LES JEUNES IHEDN

[RECHERCHE]

LA GUERRE DES ONDES

REPENSER L'APPROCHE STRATÉGIQUE SPATIALE FACE AUX NOUVELLES MENACES

Par Victoire Leglaive, Gaia Vezzosi & Killian Blatche
Groupe d'Études Scientifiques et Techniques

Ce texte n'engage que la responsabilité des auteurs. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.

SOMMAIRE

À PROPOS DE L'ARTICLE

Devenu un domaine stratégique, l'espace est confronté à des menaces invisibles qui entravent le bon fonctionnement des infrastructures orbitales. Notamment, les actes de *jamming* (brouillage) et *spoofing* (usurpation) des données transmises par les satellites mettent en péril les activités au sol. Les réalités contemporaines du contexte contesté, encombré, et conflictuel des orbites terrestres mettent ainsi à l'épreuve l'écosystème stratégique, légal, et matériel des activités spatiales. La surveillance spatiale devient une condition sine qua non au maintien de la liberté d'action, de la résilience, et de l'autonomie stratégique des activités européennes.

À PROPOS DES AUTEURS

Victoire Leglaive est élève ingénieure en double diplôme aux Mines d'Albi et à Cranfield University.

Gaia Vezzovi est étudiante en Master de Renseignement et Sécurité Internationale à King's College London.

Killian Blatche est diplômé d'un BAC+5 dans les domaines des réseaux, télécommunications et cybersécurité.

Dans l'écosystème spatial actuel, les systèmes satellitaires assurent des services critiques, notamment en matière de télécommunications, d'observation de la Terre ou de navigation. Parmi eux, les systèmes de positionnement par satellite, plus connus sous le nom *Global Navigation Satellite Systems* (GNSS), occupent une place centrale dans de nombreux secteurs civils et militaires. La navigation aérienne et maritime, la synchronisation des réseaux numériques et le bon fonctionnement de nos infrastructures essentielles reposent aujourd'hui, plus que jamais, sur la fiabilité de ces signaux.

Cependant, malgré un cadre juridique international fondé sur l'usage pacifique de l'espace, les évolutions géopolitiques récentes témoignent d'une militarisation croissante du domaine spatial. Les limites du droit spatial, conçu dans un contexte stratégique très différent, laissent aujourd'hui apparaître des zones grises qui favorisent le développement de nouvelles formes d'actions hostiles. Parmi celles-ci figurent les interférences visant notamment les systèmes GNSS, telles que le brouillage (*jamming*) ou l'usurpation de signal (*spoofing*).

Ces perturbations, de plus en plus fréquentes dans certaines régions du monde, constituent un enjeu majeur de sécurité pour les infrastructures dépendantes du positionnement et de la synchronisation satellitaire. Dans ce contexte, comprendre les mécanismes de ces interférences et les réponses techniques et stratégiques mises en place pour y faire face apparaît essentiel. Cet article propose ainsi d'analyser les vulnérabilités des systèmes GNSS face aux menaces contemporaines, tout en examinant le cadre juridique et les outils de surveillance spatiale permettant d'en limiter les risques.

Mise en situation :

Malgré un cadre juridique fondé sur l'usage pacifique de l'espace, les pratiques actuelles révèlent une militarisation croissante. Les limites du droit spatial

favorisent le développement de formes d'interférences techniques difficiles à encadrer juridiquement. Les perturbations des systèmes GNSS constituent aujourd'hui une illustration directe de ces dynamiques.

Cadre légal et stratégique

GNSS

Les systèmes de positionnement par satellite comme le GPS ou les constellations Galileo, GLONASS ou Beidou sont des infrastructures spatiales critiques. Elles permettent, grâce aux signaux émis par leurs satellites, de déterminer avec précision la localisation du récepteur sur Terre. Ces systèmes se sont généralisés, depuis une vingtaine d'années, pour fournir de nombreux services essentiels, notamment dans les transports ou bien dans l'informatique pour la synchronisation temporelle. Le fonctionnement de ces services est aujourd'hui menacé par une augmentation des perturbations des signaux GNSS.

Ces perturbations peuvent prendre différentes formes et provenir de différentes sources, à terre ou non, elles seront détaillées dans le chapitre II. Elles peuvent également être volontaires, avec par exemple un système pour brouiller le signal GNSS d'un véhicule, ou involontaires, telles la rupture de la protection d'un câble, créant un brouillage local.

Pour éviter ces perturbations, l'utilisation des fréquences est soumise à un cadre juridique précis et exigeant. En effet, en France, l'installation d'un émetteur de plus de 5 watts de puissance est soumise à autorisation et doit émettre sur une bande de fréquence préalablement attribuée. Le cadre légal national se base sur le CPCE, le Code des postes et des communications électroniques. Plusieurs agences sont chargées des missions de contrôle et de régulation : premièrement, l'Autorité de Régulation des Communications Électroniques, des Postes et de la distribution de

la presse (ARCEP) attribue les fréquences d'émission aux opérateurs de services hertziens. La seconde est l'Agence Nationale des Fréquences (ANFR), chargée d'autoriser l'implantation des installations radioélectriques et de leurs antennes, ainsi que de vérifier la compatibilité des fréquences pour éviter des « chevauchements » d'émissions. Elle assure également le maintien à jour du Fichier National des Fréquences (FNF).[1]

Régulièrement, l'ANFR mène des enquêtes à la suite de signalements de perturbations du spectre, allant du brouillage d'antennes 4G publiques, au brouillage GNSS sur un aéroport. Par exemple, en 2021, des perturbations GNSS sont repérées à proximité de l'aéroport de Marignane et attribuées à un véhicule professionnel, dont le conducteur souhaitait effacer la trace de ses trajets en manipulant son récepteur GPS. Aux yeux des experts de l'ANFR, au-delà du brouillage illégal du spectre, la localisation en zone aéroportuaire aggrave la faute. En effet, un brouilleur, même peu puissant, peut *« affecter des avions volant jusqu'à 2 000 m d'altitude, donc en pleine phase critique de décollage ou d'atterrissage »*[2]. Le conducteur interpellé encourt ainsi de six mois de prison et 30 000 € d'amende pour la possession et l'utilisation d'un brouilleur GNSS. Ce délit s'applique plus généralement à tout brouilleur d'ondes, que ce soit pour brouiller le wifi, la téléphonie mobile et le *GPS* (article L. 33-3-1 du CPCE). Il existe toutefois une dérogation uniquement dans le cadre d'activités de défense ou de sécurité intérieure.

Au niveau européen, un groupe de travail a été mis en place, sous le nom de *EU GNSS Interference Task Force* (EGITF). Il a pour but de repérer, comprendre et évaluer les risques des brouillages GNSS, de partager les bonnes pratiques et

[1] GABAY, C. Lutter contre les brouillages des systèmes de navigation par satellite [en ligne]. CNIG, 2021 [consulté le 18/02/2026]. Disponible sur : *https://cnig.gouv.fr/IMG/documents_wordpress/2021/11/20211015-VFinal-Lutter-contre-les-brouillages-des-systemes-GNSS-de-navig....pdf*.

[2] ANFR. *Brouillage d'ondes - l'ANFR mène l'enquête* [en ligne]. ANFR, 2022 [consulté le 05/03/2026]. Disponible sur : *www.anfr.fr/fileadmin/mediatheque/documents/brouillage/ANFR_25_ENQUETES-WEB-HD-2.pdf*.

expériences entre services spécialisés nationaux, dont l'ANFR fait partie. Le groupe travaille activement sur la constellation Galileo, mais anticipe également les problématiques de perturbation du signal sur la future constellation satellitaire de connectivité IRIS².

Spatial

Le traité de l'espace, adopté le 19 décembre 1966 via la résolution 2222 de l'Assemblée générale des Nations Unies, est l'un des principaux fondements juridiques sur l'exploration de l'espace extra-atmosphérique. Approuvé par ses trois dépositaires, les États-Unis, le Royaume-Uni, et l'Union Soviétique le 27 janvier 1967, le traité est aujourd'hui signé par 118 États, incluant 98 ratifications. Le traité porte non seulement sur l'espace extra-atmosphérique, mais aussi sur les autres corps célestes, telle la Lune.[3]

Cet important traité a permis la définition de règles juridiques pour l'exploration et l'utilisation de l'espace extra-atmosphérique. Ainsi, le traité convient que l'espace doit être librement exploré et utilisé par tous les États, aucun d'eux ne pouvant s'approprier ni déclarer sa souveraineté sur cette région. Il ancre plusieurs résolutions précédentes de l'ONU, notamment l'interdiction d'installer des bases et installations militaires ainsi que l'envoi, en orbite ou sur d'autres corps, d'armes nucléaires ou de destruction massive.

Plusieurs articles du traité mentionnent que l'espace extra-atmosphérique et les autres corps célestes peuvent être explorés et utilisés, mais uniquement à des fins pacifiques. Les États sont responsables des objets lancés, de leur propre chef ou par leurs entreprises nationales, ainsi que de la destinée de ces objets. En effet, si un objet lancé cause de quelconques dommages dans l'espace, sur d'autres corps

[3] Nation Unies. *Droit international de l'espace* [en ligne]. *UNOOSA*, 2017 [consulté le 15/12/2025]. Disponible sur : *www.unoosa.org/res/oosadoc/data/documents/2025/stspace/stspace61rev_3_0_html/st_space_61rev03F.pdf*.

ou sur Terre, l'État qui a procédé au lancement devra réparation envers l'État tiers impacté. Des clauses particulières, destinées aux cas où l'objet spatial n'est pas immatriculé dans le même État que celui ayant procédé au lancement, demandent une solidarité dans le partage des réparations.

Le traité impose l'immatriculation des objets spatiaux envoyés en orbite et au-delà[4]. L'État l'ayant lancé doit communiquer des informations sur l'objet lancé auprès du Secrétaire Général de l'Organisation des Nations Unies, incluant le numéro d'immatriculation, la date et lieu de lancement, les informations orbitales (période, inclinaison, apogée et périgée), l'État d'immatriculation, le propriétaire ou exploitant et la fonction générale de l'objet. Nous pourrions penser que ces informations publiques permettent un suivi orbital des objets spatiaux et qu'aucun État partie ne cache ses réelles intentions, mais ce serait ignorer plusieurs limites du traité.

Tout d'abord, les informations fournies aux Nations-Unies ne sont valables qu'au lancement de l'objet, aucune contrainte n'exige la communication de la position de l'objet dans le temps. Certains États apportent régulièrement des mises à jour sur la position des objets spatiaux sous leur registre d'immatriculation, mais ils les réalisent à leur libre discrétion. De plus, l'orbite d'un satellite à son lancement est sujette à une constante évolution naturelle due au freinage atmosphérique, mais peut également être modifiée par une opération motorisée afin d'effectuer du maintien à poste ou des manœuvres. Dans le cadre d'un remorqueur spatial civil comme les MEV[5], les manœuvres orbitales sont pacifiques, mais lorsqu'il s'agit d'un satellite militaire Russe comme Loutch/Olymp-K[6], repéré en 2020 effectuant

[4] Nations unis. « Online Index of Objects Launched into Outer Space ». *UNOOSA* [en ligne], s.d. [consulté le 03/03/2026]. Disponible sur : www.unoosa.org/oosa/osoindex/search-ng.jspx.
[5] « Space Logistics, Northrop Grumman », Northrop Grumman [en ligne], s.d. [consulté le 10/03/2026]. Disponible sur : *www.northropgrumman.com/what-we-do/space/space-logistics-services.*
[6] GRUSS, Mike. « Russian Luch Satellite Relocates — Next to Another Intelsat Craft ». *SpaceNews* [en ligne], 16/10/2015 [consulté le 10/03/2026]. Disponible sur : *spacenews.com/russian-luch-satellite-relocates-next-to-another-intelsat-craft/.*

des manœuvres à proximité d'autres satellites dans le but d'intercepter des télécommunications, la situation se complexifie. En effet, certains États mentent ou camouflent la réelle fonction des objets spatiaux lancés, avec soit une utilisation duale civile/militaire, soit sous couvert d'une fonction pacifique.

Ces limites du traité de l'espace montrent l'utilité d'un suivi des mouvements orbitaux et de la collecte de renseignement sur les objets lancés en orbite. Ce suivi est condensé dans l'acronyme SSA pour *Space Situational Awareness*, la veille de la situation spatiale. La définition et le rôle de la SSA seront détaillés dans le chapitre III.

La France s'est dotée en 2019 d'une stratégie de défense spatiale, en parallèle de la création du Commandement de l'Espace (CDE), introduisant pour la première fois la notion de SSA. L'objectif affiché est *« l'extension des capacités de connaissance de la situation spatiale »*[7]. Cette stratégie a été mise à jour en 2025, avec la stratégie spatiale 2025-2040 comportant un changement majeur pour la SSA. Précédemment, les capacités françaises s'étaient concentrées sur un suivi des orbites depuis la Terre avec des capteurs radar et des télescopes. Désormais, la France souhaite utiliser des moyens actifs avancés « dans et vers l'espace »[8]. L'objectif stratégique est de garantir l'appréciation de la situation spatiale française, mais également européenne, en anticipant les manœuvres spatiales. Pour atteindre cet objectif, la France souhaite moderniser et renforcer ses capacités de surveillance, avec l'installation de capteurs en outre-mer pour offrir un meilleur spectre de couverture sur plusieurs orbites d'intérêt. La coopération internationale, en particulier au niveau européen, est aussi désignée comme essentielle afin de joindre les technologies et données accumulées pour obtenir

[7] Ministère des armées. *Stratégie spatiale de défense 2019 – Synthèse* [en ligne]. DiCoD, 2019 [consulté le 05/03/2026]. Disponible sur : www.defense.gouv.fr/sites/default/files/cde_1/Synthese_SSD.pdf.
[8] SGDSN. *Stratégie nationale spatiale 2025-2040* [en ligne]. SGDSN, s.d. [Consulté le 05/03/2026]. Disponible sur : www.sgdsn.gouv.fr/files/files/Publications/Stratégie nationale spatiale_FR_0.pdf.

une image presque complète de l'environnement orbital, notamment au travers du partenariat *European Union Space Surveillance and Tracking* (EUSST)[9].

Spoofing et jamming : quels sont les risques contemporains ?

En septembre 2025, Eurocontrol ainsi que l'Agence de l'Union Européenne pour la Sécurité Aérienne (AESA) ont organisé un workshop afin d'établir un bilan sur les vulnérabilités des systèmes GNSS ainsi que des menaces émergentes pouvant porter préjudice à l'aviation civile.

Les données présentées à cette occasion montrent que les interférences GNSS sont désormais un phénomène durable. En 2024, d'après l'AESA, environ 30 % des événements relevaient du *spoofing* (falsification du signal) tandis que 70 % concernaient du *jamming* (brouillage). Si le brouillage reste majoritaire, la part importante du *spoofing* est particulièrement préoccupante, car il ne s'agit plus seulement d'une perte de signal, mais d'une altération délibérée de la position fournie à l'aéronef.

La répartition géographique des événements met clairement en évidence un lien avec les zones de conflits ou de fortes tensions militaires. L'Europe de l'Est, à proximité de la Russie et du conflit ukrainien, présente des zones de *jamming* sévère, parfois quasi permanent. La région de la mer Noire est également fortement touchée. Plus au sud, le Moyen-Orient, notamment autour d'Israël, du Liban, de la Syrie et de l'Irak, apparaît comme un foyer majeur de *spoofing*.

[9] Nordic Geodetic Commission. « EU GNSS Interference Task Force (EGITF) ». *NGC* [en ligne], s.d. [consulté le 18/02/2026]. Disponible sur : www.nordicgeodeticcommission.com/wp-content/uploads/2025/03/EU-Taksforce-GNSS-interference.pdf.

“Dans certains espaces aériens, les opérations en présence d’un GNSS compromis sont devenues une situation d’exploitation normale” nous dit même le rapport. Les interférences GNSS ne sont donc plus des anomalies isolées, mais un facteur de risque récurrent qui modifie durablement l’environnement de navigation de l’aviation civile européenne et augmente les risques pour les équipages et les passagers.

Jamming

Les systèmes GNSS (GPS, Galileo, etc.) sont devenus essentiels au fonctionnement de notre société. Au-delà de la navigation, ils constituent une source majeure de signaux de référence pour la synchronisation temporelle et pour de nombreux services de positionnement, de navigation et de temps (PNT). Télécommunications, réseaux électriques, transports, finance et aviation dépendent directement de la fiabilité de ces signaux. De plus, les attaques par brouillage se multiplient car elles sont techniquement accessibles : les équipements nécessaires sont relativement faciles à obtenir, et les instructions pour les utiliser circulent largement.

Le *jamming* correspond à une interférence volontaire visant à rendre un signal radio inutilisable. Il consiste à émettre un signal de forte puissance sur une fréquence identique ou proche de celle des signaux GNSS. Le brouilleur masque alors les signaux authentiques des satellites sous un bruit artificiel plus intense, empêchant le récepteur de les capter, de les suivre et de calculer une position fiable. Lors d’une telle attaque, le récepteur peut perdre totalement la navigation satellite ou afficher des dégradations et alertes multiples. La simplicité de mise en œuvre du brouillage, combinée à la dépendance croissante au GNSS, en fait une menace diffuse, peu coûteuse et aux effets potentiellement étendus, bien au-delà du seul domaine de la navigation.

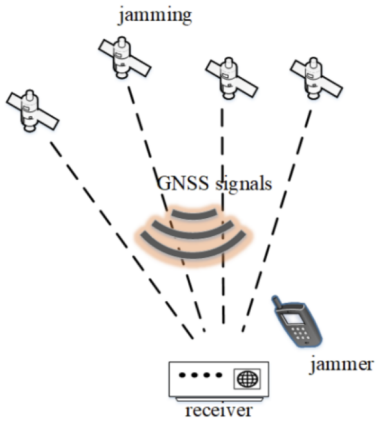


Schéma de principe de fonctionnement du *jamming*[10]

Il existe plusieurs types de *jamming* : brouillage par suppression et brouillage par leurre. Nous n'étudierons pas ici toutes les formes de brouillage qui existent. Prenons, par exemple, la forme la plus simple de *jamming*, le brouillage par suppression. Dans ce cas, le signal de navigation par satellite est supprimé par la transmission d'un signal de brouillage de forte puissance dans la bande de fréquences du signal de navigation par satellite.

$$J(t) = Acos(2\pi f_c t)$$

Où J(t) est le signal de brouillage, A est l'amplitude du signal de brouillage à fréquence unique et fc est la fréquence porteuse du signal de brouillage. On souhaite ici que :

$$J(t) \approx J_i$$

Où J_i est le signal initial que l'on souhaite brouiller.

Les méthodes actuelles les plus populaires de détection de *spoofing* et de *jamming* sont celles qui utilisent le *machine learning*. Néanmoins, ces techniques demeurent

[10] Radoš K., Brkić M. & Begušić D. « Recent Advances on Jamming and Spoofing Detection in GNSS, Applied Sciences ». *MDPI* [en ligne], 2024 [Consulté le 29/03/2026]. Disponible sur : https://www.mdpi.com/1424-8220/24/13/4210.

complexes à mettre en œuvre et sont encore majoritairement en phase d'expérimentation ou d'évaluation.

Spoofing

Le *spoofing* GNSS correspond à une attaque consistant à émettre des signaux destinés à tromper les systèmes de traitement de position ou de temps, afin qu'ils fournissent des données erronées. Concrètement, l'objectif est de faire croire au récepteur qu'il se trouve à un autre endroit tout en lui présentant des informations qui paraissent cohérentes.

L'effet d'une telle attaque sur un récepteur GNSS est particulièrement critique : l'attaquant ne se contente pas de perturber la navigation, il peut en prendre le contrôle en imposant une solution de position falsifiée. Les systèmes de navigation deviennent alors vulnérables à des erreurs invisibles pour l'utilisateur, avec des conséquences potentielles sur la sécurité des opérations et, plus largement, sur les activités humaines dépendantes du positionnement et du temps.

Le principe repose sur l'émission de faux signaux qui imitent les caractéristiques des signaux authentiques émis par les satellites. Ces signaux contrefaits sont généralement transmis avec une puissance supérieure à celle des signaux réels, afin que le récepteur les privilégie. Il commence alors à suivre ces "faux satellites" et calcule une position basée sur des informations manipulées. L'issue est une prise de contrôle de la solution de navigation du récepteur et une falsification de sa position.

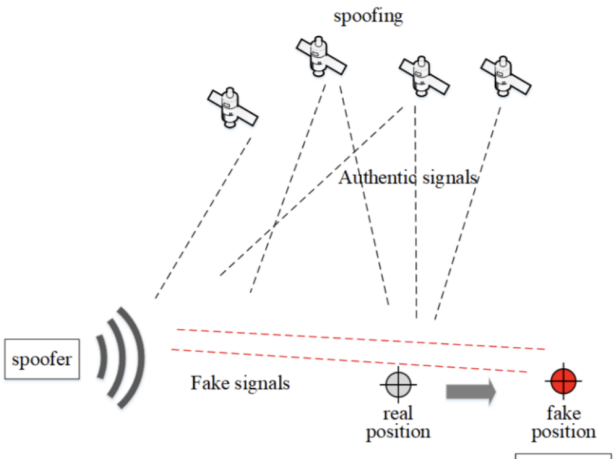
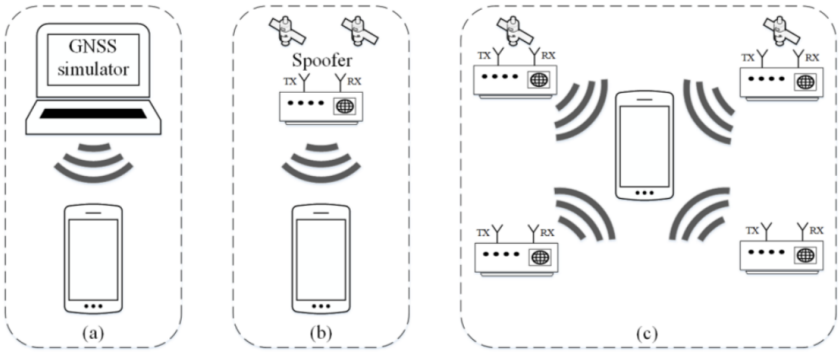


Schéma de principe du *spoofing*

Il existe plusieurs formes de *spoofing*, de complexité variable et, ici encore, nous allons nous intéresser à la plus simple. Cette dernière repose sur l'utilisation d'un simulateur de signaux GNSS capable de générer un scénario satellitaire artificiel et de l'émettre vers la cible. Ce type d'attaque peut être mis en œuvre avec du matériel relativement peu coûteux, ce qui le rend accessible. Il reste toutefois plus facile à détecter : pour supplanter les signaux réels, le signal frauduleux doit être émis avec une puissance élevée, et il présente souvent des incohérences, notamment un manque de synchronisation avec la constellation réelle.

Dans la pratique, ces attaques simples commencent fréquemment par un brouillage des signaux GNSS authentiques. Cette étape force le récepteur à perdre sa solution de navigation et à rechercher de nouveaux signaux. L'attaquant introduit alors les signaux falsifiés, que le récepteur peut accepter comme légitimes, basculant ainsi sur une position entièrement fabriquée.



Différents types d'attaque de spoofing, de la plus simple (a) à la plus complexe (c)

Dans le cas **(b)**, l'attaque repose sur un spoofer capable de générer et transmettre des signaux GNSS falsifiés vers le récepteur cible. En contrôlant des paramètres tels que le délai du code, le Doppler ou la puissance du signal, l'attaquant peut progressivement biaiser la solution de positionnement ou de temps du récepteur.

Dans le cas **(c)**, l'attaque est plus sophistiquée et utilise plusieurs émetteurs synchronisés autour de la cible. Cette configuration permet de reproduire une géométrie spatiale réaliste des satellites, rendant la détection plus difficile, notamment pour les méthodes basées sur la diversité spatiale ou l'angle d'arrivée.

Il existe néanmoins des technologies "*anti-spoofing*" ayant deux objectifs principaux :

- Tentatives de détection des attaques pour avertir les victimes que les systèmes de navigation et l'horloge ne sont pas fiables
- Le deuxième objectif est de rétablir une solution fiable et une solution de synchronisation.

Par exemple, il existe comme solution *anti-spoofing* basée sur le traitement du signal. Cette technologie essaye de trouver des incohérences ou interférences pendant l'usurpation de signal et *« détecte les sauts déraisonnables dans l'amplitude de la fréquence porteuse, la phase de codage et la phase de la fréquence porteuse, en particulier au début de l'attaque »*.

La connaissance de la situation orbitale est essentielle afin de détecter des comportements suspects ou anormaux. Cela inclut les potentielles déviations ou variation de signal d'un satellite victime de *jamming* ou de *spoofing*[11], le mouvement suspect de satellites qui pourraient porter des armes cinétiques ou électromagnétiques, le suivi de missiles, et les risques de collisions. Bien que la plupart des attaques de *jamming* et *spoofing* proviennent d'émetteurs au sol, le développement croissant de satellites furtifs réalisant des opérations de proximité (RPOs) n'exclut par leur future utilisation pour perturber les signaux des systèmes spatiaux. En 2023, le satellite russe Luch Olymp-2 avait notamment mis sous pression des satellites occidentaux par un rapprochement anormal, probablement afin d'intercepter les signaux de ceux-ci à des fins de renseignement (SIGINT).

La surveillance spatiale : un socle opérationnel

La surveillance spatiale, également nommée *Space Situational Awareness* (SSA) ou plus précisément *Space Surveillance and Tracking* (SST) permet la détection, l'identification, et l'estimation de trajectoire de satellites actifs, de débris, ou d'objets naturels. Devenue de grande importance aux forces armées en raison de la désignation de l'espace comme un domaine opérationnel, celle-ci permet à la fois la gestion sécuritaire des opérations spatiales en informant la gestion du trafic, mais également la détection de comportements anormaux ainsi que des capacités et activités d'autres États. Par exemple, les systèmes de pointe de SSA/SST peuvent attribuer un satellite à un État, établir sa catégorie et suivre ses activités en temps presque réel. La SST est réalisée traditionnellement par des infrastructures au sol, via des télescopes électro-optiques, des systèmes de suivi

[11] MENG L., YANG L., YANG W. & ZHANG L. « A Survey of GNSS Spoofing and Anti-Spoofing Technology, Remote Sensing ». *MDPI* [en ligne], 2022 [Consulté le 30/01/2026]. Disponible sur : https://doi.org/10.3390/rs14194826.

par radar, radiofréquence, ou encore laser. Néanmoins, celles-ci sont limitées dans leurs capacités de couverture orbitale, de précision de détection, et de granularité des données. Les systèmes de veille spatiale depuis les orbites sont une solution en essor, utilisant des capteurs optiques. Ces satellites de *space-based space surveillance* (SBSS) en orbite basse (LEO) sont souvent placés en orbite héliosynchrone afin de garder le Soleil en une position relative fixe d'aube ou de crépuscule, permettant l'observation d'autres satellites sans obstruction par aveuglement solaire.

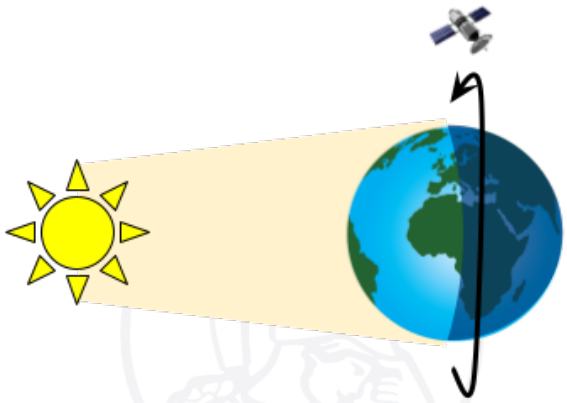


Schéma de satellite en orbite héliosynchrone (SSO).

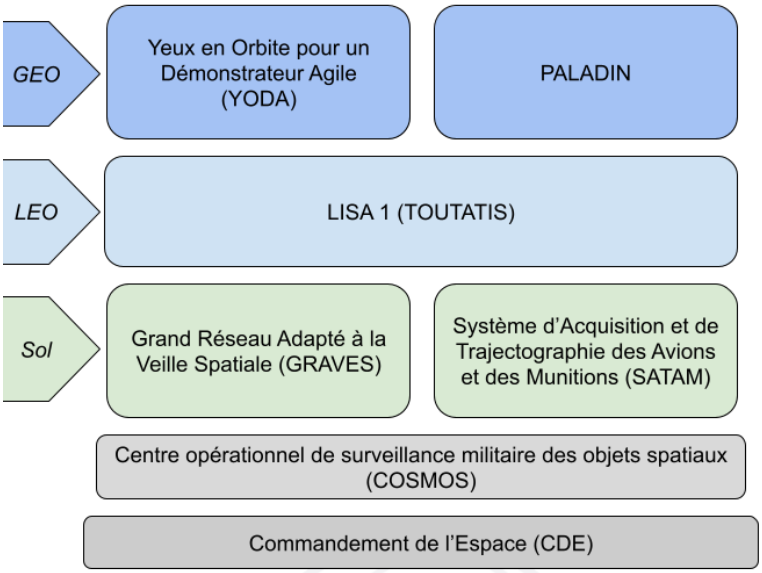
Au niveau européen, quinze agences spatiales nationales partagent leur infrastructure de SSA au sein du programme de partenariat EU SST, permettant une couverture orbitale conséquente. Ce programme *dual-use* centralise les données en un catalogue commun afin de les partager avec les États, les opérateurs, et autres acteurs publics et privés. Distincte des opérations de l'Union Européenne, l'Agence Spatiale Européenne (ESA) a son propre mandat de SSA au sein du *Space Safety Programme* (S2P), qui est toutefois centré sur le suivi d'astéroïdes, de débris, et la météorologie spatiale. La France a un rôle central dans les capacités européennes de SSA, étant le quatrième État au monde à s'être doté d'une capacité de surveillance par des outils diversifiés et pleinement intégrés dans la stratégie de défense spatiale. D'autres acteurs, tels l'Allemagne et

l'Italie, ont aujourd'hui atteint des capacités comparables, parfois supérieures à celles françaises par leur récence. En effet, la croissance quasi exponentielle des objets spatiaux et débris, la fréquence d'activités hostiles, et la volonté nationale et européenne d'acquérir une autonomie stratégique face aux États-Unis requièrent une modernisation et une expansion des capacités militaires françaises de SSA, en voie d'obsolescence.

L'écosystème français de veille spatiale

La France possède un écosystème militaire de surveillance de l'espace en expansion, sous le contrôle du Centre opérationnel de surveillance militaire des objets spatiaux (COSMOS) au sein du Commandement de l'Espace (CDE). L'intégration des informations de la SSA au sein des C2 de l'ensemble des forces armées ainsi que leur interopérabilité avec le programme EU SST et les systèmes de l'OTAN sont deux axes clés pour assurer une conduite optimale des opérations en tout milieu. Son infrastructure au sol est principalement composée du système radar bistatique GRAVES ainsi que du SATAM pour le suivi de trajectoire de munitions en LEO. Le COSMOS a aussi un droit d'usage des télescopes civils TAROT pour une observation optique des orbites. La surveillance depuis l'espace n'étant réalisée que par des systèmes civils à ce jour, plusieurs programmes militaires ont été mis en place ces dernières années pour un lancement en orbite d'ici la fin de la décennie. Notamment, le patrouilleur YODA permettra d'opérer une veille de l'orbite géostationnaire, tandis que le micro-satellite LISA-1, intégré au système d'intervention en LEO TOUTATIS, procurera les données de veille à son binôme. Enfin, la DGA a lancé en août 2025 le projet PALADIN pour une surveillance en GEO

non seulement passive, via des capteurs, mais également active, par des inspections de proximité, qui sont néanmoins coûteuses en énergie[12].



Projection des capacités militaires françaises de veille spatiale à l'horizon 2028.

Étude de cas : fonctionnement du radar GRAVES

Le système GRAVES est un radar bistatique, signifiant que son émetteur est situé à un endroit distinct de son receveur : dans ce cas, l'émetteur est proche de Dijon tandis que le receveur, composé d'une centaine d'antennes sur un disque au sol, est sur le plateau d'Albion[13]. Ce fonctionnement permet de récupérer le signal émis même si l'objet visé est furtif : en effet, certains satellites ou objets, se voulant indétectables, redirigent les ondes reçues pour que celles-ci ne retournent pas à

[12] Direction générale de l'armement. « La DGA notifie l'accord-cadre PALADIN à la société Infinite Orbits ». *DGA* [en ligne], 13/08/2025 [Consulté le 15/01/2026]. Disponible sur : www.defense.gouv.fr/dga/actualites/dga-notifie-laccord-cadre-paladin-societe-infinite-orbits.

[13] MICHAL, Thierry ; EGLIZEAUD, Jean-Pierre & BOUCHARD, Jacques. « GRAVES: The new French System for Space Surveillance ». *ESA* [en ligne], 2005 [Consulté le 05/03/2026]. Disponible sur : https://conference.sdo.esoc.esa.int/proceedings/sdc4/paper/122/SDC4-paper122.pdf.

leur radar d'origine. La présence d'un récepteur dans une autre localité permet d'assurer la collecte du signal retour, et est ainsi très pertinent en milieu militaire.

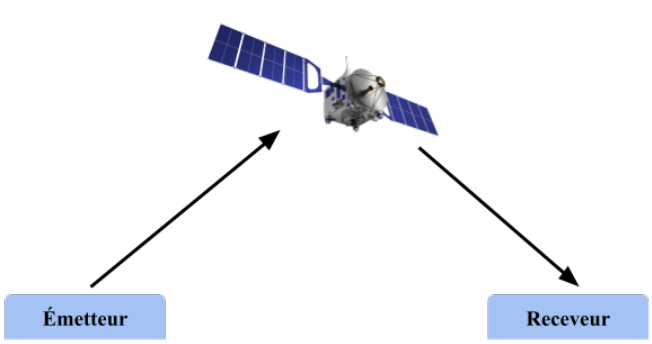


Schéma simplifié du fonctionnement d'un radar bistatique de SSA.

L'estimation de l'orbite de l'objet se fait en utilisant l'effet de Doppler : la variation de la fréquence entre son émission et sa réception due au mouvement du satellite permet d'estimer sa vitesse et sa direction. Cela est comparable au changement du son d'une ambulance en mouvement entendue par une personne en une position fixe, qui permet d'établir si le véhicule s'approche ou s'éloigne. La réitération de ces estimations au cours de plusieurs passages de l'objet permet de comprendre son orbite précise et potentiellement son identification par comparaison avec un catalogue répertoriant satellites et débris.

La formule ci-dessous résume le fonctionnement de l'effet de Doppler, où la valeur recherchée est la vitesse de l'objet v_o , qui explique la variation entre la fréquence originellement émise f et la fréquence reçue f' , alors que la vitesse des ondes v est constante et celle du récepteur v_r est à 0.

$$f' = \frac{v + v_r}{v + v_o} f$$

Modernisation des capacités françaises

Le programme d'expansion des capacités Action et Résilience Spatiale (ARES) de la DGA vise à une modernisation des services de SSA. Au-delà de simples rénovations, les systèmes sols GRAVES et SATAM seront éventuellement remplacés par un radar en bande ultra haute fréquence imageur de satellites AURORE, permettant une meilleure résolution malgré un évanouissement plus rapide de l'énergie. L'acquisition de télescopes militaires est également en projet, se concentrant sur l'intégration de technologies de pointe telles la spectroscopie et la polarimétrie. Pour la SBSS, les démonstrateurs TOUTATIS et YODA seront suivis du système EGIDE à l'horizon 2030. La recherche se concentre sur ces systèmes pour améliorer leur agilité, leur résilience, et la qualité des informations recueillies. Pour ces dernières, des efforts sont conduits afin d'avancer au-delà des systèmes optiques utilisés jusqu'ici pour diversifier les données. L'intégration de radars, systèmes d'analyse de radiofréquences ou de lasers de surveillance sur des satellites demeure toutefois un défi technique à ses débuts. Le transfert de données inter-satellites et des satellites vers le sol est aussi sujet à une transformation vers une distribution quantique de clé (QKD) afin de sécuriser les liens et résister aux attaques cyber. En pratique, la résilience de la France se développe non seulement par une diversification géographique via les territoires d'outre-mer afin d'obtenir une meilleure couverture orbitale, mais également par l'accueil de petites et moyennes entreprises du *New Space* dynamiques et innovantes qui permettront aux forces armées françaises de bénéficier rapidement de technologies spatiales de haut niveau[14].

[14] SGDSN. *op. cit.*

Conclusion

Le volume et la sophistication des nouvelles menaces à l'encontre de l'architecture orbitale remettent en question les capacités européennes matérielles et régulatoires à y répondre adéquatement. Le *jamming* et le *spoofing* sont notamment devenus un élément clé de la guerre hybride, révélant la vulnérabilité des systèmes de synchronisation et de positionnement. Le manque de clarté et précision des cadre réglementaires internationaux, européens, et nationaux regardant le droit de l'espace et des télécommunications permet un laissez-faire conséquent qui continue de croître. La détection précoce d'anomalies dans les orbites terrestres est un prérequis opérationnel critique afin de permettre une réponse rapide aux attaques et par extension construire la résilience européenne. Appliqué au domaine stratégique spatial, le brouillard de la guerre clausewitzien se manifeste par l'incomplétude de l'information de SSA, le flou juridique, et le brouillage littéral des signaux. Les stratégies spatiales européennes et nationales ont ainsi récemment marqué un tournant en mettant l'appui sur les besoins d'augmenter les capacités souveraines de défense, notamment par l'adoption de technologies innovantes.






publication@jeunes-ihedn.org