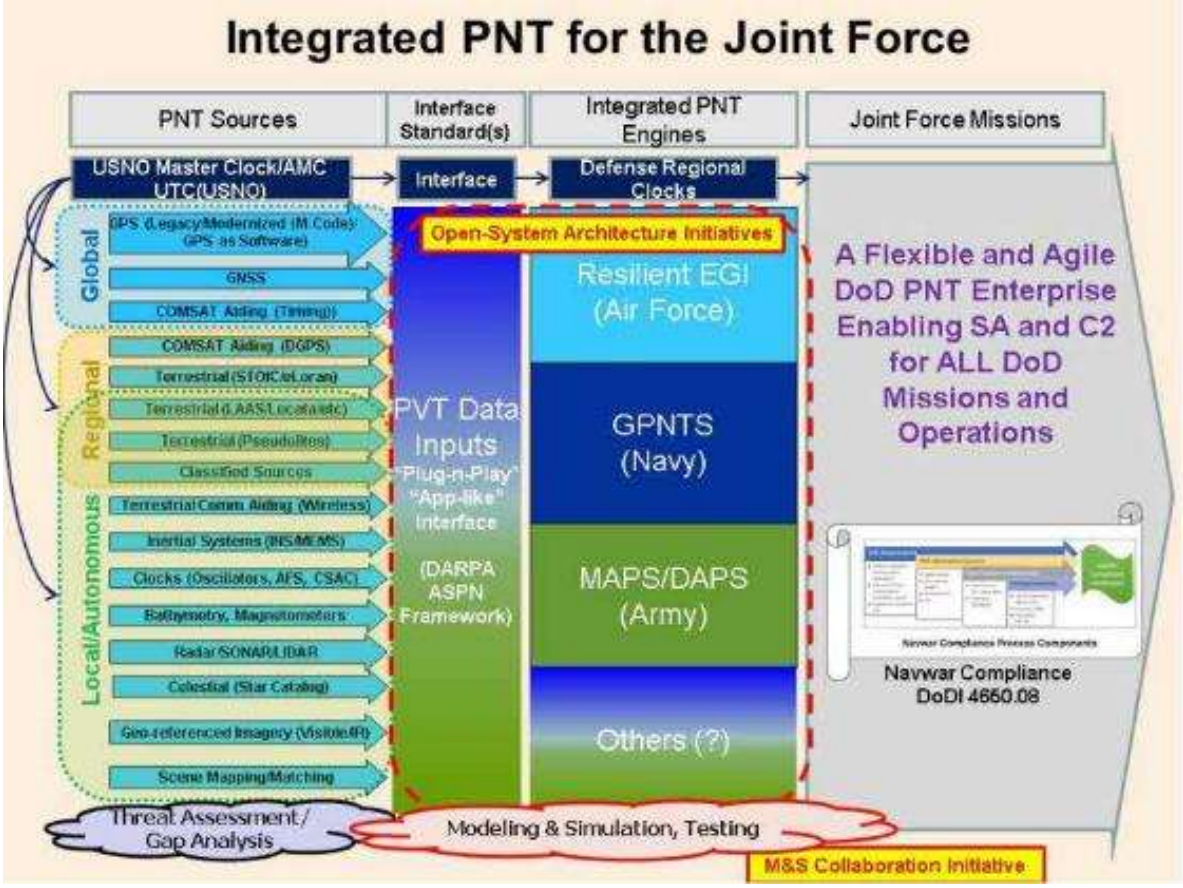
[41] Air Force Research Laboratory Public Affairs, « AFRL completes Golden Horde Collaborative Small Diameter Bomb second flight demonstration », March 5, 2021 – https://www.wpafb.af.mil/News/Article-Display/Article/2527268/afrl-completes-golden-horde-collaborative-small-diameter-bomb-second-flight-dem/

[42] Thomas Newdick, « Golden Horde Swarming Munitions Program Back On Target After Second Round Of Tests », *The War Zone*, March 3, 2021 – https://www.thedrive.com/the-war-zone/39581/golden-horde-swarming-munitions-program-back-on-target-after-second-round-of-tests

L'approche peut apparaître anachronique mais on se servira comme feuille de route d'explication de ces techniques, de la **stratégie de « l'entreprise » PNT du DoD**, publiée par son *Chief Information Officer* en 2019. Elle est en effet assez limpide et n'offre, en dépit des effets d'annonce, aucune rupture claire avec les efforts de R&D et d'acquisition déjà entrepris depuis 20 ans, tant semble long le temps d'évolution des capacités en la matière.

Compte tenu de menaces croissantes de NAVWAR, le Pentagone entend développer un PNT intégrant automatiquement des sources multiples, selon une architecture en trois couches (mondiale, régionale et locale), dans laquelle, néanmoins, **« *le GPS est et restera le principal service de PNT militaire* ».** Les sources PNT alternatives, nécessaires en cas d'environnement contesté, recouvrent peu ou prou toutes les catégories déclinées en première partie.

Figure n° 6 : VISION AMÉRICAINE D'UN PNT INTÉGRÉ AU PROFIT DE LA FORCE INTERARMÉES

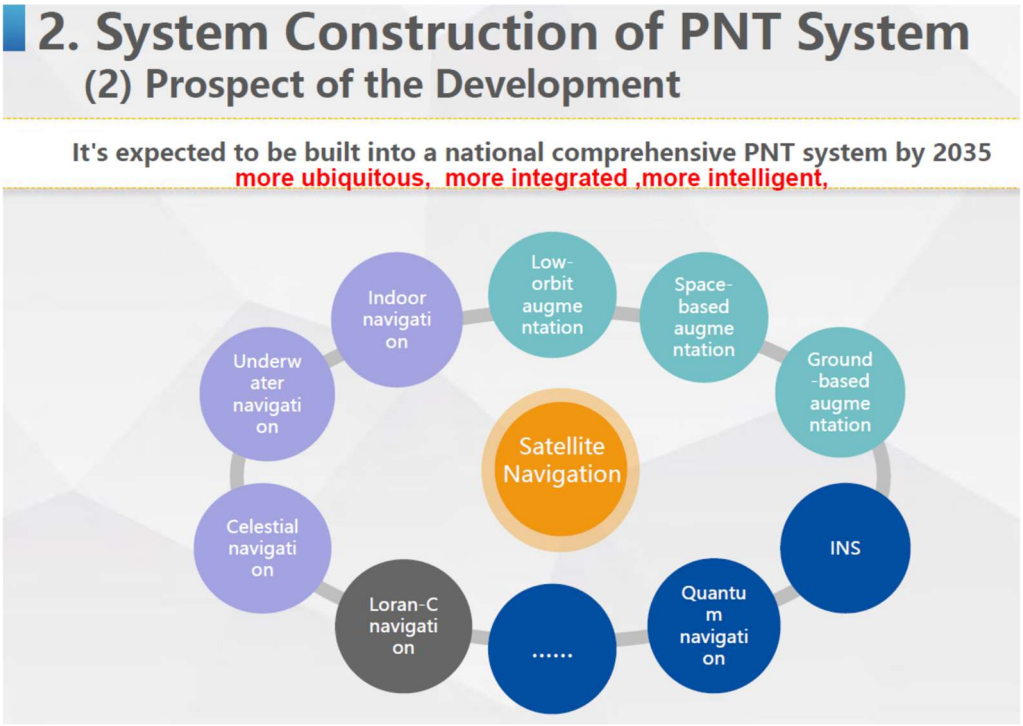


Source : DoD Chief Information Officer, Principal Staff Assistant for PNT Policy, *Strategy for the Departement of Defense Positioning, Navigation and Timing Enterprise*, Unclassified Version, November 2018, p. 28.

Bien évidemment, lorsque l'on parle de stratégie capacitaire aux États-Unis, l'essentiel se passe dans les *Services* avec la DARPA comme acteur clé de la maturation technologique. Les centres de R&D des trois départements travaillent depuis longtemps sur le GPS et les multiples sources de PNT.

On notera que **l'approche des Chinois semble rigoureusement identique :** elle reste centrée sur le système BeiDou que viendront compléter les systèmes d'augmentation spatiaux, terrestres ainsi que les nouvelles technologies autonomes[43].

Figure n° 7 : LA CONCEPTION CHINOISE DU SYSTÈME DE PNT



Source : LU Xiaochun, Update on BeiDou Navigation Satellite System and PNT System, National Time Service Center Chinese Academy of Sciences, Stanford 2019 PNT Symposium, 30th, October, 2019.

2.2. Les techniques antibrouillages développées depuis 20 ans

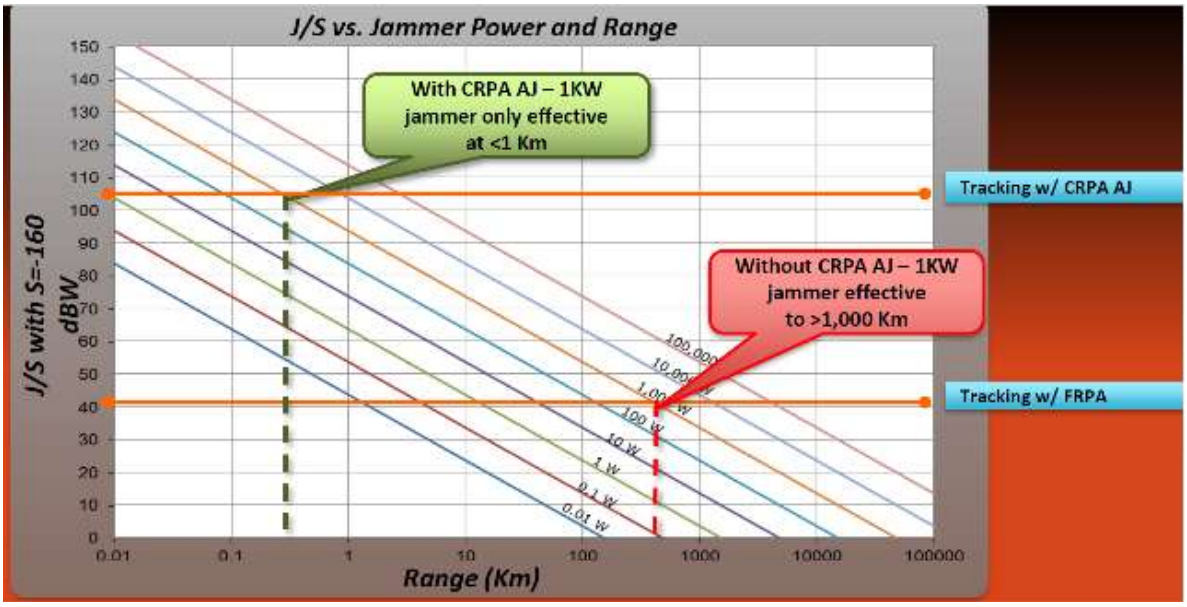
La première approche dans laquelle les institutions et industriels ont beaucoup investi pour garantir la résilience du GPS réside dans les techniques antibrouillages, c'est-à-dire une bien meilleure exploitation du signal, par des technologies tant matérielles que logicielles. Elles ont joué sur deux grands paramètres.

Le premier réside dans la nature du couplage entre le signal GNSS et la centrale inertielle des éléments mobiles. Dans un système GPS/INS « lâchement couplé », l'INS est alimenté en permanence par les deltas de cap, de vitesse et d'altitude de son IMU. Un « filtre d'intégration » (c'est-à-dire un algorithme), dit de Kalman, compare ces données avec celles de position et de vélocité transmises par le signal GNSS et calculées par les récepteurs, qui permettent alors de recaler les données de l'IMU. Le « couplage serré » (*Tight Coupling*) consiste, selon les versions, à compléter ou à remplacer dans ce filtrage les données calculées du GNSS par les données brutes tirées du signal GNSS, en l'occurrence la mesure de la « pseudo-distance » du satellite, l'effet doppler de l'onde porteuse et l'estimation de l'évolution de ces paramètres

[43] LU Xiaochun, *Update on BeiDou Navigation Satellite System and PNT System*, National Time Service Center Chinese Academy of Sciences, Stanford 2019 PNT Symposium, 30th, October, 2019 & Dana Goward, « China leads world with plan for 'comprehensive' PNT », GPS World, November 15, 2019 – https://www.gpsworld.com/china-leads-world-with-plan-for-comprehensive-pnt/

grâce aux éphémérides pour la poursuite du satellite. C'est la « cinématique temps réel » évoquée plus haut. Cette architecture permet d'améliorer le SNR à plus de 60 dB. Pour faire décrocher le P(Y) code à 10 km, il faut alors un brouilleur de 80 W[44]. Le « couplage ultraserré » qui sera disponible à l'avenir, surtout dans le monde militaire si l'on suit les industriels, consiste enfin à rajouter une boucle de *feedback* entre le filtre de Kalman et la réception du signal GNSS, permettant de mieux pister le signal du satellite à partir des données de PVT synthétisées.

Figure n° 8 : CAPACITÉ DE BROUILLAGE GPS EN FONCTION DE LA PORTÉE ET DU RAPPORT SIGNAL / BRUIT DU RÉCEPTEUR AVEC ET SANS ANTENNE À DIAGRAMME DE RAYONNEMENT CONTRÔLÉ



Soource : Mark W Johnson, APNT Campaign Lead, Collins Aerospace, A Positioning Navigation and Timing (PNT) Threat Environment Model for Military and Civilian Use, June 6, 2019.

Le second paramètre, plus important encore, est celui du réseau d'antennes du récepteur GNSS. Initialement, il s'agissait d'antennes à réception non contrôlée, des *Fixed Reception Pattern Antenna* (FRPA). Elles sont progressivement remplacées depuis 20 ans par des *Controlled Reception Pattern Antenna* (CRPA), c'est-à-dire un réseau d'antennes à plusieurs éléments calé sur la direction des satellites, ce qui permet d'évacuer les signaux provenant d'autres directions qu'il s'agisse de brouilleurs ou d'ondes réfléchies, qui constituent un problème important en zone urbaine. La principale CRPA produite en série, la GAS-1, est en service dans les forces américaines depuis 1997. Elle a renforcé le SNR de 30 dB. Les centrales INS/GPS la combinant avec le couplage serré atteignent un SNR de 90 dB. Avec ce dispositif, pour faire décrocher le P(Y) code à 10 km, il faudrait un très gros brouilleur sur camion de 80 kW[45]. Un R-330 Zhitel russe ne serait alors probablement efficace qu'à quelques kilomètres. Depuis, les dispositifs du même ordre se sont multipliés. Ce sont donc les principaux moyens antibrouillages déployés depuis deux décennies dans le monde militaire. La *Joint Direct Attack Munition* (JDAM), principale munition de précision des forces américaines, est dotée depuis 2008 de l'*Integrated GPS Anti-Jam System* (IGAS), une antenne à quatre éléments affichant 85 dB. L'effet

[44] Dr. Stew DeVilbiss, Tech Advisor, Navigation and Communications Branch, Sensors Directorate, Air Force Research Laboratory, « Position, Navigation & Time (PNT) Eco-System: Putting the Pieces Together (for Resilience) », 2 Sept 2015 – https://kittyhawkaoc.org/powerpoint_resources/AFRL-RYWN_Overview-Public_Released_20150902.pptx

[45] Dr. Stew DeVilbiss, *op. cit.*

du brouillage GPS par les Russes sur certaines frappes de JDAM ukrainiennes peut alors s'expliquer soit par la livraison de munitions fabriquées avant 2008 et non rétrofitées, soit par la présence opportune d'un engin comme le Zhitel à quelques kilomètres des cibles visées.

Il convient cependant de noter que les CRPA seules ne suffisent pas à protéger de l'usurpation[46]. De plus, comme l'espace disponible peut être limité pour accueillir le nombre d'antennes nécessaires pour mesurer les différences spatiales de provenance des signaux, **d'autres dispositifs de traitement numérique du signal ont été ajoutés** : l'ajout de la dimension temporelle (*Space-Time Adaptive Processing* – STAP), le « suivi » du signal de chaque satellite grâce à l'orientation de faisceau (*beamsteering / beamforming*) par le réseau d'antennes, etc. Ces techniques fournissent une quinzaine de décibels supplémentaires. Elles sont par exemple mises en œuvre sur le réseau G-STAR de Lockheed Martin équipant le missile de croisière JASSM depuis plus de 10 ans[47] et qui doit doter le F-35 Block 4. Un système comme le *Digital GPS Anti-jam Receiver* (DIGAR) proposé par BAE pour les plateformes aériennes (notamment le F-16) revendique par exemple 125 dB[48]. Une version miniaturisée, le *Strategic Anti-Jam Beamforming Receiver* (SABR-Y), revendiquant 100 dB, rééquipe depuis 2018 les JDAM à guidage GPS/INS de l'*Air Force* en satisfaction d'un besoin opérationnel urgent du commandement USINDOPACOM[49]. Contre ces dispositifs, les brouilleurs les plus puissants ne peuvent plus être guère efficaces qu'à quelques centaines de mètres. Toutefois, les exemples ci-dessus témoignent que si les technologies sont matures, les délais d'intégration sont particulièrement longs et restent tributaires des périodes de modernisation, de rafraîchissement technologique des plateformes ou des équipements qui les intègrent.

2.3. Le GPS proprement dit : l'avènement chaotique du M-Code

Le programme GPS n'a cessé de connaître des modernisations mais celle en cours de déploiement, planifiée il y a plus de 10 ans, est la plus importante. Elle concerne la bascule vers le GPS III, en mesure d'émettre le M-Code en remplacement du code P(Y). Il n'est pas plus intense mais sa puissance maximale est plus répartie sur les bandes de fréquences auxquelles il est émis. De surcroît, il comporte un nouveau chiffrement améliorant la sécurité des données. L'ensemble offre une vingtaine de dB supplémentaires. En cumulant l'ensemble des techniques précitées et le M-Code, un signal peut ainsi toute chose égale par ailleurs atteindre un SNR de 140 dB nécessitant une puissance de brouillage de plusieurs mégawatts pour faire décrocher le signal à 10 km. Voilà qui clôt le débat en matière de brouillage de puissance.

Malheureusement, le programme GPS constitue un exemple typique des dysfonctionnements qui affectent depuis longtemps le processus d'acquisition des moyens spatiaux américains, marqués par d'importants retards et dérapages de coûts[50]. Le problème ne vient pas tant du

[46] Michael Jones, « Spoofing in the Black Sea: What really happened? », GPS Word, October 11, 2017.

[47] Robert K. Ackerman, « Jam-Proof Signals To Guide Navigation », *Signal*, November 2001.

[48] BAe, « Digital GPS Anti-jam Receivers » – https://www.baesystems.com/en-us/product/digital-gps-anti-jam-receivers

[49] Frank Wolfe, « Air Force Buying Anti-Jam JDAM Kits in Response to PACAF Urgent Need », *Defense Daily*, 17 juillet 2020 – https://www.defensedaily.com/air-force-buying-anti-jam-jdam-kits-response-pacaf-urgent-need/air-force/ & « SABR™-Y » – https://www.baesystems.com/en-us/product/sabr-y

[50] Pour les données à jour : United States Space Force, Positioning, Navigation, and Timing Mission Area, Global Positioning System (GPS), Public Interface Control Working Group (ICWG) & Public Forum, 29 September 2021 – https://www.gps.gov/technical/icwg/meetings/2021/presentation.pdf & une analyse du programme de modernisation,

segment spatial : 8 satellites GPS III ont été lancés et la quasi-totalité des précédents (block IIR-M, IIF) sont des modèles modernisés qui émettent eux aussi déjà le M-Code (voir annexe 1).

La difficulté réside tout d'abord dans le segment de contrôle opérationnel de prochaine génération (OCX). Après trois ans de prédéfinition, sur la base de présuppositions trop optimistes, l'*US Air Force* accorde en 2010 le contrat à Raytheon sans procéder à la revue de concept préliminaire prévue par le processus pour évaluer la maturité du projet. Cette revue de concept, de même que l'évaluation détaillée de coûts, ne seront finalement réalisées qu'après coup. Or, le développement du système s'avère beaucoup plus ardu que prévu, tout particulièrement en ce qui concerne la sécurité informatique (expression de besoin initial déficiente, non-conformité de Raytheon, etc.). Pour coller à l'avancée du segment spatial, l'*USAF* en 2011 restructure le programme en trois étapes :

- Un block 0 pour fournir le système de lancement et de vérification des premiers satellites GPS III ainsi qu'une capacité opérationnelle minimale ;
- Le block 1 pour le contrôle basique de l'ensemble des satellites GPS II/III – notamment le contrôle du M-Code ;
- Le block 2 pour la pleine exploitation de l'ensemble des caractéristiques des GPS III.

Ceci a pour effet de provoquer de nouveaux retards. En 2013, une pause est décidée pour mieux évaluer les difficultés rencontrées. La livraison du Block 1 est encore ainsi retardée. Pour ne rien arranger, le Congrès enjoint l'*Air Force* de fournir les nouvelles capacités relevant du GPS III au plus tard lors de la FY18 alors même que sa maturation technologique est insuffisante. La volonté de respecter cet objectif légal a des effets en cascade, sur l'ensemble des segments du système : spatial, contrôle et utilisateur. La gestion du programme s'est améliorée depuis 2017 mais un nouveau retard a été imputé cette fois au défi de la *supply chain* : IBM, fabricant des serveurs informatiques de ce segment de contrôle, a vendu en 2014 la ligne de production concernée à Lenovo. Doter l'OCX d'équipements chinois est évidemment inacceptable pour les Américains. Il a donc fallu amender le contrat en 2020 pour les remplacer par des serveurs HP[51]. Le département de l'Air Force prévoit maintenant une mise en service de l'OCX block 1 & 2 à l'été 2024[52].

Une autre caractéristique calamiteuse des programmes spatiaux américains réside dans l'extrême décentralisation et même la dispersion du management du segment utilisateurs. Le GPS n'échappe pas à la règle. Le défi est de taille puisqu'il ne concerne pas moins de 700 types de récepteurs GPS (dont environ 200 000 systèmes terrestres) et les applications correspondantes. Le principal programme de modernisation afférent est le ***Military GPS User Equipment*** **(MGUE)** qui consiste à installer une carte de réception du M-Code sur l'ensemble de ces récepteurs.

La démarche de l'USAF comprend deux incréments. Le premier est tout d'abord de doter les plateformes de ces MGUE. Les contrats ont été passés pour ce faire avec L3 Technologies, Raytheon et Rockwell Collins. Après de nombreux délais liés aux difficultés techniques de sa

---

United States Government Accountability Office, *Global Positioning System: Better Planning and Coordination Needed to Improve Prospects for Fielding Modernized Capability,* GAO-18-74, December 2017 – https://www.gao.gov/assets/690/688936.pdf

[51] Maddie Saines, « GPS OCX still delayed and lawmakers are not happy », *GPS World*, August 24, 2023.

[52] Theresa Hitchens, « Next-gen GPS ground system expected to come online this summer: Calvelli », *Breaking Defense*, November 07, 2023.

mise au point et à la diversité des acteurs impliqués, la certification des cartes embarquées sur les premières plateformes (*Joint Light Tactical Vehicle*, bombardier B2, blindés Stryker, destroyers DDG-51) a été réalisée en 2020… soit 11 ans après le lancement du premier satellite en mesure de diffuser ce signal. Le second incrément porte sur les récepteurs miniaturisés pour les vecteurs spatiaux, les postes portables ou encore les munitions de précision. Leur mise au point pose des défis importants en matière de SWAP et les démonstrations de ces équipements ne seront achevées qu'en 2025. Cela étant, plusieurs autres programmes sont déjà en cours pour doter d'autres plateformes de la capacité de réception du M-Code, comme le F-22 Raptor et l'E-2D Hawkeye dans le cadre de l'EGI-Modernization de l'USAF.

2.4. Les nouvelles capacités spatiales

Le DoD travaille sur de multiples autres axes de compléments spatiaux au GPS. Les principales initiatives sont les suivantes :

- **L'expérimentation NTS-3.** Elle représente l'une des trois principales initiatives de R&D (*Vanguard*) de l'*Air Force*. Elle consiste à tester de nouvelles technologies de GNSS : un satellite en GEO doit expérimenter des signaux reprogrammables, orientables régionalement en fonction du besoin (exactement comme les SATCOM), de nouvelles signatures anti-usurpation, etc. ; des récepteurs *software-defined*, de nouvelles antennes côté utilisateur et un segment de contrôle plus autonome. Le satellite doit être lancé en 2023[53]. Ces technologies pourront être mises en œuvre par de nouvelles constellations et/ou intégrées dans les incréments suivants du GPS ;

- **L'architecture de la *Space Development Agency* (SDA)[54]**. La SDA a développé la *Proliferated Warfighter Architecture* (PWSA), une vaste architecture comprenant plusieurs constellations totalisant des centaines de mini satellites en LEO et interfaçant ces dernières avec les constellations existantes, afin d'améliorer drastiquement l'efficacité et la résilience des services spatiaux aux forces américaines. Toutes les couches de services spatiaux sont concernées (SATCOM, alerte avancée, ISR… et PNT naturellement). Cette ***Navigation Layer*** vise à fournir, en cas d'interdiction du GPS, des capacités PNT indépendantes aux utilisateurs des différents milieux, à commencer d'ailleurs par l'architecture elle-même dont les satellites mais aussi les terminaux de surface opèreront en réseau (*crosslink*) grâce à des liaisons optiques (laser). Cette couche doit tout d'abord améliorer la conscience situationnelle de l'état des émissions GPS. Elle doit surtout combiner de multiples sources autonomes (horloges atomiques, INS, navigation astronomique, etc.) à facteur SWAP réduit, ainsi que les mesures de distance et de synchronisation fondées sur des stations sol fournissant un positionnement de référence et le *crosslink* entre satellites. Ces sources seront intégrées avec de nouveaux logiciels embarqués comme l'*Orbit and Clock Determination Application* (OCDA). Ces capacités PNT seront intégrées dans les satellites de la couche

[53] Air Force Research Laboratory, « Navigation Technology Satellite – 3 (NTS-3) » – https://afresearchlab.com/ technology/space-vehicles/successstories/nts-3

[54] Space Development Agency, *Mission Specific Applications Prototype, Broad Agency Announcement*, 26 January 2020 – https://govtribe.com/file/government-file/hq085020s0002-hq085020s0002-amendment-0001-dot-pdf & Tim Boudreaux, Chief, SDA Transport Cell, *Mission Payloads and Capabilities Overview*, Présentation, Industry Day, dans la vidéo *Constellation, SV and Mission Payloads* (29 MIN/276MB) ; 18 :00, 07/08/2021 – https://sdat1tlindustryday.s3.us-east-2.amazonaws.com/Industry+Day_07-08+Constellation+SV+and+Mission+Payloads.mp4
accessible via https://www.sda.mil/wp-content/uploads/2021/08/SDA-T1TL-Industry-Day-Agenda-with-Links.pdf

SATCOM ce qui doit permettre de transmettre ces données PVT aux utilisateurs via les terminaux en bande Ka, les liaisons optiques et la liaison de données tactique L16 que les satellites vont également relayer. Tout cela n'est pas de la science-fiction ou du long terme. La Tranche 0 de 28 satellites, qui doit assurer « l'immersion des combattants » ainsi qu'une « capacité régionale périodique » a été lancée par SpaceX en 2023. La Tranche 1 devant comprendre 177 satellites doit être mise à poste en 2025. Bien entendu, le déploiement de ces technologies est incrémental. Pour la couche PNT, les capacités les plus significatives (*Situational Awareness* et données PNT alternatives) sont attendues pour la Tranche 2 qui doit être lancée en 2027 afin de fournir un « accès global persistant » aux *Services*, correspondant à la capacité nominale fixée pour cette architecture[55]. Reste à mesurer quand les programmes de segments utilisateurs des *Services* permettront d'exploiter ces nouvelles capacités.

De façon plus générale, l'exploitation de la LEO pour le PNT a pris un peu de retard par rapport à l'observation et aux communications mais serait promise là encore à un brillant avenir selon Brian Manning le PDG de Xona Space Systems, une entreprise californienne spécialisée dans cette technologie. Le signal, aussi précis mais plus puissant que celui des GNSS actuel, est donc non seulement plus résilient, plus économe de traitement mais peut atteindre des utilisateurs en intérieur sans infrastructures de relais[56].

Dans le domaine commercial, un excellent exemple de ces capacités nous est fourni par Iridium, la constellation SATCOM de 66 satellites, en pleine transition vers une nouvelle génération, Iridium Next. L'entreprise se positionne clairement dans la fourniture de services complémentaires au GPS. Associée à l'entreprise Satelle qui a conçu le système de PNT, elle propose depuis 2016 un service de *Satellite Time and Location* (STL), qui fournit un signal environ 1 000 fois plus puissant que le GPS, d'une précision de 20 à 50 mètres et inférieur à 1 µSec en timing[57].

La LEO fait aussi pleinement partie des projets de l'ESA. Cette dernière a ainsi lancé un programme de démonstrateur *Next Generation Network Assisted Position, Navigation and Timing (PNT) Assurance* (NG-NAPA) confié à un consortium mené par Telespazio UK (incluant Thales Services Numériques) qui intégrera les signaux d'Iridium, ceux des émetteurs 5G et les services chiffrés des GNSS[58].

La Chine est également dans cette logique. Pékin poursuit le programme CentiSpace de charge utile expérimentale de PNT en LEO dont le premier lancement a eu lieu en 2018. Les Émirats arabes unis auraient également pour intention d'investir dans ce domaine[59].

---

[55] Voir le site de la SDA, bien documenté : https://www.sda.mil/

[56] Peter Gutierrez, « Fleshing Out the LEO PNT Landscape », *Inside GNSS*, March 14, 2022 – https://insidegnss.com/fleshing-out-the-leo-pnt-landscape/

[57] *Current operational Status of LEO-Satellite-Based Time and Location,* présentation Satelle, 2016 – https://www.gps.gov/governance/advisory/meetings/2018-05/gutt.pdf

[58] « ESA Awards Contract for Network-Assisted PNT Assurance, Involving Iridium », *Inside GNSS*, November 19, 2021 – https://insidegnss.com/esa-awards-contract-for-network-assisted-pnt-assurance-involving-iridium/

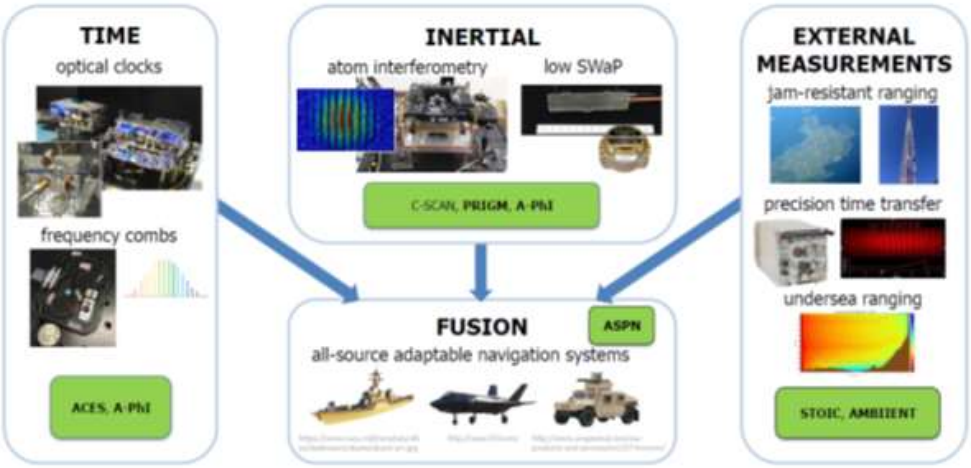
[59] Peter Gutierrez, *op. cit.* & Anonyme, « China's New Space Launch Race: ExPace Successfully Launches Centispace-1-S1 On Kuaizhou-1A Launch Vehicle », *Space Watch Global* – https://spacewatch.global/2018/10/chinas-new-space-launch-race-expace-successfully-launches-centispace-1-s1-on-kuaizhou-1a-launch-vehicle/

Enfin, la stratégie PNT américaine envisage dans le futur, « si nécessaire », « l'option » de recourir aux GNSS alliés, en l'occurrence Galileo et QZSS visant à renforcer ces GNSS. Dans ce sens, les autres puissances, exploitant déjà le GPS, sont sans doute plus avancées dans cette exploitation multi-GNSS.

2.5. Les solutions alternatives aux GPS / GNSS

Pour donner un aperçu des technologies en cours de développement afin de compléter le GPS, on se réfèrera aux travaux de la DARPA qui travaille sur l'ensemble de la gamme de ces solutions alternatives.

Figure n° 9 : LES PRINCIPAUX PROGRAMMES DE PNT DE LA DARPA



Source : John Burke, Program Manager, DARPA/MTO, DARPA Positioning, Navigation, and Timing (PNT) Technology and their Impacts on GPS users, GPS Advisory Board, 6 June 2019.

2.5.1. Les solutions de GBAS et de PNT alternatives

Les forces américaines ont exploré tout d'abord les solutions de **Pseudolites**, donc des répétiteurs de GPS mobiles, terrestres et aéroportés sur drones. La technique est évidemment intéressante mais elle pose tout de même des défis de taille, en particulier concernant la configuration et la géométrie du dispositif. Les pseudolites doivent en effet être positionnés de façon à éviter la « dilution de précision », c'est-à-dire être suffisamment espacés les uns des autres pour garantir une tri-latéralisation optimale, ce qui peut s'avérer très aléatoire pour des récepteurs mobiles. S'ils sont utilisés en augmentation du GNSS, se pose également la question du différentiel de puissance du signal avec les satellites qui, s'il est mal géré, peut aboutir non pas à les compléter mais à les masquer, ce qui signifie créer en réalité un brouilleur GNSS. L'*US Army* a donc testé cette solution en 2017-18 mais a mis un terme au programme en 2019.

En ce qui concerne les sources PNT alternatives, **les signaux d'opportunité** font systématiquement partie des solutions évoquées. De fait, ils ne nécessitent pas d'infrastructures dédiées ; leur intensité peut être largement suffisante pour la navigation dans un secteur donné, y compris dans des zones urbaines aux multiples masques pour les GNSS ; les développements des technologies de radio logicielles permettent de disposer de plus en plus de sources elles-mêmes résilientes aux interférences. Pour autant, les défis sont énormes voire contraignants si on les

cumule : tout d'abord, ce ne sont pas des signaux taillés pour la navigation, hormis certains comme les réseaux 5G à venir. Ils n'incluent pas de données de timing. De plus, les émetteurs ne sont pas forcément positionnés de façon optimale, ce qui peut générer, là encore, une dilution de la précision. Ensuite, pour que cette source soit intéressante, il faut pouvoir recevoir plusieurs types de signaux. Il est donc nécessaire de disposer de dispositifs en mesure de travailler sur plusieurs bandes de fréquence. Même à l'ère de la *Sofware-Defined Networking* et des serveurs de communication, cette diversité de signaux peut s'avérer un défi en termes d'équipement. Ensuite, il faut connaître la position géoréférencée de chaque émetteur. Si le renseignement n'est pas disponible, le positionnement doit alors se fonder sur un travail de positionnement relatif à base de capteurs. Enfin, reste la question de la sécurité et de l'intégration de signaux exogènes non contrôlés[60].

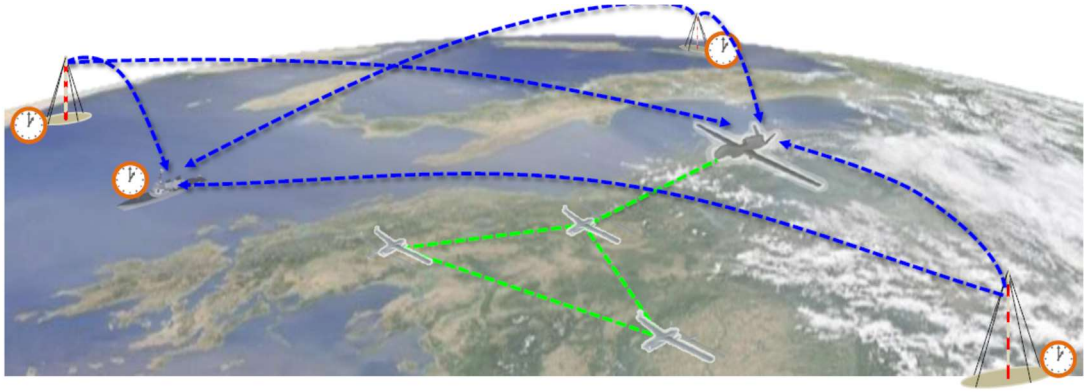
Si les Pseudolites comme l'exploitation des signaux d'opportunité semblent ne pas déboucher (du moins jusqu'à présent), il semble que d'autres approches progressent comme **le positionnement/navigation par réseau VLF** (*Very Low Frequency* soit 3-30 kHZ). Il s'agit du retour d'une technique de positionnement déjà mise en œuvre par les forces navales pendant la Guerre froide : les Américains ont employé le système OMEGA de huit émetteurs jusqu'en 1997 et les Soviétiques avaient un équipement équivalent. La précision était de 1 à 4 MN et dépendait beaucoup des perturbations ionosphériques très prégnantes à ces fréquences. La synchronisation des émetteurs distants de plusieurs milliers de kilomètres était également un défi. Le programme de la DARPA ***Spatial, Temporal and Orientation Information in Contested Environments*** **(STOIC)** a permis de réaliser des avancées importantes rendant à nouveau cette approche crédible comme substitut au GNSS :

- Le système de positionnement par tri-latéralisation recourant au réseau VLF. Les expérimentations réalisées par la DARPA, fondées sur une bien meilleure modélisation des phénomènes ionosphériques, ont permis d'atteindre une précision située entre 450 et 40 m ;
- De nouvelles horloges permettant la synchronisation de ces émetteurs VLF (voir ci-dessous) ;
- Mais aussi le transfert des données temporelles aux éléments de la frange tactique (drones, munitions) via les réseaux de liaisons de données tactiques permettant *a minima* les opérations des réseaux de communication (de l'ordre de la microsecondes) mais visant la picoseconde dans un second temps[61].

[60] J.F. Raquet, M.M. Miller (2007), *Issues and Approaches for Navigation Using Signals of Opportunity. In Military Capabilities Enabled by Advances in Navigation Sensors,* Meeting Proceedings RTO-MP-SET-104, Paper 9. NATO RTO, pp. 9-1 – 9-14 & Michael Jones, « Signals of opportunity: Holy Grail or a waste of time? », GPS World, February 22, 2018 – https://www.gpsworld.com/signals-of-opportunity-holy-grail-or-a-waste-of-time/

[61] John Burke, Program Manager, DARPA/MTO, *DARPA Positioning, Navigation, and Timing (PNT) Technology and their Impacts on GPS users*, GPS Advisory Board, 6 June 2019.

Figure n° 10 : REPRÉSENTATION DU PROGRAMME *SPATIAL, TEMPORAL AND ORIENTATION INFORMATION IN CONTESTED ENVIRONMENTS* (STOIC) DE LA DARPA



Source : John Burke, Program Manager, DARPA/MTO, *DARPA Positioning, Navigation, and Timing (PNT) Technology and their Impacts on GPS users*, GPS Advisory Board, 6 June 2019.

L'US Navy a repris l'exploration de la solution, en témoigne l'appel d'offres passé en décembre 2020 sous forme de sollicitation *small business* pour la réalisation d'un prototype de *Navigational Positioning Source Using Very Low Frequency Signals*, dont les spécifications sont une précision en positionnement d'un demi-nautique et en vélocité, de 0,1 nœud pendant une heure[62]. Rien d'accessible n'a cependant été publié depuis.

Enfin, **le LORAN connaît une résurrection partielle**. Avec le GNSS, l'Amérique du Nord et l'Europe ont progressivement démantelé presque toutes leurs infrastructures de LORAN-C depuis plus de 20 ans, à la différence de pays comme la Russie (système Chayka), la Chine, la Corée du Sud et l'Arabie Saoudite. Ces derniers réinvestissent dans ce système en misant sur sa nouvelle version, le « eLORAN », développé par les Américains et Britanniques. Les Russes considèrent d'ailleurs le Chayka – qui fournirait une précision de quelques dizaines de mètres sur l'Ukraine – comme un véritable système de réserve en cas d'interdiction du GPS et du Glonass et il n'est pas impossible qu'il rentre en ligne de compte pour garantir la résilience du P/N russe offrant une plus grande liberté de manœuvre à l'armée pour mener des actions de NAVWAR offensives en Ukraine[63]. Les nouveaux réseaux eLORAN affichent une précision de 10-20 mètres, sont synchronisés UTC, atteignent partiellement les espaces enterrés, sous-marins et il est difficile de les brouiller. En dépit de ces avantages, les autorités américaines n'ont encore pris aucune décision d'investissement spécifique permettant de le remettre sur pied dans leur zone[64].

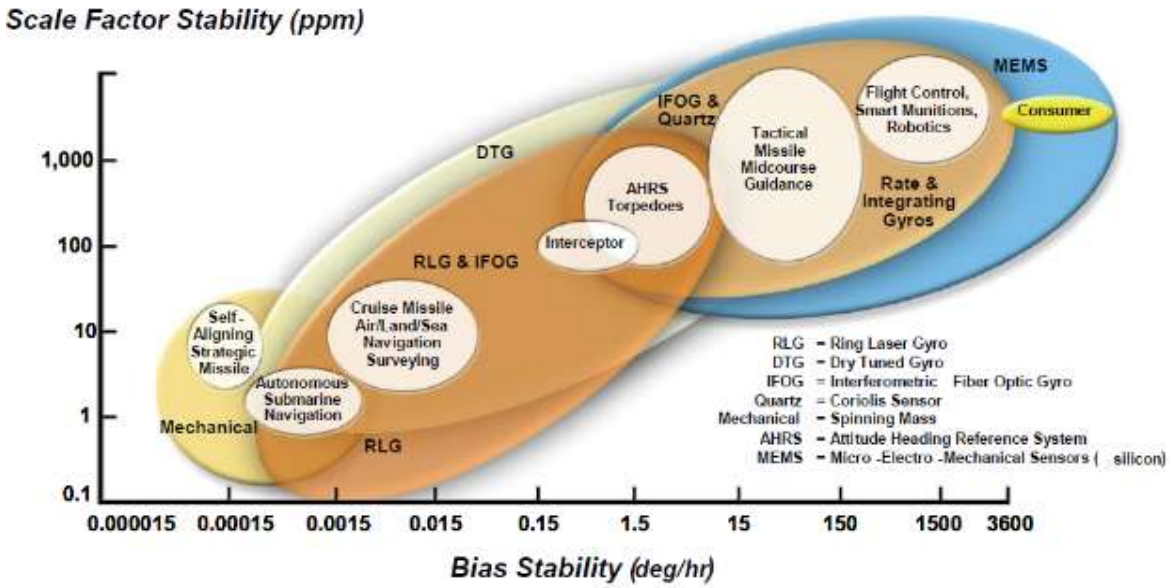
[62] « Navigational Positioning Source Using Very Low Frequency Signals », SBIR STTR, December 08, 2020 – https://www.sbir.gov/node/1837983

[63] Tracy Cozzens, « Russia expected to ditch GLONASS for Loran in Ukraine invasion », *GNSS World*, February 17, 2022 – https://www.gpsworld.com/russia-expected-to-ditch-glonass-for-loran-in-ukraine-invasion/

[64] Matteo Luccio, « eLoran: Part of the solution to GNSS vulnerability », *GPS World*, November 3, 2021 – https://www.gpsworld.com/eloran-part-of-the-solution-to-gnss-vulnerability/

2.5.2. Les nouvelles centrales inertielles : la diffusion d'une qualité de « niveau navigation » aux drones et munitions

Figure n° 11 : PERFORMANCES DES DIFFÉRENTES TECHNOLOGIES DE CENTRALES INERTIELLES



Source : George T. Schmidt, *Navigation Sensors and Systems in GNSS Degraded and Denied Environments* STO-EN-SET-197, NATO STO, 2013, pp. 1-6

Sans devoir (et pouvoir) rentrer dans les détails, on se fondera sur le schéma ci-dessus qui compare les biais de stabilité des différentes technologies de navigation autonomes. Il montre que les plus précises et les plus stables au mouvement du mobile, celles atteignant une « *navigation grade* », restent les gyroscopes mécaniques les plus élaborés, ensuite celles à laser, à fibre optique ou à « suspension accordée » (*dry-tuned gyro*). Leur volume est un facteur critique de précision : plus l'IMU est grande, plus elle garantit une finesse de mesure. Les comparaisons relatives aux accéléromètres sont du même ordre. Bénéficient de ce niveau les missiles balistiques de dissuasion nucléaire et les sous-marins, dans une moindre mesure les missiles de croisière et plateformes. Cela étant, dans la pratique, les sous-marins recalent eux-aussi ces centrales avec les GNSS lorsqu'ils reviennent à immersion périscopique, pour communiquer par exemple. Ces centrales sont des technologies coûteuses, de plusieurs centaines de milliers de dollars l'unité, impossibles à produire en grande série.

Les missiles tactiques, les drones ou encore les munitions guidées bénéficient ou peuvent bénéficier d'INS plus compacts reposant sur une **nouvelle génération d'instruments de mesure basés sur des systèmes micro-électromécaniques (MEMS – *Micro Electro Mechanical Systems)***.

En matière d'INS, la DARPA a tout particulièrement œuvré sur le **guidage autonome des munitions de précisions**, avec le programme *Precise Robust Inertial Guidance for Munitions* (PRIGM). Sa première phase, *Navigation-Grade Inertial Measurement Unit* (NGIMU), menée sur 2016-2019 a consisté à murir (à un niveau TRL 6) une nouvelle avancée en matière d'unité de mesures inertielles à MEMS garantissant une « qualité navigation » (0,01°/hr, 5 ppm en ce qui concerne le gyroscope, par référence au schéma supra). Ce qui permet de conserver un cercle d'erreur probable (CEP) de 10 m sur des temps de vol excédant les 3 minutes, soit des distances de quelques dizaines de kilomètres pour une arme subsonique. L'INS doit également résister à 60 G

pour les obus guidés[65]. Le fabricant Honeywell qui a obtenu le contrat, a réalisé dans ce cadre une nouvelle centrale, la HG7930, pour laquelle il revendique un biais de 0,06°/hr et 13 ppm[66]. Bien qu'inférieures aux spécifications initiales en ce qui concerne le gyroscope (mais pas l'accéléromètre), ce sont des performances effectivement dans la moyenne des INS à gyrolaser / accéléromètres à Quartz des plateformes mais qui restent en deçà des plus sophistiquées comme la HG 9900 d'un volume de 100 l, du même fabricant. Selon nos calculs, elle pourrait cependant ne permettre de maintenir un CEP de 10 m que sur une dizaine de kilomètres. La transition au profit des *Services* est programmée pour 2022, selon les données budgétaires FY21. Une seconde phase, *Advanced Inertial Micro Sensor* (AIMS), visant une performance équivalente étendue cette fois à 18 minutes, a été menée en parallèle. Plusieurs pistes semblaient avoir été considérées en 2016 : gyroscope photonique, combinaison gyroscope/MEMS, combinaison MEMS/optique, gyroscopes et accéléromètres acoustiques. Peu d'éléments ont été dévoilés depuis.

Cela étant, prenons l'exemple d'une JDAM d'environ 30 km de portée. Comme nous l'avons vu, les antennes CRPA, même la déjà ancienne IGAS et à plus forte raison la SABR-Y, permettent de se rapprocher suffisamment des brouilleurs tactiques les plus puissants du moment pour que ce type de NGIMU aide à franchir sans GNSS les 10 derniers kilomètres tout en réalisant une frappe largement précise. Le CEP de 10 mètres nécessiterait cependant d'employer un peu plus de munitions en fonction de l'effet recherché.

2.5.3. La miniaturisation des capacités de synchronisation

Les horloges atomiques, fonctionnant sur la mesure de la résonance d'une transition d'état d'atomes de césium, de rubidium ou d'hydrogène, représentent depuis des décennies le meilleur type d'outils de calcul du temps, le plus stable dans la durée. Il en existe de nombreux types offrant différentes solutions de performances, de contraintes SWAP et de coût. Les GNSS reposent sur de telles horloges. Plusieurs sont embarquées sur les satellites (les plus performantes étant celles de Galileo), elles-mêmes synchronisées avec une horloge principale de plus haute performance (celle de l'U.S. Naval Observatory pour le GPS par exemple). Tout le défi consiste à tenter de transcrire un niveau de précision s'en approchant sur des dispositifs de plus en plus miniaturisés. Durant les années 2000, grâce à un financement continu de la DARPA, un écosystème composé des chercheurs du *National Institute of Standards and Technology* (NIST), du *Sandia National Laboratories* ou encore de Symmetricom (devenu Microchip puis Microsemi) parvient à développer **l'horloge atomique miniature (*Miniature Atomic Clock* – MAC) puis l'horloge atomique de la taille d'une puce (*Chip-Scale Atomic Clock* – CSAC)** encore plus réduite (15 cm^3). Elles exploitent le phénomène quantique de piégeage cohérent de population (*Coherent Population Trapping* – CPT) d'atomes grâce à des lasers. Les deux technologies sont commercialisées par Symmetricom respectivement en 2008 et 2011. Microsemi a vendu de 2011 à 2018 environ 95 000 CSAC, principalement aux forces américaines. Depuis, plusieurs autres vendeurs – chinois, britanniques, israéliens et japonais – proposent des CSAC de différentes technologies. La seule entreprise européenne présente sur ce marché est Oriola,

[65] Dr Robert Lutwak, Program Manager, DARPA Microsystems Technology Office (MTO), *Emerging Microsystem Technologies for Autonomous Positioning, Navigation, and Timing (PNT),* National Space-Based PNT Advisory Board, May 18, 2016 – https://www.gps.gov/governance/advisory/meetings/2016-05/lutwak.pdf

[66] Burgess R. Johnson et alii, *MEMS IMU for GPS-Denied Navigation*, diapositive, ERI Summit, DARPA, 2020 – https://eri-summit.darpa.mil/docs/ERIsummit2020/posters/26P_PRIGM_Polcawich_Honeywell_Poster.pdf

devenue filiale de Safran, qui propose déjà une horloge intermédiaire entre une MAC et une CSAC. Ces dispositifs offrent des stabilités de fréquences bien supérieures aux oscillateurs à Quartz tout en étant plus compacts ce qui permet leur emploi sur de multiples plateformes. Les MAC ou horloges comparables n'ont pas les dimensions pour être intégrées dans des dispositifs portables, ce que visent précisément les CSAC. Cela étant, ces dernières coûtent plusieurs milliers de dollars et sont environ dix fois moins stables[67]. Par exemple, la dérive temporelle, qui dépasse la dizaine de microsecondes en une heure, ne permet pas en l'état, de poursuivre la synchronisation des communications au-delà de cette durée, sans recalage. À titre de comparaison, l'horloge d'Oriola tiendrait la microseconde sur la journée. La plage de fonctionnement en température de ces CSAC reste également limitée. Ces systèmes permettent ainsi aux opérateurs tactiques de s'affranchir d'une rupture temporaire des signaux GNSS mais pas de poursuivre les synchronisations si les constellations sont mises hors service.

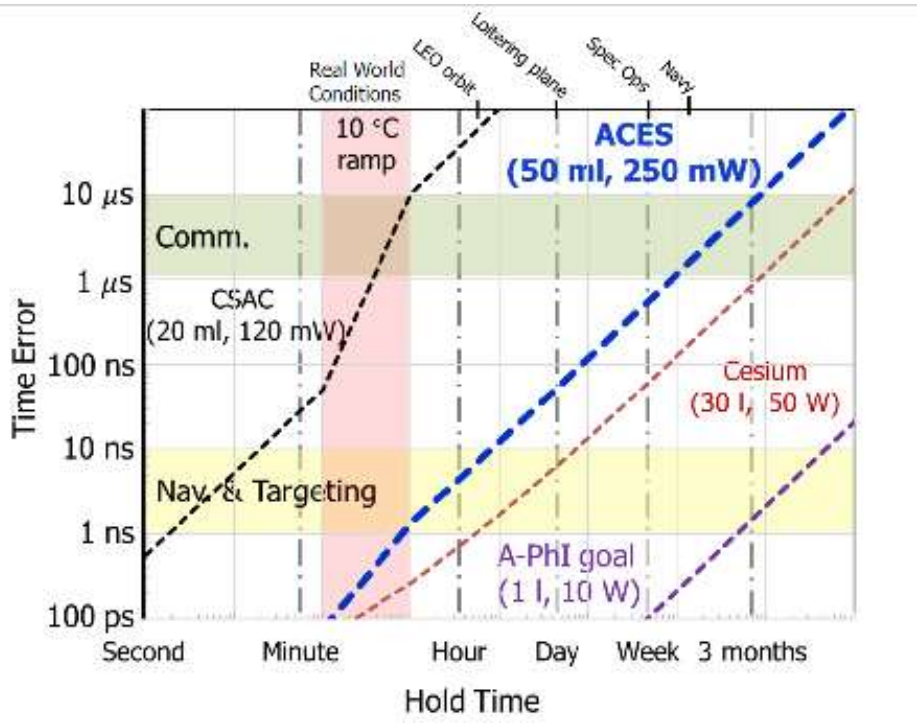
La DARPA a donc repris les travaux au milieu des années 2010, dans le cadre du programme *Atomic Clock with Enhanced Stability* (ACES). Ils visent à repousser cette dérive d'une microseconde à des durées de l'ordre du mois. Les performances se rapprocheraient ainsi de celles des grosses horloges atomiques au Césium, ce qui permettrait en théorie de garantir par exemple une synchronisation des réseaux de communication pendant un à deux mois sans GNSS. Les travaux ont débouché sur trois concepts. Celui développé par une équipe réunissant le NIST, Calltech et Stanford fonctionne à la vapeur d'atomes de rubidium dont les oscillations sont mesurées par laser, offrant une amélioration de l'ordre d'un facteur de 50 par rapport aux meilleures CSAC. Un autre, développé par Honeywell, fonctionne par « piège magnéto-optique » de ces atomes du Rubidium par une puce 3D permettant de se passer des dispositifs optiques classiques (miroirs, lentilles, etc.). Un troisième, élaboré par le *Jet Propulsion Laboratory* (JPL) de la NASA, serait le plus performant. La technologie développée pour la mesure du temps en espace profond fonctionne au mercure ionisé et aux lampes à ultraviolet au lieu des lasers, atteignant les métriques fixées par la DARPA tout en étant immune aux variations environnementales[68]. Selon l'expert Martino Travagnin du *Joint Research Center* de l'UE[69], ces différentes technologies présentent chacune d'énormes défis soit de maturation soit d'intégration sur une CSAC. On en retire qu'une commercialisation serait au mieux une affaire de moyen terme. À noter que seuls les Américains semblent poursuivre cet effort de développement d'une CSAC de nouvelle génération.

[67] Voir le rapport très complet de Travagnin, *M, Chip-Scale Atomic Clocks: Physics, technologies, and applications*, EUR 30790 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-40666-2, doi:10.2760/278540, JRC125394.

[68] « DARPA Making Progress on Miniaturized Atomic Clocks for Future PNT Applications », 20 août 2019 – https://www.darpa.mil/news-events/2019-08-20

[69] Travagnin, M, *Next-generation Chip Scale Atomic Clocks: Assessing the emerging physical platforms: microwave transitions in cold atoms and in trapped ions, and optical transitions in warm vapours*, EUR 31003 EN, Publication Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48726-5, doi:10.2760/525422, JRC128331.

Figure n° 12 : CIBLES DE PERFORMANCE DES DIFFÉRENTS PROGRAMMES DE *TIMING* DE LA DARPA COMPARÉS AUX TECHNOLOGIES EXISTANTES



Source : John Burke, Program Manager, DARPA/MTO, *DARPA Positioning, Navigation, and Timing (PNT) Technology and their Impacts on GPS users*, GPS Advisory Board, 6 June 2019.

Pour le plus long terme, tant pour les horloges que pour les gyroscopes, l'agence développe l'A-PhI (*Atomic Photonic Integration*), exploitant la technologie de l'horloge de spectroscopie d'atomes piégés, grâce à des dispositifs optiques et des tubes à vide, garantissant une stabilité à l'échelle de plusieurs mois voire années. En raison de ces dispositifs, les horloges sont aujourd'hui de très grande dimension. A-PhI fait partie des recherches visant à développer des circuits optiques au laser, intégrés sur cartes (*Photonic Integrated Circuit* – PIC), embarquables sur des plateformes. Appliquée dans un gyroscope, la technologie permettrait de tenir un CEP de 10 mètres sur un temps de vol de l'ordre de deux semaines ! On est cependant encore loin d'applications opérationnelles.

2.5.4. Les nombreuses initiatives de positionnement, de navigation autonomes et de guidage aidées par les capteurs et la métrologie

La résilience en cas de déni de GNSS passe enfin par les nombreuses recherches et initiatives programmatiques déjà prises, en matière de navigation et de guidage aidées par capteurs.

A. La multimodalité du guidage des armes de précision

Tout d'abord, les guidages terminaux des munitions de précision s'éloignent depuis plusieurs années de la simple frappe sur coordonnées GNSS qui était devenue la tendance centrale de la frappe de précision à partir du milieu des années 1990. Désormais, le guidage des armes récentes repose de plus en plus sur des solutions multimodales, à base d'autodirecteurs radars et/ou infrarouges mais aussi sur le développement des *Network-Enabled Weapons* (NEW) pour l'engagement sur cible mobile. Par exemple, la nouvelle *Small Diameter Bomb II*, la GBU-53/B

StormBreaker, récemment entrée en service avec beaucoup de retard, mise en œuvre par les forces américaines et australiennes, dispose de l'ensemble de ces caractéristiques. C'est une NEW et elle dispose d'un guidage terminal tri-modes (laser semi-actif, radar millimétrique, infrarouge).

B. Le foisonnement des techniques de positionnement et de navigation relative par corrélation d'image avec l'environnement

Le missile Tomahawk fournit une excellente synthèse de l'histoire de la prise en compte de ces différentes technologies. Précédant le GNSS, à l'époque de la fin de la Guerre froide et de la guerre du Golfe, les premières versions de ce missile reposent, pour assurer leur guidage, sur un double dispositif, d'une part le *Terrain Contour Matching* (TERCOM) permettant la navigation par comparaison entre les données topographiques fournies par un radar altimétrique et une carte isoligne pré-enregistrée, d'autre part un guidage terminal réalisé par *Digitized Scene-Mapping Area Correlator* (DSMAC) soit une première technologie de reconnaissance automatique de cible par corrélation entre les données du capteur optique et les images numérisées, elles aussi préenregistrées. Cela étant, le procédé repose sur une planification lourde. Le besoin de disposer de modèle numérique d'élévation de terrain et d'une imagerie se heurte aux capacités limitées de l'informatique embarquée, d'où le recours au GPS beaucoup plus flexible à partir du block III dans les années 1990. Le Block IV Tactical Tomahawk dispose à partir des années 2000 d'un des premiers réseaux d'antennes CRPA avec orientation de faisceau (l'*Anti-jam GPS Receiver* – AGR) et se voit adjoindre une liaison SATCOM bidirectionnelle permettant la mise à jour des données de mission en vol, ce qui en fait l'une des premières munitions maraudeuses[70]. Il n'en reste pas moins que le saut de génération en matière de numérisation permet, sur les Block IV puis V, de se reposer à nouveau en cas de besoin sur un couple TERCOM / DSMAC modernisé et infiniment plus flexible d'utilisation qu'auparavant[71].

L'ensemble est particulièrement efficace et le TERCOM est largement utilisé depuis des décennies sur de multiples autres missiles de croisière américains, soviétiques, comme sur notre SCALP. Le missile chinois CJ-10 reprend lui aussi le couple TERCOM/DSMAC. Le DSMAC est utilisé également sur d'autres munitions que les missiles de croisière, comme les bombes Spice de Rafael.

La prolifération des drones et robots terrestres mais aussi les perspectives de développement des véhicules autonomes génèrent une masse toujours plus importante de recherches, civiles comme militaires, en techniques de **navigation basée sur le visuel** (*Vision Based Navigation* – VBN). Une large partie a recours à l'odométrie visuelle (OV), c'est-à-dire le positionnement et la trajectoire de la plateforme à partir de son mouvement relatif à son environnement. Les capteurs étaient en général des caméras stéréoscopiques ou encore le *Light Detection And Ranging* (LIDAR), c'est-à-dire au radar par laser. Cela étant, le coût de ces dispositifs favorise maintenant l'emploi de caméras uniques associées à des algorithmes de reconstruction 3D de la zone scannée. Les images sont traitées afin d'en extraire les points de repères (les amers).

---

[70] Voir par exemple, Direction of Program Executive Officer for Unmanned Aviation And Strike Weapons, *U.S. Navy Tomahawk Cruise Missile Weapons System Technical Manual*, July 4, 2011 – https://publicintelligence.net/u-s-navy-tomahawk-cruise-missile-weapons-system-technical-manual/

[71] Raymond McConoly, « How Tomahawk Finds Its Target », *Naval Post*, May 22, 2021 – https://navalpost.com/ how-tomahawk-missile-find-its-target/

Puis, ces derniers sont corrélés avec une base de données d'images en exploitant les techniques d'intelligence artificielle de reconnaissance de forme. Une autre famille de technique de navigation dérivée de l'OV est celle de la localisation et de la cartographie simultanées, (*Simultaneous Localization And Mapping* – SLAM) dans laquelle le robot réalise en parallèle la cartographie de son environnement, la création de la scène et sa localisation, une technique rendue nécessaire pour les cas dans lesquels il n'existe pas de base de données ou de cartes préalablement établies de la zone considérée. Le système procède de techniques d'analyse probabiliste[72]. Sans surprise, les techniques de SLAM constituent un élément central des programmes de robots de l'*US Army*[73]. À titre d'exemple de ces évolutions, la société Helsing a développé une technologie d'IA embarquée exploitant ces différentes sources (odométrie, SLAM, corrélation d'image) pour garantir une « navigation sure » et une capacité de génération de coordonnées de niveau TLE 1 pour les feux de précision[74].

Cela étant, ces techniques, du TERCOM à la reconnaissance d'image, souffrent d'une limitation de taille : elles ne fonctionnent que si l'environnement offre des points de repère. Elles seront donc inopérantes en milieu maritime ou encore sur de vastes plaines désertiques.

C. La navigation astronomique

La navigation astronomique, l'une des plus anciennes techniques en la matière, connaît, elle aussi, un regain d'intérêt. Des centrales de navigation fournissent un instrument de corrélation depuis la Guerre froide sur certaines grosses plateformes de l'USAF (SR-71, B-2, RC-135 notamment) et continuent d'être employées. Elle pourrait au demeurant être déployée également sur les futurs B-21. Le système contribue également au recalage de navigation des missiles balistiques intercontinentaux (ICBM et SLBM). La *Navy* a ré-institué progressivement dans les années 2010 l'entraînement de ses officiers de quart à l'utilisation de ces techniques en exploitant un système aidé par ordinateur développé dans les années 1990 mais dont l'utilisation prend encore plusieurs minutes et prête le flanc à l'erreur humaine. Suite aux multiples incidents de navigation connus par ses navires, tirant également expérience de l'usurpation russe en mer Noire, elle a lancé un programme d'adaptation sur ses bâtiments d'un système d'*Automated Celestial Navigation System* (ACNS) un peu analogue à ceux qui équipent les appareils de l'*Air Force*. Ce d'autant que la technologie de CELNAV est maintenant efficace en plein jour puisque les systèmes ne recueillent non plus uniquement la lumière visible des étoiles mais leur signal infrarouge[75].

---

[72] Pour une description compréhensible à un non-initié voir M. Abouzahir Mohamed, « Algorithmes SLAM: Vers une Implémentation Embarquée », Thèse de doctorat de l'Université Paris-Saclay préparée à l'Université Paris Sud, École doctorale n° 580, Sciences et technologies de l'information et de la communication, Spécialité de doctorat : Robotique, Thèse présentée et soutenue à "Agadir, Maroc", le 25 février 2017 – https://www.electronique-mixte.fr/wp-content/uploads/2018/09/Cours-acc%C3%A9l%C3%A9ration-mat%C3%A9rielle-19.pdf

[73] Eric Spero, Program Manager, *Scalable, Adaptive, and Resilient Autonomy (SARA)*, U.S. Army Combat Capabilities Development Command – Army Research Laboratory, 19 Feb 2021, https://www.arl.army.mil/wp-content/uploads/2021/02/SARA_Sprint_2_Webinar_vFinal.pdf

[74] Etienne De Geloes, Tamar Gomez, Mattis Paulin, « La navigation basée vision dans un contexte de brouillage GPS : l'apport de l'IA à la résilience des drones au combat », Helsing, présentation au colloque Combat aéroterrestre 2035, Versailles, 15 novembre 2023.

[75] LTJG Kyle Cregge, USN, Automated Celestial Navigation for the Navy Cold War-era technology could provide an alternative to GPS, *The Maritime Executive*, DEC 13, 2017 – https://www.maritime-executive.com/blog/automated-celestial-navigation-for-the-navy

D. La navigation par gravimétrie

La gravimétrie, qui consiste à mesurer le champ de pesanteur de la Terre, est également un domaine de métrologie ancien, incarné à partir du XVIIIème siècle par les pendules. Au XXème siècle, d'autres techniques, les gravimètres à ressort puis à supraconducteurs démultiplient la précision de ces mesures relatives. L'utilisation de la gravimétrie à des fins de navigation n'apparaît néanmoins que récemment, avec la gravimétrie balistique, proposant une mesure absolue, ne nécessitant pas de recalibrage de l'instrument. Elle semble atteindre un niveau de maturité opérationnelle. Elle exploite les propriétés de la physique quantique. La technique est celle de l'interférométrie entre atomes refroidis au laser, sensibles au champ magnétique, lâchés en chute libre dans un tube à vide, placés en état de superposition puis mesurés par d'autres lasers durant cette chute. Elle offre une précision inédite de mesures de rotation, d'accélération et de timing. Elle devrait ainsi permettre à des centrales inertielles gravimétriques d'atteindre des précisions de navigation supérieures à celle du GPS, de plus totalement autonomes et sûres. Elle sera particulièrement utile aux sous-marins, privés par essence des services GNSS et utilisant de grosses centrales, performantes mais coûteuses.

Le principal défi a longtemps résidé dans le facteur *Size, Weight and Power* (SWAP) de tels systèmes mais la technologie a atteint des seuils d'intégration sur plateforme. En témoigne le Gravimètre interférométrique de recherche à atomes froids embarquable (GIRAFE), fonctionnant avec des nuages d'atomes de rubidium, conçu par l'ONERA et testé avec succès sur des plateformes navale et aérienne par le service hydrographique et océanographique (SHOM) de la Marine[76]. La résolution spatiale obtenue lors de la première campagne de 2015 a atteint 500 m. Une seconde campagne a permis d'obtenir ces résultats en dépit d'une houle de 5 à 6 mètres. En 2017, une version de l'appareil a été testée en avion[77]. La France semble ainsi en avance dans ce domaine. Le marché passé en 2020 par la DGA à l'ONERA prévoyant la livraison de plusieurs GIRAFE fera de cette technologie l'un des piliers de la Capacité Hydrographique et Océanographique Future (CHOF) de la Marine d'ici la fin de la décennie[78]. Cet effort de cartographie des fluctuations de ce champ de gravité (qui sont également dynamiques) nécessitera probablement des années et il faudra acquérir les capteurs permettant de l'exploiter sur les différentes plates-formes. Il s'agit donc d'une solution de long terme.

Par ailleurs, comme l'expliquait en 2013 le doctorant Landry Huet, la sensibilité de la mesure par « atome lâché » est « *proportionnelle à la hauteur de l'instrument, et les performances actuelles sont obtenues pour des chutes de l'ordre du mètre* »[79]. Ceci limite l'emport de ces accéléromètres à de grosses plateformes. Une entreprise comme Thalès œuvre donc depuis plus de 10 ans à une technologie d'atomes piégés en mesure d'être embarquée sur puce avec, tout d'abord, le programme de Capteurs atomiques sur puce (CATS) et plus récemment en coordonnant le projet européen QuantaQuest[80]. Les recherches portent notamment sur la

---

[76] « Quand les technologies quantiques prennent le large », *The Conversation*, 24 février 2021, https://theconversation.com/quand-les-technologies-quantiques-prennent-le-large-152834

[77] ONERA, « L'ONERA invente avec le SHOM la cartographie de pesanteur à précision "atomique" », 3 février 2016.

[78] ONERA, « L'ONERA va fournir des gravimètres quantiques au ministère des Armées », 4 novembre 2020.

[79] Landry Huet, *Thales Underwater Systems, Thales Research And Technology*, Université Paris Est – École Doctorale MSTIC, « Gravimétrie atomique sur puce et applications embarquées », Thèse de doctorat en Sciences et Technologies de l'Information Géographique, soutenue le 11 janvier 2013, p. 19 – https://theses.hal.science/tel-00839785v2

[80] « Des capteurs inertiels à atomes froids sur puce », CNRS, 25 février 2021 – https://www.iledefrance-meudon.cnrs.fr/fr/cnrsinfo/des-capteurs-inertiels-atomes-froids-sur-puce

réduction de la consommation électrique, la capacité à intégrer un plus grand nombre de composants sur la puce (dont les techniques de piégeage) ou encore l'interconnexion de plusieurs capteurs. Les concepteurs voient notamment dans ces systèmes des capteurs de premier ordre pour la navigation sous-marine ou l'évitement des navires.

E. La navigation magnétique

La **navigation magnétique (MAGNAV)** se base sur les spécificités du champ magnétique crustal (de la croute terrestre, la lithosphère) provenant de la magnétisation des minéraux notamment. Le Dr Aaron Canciani a par exemple travaillé à l'*Air Force Institute of Technology*, en lien avec le MIT, sur le développement de cartes précises d'anomalies magnétiques, plus précisément de cartes relevant les mesures de différences d'intensité par rapport au champ géomagnétique de référence, l'*International Geomagnetic Reference Field* (IGRF) élaboré et mis à jour tous les 5 ans par l'*International Association of Geomagnetism and* Aeronomy (IAGA). La technique est connue mais les résultats enregistrés jusque-là étaient décevants. Ils provenaient en effet de l'insuffisante précision des cartes existantes, par exemple la *World Digital Magnetic Anomaly Map.* Avec un effort conséquent de GEOINT (des cartes réalisées avec des relevés plus précis et bien géoréférencés), un appareillage bien calibré et les bons algorithmes de traitement (notamment les mesures de correction des autres champs EM à commencer par celui de l'appareil), les tests menés par le scientifique ont montré une précision de navigation de quelques dizaines de mètres à basse altitude (l'altitude est une donnée importante). La solution apparaît particulièrement séduisante car elle ne dépend pas de la visibilité de la référence comme les autres approches aidées par capteur, elle est passive, ne peut être brouillée, et elle est efficace également pour le milieu naval à la différence des techniques de suivi de terrain[81]. La complexité des conditions de réalisation de ce mode de navigation rend toutefois incertaine une concrétisation de cette approche.

La DARPA poursuit pour sa part le programme *Atomic Magnetic Biological Imaging in Earth's Native Terrain* (AMBIIENT) dans lequel elle explore les technologies de détection et d'imagerie des signaux magnétiques biologiques, y compris à des fins de navigation.

F. La navigation acoustique

Le PNT en milieu sous-marin pose des défis particuliers dans la mesure où les signaux GNSS ne parviennent pas aux différents moyens submersibles en plongée. En ce qui concerne le P/N, les sous-marins disposent toutefois des technologies de centrale inertielle les plus sophistiquées.

Pour fournir une capacité supplémentaire, moins coûteuse et ne nécessitant pas de recalage en surface, mais aussi permettre la navigation des autres mobiles comme les drones (*Unmanned Undersea Vehicle* – UUV), la principale technologie alternative est celle de la navigation acoustique, ce depuis plusieurs décennies. Elle repose sur la tri-latéralisation entre émissions de balises transpondeuses, déposées sur les fonds marins, bien géoréférencées (navigation absolue) ou flottantes (qui peuvent être déployées sur des navires de surface également), offrant

[81] Bill Schweber, « Magnetic-Field Navigation as an 'Alternative' GPS? », Electronic Design, Oct. 27, 2020 – https://www.electronicdesign.com/markets/article/21211037/magneticfield-navigation-as-an-alternative-gps & Aaron J. Canciani, *Absolute Positioning Using the Earth's Magnetic Anomaly Field*), Air Force Institute of Technology Theses and Dissertations 251, 2016 – https://scholar.afit.edu/cgi/viewcontent.cgi?article=1250&context=etd

une solution de positionnement relatif, moins précis mais plus flexible. Ces dispositifs s'accompagnent d'algorithmes de positionnement de la plateforme. L'US *Navy* explore des solutions très avancées reposant sur ces techniques : adaptation du *Submerged Acoustic Navigation System* (SANS) de *Mikel Inc.*, déployé sur les SNA, ou encore le *Portable Underwater Global Positioning System* (PUG)[82]. C'est aussi le principe du *Positioning System for Deep Ocean Navigation* (POSYDON) lancé par la DARPA en 2015 et développé par BAe, le MIT et l'Université du Texas. Ce vaste programme ambitionne de créer un véritable GPS sous-marin en développant de nouvelles formes d'ondes acoustiques et une meilleure modélisation de la propagation de ces ondes. Une autre technique est celle de la centrale inertielle aidée par DVL (*Doppler Velocity Log*) consistant à calculer la vélocité du drone grâce à l'effet doppler de la réflexion sonar sur des hauts fonds.

2.6. L'évolution des cadres de référence : deux exemples

La *Navigation Warfare* et les capacités de PNT sont aussi dépendantes de l'évolution des cadres des repères, des normes de référence. Sans pouvoir dans le cadre de cette note traiter avec exhaustivité ce vaste écosystème scientifique, nous en évoquerons deux aspects qui semblent particulièrement critiques pour notre problématique.

2.6.1. L'évolution du WGS-84 et du GEOINT : un impact important sur le PNT

La *National Geospatial Intelligence Agency* (NGA) américaine estime le GEOINT en révolution permanente. Dans sa stratégie capacitaire, dont une mise à jour est proposée par le *Tech Focus Area 2022*, elle place l'*Assured Positioning, Navigation, Timing, and Targeting* (APNT&T) au centre de ses priorités. Pour ce faire, elle compte investir sur quatre axes :

- Moderniser et transformer le repère de référence WGS-84 dont elle a la charge, cadre du GPS comme du GEOINT américain. Cette modernisation (portant sur les processus ou encore l'inclusion de beaucoup plus de techniques d'intelligence artificielle) concernerait les trois composantes majeures du système : *Terrestrial Reference Frame*, *Earth Gravitational Model*, et le *World Magnetic Model* ;
- Améliorer la précision des opérations sans GPS via une meilleure définition des besoins minimums en APNT&T, une redéfinition de la façon d'utiliser ce système, le développement de techniques de diffusion du WGS-84 et de modèles de théâtre plus fins et incluant de nouvelles phénoménologies. On comprend par exemple de ces deux points que la démarche devrait contribuer à crédibiliser les solutions de NAVMAG ;
- Une modélisation planétaire plus dynamique ;
- L'automatisation plus poussée encore du GEOINT de précision, en particulier du traitement de l'imagerie et de l'extraction de coordonnées à fins de ciblage[83].

[82] NAVSEA Warfare Centers & NR&DTE, *ANTX 2016, Participants and Technologies* – https://www.navsea.navy.mil/Portals/103/Documents/NUWC_Newport/ANTXdocs/PlaybillANTX2016.pdf?ver=2017-05-12-105159-150

[83] *NGA Tech Focus Areas 2022*, GEOINT Symposium, Denver (Co), 24-27 April 2022.

Tout ceci ne constitue pas en soi une révolution mais une accélération dans un monde du GEOINT dont les productions contribuent déjà largement à optimiser l'information de PNT. Ainsi, la société Vricon, lancée par DigitalGlobe (Maxar) et Saab en 2015, développe à partir de multiples sources d'imagerie, les techniques et produits de modélisation de surface 3D géoréférencés avec une résolution de 50 cm et une précision en position de moins de trois mètres, pour la cartographie, l'observation de la Terre, le ciblage ou encore la simulation. Son application *Precision 3D Registration* permettant cette modélisation est proposée à l'intégration sur les systèmes ISR (satellites, nacelles de reconnaissance, etc.)[84]. On comprend que ce type de technologie va considérablement faciliter le P/N de précision relative à base de capteurs.

2.6.2. La cartographie des fonds marins

Un autre grand secteur d'investigation du cadre de référence du PNT réside évidemment dans la cartographie des fonds marins, préalable indispensable à une meilleure exploitation des océans, mais aussi au développement des opérations sous-marines, tout particulièrement de la *Seabed Warfare*. Comme le rappelle le rapport du groupe de travail associé à la stratégie ministérielle de maîtrise des fonds marins : « *Les fonds marins sont encore mal connus : à peine 20% de la topographie des fonds marins a fait l'objet d'une mesure précise – même ponctuelle – par sondeur acoustique et seuls 2% des fonds marins sont connus avec une précision métrique* »[85].

Le rapport cite en cela le vaste programme collaboratif *Seabed 2030* lancé par la *Nippon Foundation of Japan* et la *General Bathymetric Chart of the Oceans* (GEBCO) de l'organisation hydrographique internationale de l'UNSECO, qui ambitionne de cartographier l'ensemble de ces fonds en 2030. Répartis sur plusieurs centres régionaux, le projet consiste à coordonner les efforts de recueil de données et à rassembler le maximum de données bathymétriques de formats très hétérogènes, à les fusionner avec un processus unique de mise en grille, de filtrage et de modélisation 3D. Les défis sont évidemment énormes : technologiques d'abord car les principaux modes, le sondeur multifaisceaux et le LIDAR pour les eaux peu profondes, sont précis mais d'une fauchée réduite, ce qui rend le processus très long. Il faudrait donc reposer sur d'autres technologies. La GEBCO entend donc développer le crowdsourcing de données bathymétriques dans les zones fréquentées et mener des campagnes de financement pour un plus grand nombre des campagnes plus spécialisées, etc.[86].

Les grandes puissances (Chine, Russie, bien sûr États-Unis mais aussi Inde ou encore Japon) rivalisent d'efforts à leur niveau. Par exemple, les États-Unis ont créé un *Ocean Policy Committee* (OPC) lequel a mis sur pied le *National Ocean Mapping, Exploration, and Characteriza-*

[84] Site de Maxar, « Precision 3D Registration » – https://www.maxar.com/products/precision-3d-registration

[85] Ministère des armées, *Stratégie ministérielle de maîtrise des fonds marins*, Rapport du groupe de travail, février 2022, p. 13 – https://www.defense.gouv.fr/sites/default/files/ministere-armees/20220210_LANCEMENT%20STRATEGIE%20FONDS%20MARINS_strat%C3%A9gie%20-%202.pdf

[86] Larry Mayer et alii, « The Nippon Foundation—GEBCO Seabed 2030 Project: The Quest to See the World's Oceans Completely Mapped by 2030 », *Geosciences*, Vol. 8, Issue 2, 8 February 2018 – https://www.mdpi.com/2076-3263/8/2/63/html

tion (NOMEC) *Council* en juin 2020. La stratégie éponyme en cours de planification est de cartographier les fonds, explorer et caractériser l'ensemble de l'environnement des ZEE au profit de l'ensemble des acteurs du monde maritime américain[87].

2.7. L'intégration de ces multiples techniques : la question des architectures

Développer et murir une large gamme de solutions ne suffit pas. Dans la mesure où aucune d'elles ne permet individuellement d'offrir une qualité ou une polyvalence d'information PNT équivalente au GNSS, l'intégration de plusieurs d'entre elles est nécessaire. La question des procédés et en particulier des architectures se pose donc outre-Atlantique avec une acuité aussi importante que les sources elles-mêmes.

Chaque *Service* a mis sur pied des programmes d'intégration de ces différentes solutions :

- L'Army poursuit ainsi, sous la coordination d'une équipe pluridisciplinaire (*Cross Functional Team*) de l'Army Futures Command, dans le cadre de son vaste plan de modernisation visant à établir une force multidomaine, son programme d'*Assured PNT* (A-PNT) et ses traductions capacitaires pour le combat embarqué (*Mounted A-PNT System* – MAPS) et le combat débarqué (*Dismounted A-PNT System* – DAPS). La même équipe coordonne également les travaux sur les autres services spatiaux et la NAVWAR offensive ;
- L'Air Force est bien sûr responsable du GPS et de multiples autres initiatives de PNT et son principal programme d'intégration réside dans les déclinaisons de son « entreprise » *Embedded GPS/Inertial* (EGI) à vocation interarmées, existant depuis la fin des années 1990 et portant comme son nom l'indique sur la complémentarité GPS et centrales inertielles des plateformes aériennes américaines ;
- La principale architecture de la Navy est le *Global Positioning System-Based Positioning, Navigation and Timing Services* (GPNTS) laquelle, comme son nom ne l'indique pas forcément, a elle aussi vocation à intégrer de multiples solutions PNT alternatives.

Comme pour l'ensemble des acquisitions du Pentagone depuis quelques années, l'intégration du PNT doit se faire au sein d'architectures ouvertes et modulaires (MOSA – *Modular Open Systems Architecture*) favorisant l'interopérabilité, la rapidité de modernisation et la réduction des coûts. En 2021, l'Army et la Navy avaient développé leur MOSA de référence et l'Air Force venait de commencer la sienne. Au niveau de l'ensemble du DoD, c'est l'Army qui est le service pilote pour l'architecture de référence PNT[88]. Ces architectures fournissent les spécifications de base puis exploitent le développement de quelques grands standards d'interface matériels et logiciels définis par les acteurs de la BITD américaine réunis en de vastes consortiums. En ce qui

[87] National Ocean Mapping, Exploration, and Characterization Council of the Ocean Science and Technology Subcommittee & Ocean Policy Committee, *Implementation Plan for the National Strategy for Ocean Mapping, Exploring, and Characterizing the United States Exclusive Economic Zone* – https://iocm.noaa.gov/about/documents/strategic-plans/210107-FINALNOMECImplementationPlan-Clean.pdf

[88] United States Government Accountability Office, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS*, Report to the Committee on Armed Services, U.S. Senate, May 2021, p. 18.

concerne le PNT, il semble que les plus importantes soient la *C5ISR/EW Modular Open Suite of Standards* (CMOSS) pour l'Army et la *Sensor Open Systems Architecture* (SOSA) plus large[89].

L'OTAN vient également de lancer le développement d'une *NATO PNT Open System Architecture* avec le même type d'objectifs de parvenir à une définition de standards permettant une intégration de type *plug-and-play* de sources PNT variées[90].

2.8. Des solutions alternatives de données PVT qui peinent à se faire une place

On le voit, les solutions ne manquent pas. Pourtant, la résilience des capacités PNT progresse très lentement et peu de programmes de solutions alternatives ont franchi la « vallée de la mort » entre les projets R&D et les programmes d'acquisition, hormis bien entendu dans les missions où elles sont absolument requises. De fait, bien des obstacles se posent aux États-Unis pour la réalisation de la stratégie PNT articulée en 2018.

Il y a bien sûr, classiquement, le volet technologique et la complexité des programmes. C'est le cas en particulier du GPS lui-même mais ce n'est pas le plus contraignant en ce qui concerne bien des solutions alternatives. Le défi principal réside comme souvent dans la bureaucratie et la politique. Comme un expert de l'institution l'a résumé aux investigateurs du *Government Accountability Office* qui ont consacré une importante étude au sujet : « *PNT—it's everyone's need, but nobody's business* »[91]. Ainsi, la priorisation à bon niveau de la problématique PNT n'est présente qu'au niveau *service*. Il n'existe, comme dans bien d'autres domaines capacitaires, aucun bureau central chargé de coordonner les programmes d'alternatives au GPS. Même dans chaque armée, si l'assurance du PNT figure désormais en bonne place des priorités de développement technologique et même capacitaire, la mise en œuvre effective des solutions alternatives innovantes peine à s'affirmer dans une myriade de programmes où elles ne constituent pas toujours une priorité. Il semble que cette prise en compte soit effective lorsqu'elle est imposée aux responsables de programme.

Ce paysage bureaucratique résonne en effet avec la dimension culturelle. Le référentiel dominant au sein des forces consiste à confondre PNT et GPS, perpétué en cela par une stratégie maintenant le GPS au centre de cette fonction. On notera ici une différence notable avec l'approche française, plus flexible (voir partie suivante). Ce biais aboutit donc à maximiser les spécifications PNT de tout système à ce niveau. L'expression fine des besoins, qui pourraient, en réalité, être inférieurs aux services offerts par le GPS pour bien des missions et systèmes, est ainsi souvent mal réalisée. Dans ce contexte de définitions insuffisantes du besoin, les contraintes additionnelles associées au coût, à la spécificité de la technique considérée ou encore

[89] Sally Cole, « CMOSS: Building-block architecture brings speed, cost benefits », Military Embedded Systems, November 29, 2021 – https://militaryembedded.com/comms/communications/cmoss-building-block-architecture-brings-speed-cost-benefits#:~:text=The%20C4ISR%2FElectronic%20Warfare%20Modular,long%2Dterm%20life%20cycle%20costs & Jaspreet Gill, « Army seeking white papers for Assured PNT CMOSS effort », *Inside Defens*e, December 21, 2020 – https://insidedefense.com/insider/army-seeking-white-papers-assured-pnt-cmoss-effort

[90] NATO STO, « NATO PNT Open System Architecture & Standards to Ensure PNT in NAVWAR Environments », 11 mai 2022 – https://www.sto.nato.int/_layouts/mobile/dispform.aspx?List=b2aac100%2Dbe82%2D43ce%2D886f%2D0a467bd6baa9&View=7d98007a%2Dc441%2D4dae%2Db0f6%2D1ce7c6fd45f0&ID=17050

[91] United States Government Accountability Office, *Defense Navigation Capabilities, op. cit.*, p. 31.

à la complexité d'intégration de ces nouvelles technologies ne plaident pas pour leur prise en compte.

En outre, l'offre industrielle, correspondant à ces solutions très diverses, est assez fragmentée. Chaque solution prise individuellement ne permet donc pas des économies d'échelle suffisantes pour consolider les marchés. Ce n'est pas le cas de bien des technologies civiles mais il semble que le Pentagone doive encore progresser pour mieux intégrer ces innovations commerciales.

Enfin, en dépit d'un discours sur la menace bien diffusé, il est probable que les mesures déjà prises pour rendre le GPS plus robuste mais aussi l'absence de RETEX réellement alarmiste, n'incitent pas en réalité à un sentiment d'urgence en faveur d'un renforcement de la résilience, bien que les entretiens restitués par l'étude du GAO ne l'expliquent pas de cette façon. En bref, sans réel péril en la demeure, pourquoi faire plus compliqué, moins polyvalent, peut-être plus cher, voire moins performant que le GPS ?

Partie 3 – Implications / recommandations pour les armées

Que tirer de cette revue de technologies pour nos armées ? Pour tenter de répondre à cette interrogation, cette partie propose tout d'abord une synthèse des niveaux de menaces et de l'impact des technologies en cours d'acquisition sur la résilience du PNT. Elle présente ensuite différentes initiatives en cours au sein de nos armées et valables pour chacune. Ce n'est qu'ensuite que la note consacre des développements propres à chaque armée. Chaque développement présente la problématique du milieu considéré, en particulier en ce qui concerne la dépendance au GNSS, donc la criticité de la menace, puis la situation de l'armée dans la mesure où l'auteur peut l'estimer, enfin propose des recommandations. Rappelons sur ce plan que cette analyse présente un point de vue externe à l'institution, réalisé *in abstracto* des réflexions et initiatives programmatiques des armées.

1. Synthèse sur les niveaux de menaces et de résilience actuelle

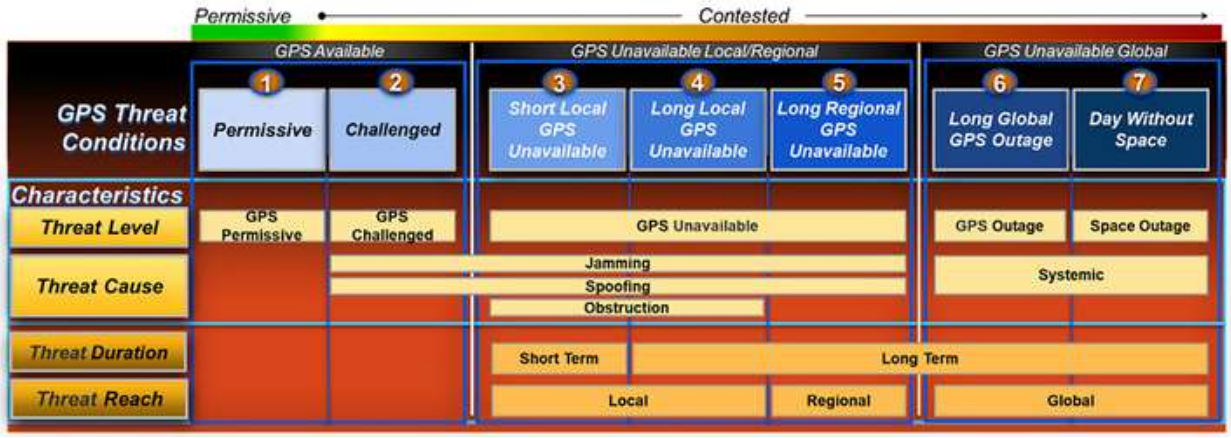
Nous reprendrons la classification de Collins Aerospace / BAE[92] pour synthétiser ces différents niveaux de menace. On distinguera ainsi :

- Un environnement où les GNSS sont disponibles, bien que parfois perturbés (cas 2). Ce type de situation peut se retrouver dans les engagements dans les zones que nous pourrions qualifier de « faible densité technique » comme l'Afrique subsaharienne ;
- Les cas de figure où les GNSS sont indisponibles en raison soit d'attaque électronique, soit tout simplement de la configuration de l'environnement opérationnel, au niveau tactique pour une durée courte de quelques heures (cas 3), que peuvent palier les centrales inertielles en ce qui concerne les données P/N, ou plus longtemps (cas 4). L'indisponibilité peut se concevoir également au niveau du théâtre (cas 5). Ce cas de figure pourrait se rencontrer de plus en plus souvent à l'avenir dans l'essentiel des zones de conflit MED/POMO et évidemment dans l'Est européen, sachant que la guerre en cours rend impossible toute assertion tendancielle concernant la Russie. Le club des pays disposant de ces capacités de GE offensives reste réduit : États-Unis, Chine, certains pays européens, puissances régionales : Israël, Iran, Turquie, Égypte, Inde, Corée du Nord, plus récemment Pakistan. Il s'élargit lentement, par exemple aux pays du Golfe ;

[92] Justin Wymore, BAE Systems, « Preserving operational capabilities by hardening GPS », *Military Embedded Systems*, December 02, 2021 – https://militaryembedded.com/comms/gps/preserving-operational-capabilities-by-hardening-gps

- Restent enfin les cas où les systèmes GNSS (cas 6) et même la majeure partie des capacités spatiales (cas 7) sont mis hors d'usage. Pour l'instant, ce niveau de « menace » ne réside que dans le risque d'une catastrophe géomagnétique majeure.

Figure n° 13 : CLASSIFICATION DES DIFFÉRENTS DEGRÉS DE MENACE PESANT SUR LE GPS

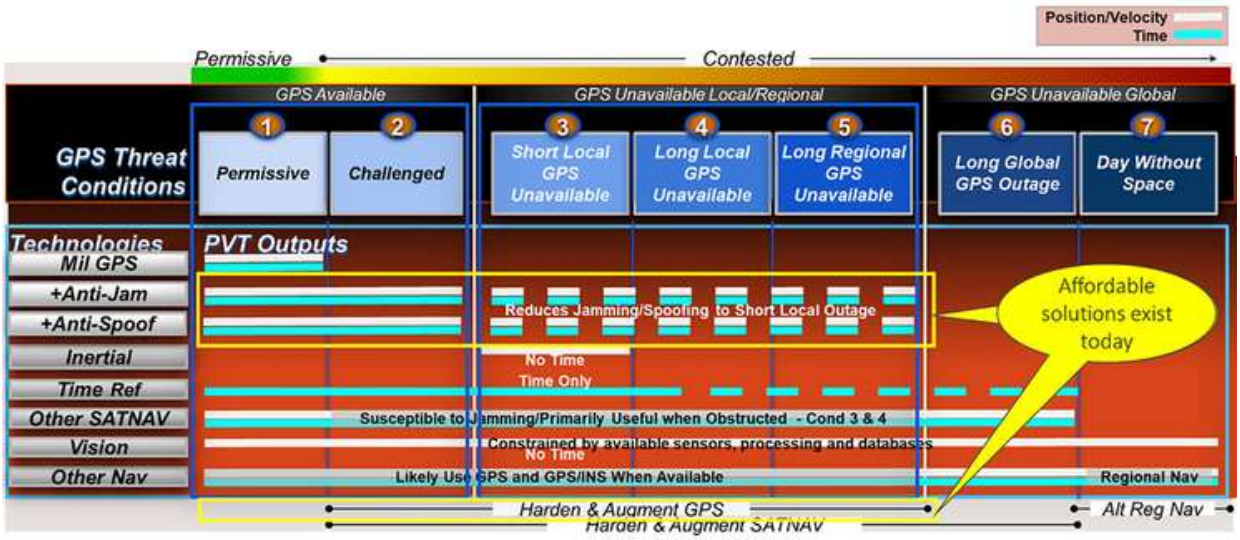


Source : Mark W. Johnson, APNT Campaign Lead, Collins Aerospace, *A Positioning Navigation and Timing (PNT) Threat Environment Model for Military and Civilian Use,* June 6, 2019.

La dissémination du couplage étroit INS/GPS, des antennes à diagramme de rayonnement contrôlé avec orientation de faisceau, la certes difficile mais inéluctable diffusion du M-Code aboutissent à restreindre de plus en plus drastiquement à court-moyen terme les capacités de la NAVWAR offensive classique à base de brouillage de puissance. La portée effective de ces brouilleurs se réduit à quelques kilomètres face à un appareillage complet de la sorte. La menace tant redoutée d'interdiction de zone du GNSS, pilier de l'A2/AD, va progressivement céder le pas à une logique de défense de point de sites fixes ou d'unités voire à la simple autoprotection. La réduction des capacités d'usurpation type *meaconing* est peut-être moins évidente mais les technologies progressent également pour compliquer le procédé. Sur ce plan, la combinaison de plusieurs GNSS, déjà actée sur l'essentiel des récepteurs commerciaux, rend peut-être la société civile plus résiliente, transitoirement, que le monde militaire. On peut en conclure que, pour un appareil de force investissant activement dans ces technologies de renforcement des GNSS, la dangerosité des menaces brouillage / usurpation devient de plus en plus réduite… à condition que l'investissement dans l'ensemble des technologies antibrouillage soit soutenu.

En revanche, les menaces pesant sur les constellations GNSS proprement dites sont théoriquement à considérer à l'échelle du temps de l'étude, de la part des grandes puissances poursuivant leur montée en puissance dans le domaine du *counterspace*, à commencer par les capacités de RPO. À cette extrémité du spectre capacitaire, en dehors des États-Unis, on ne voit guère que la Chine en mesure de suivre ce schéma dans les 15 prochaines années. La situation dans laquelle s'est plongée la Russie l'écarte du jeu. Or, dans le même temps, les solutions de PNT spatial complémentaires murissent très vite, à commencer par les services en LEO (Iridium, constellation de la SDA, etc.) ce qui va rendre la tâche de tout acteur du *counterspace* d'autant plus difficile. À cet horizon, on ne doit cependant pas exclure des percées dans le domaine de la LIO rendant ces constellations plus vulnérables. C'est dans cette perspective que les solutions autonomes à base de capteurs prennent tout leur sens.

Figure n° 14 : CLASSIFICATION DES SOLUTIONS TECHNOLOGIQUES DE RÉSILIENCE EN FONCTION DES DEGRÉS DE MENACE PESANT SUR LE GPS



Source : Mark W. Johnson, APNT Campaign Lead, Collins Aerospace, *A Positioning Navigation and Timing (PNT) Threat Environment Model for Military and Civilian Use,* June 6, 2019.

Le domaine PNT civil n'est pas dans le périmètre de cette note mais il n'est pas inutile de rappeler sa situation en matière de résilience. Le débat est en la matière ouvert. La plupart des travaux mettent en avant les différentes menaces et l'impact catastrophique qu'elles auraient sur nos sociétés. Cependant, un récent rapport de la *Rand* au profit du *Department of Homeland Security* (DHS)[93], tranchant au demeurant avec les propres analyses de cette administration, tend à relativiser l'impact de ces menaces sur les réseaux d'infrastructures américains. Les chercheurs distinguent les perturbations d'ampleur nationale (guerre haute intensité, tempête géomagnétique) très peu probables, les attaques par négligence (le brouilleur de véhicule pour éviter le traçage par GPS par exemple) et l'attaque terroriste, qui n'a jamais été tentée. Dans les deux derniers cas, ces risques sont par essence locaux et dans le cas d'une attaque intentionnelle, nécessitent des conditions de positionnement et de temporalité drastiques pour être réellement efficaces tout en s'exposant à des contre-mesures par les forces de l'ordre. Ces attaques seraient donc limitées dans le temps. Leur efficacité reste d'ailleurs questionnable pour deux raisons centrales : d'une part, de multiples activités ne nécessitent pas de PNT de précision de niveau GNSS, d'autre part, il existe déjà de multiples sources alternatives de PNT relatif (que nous avons évoquées en première partie). Les auteurs notent que ni le brouillage accidentel de l'US Navy à San Diego, ni la perte du GPS sur une partie de la Norvège en 2018, ni même les brouillages à grande échelle menés par la Corée du Nord sur la partie nord de la Corée du Sud n'ont provoqué de chaos, de pertes humaines et même de perturbations critiques de l'activité économique et sociétale.

[93] Richard Mason *et alii*, « Analyzing a More Resilient National Positioning, Navigation, and Timing Capability », *Rand Corporation*, 2021 – https://www.rand.org/pubs/research_reports/RR2970.html

2. Implications selon les milieux et recommandations pour nos armées

2.1. Remarques transverses aux différents milieux

Plusieurs développements programmatiques affectant l'ensemble des armées sont tout d'abord à signaler.

Comme évoqué dans la seconde partie, l'enjeu majeur en matière de NAVWAR fondée sur la guerre électronique réside dans la conscience situationnelle relative aux sources des interférences. Dans ce domaine, on ne peut donc que souligner la criticité d'un programme comme le *Space and ground-based NAVWAR surveillance* lancé en 2021 sur financement du Fonds de défense européen.

Ensuite, le programme OMEGA [Opération de Modernisation des Équipements GNSS des Armées] apparaît lui aussi d'une importance cruciale dans la résilience de nos armées. Ce programme vise à développer des récepteurs multi-GNSS conservant le bénéficie du GPS III tout en tirant partie de Galileo :

- Son premier incrément comprend le développement de ces récepteurs sur plusieurs plateformes notamment le Rafale et le porte-avions *Charles de Gaulle* ;
- Un second incrément incorpore la production de récepteurs P3TS (*Plug and Play Positioning and Timing System*) sur lequel nous revenons ci-dessous, dans la section sur le milieu terrestre ;
- Pour la suite, le développement d'un récepteur GPS/Galileo pour munitions guidées.

OMEGA n'offre pas en soi de réponse au brouillage de puissance car les SNR des différents GNSS ne se cumulent pas. En revanche, il permet, à l'instar des systèmes civils de dernière génération, de limiter considérablement les risques d'usurpation dans la mesure où cette menace porte – en l'état – sur un signal donné.

Nous comprenons également que la France, avec la Grande-Bretagne, l'Allemagne et la Corée du Sud, a signé un accord de trois ans avec les États-Unis pour disposer à des fins de test et évaluation, depuis 2021, des cartes *Military GPS User Equipment* (MGUE) fournies par le *Space and Missile Systems Center*[94]. Reste à voir comment ces dispositifs s'intègreront avec OMEGA.

D'autres solutions pouvant concerner les trois milieux semblent très intéressantes. Tel est le cas des réseaux VLF. Toutefois, nous comprenons qu'il pourrait être nécessaire pour ce faire de mettre sur pied de nouvelles installations dans nos DROM-COM, ce qui interroge sur la rentabilité d'une telle option.

À l'avenir, la question du PNT est à poser à l'aune de la transformation des armées dans la prise en compte du combat multimilieux / multichamps (M2MC) au niveau tactique, dont une

[94] Tracy Cozzens, « Military GPS user equipment capability heads to allies », GPS World, March 30, 2021 – https://www.gpsworld.com/military-gps-user-equipment-capability-heads-to-allies/

des dimensions principales est l'extension du domaine de l'intégration air-surface et du combat collaboratif interarmées, dans sa plus large acception. L'un des éléments programmatiques de ce M2MC tactique réside à moyen terme dans la fédération des SIC tactiques existants ou planifiés à court terme au sein du « réseau multi-senseurs / multi-effecteurs » (RM2SE) et à plus long terme dans la convergence des grands programmes de SIC : TITAN, Veille / combat naval collaboratif, système global de combat aérien / système de combat aérien futur.

En matière de PNT, l'une des composantes de cette convergence exige probablement de se fonder sur des solutions de précision absolue : non seulement les GNSS mais aussi des solutions de secours dans les cas d'indisponibilité totale des GNSS. Ces solutions absolues se posent en particulier en matière de synchronisation de système de systèmes, de positionnement partagé, mais aussi de techniques de géoréférencement communes permettant, entre autres l'extraction de coordonnées. Parmi ces exigences, la synchronisation est peut-être la question la plus simple à régler toute proportion gardée. Il serait en effet logique de définir une procédure interarmées de sélection, en fonction du contexte, d'une source de timing de référence et sa diffusion au sein des réseaux de transmission qui seront de plus en plus hybrides dans le RM2SE. Les impératifs de l'interopérabilité multinationale incitent également, si ce n'est déjà le cas, à promouvoir un tel standard dans les futures itérations du *Federated Mission Networking* de l'OTAN. En ce qui concerne le P/N, on peine à identifier une unique solution satisfaisante en multimilieux, qui soit en plus d'un coût abordable. Ceci implique effectivement, comme aux États-Unis ou en Chine, la définition d'un écosystème de solutions complémentaires. L'enjeu est que ces solutions de P/N pour les missions relevant du M2MC soient suffisamment précises et qu'elles soient absolues.

2.2. Le milieu terrestre

2.2.1. Implications

Le milieu terrestre, de façon générale, est le plus susceptible d'être affecté par l'interdiction des GNSS, si l'on considère l'ensemble du système de force. La puissance des brouilleurs ou moyens d'usurpation, leur portée en ligne de vue, de quelques dizaines de kilomètres, sont susceptibles théoriquement d'affecter l'ensemble des fonctions opérationnelles dans une zone d'action tactique d'un échelon brigade et en dessous : commandement (tenue de la SITAC), positionnement et navigation des unités de mêlée, pointage voire guidage de précision des feux indirects, synchronisation des réseaux, etc.

La fonction la plus vulnérable est sans doute celle du combat débarqué car les combattants ne peuvent pas alors se reposer sur les moyens techniques (INS, antennes) équipant les plateformes. Cela étant, c'est aussi le milieu qui, en raison de la nature des actions et activités qui s'y déroulent, présente peut-être la plus grande diversité en termes de besoins de précision de PNT. En clair, l'indisponibilité des GNSS peut dégrader considérablement les performances des fonctions opérationnelles mais difficilement les interdire pour la plupart. Illustrant cette réalité, l'armée de Terre appréhende son besoin en information PNT en répartissant les cas d'usage selon 5 niveaux, fondés sur les critères de précision et de sécurité. Elles vont du

niveau 0 (normes civiles) au niveau 4 (niveau de précision et de sécurité maximale). Le problème qui se pose aux forces terrestres tient d'ailleurs plus souvent de l'indisponibilité que du manque de précision de l'information PNT[95].

La criticité de la vulnérabilité s'accroit bien évidemment à l'aune des évolutions majeures du combat terrestre à l'avenir :

- Le combat collaboratif connecté qui exige un GEOINT très précis dans l'espace et le temps ainsi qu'un volume accru de données PVT de grande précision permettant les échanges de données entre plateforme et la synchronisation de leurs actions ;
- L'accroissement de la précision et de la portée des feux qui exigent un investissement croissant dans la navigation et le guidage des roquettes et missiles tactiques ;
- Les systèmes robotisés autonomes, qui nécessitent une gamme de solutions PNT elles-aussi autonomes.

Cela étant, comme le premier mois de la guerre en Ukraine a semblé le montrer, l'imbrication des dispositifs dans un contexte d'engagement non linéaire peut considérablement compliquer la tâche de l'attaquant. Depuis, le brouillage des GNSS est omniprésent dans le contexte d'affrontement linéaire qui caractérise cette guerre. Les effets fratricides générés par des brouilleurs déployés sur les arrières pour éviter les feux dans la profondeur ukrainiens semblent légions. La capacité à réaliser des actions de brouillage ou d'usurpation particulièrement sélectives, tant sur le plan géographique que sur celui du management de ses opérations dans le champ électromagnétique (EMSO), est encore une perspective distante. À l'horizon de l'étude, le développement technologique, allant dans le sens d'une plus grande flexibilité des EMSO, devrait logiquement améliorer cette capacité.

2.2.2. Comment se situe à cet égard notre force opérationnelle terrestre ?

Dans la dotation des forces terrestres, les industriels de défense se concentrent logiquement sur les équipements, comme le DAGR, correspondant à un niveau 2 ou 3 dans la classification de l'Adt. En complément de ces dispositifs, un officier de STAT et un ingénieur de la DGA ont conçu le P3TS, déjà évoqué. C'est un récepteur intégré sur tablette recevant les signaux civils GPS/Galileo/Glonass. Il est donc conçu pour les cas d'usage de niveau 1, en premier lieu l'entraînement ou certaines situations peu critiques, permettant l'accès à des données PNT aux plateformes ou combattants débarqués non dotés de DAGR (donc ne recevant pas le P(Y) du GPS). L'outil affiche tout de même certaines performances bien meilleures qu'un DAGR (par exemple en matière d'autonomie énergétique et de vitesse de resynchronisation) et dispose de capacités « fines » de détection de leurrage et de spoofing. Les premières acquisitions de série ont commencé en 2023 dans le cadre du programme OMEGA, 6 300 exemplaires devant *in fine* doter les forces terrestres.

Un autre point positif est que le PR4G, le réseau tactique historique des forces terrestres et qui fournit le premier substrat initial de transmission du SICS, permet une transmission des données PNT par rebonds, donnant semble-t-il satisfaction. Le P3TS figure parmi les sources de PNT transitant par le PR4G pour alimenter le SICS.

[95] Entretien avec un officier de l'armée de Terre, spécialiste de cette fonction PNT.

Pour l'avenir, la force Scorpion nous semble déjà disposer de multiples éléments garantissant, du moins en partie, sa résilience dans le cas 3 d'une indisponibilité de durée réduite des GNSS, si l'on se réfère aux équipements de navigation des principales plateformes de combat :

- INS Epsilon™ 10 de Safran sur le Griffon utilisable en backup en cas d'interdiction GNSS ;
- INS TopAxyz à gyroscope laser de Thalès, plus précise, pour les véhicules Jaguar ;
- INS Sigma 30 sur canons Caesar puis Geonyx à gyroscopes à résonateur hémisphérique de Safran, plus compacte tout en étant presqu'aussi précise, permettant le pointage de précision des feux.

La question de la vulnérabilité des équipements du combattant débarqué est peut-être plus critique.

Le nouveau système radio CONTACT qui remplacera incrémentalement et avec retard le PR4G devrait, comme ce dernier, être assez résilient à une indisponibilité des GNSS. Il mettra par exemple en œuvre en effet la forme d'onde à haut débit HDRWF (*High Data Rate Wave Form*) développée dans le cadre du programme ESSOR (*European Secure SOftware defined Radio*). Or, la conception de la FO a bien intégré cette contrainte d'absence potentielle du GNSS. Dans un réseau HDRWF, les nœuds qui le composent (allant à un maximum de 200) peuvent se synchroniser, même avec des sources de timing différentes. Si le GNSS est l'une d'elles, les algorithmes permettent d'homogénéiser la synchronisation sur cette référence mais le réseau peut faire sans ces systèmes satellitaires[96]. Toute la question est alors de déterminer une autre source de référence.

2.2.3. Recommandations

En ce qui concerne les sources PNT, pour le court-moyen terme, une solution consisterait à combiner les récepteurs multi-GNSS développés dans le cadre d'OMEGA avec des réseaux d'antennes CRPA au moins pour les PC de GTIA ou les plateformes de commandement en mesure de réduire comme nous l'avons vu, l'efficacité des brouilleurs. L'acquisition d'un système comme le TopShield de Thalès, un récepteur GPS à CRPA, compatible avec le PRS de Galileo, ou un dérivé de celui-ci (car c'est un récepteur *a priori* prévu pour les plateformes aériennes) ferait à cet égard sens, nonobstant bien sûr les questions de coût, ignorées de l'auteur. Autre mesure de résilience de court terme, l'acquisition de services Iridium comme le STL pour augmenter / vérifier les données GNSS et étendre leur couverture en ce qui concerne le Timing.

Ensuite, l'*US Army* met en œuvre, dans le cadre du *Dismounted Assured-PNT*, la transmission des données PNT via le Nett Warrior. De même, les technologies 5G permettront la transmission de données PNT. C'est une piste crédible à suivre pour l'armée de Terre pour de futurs incréments de CONTACT.

La question reste de développer sur le plus long terme une source ou plusieurs sources de PNT alternatives aux GNSS.

---

[96] Christian Serra et alii, « ESSOR HDRWF – Capabilities and Perspectives of an Innovative Coalition Waveform », *MILCOM 2013 – 2013 IEEE Military Communications Conference*, Novembre 2013, pp. 1 et 4 – https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Referencias/Attachments/51/ESSOR_INNOVATIVE%20COALITION%20WAFEFORM.pdf

En ce qui concerne le P/N, un procédé particulièrement intéressant serait sans doute la navigation magnétique, tout temps, invulnérable à l'attaque électronique, dans la mesure où elle gagnera en précision. C'est possible puisque les paramètres les plus contraignants, à savoir là encore la cartographie et le traitement, relèvent d'avancées informatiques susceptibles d'être assez rapides à l'échelle de temps de l'étude. Comme il est douteux que l'on puisse généraliser cette solution à l'ensemble des éléments, il faut alors envisager une diffusion de ces données de positionnement, soit par une transmission par réseau comme évoqué supra, soit par des relais.

Pour les éléments coupés du réseau, la solution la plus convaincante dès à présent semble le P/N basé sur la vision (combinant odométrie visuelle, corrélation d'image, etc.) s'il est associé aux avancées du GEOINT, permettant les extractions de coordonnées de façon beaucoup plus rapide et fiable. Il n'est donc pas étonnant de retrouver les productions de la société Helsing parmi les centres d'intérêt de l'armée de Terre.

En ce qui concerne la synchronisation, la solution viendrait peut-être de l'interconnexion croissante des réseaux de LDT, permettant à SICS de disposer de la référence temporelle développée à l'échelon supérieur et cadençant le futur programme TITAN. D'autres possibilités existent sans doute, par exemple le calage sur le timing d'autres réseaux comme la L16. Comme nous l'avons vu, les réseaux planifiés tels CONTACT devraient permettre ces sources de synchronisations différentes. Comme évoqué supra, le combat M2MC suppose de trouver sur ce plan une solution de synchronisation interarmées.

En parallèle de cette résilience du PNT, il serait intéressant d'inclure dans la prochaine génération de feux indirects une capacité de frappe HOJ afin, précisément, de réduire la menace brouillage la plus problématique.

2.3. Les milieux aérien et spatial

2.3.1. Implications

Le milieu aérien est sans doute dans une situation un peu paradoxale à l'égard des GNSS. Le cadre spatial de l'action des forces aériennes s'étendant bien au-delà de la ligne de vue, elles ne sont vulnérables à l'attaque électronique, *a fortiori* de surface, que sur une fraction de leur zone d'opération, en particulier en ce qui concerne les missions d'appui aérien rapproché, d'interdiction et de SEAD. En revanche, cette vulnérabilité apparaît en nature beaucoup plus critique. En ce qui concerne le réseau, l'interdiction des GNSS peut affecter le fonctionnement des réseaux radio. Les facteurs de résilience existent cependant déjà, comme l'usage de la L16 dont les réseaux disposent de leur propre temps de référence.

C'est plus encore dans le domaine du positionnement et de la navigation que le GNSS fait la différence. Si les centrales inertielles permettent aux grandes plateformes de s'extraire transitoirement de leur dépendance avec cependant une dégradation de leur performance, c'est bien sûr la frappe de précision à distance de sécurité, devenue l'alpha et l'oméga des effets réalisés par les puissances aériennes occidentales, imitées depuis par bien d'autres, qui est le domaine tactique le plus vulnérable. Le GNSS n'est plus ici un « *enhancer* » mais un « *enabler* » dont l'indisponibilité est susceptible de remettre en cause la mission.

Il convient d'ajouter un autre effet. Même si cette note se concentre sur la question militaire, la prise en compte du trafic aérien civil est nécessaire, en phase de contestation ou sur les espaces adjacents au théâtre en phase de conflit armé. Les appareils commerciaux sont plus vulnérables au brouillage des GNSS. S'il n'est pas appréhendé, le brouillage peut provoquer d'énormes complications de management de l'espace aérien voire des catastrophes.

À l'avenir, de prime abord, les effets d'une éventuelle indisponibilité des GNSS peuvent mécaniquement s'accroître au fur et à mesure que la puissance aérienne, pour réaliser ses effets, va incorporer un volume croissant de drones de petite dimension n'étant pas en mesure d'accommoder des centrales INS imposantes et coûteuses. C'est donc mécaniquement dans ce milieu que s'affirment le plus les solutions antibrouillage à base de CRPA, dont le rejet d'interférence bénéficie des écarts d'angle d'arrivée des signaux de brouillage surface-air par rapport aux satellites, et de guidages terminaux multimodes. Il bénéficie également des solutions de navigation relative à base de capteurs qui prolifèrent au profit des missiles de croisière, des drones comme, probablement à l'avenir, des munitions maraudeuses.

À bien des égards, la puissance aérienne américaine dispose déjà de l'ensemble de la chaîne de moyens lui permettant de mener à bien ses frappes de précision à moyen terme : même face à un brouillage de grande puissance, les INS/GPS étroitement couplés et les antennes CRPA devraient offrir une liberté d'action suffisante aux appareils comme aux munitions de précision, dont les futures centrales à MEMS garantiront alors si nécessaire la navigation de précision dans les phases terminales de vol vers leurs objectifs sur les quelques kilomètres où le GPS est interdit.

Les défis ne manquent pas cependant, à commencer par le développement de solutions sans GNSS dans les cas 8-9 de l'échelle évoquée et suffisamment peu coûteuses pour être diffusées en grand nombre.

2.3.2. Situation de nos forces

Les grandes plateformes de l'armée de l'Air et de l'Espace disposent déjà de centrale INS offrant des performances de dérive de « qualité navigation ». C'est par exemple le cas de la Sigma 95 du Rafale, selon Safran[97]. On peut donc estimer qu'un brouillage surface-air en ligne de vue, donc de 150-200 km de portée, n'aurait qu'un impact limité à une dérive de quelques centaines de mètres. Par ailleurs, en ce qui concerne les munitions, les AASM disposent d'un guidage terminal modulaire et le SCALP dispose d'un TERCOM.

Le problème central reste donc surtout la navigation des missiles de croisière ou encore des AASM et la capacité à exécuter de la frappe sur coordonnées. La phase en cours du programme OMEGA devrait fournir un premier élément de réponse.

2.3.3. Recommandations

À court-moyen terme, il serait sans doute intéressant de suivre la voie de l'USAF en renforçant les capacités antibrouillages, donc en dotant d'antennes CRPA les armes de précision à distance de sécurité et à l'avenir les *remote carriers* du SCAF.

[97] Voir fiche du constructeur : https://omnirole-rafale.com/wp-content/uploads/2018/05/Naviation-inertielle-Rafale.pdf

Quant aux solutions en cas d'indisponibilité de longue durée voire de neutralisation des GNSS, nous comprenons que l'armée de l'Air et de l'Espace étudie la mise en œuvre d'un système de visée stellaire élaborée par la Sodern, sélectionné par l'AID et la DGA, pour un emport sur ses grandes plateformes. Cela fait tout à fait sens pour une navigation haute altitude ou par beau temps mais le système resterait par exemple inopérant dans une mission de pénétration par des Rafale ou des NGF à basse altitude par mauvais temps. À moins que la solution ne réside là encore dans le réseau formé par le SGAF/SCAF : une ou plusieurs plateformes opère-rai(ent) à haute altitude et servirai(ent) de relais de données de positionnement/navigation, type pseudolites, qui seraient alors transmises pour recalage aux différents intervenants du cloud (NGF, *remote carriers*) via les futurs incréments du réseau CONTACT ou la nouvelle LDT haut débit, lesquels transmettraient par ailleurs les données de timing nécessaire aux tâches de synchronisation.

Il pourrait être par ailleurs opportun d'évaluer d'autres options de sources de PNT. Par exemple, l'une d'elles pourrait être à court terme le recours aux services PNT d'Iridium, dans la mesure où les AWACS bénéficient déjà des SATCOM de cette constellation.

Enfin, comme pour les feux terrestres, le développement d'une capacité de frappe HOJ, par exemple sur les munitions type A2SM ou sur un type de *remote carriers*, pourrait faire sens.

Sur le plan spatial, la résilience de la NAVWAR, en l'occurrence la contribution à la protection de Galileo ou encore d'EGNOSS, s'inscrit dans le cadre des mesures déjà engagées en matière de SSA et de protection des constellations. En matière de protection passive, si l'analyse de la seconde partie s'avère pertinente, il serait bien sûr opportun d'inclure dans la conception de la structure des prochains satellites de Galileo des éléments tels que des revêtements réflec-tifs permettant de compliquer plus encore le défi posé à une éventuelle menace de laser Terre-espace de grande puissance.

2.4. Le milieu maritime

2.4.1. Implications et situation des forces navales

Il convient sans doute de distinguer deux problématiques :

- Celle du milieu maritime aérien et de surface, qui se rapproche, avec des spécificités, de celles des autres milieux ;
- Celle, beaucoup plus spécifique, du milieu sous-marin.

A. Le milieu de surface et aérien

En ce qui concerne le milieu maritime de surface, de façon générale, l'indisponibilité ou le leurrage des GNSS peut entraîner des perturbations sur le fonctionnement de la navigation bien sûr, ce d'autant que le trafic maritime repose largement maintenant sur l'AIS largement dépendant du GPS ; mais aussi des radars et de certains moyens de communication. Faute de point de référence d'une part, de l'évolution lente de la plateforme d'autre part, la dangero-sité d'attaque d'usurpation se pose avec plus d'acuité encore que dans les autres milieux, comme les incidents et tests l'ont montré. Cependant, comme nous l'avons vu, il existe des

sources de PN de secours, à commencer par la navigation à la carte et au compas magnétique. Le plus efficace car plus rapide, est le système eLORAN… dans les zones où il est actif. Tout réside en fait dans la détectabilité de l'usurpation.

Les plateformes des forces navales sont équipées de centrales inertielles leur permettant de conserver leur navigation en cas de brouillage pendant plusieurs heures du P(Y), bientôt du M-Code, ou de ses équivalents chiffrés Galileo, contre les modes d'action d'usurpation par fabrication. Par exemple, la centrale INS Sigma 40 à gyrolaser de Safran, dont les différentes variantes dotent l'ensemble de nos navires de premier rang, disposerait d'une « qualité navigation » avec une dérive d'un MN comprise entre 8 et 24 heures sans recalage.

Ces plateformes restent toutefois potentiellement vulnérables au *Meaconing*. Cependant, le programme OMEGA devrait là encore à terme contribuer à limiter considérablement le risque. Le brouillage de puissance peut en revanche avoir un impact sur la synchronisation des radars et des SIC. Ainsi, la documentation en source ouverte sur la Liaison 22 ne mentionne pas de dispositif *antispoofing* spécifique. Elle fonctionne en TDMA sur le temps UTC fourni par le GPS, sauf si la plateforme est dotée d'une source spécifique. Ces vulnérabilités sont peut-être plus critiques encore en ce qui concerne les éléments embarqués : UAVs, hélicoptères, fast boat. Elles peuvent donc entraver significativement de multiples missions telles que les opérations de lutte ASM ou de reconnaissance et le ciblage au-delà de la ligne d'horizon.

Des degrés de menace sont aussi probablement à distinguer en fonction de la zone de ces opérations navales :

- Dès à présent, ces menaces concernent les espaces littoraux, les mers fermées et plus généralement les cas où un aéronef ou un navire de brouillage est en ligne de vue, tant en ce qui concerne la navigation que la synchronisation des radars et SIC ;
- À plus long terme, dans les cas 8-9 de la typologie supra, la menace sera présente pour l'action de haute mer, hors ligne de vue d'un bâtiment adverse, en particulier pour la synchronisation des radars et SIC.

Restent les perspectives d'utilisation de plus en plus massive de drones de surface (USV). Elles s'accompagnent du développement de multiples solutions de P/N en zone littorale combinant voire intégrant des radars de suivi des côtes, des systèmes à DVL ou encore des systèmes de navigation astronomique. Ces plateformes pourraient également recevoir comme celles des autres milieux des dispositifs CRPA. Une nouvelle fois, le problème reste probablement la navigation des petits USV en haute mer en absence prolongée de GNSS.

B. Le milieu sous-marin

Dans le cas des opérations sous-marines, il nous semble que la vulnérabilité liée à l'interdiction des GNSS serait moins critique, sans cependant être négligeable, dans la mesure où ces derniers restent utilisés pour le recalage des centrales inertielles. Comme évoqué en partie précédente sur la navigation acoustique, le développement de la *Seabed Warfare* pose moins la question de la résilience que celle de l'exploration ou de l'amélioration de solutions de PNT fondées sur les développements de la recherche bathymétrique.

2.4.2. Recommandations

Compte tenu de ces menaces, le choix du MINARM d'investir dans la navigation gravimétrique fait particulièrement sens. Il s'agit cependant bien là d'une solution opérationnelle de long terme. Les deux nouveaux bâtiments hydrographiques de nouvelle génération devant constituer les piliers de la Capacité hydro-océanographique future de la Marine au profit du SHOM mettront en œuvre, entre autres multiples autres capteurs, le gravimètre GIRAFE2 déjà évoqué. Ces deux navires doivent être mis en service en 2027 et 2028[98]. Ensuite, il faudrait compter avec les délais nécessaires aux réalisations des campagnes de levés par ces nouveaux moyens, au traitement des données et à la production cartographique. Par ailleurs, pour tirer parti de ces données, les bâtiments de la Marine devront eux-mêmes être dotés des capteurs appropriés. Enfin, qu'en est-il de la cartographie des zones de tension dans lesquelles ces navires ne pourront effectuer des levés ?

Plusieurs pistes complémentaires viennent à l'esprit. L'une d'elles serait probablement de rendre plus résilientes les plateformes aériennes comme les hélicoptères, drones et les petites embarcations qui peuvent être les premières victimes d'action de NAVWAR comme illustré par le cas iranien. Les doter par exemple de terminaux P3TS et d'antennes CRPA ferait sens.

Une autre mesure, de plus grande ampleur, résiderait dans le réinvestissement dans le LORAN et la transformation des installations en eLORAN. Elle offrirait un moyen de positionnement précis sur l'ensemble des mers fermées de l'arc de crise et l'Atlantique nord. Les opérations dans la profondeur des océans (Atlantique, Indien ou Pacifique) ne seraient cependant pas couvertes.

En matière de synchronisation, une piste pourrait être de rendre plus résiliente les capacités autonomes des grandes plateformes en les dotant d'une capacité de timing UTC propre, typiquement à une horloge atomique (par exemple une horloge au Césium permettant de conserver un temps stable à la microseconde près sur plusieurs mois). C'est d'ailleurs ce qu'ont fait les Britanniques sur le HMS *Prince of Wales*[99].

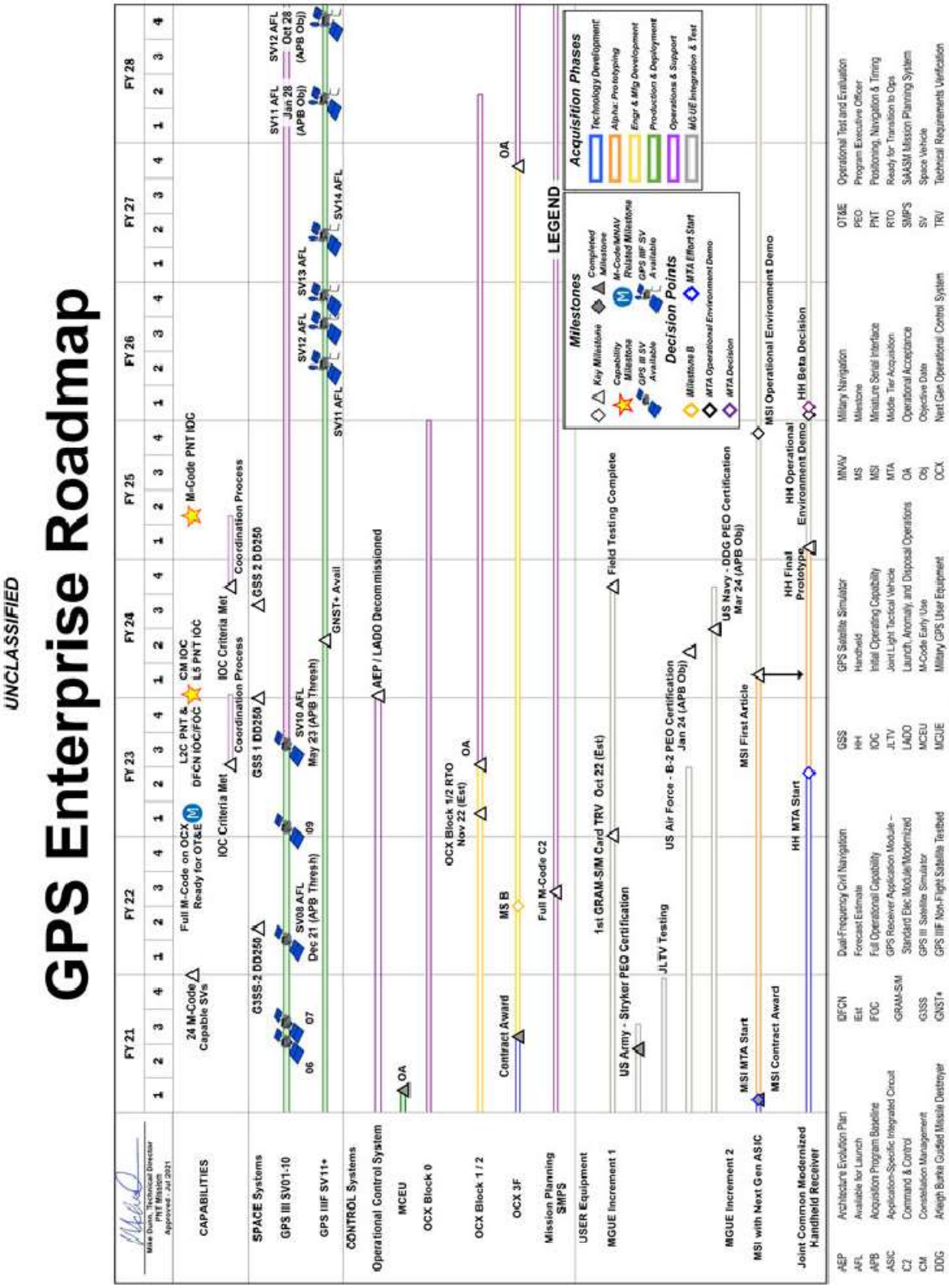
Enfin, on peut émettre l'idée, comme pour les autres milieux, d'une diffusion en réseau en étoiles, des données PNT les plus sures, provenant des plateformes les plus résilientes au sein du groupe naval.

---

[98] SHOM, Capacité Hydro-Océanographique Future (CHOF), présentation, mai 2021.

[99] « UK Royal Navy installs atomic clock on HMS Prince of Wales », *Naval Technology*, March 14, 2022 – https://www.naval-technology.com/news/uk-royal-navy-installs-atomic-clock-on-hms-prince-of-wales/

Annexe I FEUILLE DE ROUTE DU PROGRAMME GPS



Source : Tracy Cozzens, « Space Force releases new GPS Roadmap, doc changes », GPS World, January 20, 2022
https://www.gpsworld.com/space-force-releases-new-gps-roadmap-doc-changes/