Etude d'Impact GNSS

Référentiel à l'usage des utilisateurs des services GNSS

22.10.2021

Version Initiale

SI06 - V1.0

|  |  |
| --- | --- |
| Rédigé par | Aurélien FOURNET, FDC  César EL-BEZ, FDC  Franck MANGIN, FDC |
| Approuvé par © | Franck MANGIN, FDC |

Table des Matières

[1 Introduction 4](#_Toc85550011)

[2 Qu’est-ce que le GNSS 5](#_Toc85550012)

[2.1 Principes de fonctionnement 5](#_Toc85550013)

[2.1.1 Composantes des systèmes GNSS 5](#_Toc85550014)

[2.1.2 Principe de positionnement et d’estimation du temps par GNSS 6](#_Toc85550015)

[2.2 Mesures de performance du GNSS 7](#_Toc85550016)

[2.3 Principaux systèmes existants 10](#_Toc85550017)

[3 Menaces pesant sur les GNSS 14](#_Toc85550018)

[3.1 Identification des sources d’altération de l’information GNSS 14](#_Toc85550019)

[3.1.1 Segments Sol et Spatial 16](#_Toc85550022)

[3.1.2 Signal (Segment Utilisateur) 18](#_Toc85550023)

[3.1.3 Récepteur (Segment Utilisateur) 21](#_Toc85550024)

[3.2 Identification des profils d’attaquants 22](#_Toc85550025)

[3.3 Caractérisation des menaces 23](#_Toc85550026)

[3.3.1 Définition d’échelles communes 23](#_Toc85550027)

[3.3.2 Segments Sol et Spatial 25](#_Toc85550028)

[3.3.3 Signal (Segment Utilisateur) 27](#_Toc85550029)

[3.3.4 Récepteur (Segment Utilisateur) 35](#_Toc85550030)

[3.3.5 Synthèse de la caractérisation 36](#_Toc85550031)

[4 Contremesures en cas de menaces GNSS 38](#_Toc85550032)

[4.1 Contremesures techniques 38](#_Toc85550033)

[4.2 Contremesures procédurales – Rôle de l’ANFR 39](#_Toc85550034)

Table des Annexes

[Annexe 1 Etudes d’impact GNSS par secteur 41](#_Toc85550039)

[Annexe 2 Abréviations et Sigles 42](#_Toc85550040)

[Annexe 3 Suivi des éditions 50](#_Toc85550041)

Liste des Figures

[Figure 1 : Segments GNSS 5](#_Toc85550042)

[Figure 2 : Triangulation appliquée au GNSS 6](#_Toc85550043)

[Figure 3 : Intercorrélation entre le code du récepteur et le code du satellite 7](#_Toc85550044)

[Figure 4: Zones de services des différents systèmes SBAS (source : GSA) 12](#_Toc85550045)

[Figure 5 : Classification des sources d’altération des GNSS 15](#_Toc85550046)

[Figure 6 : Organisation de la direction du contrôle du spectre de l’ANFR 40](#_Toc85550047)

Liste des Tableaux

[Tableau 1: Exemple de valeur de sensibilité suivant le secteur considéré 9](#_Toc85550048)

[Tableau 2 : Caractéristiques des différentes constellations globales GNSS 11](#_Toc85550049)

[Tableau 3: Caractéristiques des différents systèmes SBAS (source : GSA) 12](#_Toc85550050)

[Tableau 4 : Sources potentielles d'interférences non intentionnelles 20](#_Toc85550051)

[Tableau 5: Echelle des niveaux de gravités pour un récepteur GNSS 23](#_Toc85550052)

[Tableau 6: Echelle des niveaux de taille des zones impactées par la menace 24](#_Toc85550053)

[Tableau 7: Echelle des niveaux de durée des menaces 24](#_Toc85550054)

[Tableau 8: Echelle des niveaux de probabilités d'occurrences pour une menace 24](#_Toc85550055)

[Tableau 9: Synthèse et caractérisation des menaces sur le GNSS 36](#_Toc85550056)

# Introduction

De nombreuses entités publiques et privées utilisent des données PNT (Positionnement, Navigation et Temps) générées par des moyens de navigation par satellite. Ces moyens, regroupés sous le terme GNSS (Global Navigation Satellite System), sont exposés à des menaces susceptibles de conduire à une dégradation des informations globales de synchronisation temporelle et de géolocalisation utilisées par les opérateurs des entités concernées.

Dans ce contexte, la société FDC a été mandatée par la Fédération de Recherche FIRST-TF, ci-après « le CNRS » pour conduire une étude destinée à améliorer la compréhension des effets d’une altération des informations GNSS sur le fonctionnement de systèmes utilisés par plusieurs Secteurs d’Activité d’Importance Vitale (SAIV) de la société civile et étudier son impact.

Pour atteindre cet objectif, une analyse initiale basée sur les résultats d’études antérieures a été complétée par des recherches bibliographiques ciblées et l’organisation de consultations auprès d’acteurs majeurs de plusieurs Secteurs d’Activité d’Importance Vitale.

Le présent document constitue un référentiel à l'usage des chefs de projets utilisateurs des services fournis par le GNSS. Son objectif est de faciliter la conduite ultérieure d’analyses de risque à partir d’études d’impacts présentées pour chaque secteur.

Ce référentiel est constitué du présent document (non classifié) complété de plusieurs documents (Diffusion Restreinte/Spécial France) distincts annexés. Le présent document introduit les GNSS et caractérise les principales catégories de menaces pesant sur ces systèmes. Chacune de ses annexes est dédiée à l’étude d’impact des altérations du GNSS pour un des secteurs couverts par cette étude.

# Qu’est-ce que le GNSS

## Principes de fonctionnement

### Composantes des systèmes GNSS

Un système GNSS est composé de trois segments comme illustré sur la Figure 1 ci-dessous.

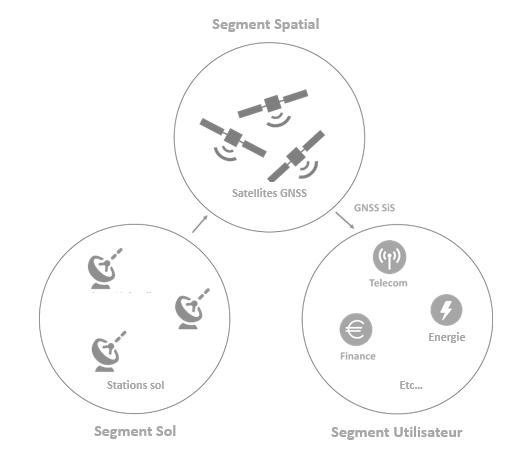


Figure 1 : Segments GNSS

* Le segment spatial désigne les constellations de satellites transmettant en continu des signaux de mesure de distances dans l’espace (SiS) ;
* Le segment sol suit les satellites et leur transfère régulièrement des informations sur leurs positionnements ainsi que des corrections à destination de leurs horloges atomiques (raccordement de chaque horloge satellite à l'échelle de temps globale de la constellation GNSS). Les informations de positionnement des satellites sont ensuite datées et transmises aux utilisateurs sous forme de « messages de navigation » intégrés aux SiS ;
* Le segment utilisateur désigne les récepteurs utilisant les signaux envoyés par les satellites (SiS) afin de calculer leurs données de Positions, de Vitesse et de Temps (PVT).

### Principe de positionnement et d’estimation du temps par GNSS

La localisation par GNSS repose sur le principe de triangulation basé sur une estimation des distances séparant le récepteur de chacun des satellites visibles. Ces distances sont obtenues à partir du calcul du temps séparant l’émission et la réception d’un signal satellitaire, sachant que ce dernier se propage à la vitesse de la lumière. Pour calculer sa position, l’utilisateur doit donc également avoir connaissance du temps GNSS utilisé par les satellites.

Une mesure GNSS consiste donc à calculer quatre variables : les trois variables de position du récepteur plus l'écart de temps entre la référence du récepteur et l'horloge embarquée à bord du satellite. Quatre satellites sont donc à minima nécessaires pour réaliser une mesure GNSS.

On notera que si on considère connue la différence de référence temporelle du récepteur et des satellites, trois satellites suffisent pour positionner l’utilisateur. Même si trois sphères s’interceptent en deux points distincts, une des solutions peut toujours être invalidée car la position ou la vitesse qui lui sont associées peuvent être considérées comme aberrantes (non positionnée sur la surface de la Terre, etc.).

La figure ci-dessous illustre le principe de triangulation appliqué au GNSS.

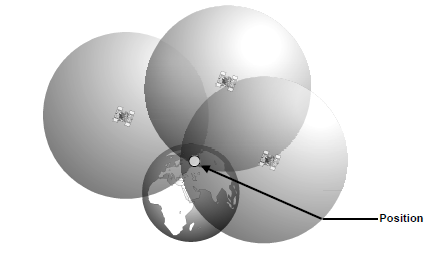


Figure 2 : Triangulation appliquée au GNSS

Les satellites transmettent deux types de données : les codes PRN (Pseudo Random Noise) et les messages de navigation. Les codes PRN sont utilisés pour le calcul des distances récepteur-satellites et permettent d’identifier les satellites. Un même récepteur est ainsi capable de recevoir les signaux de différents satellites. Les messages de navigation contiennent, quant à eux, diverses informations comme la position du satellite émetteur, son état, des données atmosphériques, le paramètre de raccordement de l’horloge du satellite à l’échelle de temps globale de la constellation GNSS. Ces informations permettent en particulier de corriger certaines erreurs affectant le calcul de la distance géométrique parcourue par un signal entre un satellite et le récepteur.

La position des satellites doit être continuellement surveillée afin d’assurer l’exactitude de la mesure GNSS. Pour ce faire, les orbites des satellites sont continuellement contrôlées par le segment sol. Chaque satellite reçoit donc fréquemment des corrections de l’estimation de sa position, qu’il intègre au message de navigation.

Déterminer le temps de trajet de l’onde avec exactitude est également primordial car, sa vitesse de propagation étant proche de celle de la lumière, la moindre erreur sur cette mesure entraine une incertitude importante sur la distance récepteur-satellite calculée. A titre d’exemple, une erreur d’une microseconde sur la mesure du temps de parcours entraine une erreur de 300 m sur le calcul de la distance parcourue par le signal.

Pour assurer un niveau d’exactitude adéquat des mesures de distance, le récepteur génère tout d’abord les codes émis par chacun des satellites poursuivis, ces codes binaires étant en effet prédéfinis et propres à chaque satellite. L’application du principe d’inter corrélation entre les codes générés et reçus permet au récepteur de déterminer l’époque d’arrivée du signal dans son référentiel. Dès lors, l’écart de temps entre les deux époques peut être calculé. Cet écart de temps, corrigé de la distance géométrique ainsi que d'autres sources d'erreurs, permet de mesurer l'écart de temps entre la référence du récepteur et l'horloge du satellite ou l'échelle de temps de la constellation.

Ainsi, l’exactitude de la mesure du temps de propagation dépend également de la qualité de la corrélation entre les codes émis par le récepteur et les codes correspondants émis par les satellites (voir Figure 3).



Figure 3 : Intercorrélation entre le code du récepteur et le code du satellite

La détermination de la position exacte des satellites est également délicate puisque les satellites suivent une trajectoire quasi elliptique. Ainsi, il est également nécessaire de continuellement corriger l’estimation de leurs positions pour assurer la précision requise du calcul de la position du récepteur. Chaque satellite reçoit donc fréquemment la correction de l’estimation de sa position qu’il intègre au « message de navigation » envoyé à l’utilisateur.

## Mesures de performance du GNSS

Afin d’évaluer les conditions d’utilisation de l’information GNSS, les paramètres suivants de mesure de performance ont été définis :

* **Incertitude de la mesure GNSS** : paramètre non négatif qui caractérise la dispersion des valeurs attribuées à la valeur vraie de la grandeur (position ou temps) que l’on veut mesurer avec le récepteur GNSS. Il peut être l'écart-type des mesures (ou un de ses multiples), en m pour la position, en s pour le temps ;
* **Exactitude de la mesure GNSS** : Désigne l’étroitesse de l’accord entre la valeur mesurée par un récepteur GNSS et la valeur vraie de la grandeur (position ou temps) que l’on veut mesurer. Les exigences sur l’exactitude des mesures GNSS dépendent fortement des applications et sont souvent exprimées sous forme statistique comme la combinaison d’une incertitude-type de la mesure (95ième percentile) et d’une erreur de justesse de la mesure (biais de mesure). L’exactitude de la mesure GNSS concerne soit les informations de positionnement horizontal, soit les informations de positionnement vertical, soit les informations de temps. Ces différentes exactitudes sont définies ci-dessous :
* **Exactitude de la position horizontale**: estimation statistique de l’étroitesse de l’accord entre la position horizontale mesurée par le récepteur GNSS et la position horizontale vraie de l’utilisateur ;
* **Exactitude de la position verticale :** estimationstatistique de l’étroitesse de l’accord entre la position verticale mesurée par le récepteur GNSS et la position verticale vraie de l’utilisateur. Cette exigence est applicable lorsque le guidage vertical est requis comme par exemple pour les approches dans l’aviation civile ;
* **Précision de la mesure** : ce terme ne fait plus partie du vocabulaire international de la métrologie à cause de son utilisation courante trop large. Cependant ce terme reste largement employé par de nombreux utilisateurs du GNSS lors de l’expression de leurs besoins. Il se peut donc que ce rapport utilise le terme de précision notamment lors des chapitres identifiants les « besoins et usages des opérateurs majeurs ». L’usage du terme précision sera alors à interpréter comme un ordre de grandeur indiquant l’amplitude maximale (issue de la combinaison biais et incertitude) de l’écart entre une mesure absolue du récepteur GNSS (position ou temps) et une référence (position vraie ou échelle de temps GNSS) tolérée par une même application ;
* **Intégrité :** Désigne la mesure de la confiance dans les informations de position ou de temps estimées par le récepteur GNSS. Ce paramètre est généralement exprimé comme la probabilité que l’erreur de position estimée par le récepteur GNSS dépasse une certaine limite préalablement définie sans que l’utilisateur en soit averti. La mesure de cette intégrité dépend fortement de la criticité de l’application concernée. En effet, plus l’application est critique, plus l’intégrité tend à être définie par la surveillance d’un ensemble important de paramètres mesurables.
* **Niveau de protection :** Désigne les limites de l’erreur statistique permettant de borner l’information GNSS calculée par le récepteur ;
* **Limite d’alerte :** Désigne la tolérance d’erreur d’un paramètre au -delà de laquelle une alerte sera émise par le système ;
* **Temps d’alerte :** Définit le temps maximal autorisé entre l’apparition d’une défaillance et le moment où l’utilisateur est informé ;
* **Risque d’intégrité :** Désigne le fait que les valeurs calculées par le récepteur GNSS puissent être en dehors des seuils limites de tolérance définis mais que l’information soit considérée comme disponible et qu’aucune alerte ne soit émise par le système avant la fin du temps d’alerte. Pour les systèmes critiques, le risque d’intégrité peut être défini comme le taux de risque tolérable qui est dérivé de l’analyse de risque de l’application.
* **Disponibilité :** Désigne le pourcentage de temps où l’information GNSS peut être traitée par l’utilisateur. Les exigences en termes de disponibilité varient fortement selon les applications concernées mais, en générale, elles sont comprises entre 95% et 99.9%. C’est l’un des paramètres de performance les plus importants pour les applications critiques. Il existe deux différents types de disponibilité :
* La disponibilité système qui désigne le pourcentage de temps où le GNSS permet à l’utilisateur de traiter son information ;
* La disponibilité globale qui prend en plus en compte les performances du récepteur et l’environnement de l’utilisateur.
* **Continuité :** Capacité de fournir sans interruption la performance requise durant une opération une fois cette dernière démarrée. La continuité est généralement exprimée comme le risque de discontinuité ;
* **Sensibilité GNSS :** Désigne la force minimale du signal GNSS à l’antenne détectable par le récepteur (exprimé en dBW ou en dBm)[[1]](#footnote-1). La sensibilité GNSS dépend du secteur d’activité considéré. Le tableau suivant donne certaines valeurs de sensibilité :

|  |  |  |  |
| --- | --- | --- | --- |
|  | Aviation | Maritime | Automobile |
| Sensibilité (usuelle) | -135 dBm (acquisition)  -140 dBm (poursuite) | -130 dBm (acquisition)  -135 dBm (poursuite) | -147 dBm (acquisition)  -162 dBm (poursuite) |

Tableau : Exemple de valeur de sensibilité suivant le secteur considéré[[2]](#footnote-2)

* **Robustesse :** En lien avec le leurrage et le brouillage, la robustesse est un paramètre qualitatif permettant de qualifier le type d’attaque ou d’interférence qu’un récepteur est capable de mitiger. Ces mitigations peuvent inclure l’authentification de l’information pour assurer à l’utilisateur que le signal reçu provient d’une source valide. La notion de robustesse inclus les sous paramètres suivants :
* **L’authenticité de l’information** qui définit un niveau de garantie que l’information fournie par le système de positionnement a été calculée à partir de signaux réels. Le leurrage par radio fréquence peut affecter un système de positionnement, lui faisant produire de fausses données ;
* **La robustesse aux interférences**qui définit la capacité du système de positionnement à opérer sous certaines conditions d’interférence et à maintenir le service de positionnement au niveau exigé ;
* **Traçabilité à l’UTC :** Les laboratoires nationaux de métrologie assurent une « traçabilité métrologique » à l'UTC de leur échelle de temps UTC(k) au sens de la norme ISO 17025-2017. La traçabilité au sens de la norme ISO 17025-2017 n’est pas assurée par les services GNSS. Les mesures GNSS ne permettent donc pas d’assurer une traçabilité validée à l'UTC. Dans le cadre de cette étude, les besoins en traçabilité à l’UTC n’impliqueront pas nécessairement une traçabilité au sens de la norme ISO 17025-2017.

## Principaux systèmes existants

Les signaux GNSS peuvent être fournis par de multiples systèmes, incluant des constellations globales ou régionales et des systèmes d’augmentation SBAS (Satellite-Based Augmentation System) assurant une diffusion de corrections via des satellites géostationnaires.

Les constellations globales actuelles sont les suivantes :

* **GPS** : Le premier GNSS, totalement opérationnel depuis 1995, est géré par le département de la défense américain. Il est actuellement en cours de modernisation avec le déploiement de nouveaux satellites GPS III ;
* **GLONASS** : Le GNSS russe, totalement opérationnel depuis 2011, est géré par les forces de défense aérospatiales russe. La dernière génération de satellites, GLONASS-K est entrée en service en février 2016 ;
* **Galileo** : C’est le système GNSS européen actuellement en cours de déploiement. En plus du service ouvert de haute qualité basé sur des signaux émis dans les bandes E1 et E5, Galileo est également la première constellation GNSS à mettre à disposition un lien retour pour les utilisateurs en détresse. Galileo propose également d’autres capacités uniques comme une fonction d’authentification du message de navigation (OS-NMA) ainsi qu’un signal de navigation crypté mis en œuvre dans un service d’authentification commercial (CAS). OS-NMA et CAS représentent les premières protections contre le leurrage mises à disposition de tous les utilisateurs civils du GNSS. Galileo va également permettre un accès gratuit à un service de haute précision, le HAS (High Accuracy Service). Enfin, Galileo intègre un service régulé, le PRS (Public Regulated Service), réservé aux utilisateurs autorisés par les gouvernements pour les applications sensibles nécessitant un haut niveau de continuité de service ;
* **BeiDou (Phase 3) ou BDS-3** : Le GNSS chinois est actuellement en cours de déploiement dans le but de remplacer l’actuel système régional. BeiDou est géré par le bureau chinois des satellites de navigation. Avec le système de positionnement régional, BeiDou représente aujourd’hui la plus grande constellation de satellites.

Le tableau ci-dessous détaille les caractéristiques principales des constellations de chacun de ces systèmes :

Tableau 2 : Caractéristiques des différentes constellations globales GNSS

| Paramètre | GPS | GLONASS | Galileo | BeiDou |
| --- | --- | --- | --- | --- |
| Période orbitale | 11h58m | 11h15m | 14h04m | 12h37m |
| Hauteur orbitale | 20 200 km | 19 100 km | 23 222 km | 21 150 km |
| Inclinaison | 55° | 64.8° | 56° | 55° |
| Nombre de plan orbitaux | 6 | 3 | 3 | 6 |
| Nombre de satellites | 24 opérationnels et 6 de rechange | 21 opérationnels et 3 de rechange | 24 opérationnels et 6 de rechange | 27 MEOs + 5 GEOs + 3 IGSOs |
| Cadre de référence | WGS-84 | PZ90 | GTRF | CGCS2000 |
| Temps de référence | GPS Time  (GPST) | GLONASS Time (GLONASST) | Galileo System Time (GST) | BeiDou Time  (BDT) |
| Niveau de performance | Précision horizontale moyenne (95%) < 9 m  Précision verticale moyenne (95%) < 15 m  Précision temporelle moyenne 40 ns[[3]](#footnote-3) | Précision horizontale moyenne (95%) 5m  Précision verticale moyenne (95%) 10m[[4]](#footnote-4)  Précision temporelle moyenne non renseignée | Précision horizontale moyenne (95%) < 4m (Galileo Open Service)  Précision verticale moyenne (95%) < 8m (Galileo Open Service) [[5]](#footnote-5)  Précision temporelle moyenne  30 ns (Galileo Open Service)[[6]](#footnote-6) | Précision horizontale moyenne (95%)  10m  Précision verticale moyenne (95%)  10m[[7]](#footnote-7)  Précision temporelle moyenne  50 ns[[8]](#footnote-8) |

En plus de ces constellations globales, il existe plusieurs systèmes d’augmentation permettant d’augmenter l’exactitude de l’information GNSS. Parmi ces systèmes, les SBAS (Satellite Based Augmentation Systems) délivrent en temps réel des corrections permettant d’accroitre l’exactitude des mesures GNSS tout en garantissant leur intégrité. Initialement développés dans les années 1990 pour introduire le GPS dans le domaine de l’aviation civile, leur utilisation est en train de s’étendre à de nombreux autres secteurs comme le ferroviaire. Il existe aujourd’hui quatre SBAS opérationnels (WAAS aux Etats-Unis, MASA au Japon, GAGAN en Inde et EGNOS en Europe) et cinq SBAB additionnels en cours de développement (SDCM en Russie, BDSAS en Chine, A-SBAS pour l’ASECNA, KASS en Corée du Sud et SPAN en Australie et Nouvelle-Zélande). La figure suivante représente ces différents systèmes et leur zone de service :

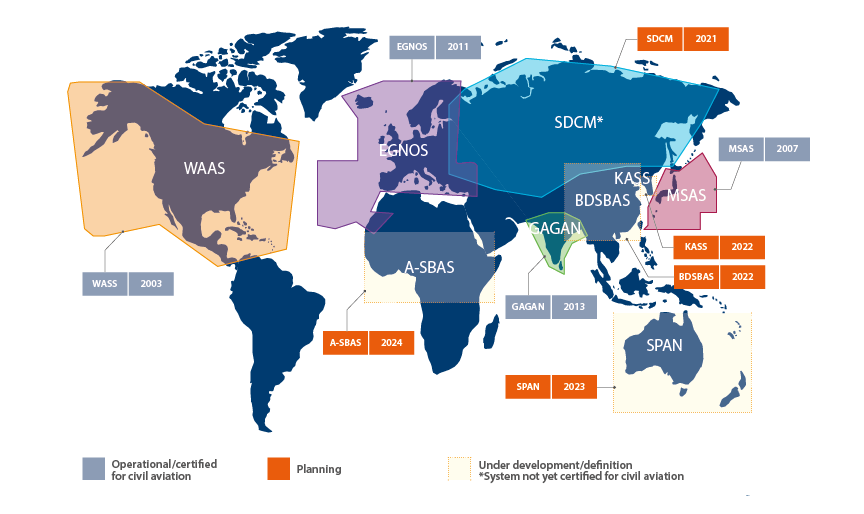


Figure : Zones de services des différents systèmes SBAS (source : GSA)

Les principales caractéristiques des systèmes SBAS sont données par le tableau ci-dessous :

Tableau : Caractéristiques des différents systèmes SBAS (source : GSA)

| Nom | Précision | Constellations supportées | Détenu par |
| --- | --- | --- | --- |
| A-SBAS | N/A | Actuellement : GPS Future : GPS + Galileo | ASECNA |
| BDSBAS | Horizontal : < 5 m Vertical : < 8 m | Actuellement : BDS + GPS + GLONASS Future : BDS + GPS + GLONASS + Galileo | Chine |
| EGNOS | Horizontal : < 1 m Vertical : < 1.5 m | Actuellement : GPS Future (EGNOS V3) : GPS + Galileo | Union Européenne |
| GAGAN | Horizontal : 1.5 m Vertical : 2.5 m | GPS | Inde |
| KASS | Horizontal : < 1 m Vertical : < 1.7 m | GPS | Corée |
| MSAS | < 2 m | Actuellement : GPS Future (MSAS V4): GPS + GLONASS + Galileo + BeiDou + QZSS | Japon |
| SDCM | Horizontal : 0.5 m Vertical : 0.8 m | Actuellement : GPS + GLONASS Future : GPS + GLONASS + Galileo + BeiDou | Russie |
| SPAN | < 1 m | Actuellement : GPS Future : GPS + Galileo | Australie et Nouvelle-Zélande |
| WAAS | Horizontal : <1 m Vertical : < 1.5 m | GPS | Etats-Unis |

# Menaces pesant sur les GNSS

L’objectif de ce paragraphe est de caractériser l’ensemble des menaces pesant sur les GNSS, chaque menace étant liée à un type altérations de l’information GNSS, d’origine naturelle, ou produite intentionnellement ou non par un attaquant.

Dans les paragraphes suivants sont identifiés les sources d’altérations potentielles des GNSS et, le cas échéant, les profils des responsables de ces attaques. Les menaces correspondantes sont ensuite caractérisées.

## Identification des sources d’altération de l’information GNSS

Les signaux ouverts du GNSS peuvent être facilement altérés. Les nombreuses sources potentielles d’altération, intentionnelles ou non, sont répertoriées dans la Figure 5 ci-dessous. Elles sont présentées plus en détail dans les paragraphes suivants en fonction du segment GNSS concerné par l’altération.

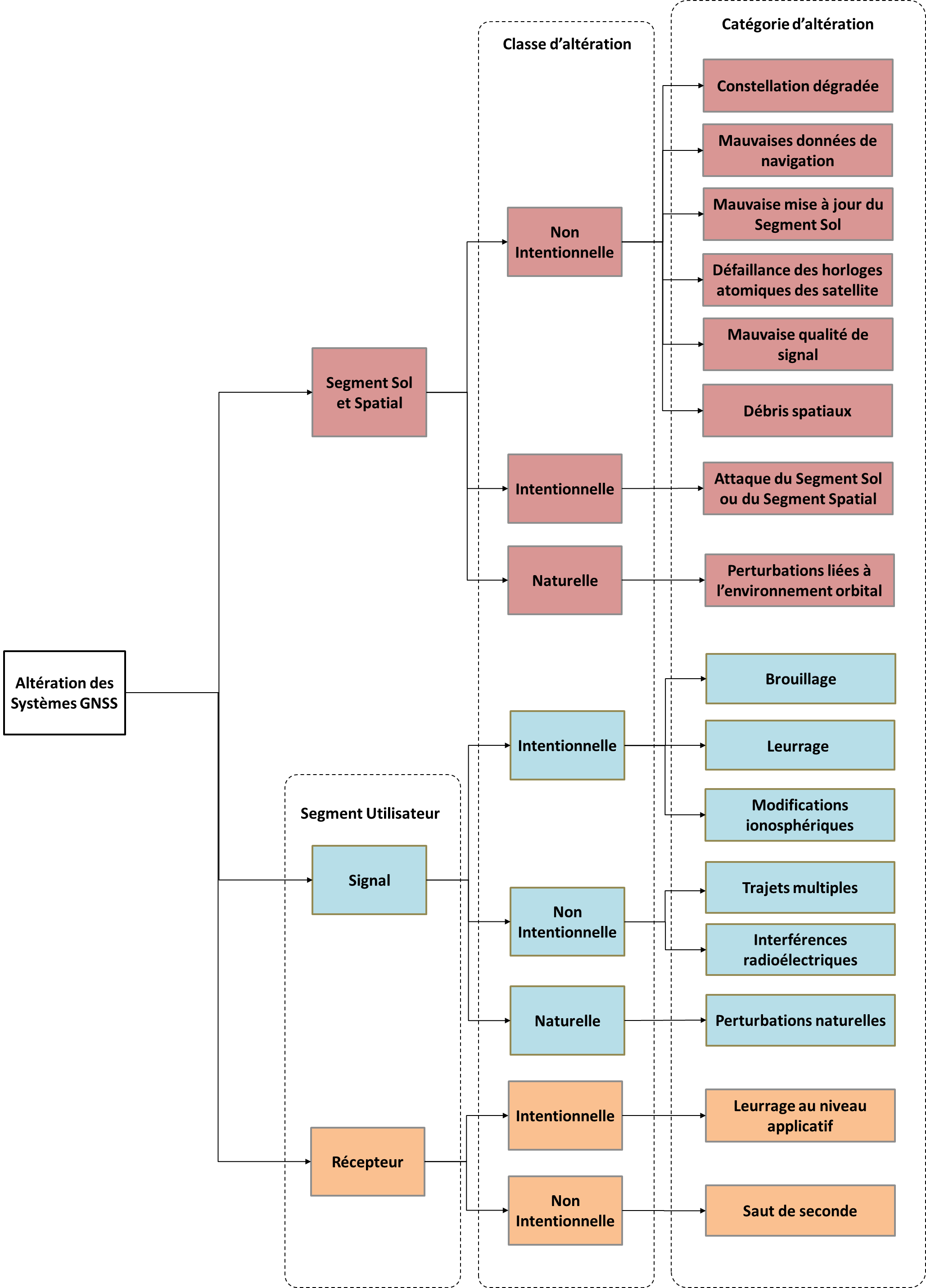
**

Figure 5 : Classification des sources d’altération des GNSS

### Segments Sol et Spatial

#### Non intentionnelle

Les principales altérations que peuvent subir les segments spatial et sol d’un GNSS, sont les suivantes :

* **Constellation dégradée** : il s’agit d’une altération à long terme liée à un manque de satellites fonctionnels au sein d’une même constellation. Ce manque pourrait par exemple être lié à des pannes et/ou des avaries sur les satellites, ou à une dégradation de performance des satellites les plus anciens combinée à des retards dans la livraison des satellites nouvelle génération (ce type d’altération a affecté la constellation GLONASS au début des années 2000) ;
* **Mauvaises données de navigation** : lorsque des données de navigation erronées ou obsolètes sont téléchargées puis diffusées par les satellites GNSS, les récepteurs les utilisant fournissent alors des informations de position et de temps erronées aux utilisateurs ;
* **Mauvaise mise à jour du segment sol** : des erreurs de mise à jour au niveau du segment sol peuvent entraîner des pannes sur certains systèmes informatiques et à l’extrême, conduire à une indisponibilité totale de la constellation GNSS jusqu’à l’identification et la résolution du problème ;
* **Défaillance des horloges atomiques des satellites (sauts et dérives d’horloge)**[[9]](#footnote-9): Le bon fonctionnement du GNSS dépend des performances en précision des horloges atomiques embarquées sur les satellites (mesurée sur 48 heures). Ces horloges peuvent en effet, en vieillissant, présenter des modes de défaillances comme des sauts de fréquence engendrant des dérives linéaires de phase. Un saut de fréquence peut avoir pour conséquence un changement brutal du signal transmis sans notification préalable avec des dérives de phase pouvant être difficiles à détecter et corriger depuis le sol car très faibles et parfois proches des effets d'un mouvement relatif entre satellites et récepteur GNSS. Un exemple de défaillance d'horloge est celui du PRN 23 le 1er janvier 2004 qui a introduit des erreurs allant jusqu'au kilomètre ;
* **Mauvaise qualité de signal** : Un défaut dans la modulation ou la génération du signal au niveau des satellites peut se traduire par la diffusion d’un signal de mauvaise qualité susceptible d’entraîner une réponse imprévisible des récepteurs au niveau utilisateur ;
* **Débris spatiaux** : Plus de 500 000 débris spatiaux gravitent autour de la terre à des vitesses pouvant atteindre les 28 000 km/h. Ces vitesses sont assez importantes pour que même des débris de très petite taille puissent endommager un satellite ou tout autre engin spatial. Le nombre croissant de ces débris spatiaux augmentent d’autant les dangers potentiels pour les satellites GNSS, lors de leurs lancements ou même sur leurs orbites.

#### Intentionnelle

Le segment sol des systèmes GNSS est conçu pour résister à des attaques de type militaire, il peut toutefois présenter des vulnérabilités résiduelles face à certaines actions terroristes ou cyberattaques. En effet, la résistance des systèmes GNSS aux types d’attaques menées dans le cadre de conflits militaires est essentiellement assurée par de la redondance. Ces mesures ne protègent toutefois pas ces systèmes GNSS contre des actions terroristes ou des cyberattaques coordonnées.

Le segment spatial des systèmes GNSS présente également des vulnérabilités à des attaques intentionnelles qui pourraient être conduites à partir du sol ou de l’espace. Ces attaques correspondent à des types d’armement particuliers qui peuvent être classées en plusieurs catégories :

* Armes à énergie cinétique
* Armes à énergie dirigée (lasers, radio-fréquence)
* Armes à faisceaux de particules

Les menaces intentionnelles sur les segments sol et spatial ne sont pas traitées plus en détail dans le cadre de la présente étude.

#### Naturelle

**Perturbations liées à l’environnement orbital** : Des évènements solaires extrêmes peuvent potentiellement avoir un impact sur le bon fonctionnement des satellites GNSS. De tels incidents peuvent les affecter de manière temporaire ou irréversible. Ces évènements peuvent être classés en plusieurs catégories :

* **Eruption solaire[[10]](#footnote-10) :** elle se manifeste par une variation soudaine, rapide et intense de luminosité. Une éruption solaire se produit lorsque l’énergie magnétique accumulée dans l’atmosphère solaire est soudainement libérée. Le rayonnement correspondant est alors émis sur quasiment l’ensemble du spectre électromagnétique ;
* **Tempête de radiation[[11]](#footnote-11)** : Les tempêtes de radiation solaires sont le plus souvent provoquées par des éruptions magnétiques accompagnant les éruptions solaires. Ces éjections provoquent l’accélération de particules chargées positivement jusqu’à des vitesses très élevées. En atteignant la Terre ces protons pénètrent dans la magnétosphère qui protège la planète des particules magnétiques plus faibles en énergie. Une fois dans la magnétosphère, ces particules sont guidées le long des lignes de champs magnétiques et pénètrent dans l’atmosphère au niveau des pôles Nord et Sud ;
* **Tempête géomagnétique / Ejection massive de masse coronale ou évènement de Carrington[[12]](#footnote-12) :** Une tempête géomagnétique est un bouleversement majeur de la magnétosphère terrestre qui se produit lors d’un important transfert d’énergie entre un vent solaire (flux de plasma constitué essentiellement d'ions et d'électrons qui sont éjectés de la haute atmosphère du Soleil) et l’environnement spatial terrestre. Les plus grandes tempêtes géomagnétiques s’accompagnent d’éjections de masse coronale solaire (Coronal Mass Ejections / CMEs) à l’occasion desquelles environ un milliard de tonnes de plasma solaire, et le champ magnétique correspondant, pourraient être envoyés en direction de la Terre. Le 23 juillet 2012 une gigantesque tempête solaire, potentiellement très dangereuse, a frôlé la Terre. De telles tempêtes solaires sont totalement imprévisibles et pourraient avoir lieu une fois tous les 100 ou 200 ans.

### Signal (Segment Utilisateur)

#### Intentionnelle

Les altérations qualifiées d’intentionnelles sur le signal reçu au niveau du segment utilisateur, peuvent être classées en trois catégories : le brouillage, le leurrage et les modifications ionosphériques.

* **Le brouillage :** Il peut être défini comme une attaque réalisée par émission de signaux de type bruits sur les fréquences utilisées par les systèmes GNSS. Le brouillage est le plus souvent généré par des civils mal intentionnés ou mal informés dont la motivation est de protéger leur vie privée ou d’éviter de payer les frais d’utilisation d’un service, mais il peut également être mis en œuvre par des criminels l’utilisant pour commettre leurs méfaits, notamment pour le vol de biens protégés par des pisteurs GNSS (voitures de luxe, cargaisons, ...). Le brouillage illégal vise à empêcher l’accès aux services GNSS en perturbant la réception et la poursuite des signaux, et dès lors la fourniture des données temps et de position par les récepteurs GNSS. Bien que la commercialisation et l’utilisation de brouilleurs GNSS, même de faible puissance, soit illégale dans la plupart des pays, on en trouve en vente sur internet. Ces brouilleurs (également appelés dispositifs de protection de la vie privée) commercialisés sur Internet, produisent des types de signaux variés mettant en œuvre différentes techniques de modulation (signal à balayage, signal pulsé), sur différentes bandes de fréquences (fréquence unique, bande étroite ou large) et avec des puissances différentes. Ces brouilleurs peuvent simultanément interférer avec plusieurs bandes de fréquences GNSS. De plus en fonction de sa puissance, et avec une différence possible dans les plans horizontal et vertical, un brouilleur peut avoir une portée allant de quelques mètres à plusieurs kilomètres voire centaines de kilomètres ;
* **Le leurrage :** Il consiste en l’émission de faux signaux GNSS destinés à fausser les données de position, de vitesse ou de temps, fournies aux utilisateurs par les récepteurs. Les signaux ainsi émis peuvent être totalement créés ou bien résulter de la falsification de signaux GNSS préalablement enregistrés. La plus simple des attaques par leurrage consiste à recevoir des signaux GNSS et à les retransmettre sans aucune modification, on appelle cette technique le « meaconing ». Une méthode de complexité intermédiaire consiste à enregistrer un signal GNSS, à modifier les informations contenues dans le message de navigation et à retransmettre le signal de leurrage ainsi généré. Enfin, les attaques les plus élaborées consistent à générer à la fois les modulations GNSS et les données de navigation. Ces signaux peuvent être transmis avec ou sans synchronisation des codes d’étalement simulés et réels des satellites. Néanmoins, plus le signal GNSS généré est synchronisé de façon précise avec celui du satellite visé, plus l’attaque par leurrage sera efficace ;
* **Les modifications ionosphériques** : Ces modifications peuvent être générées par des explosions nucléaires. En effet, l’énergie libérée par une telle explosion crée des arcs hautement ionisés dans l’atmosphère susceptibles d’impacter significativement le fonctionnement des radars, des systèmes de télécommunication ainsi que des récepteurs GNSS. Les opérations GNSS peuvent être en particulier touchées des semaines durant, en raison de la propagation de ces anomalies dans le temps.

Des formes particulières de brouillage et de leurrage caractérisées par des attaquants de type « Nation » avec des enjeux de type sécuritaire ou géopolitique ont été mis en œuvre ces dernières années avec une certaine régularité (ex : indisponibilité du signal GPS dans la zone touchée par la guerre des Balkans[[13]](#footnote-13), brouillages du GPS par la Corée du Nord[[14]](#footnote-14), attaques du GNSS en Russie et en Syrie[[15]](#footnote-15), ou encore brouillage du signal en Ukraine[[16]](#footnote-16)). Ces opérations de suppression ou de perturbation d’accès au service GNSS peuvent avoir différentes motivations et reposer sur différents concepts d'opération. Il peut par exemple s’agir d’attaques de type militaire sélective (visant uniquement les services GNSS ouverts) ou non discriminante, menée sur une zone géographique définie. Le concept NAVWAR (NAVigation WARfare) de l’OTAN est un exemple de perturbation sélective de l’utilisation du GNSS qui vise à contrer les opérations ennemies sans pour autant affecter les opérations alliées. Comme dans d'autres domaines de la guerre électronique, la perturbation des capacités PNT fournies par les GNSS est souvent faite avant toute phase de combat « classique » ou pour la défense d’installations stratégiques. Il est à noter que cette forme particulière de brouillage/leurrage couvre également les mesures de perturbation de la réception des signaux GNSS prises pour la protection des VIP du monde politique.

#### Non intentionnelle

En matière de réception des signaux GNSS, deux principales altérations non intentionnelles peuvent être retenues : les trajets multiples, les interférences radioélectriques (Radio Frequency Interferences ou RFI).

* **Les trajets multiples** : c’est le phénomène par lequel un signal donné arrive au récepteur par plusieurs chemins après de multiples réflexions et réfractions. Les trajets multiples représentent l’une des plus importantes sources d’erreurs dans les systèmes GNSS. Les causes principales des trajets multiples sont la proximité entre l’antenne du récepteur GNSS et une infrastructure réfléchissante, combinée avec des signaux GNSS reçus avec une faible élévation par rapport à l’horizon. Ce phénomène affecte aussi bien les mesures de phases que de code, et les effets varient en fonction des fréquences reçues ;
* **Les interférences radioélectriques :** Elles peuvent être définies comme des émissions radio par un équipement radioélectrique en défaut, non conforme ou utilisé de manière non conforme, ou bien par des émissions de parasites électromagnétiques par un équipement radioélectrique ou électrique. De telles transmissions non intentionnelles peuvent provenir de rayonnement d’harmoniques ou de signaux parasites générés dans des bandes adjacentes par des émetteurs commerciaux défectueux ou dont l’installation a été mal réalisée. Un cas de figure consiste en un défaut d’isolation d’une antenne GNSS[[17]](#footnote-17) (souvent vieillissante et présentant des défauts d’adaptations en impédance) entrainant une réémission partielle du signal GNSS reçu. Ces signaux réémis se comportent comme des interférences radioélectriques pour les antennes GNSS proches. Un tel cas de figure peut même avoir des effets similaires à ceux d’une attaque GNSS de type « meaconing » sur les antennes GNSS situées à proximité. Cette catégorie d’altération englobe également les répéteurs GNSS « indoor » mal confinés, susceptibles de générer des perturbations de type leurrage en transmettant ses signaux à l’extérieur, causant ainsi la réception de signaux GNSS erronés par les récepteurs environnants. Les répéteurs mal configurés/mal confinés représentent un risque émergent d’interférence qui ne peut que croître dans le futur. Ces types d’interférences radioélectriques peuvent perdurer plusieurs jours jusqu’à l’identification de leurs origines et le remplacement du système défectueux.

Plusieurs sources potentielles d'interférences non intentionnelles vis-à-vis du GNSS peuvent être identifiées. Le Tableau 4 ci-dessous présente les principales d’entre elles.

Tableau 4 : Sources potentielles d'interférences non intentionnelles

| Type de signal | Gamme de fréquence (MHz) | Niveau de puissance | Localisation | Bandes de fréquence concernées |
| --- | --- | --- | --- | --- |
| TV (UHF) | 500-860 | Elevé | Mondiale | E5/L5, L2, E6, E1/L1 |
| CT2/+ | 864-948 | Faible | Europe du Nord | E1/L1 |
| DAB | 1452-1492 | Elevé | Europe, Canada, potentiellement mondiale | E1/L1, E6 |
| GSM | 824-960 / 1710-1990 | Moyen | Mondiale, principalement Europe et Amérique du Nord | E1/L1 |
| TDMA, IS-54 | 854-894 /  1850-1990 | Moyen | Amérique du Nord, Centrale et Russie | E1/L1 |
| CDMA, IS-95 | 824-894 | Moyen | Principalement Amérique du Nord, Extrême-Orient, Australie | E1/L1 |
| DECT | 1880-1900 | Faible | Europe, Australie, Russie, Amérique Centrale et du Sud | E1/L1 |
| PHS | 1895-1918 | Faible | Amérique du Nord et Extrême-Orient | E1/L1 |
| UMTS /WCDMA | 1900-2170 | Moyen | Mondiale | E1/L1 |
| Bluetooth | 2402-2495 | Faible | Mondiale | E1/L1 |
| WLAN (IEEE802.11b) | 2410-2483 | Faible | Mondiale | E1/L1 |
| UWB | 1000-3000 | Faible | Mondiale | E1/L1, L2, E6, E1/L1 |
| 4G LTE | 1500-1700 | Elevé | Mondiale | E1/L1 |
| 5G[[18]](#footnote-18) | 700 /3500 | Elevé | Mondiale | E1/L1, L2, E6, E1/L1 |
| Ligado (5G IoT network in the L-band)[[19]](#footnote-19) | 1526-1536 / 1627.5- 1637.5 / 1646.5 – 1656.5 | Moyen (9.8dbW limite) | Amérique du Nord | E1/L1 |

#### Naturelle

Les altérations sur les signaux GNSS peuvent également être d’origine naturelle comme en particulier les phénomènes de **scintillations ionosphériques**.

Parmi les perturbations naturelles envisageables, les phénomènes de scintillation ionosphériques sont en effet les plus critiques et leurs effets varient en fonction de nombreux facteurs tels que les saisons ou la position géomagnétique. Ces phénomènes affectent la précision du positionnement GNSS et peuvent même entrainer une perte de signal durant des épisodes particulièrement intenses, en particulier dans les régions de basse latitude.

### Récepteur (Segment Utilisateur)

#### Intentionnelle

L’utilisation de simulateurs de signaux RF (Voir §3.1.2.1) n’est pas l’unique ni le plus simple moyen de leurrer une application GNSS. Des méthodes impliquant **la couche applicative** des récepteurs existent également.

#### Non intentionnelle

Le message de navigation des satellites GNSS intègre un paramètre permettant de relier le temps GPS au temps UTC (Temps Universel Coordonné). Cette relation est assurée grâce à l’utilisation de secondes intercalaires. Le processus de mise en œuvre de ces secondes intercalaires, prévoit que l'équipement utilisateur prend en compte la notification d’un futur saut de temps lié aux secondes intercalaires (ΔtLSF) en l’associant avec le numéro de semaine (WNLSF) et le numéro de jour (DN) à la fin desquelles la seconde intercalaire devient valide.

Le fonctionnement d’un récepteur GNSS peut être gravement affecté voir interrompu par un saut de seconde intercalaire. Même lorsque qu’un saut de temps est planifié par les opérateurs d’un système GNSS, cet évènement sera considéré comme une altération pour le bon fonctionnement de leurs équipements par la plupart des utilisateurs et fabricants de récepteurs GNSS. Appréhender une seconde intercalaire (c’est à dire une minute qui ne durerait pas 60 secondes) est un défi technique et des stratégies doivent être mises en œuvre pour éviter des pannes dans les applications PNT.

## Identification des profils d’attaquants

Les profils d'attaquants du GNSS identifiés dans le cadre de la présente étude sont décrits ci-dessous. Il est à noter que ces attaques peuvent être intentionnelles ou non.

* **Nations** : États employant des personnes qui collectent des informations de manière professionnelle et commettent des attaques sur le GNSS pour leur gouvernement ;
* **Groupes terroristes** : les terroristes sont politiquement motivés et ont leur propre agenda politique qu'ils utilisent pour sélectionner des cibles. Ce profil d’attaquant peut vouloir brouiller le GNSS sur une zone fixe importante en utilisant par exemple des petits brouilleurs en nombre ;
* **Groupes criminels organisés** : le crime organisé cible des informations ou des biens qui ont de la valeur pour eux et qui peuvent être convertis en argent. Ces biens peuvent être des voitures de luxe, des cargaisons de valeur, etc., protégés par des « trackers » GNSS dont les criminels veulent perturber le fonctionnement. Ce profil d’attaquant peut également vouloir brouiller le GNSS sur une zone fixe plus importante en utilisant par exemple des petits brouilleurs en nombre ;
* **Pirates (amateurs ou professionnels)** : les pirates professionnels et amateurs ont généralement le même intérêt que le crime organisé mais interviennent dans une logique plus individuelle ;
* **Employés (mécontents ou malhonnêtes)** : les employés peuvent attaquer les entités ou les infrastructures dans lesquelles ils travaillent pour diverses raisons (par exemple pour l'argent, une déception professionnelle etc.) ;
* **Individus (malveillants et/ou peu conscients des conséquences de leurs actions) :** les particuliers utilisent des récepteurs GNSS dont ils peuvent vouloir perturber le fonctionnement, par exemple en cas de relations commerciales avec des prestataires de services (modèle de paiement à l'utilisation), afin de protéger leur vie privée ou pour dissimuler une activité salariée non déclarée. La protection de leur vie privée peut également les mener à utiliser des brouilleurs anti-drones (cas des VIP du monde du sport/spectacle). Lors de l'utilisation de brouilleurs destinés à perturber leurs propres récepteurs GNSS, ces citoyens affecteront également les équipements de réception GNSS à proximité ;
* **Propriétaires d’équipements radioélectriques** **et électroniques** : certains équipements radioélectriques et électroniques peuvent être à l’origine d’émissions perturbant la réception des signaux GNSS de façon non intentionnelle. On peut les classer en plusieurs catégories :
* Equipements en défaut ;
* Equipements non conformes ;
* Equipements utilisés de manière non conforme ;
* Equipement émettant en excès des parasites dans la bande GNSS.

## Caractérisation des menaces

L’objectif de ce paragraphe est de caractériser les principales menaces pesant sur les GNSS. Les menaces considérées sont classées par rapport au type d’altération auquel elles correspondent..

### Définition d’échelles communes

Afin de caractériser de la manière la plus homogène possible les différentes menaces envisageables pour le GNSS, il est proposé d’adopter quatre échelles communes de niveau pour les paramètres suivants :

* Gravité au niveau du récepteur GNSS
* Taille de la zone impactée
* Durée de la menace
* Probabilité d’occurrence

Tableau 5: Echelle des niveaux de gravités pour un récepteur GNSS

| Gravité | Description |
| --- | --- |
| Critique | Incapacité pour le récepteur GNSS de donner une information de position ou de temps pendant une longue durée ou bien fourniture par le récepteur GNSS d’une information de temps et de position erronée sans moyen de détection pour l’utilisateur |
| Grave | Incapacité pour le récepteur GNSS de donner une information de position ou de temps pendant une durée limitée ou bien dégradation importante des performances du récepteur GNSS (précision supérieure à 300 mètres / incertitude de l’ordre de la milliseconde) pendant une longue durée |
| Significative | Dégradation significative des performances du récepteur GNSS (précision inférieure à 300 mètres / incertitude de l’ordre de la microseconde) pendant une longue durée |
| Mineure | Dégradation mineure des performances du récepteur GNSS (précision inférieure à 30 mètres / incertitude de l’ordre de la nanoseconde). Le récepteur GNSS reste toujours capable de fournir une position ou une source de temps relativement précise |

Tableau 6: Echelle des niveaux de taille des zones impactées par la menace

|  |  |
| --- | --- |
| Taille de zone | Description |
| Large | La menace considérée peut impacter une zone supérieure à quelques milliers de kilomètres |
| Etendue | La menace considérée peut impacter une zone de quelques centaines de kilomètres |
| Limitée | La menace considérée peut impacter une zone de quelques dizaines de kilomètres |
| Restreinte | La menace considérée peut impacter une zone de quelques dizaines de mètres |

Tableau 7: Echelle des niveaux de durée des menaces

|  |  |
| --- | --- |
| Durée | Description |
| Longue | La menace considérée peut avoir un effet sur plusieurs jours |
| Limitée | La menace considérée peut avoir un effet sur plusieurs heures voir plus d’une journée |
| Courte | La menace considérée peut avoir un effet sur plusieurs dizaines de minutes voir plus d’une heure |

Tableau 8: Echelle des niveaux de probabilités d'occurrences pour une menace

|  |  |
| --- | --- |
| Probabilité | Description |
| Fréquent | La menace considérée peut apparaitre plusieurs fois dans la même journée |
| Probable | La menace considérée peut apparaitre plusieurs fois dans le même mois |
| Occasionnel | La menace considérée peut apparaitre plusieurs fois dans la même année |
| Eloigné | La menace considérée peut apparaitre plusieurs fois sur plusieurs années |
| Improbable | La menace considérée n’a pas été observée pendant des dizaines d’années |

### Segments Sol et Spatial

#### Non intentionnelle

Menace de type 1 : Panne majeure d’un satellite

Une panne satellite majeure se produit lorsque l’erreur en distance sur le signal émis par un satellite valide est considérée comme intolérable car supérieure à 4,42 fois l’erreur nominale (User Range Accuracy) ou supérieure à 30 mètres. Ces pannes peuvent avoir diverses origines comme une défaillance de l’horloge satellite, de mauvaises données de navigation (correction d’horloge, éphémérides) transmises par le satellite, ou même un impact avec des débris spatiaux.

* **Gravité** : Significative - Biais d’erreur important sur les informations de position et de temps fournies par les récepteurs GNSS
* **Zone** : Large – mondiale
* **Durée :** Limitée – la durée moyenne d’une panne satellite est donnée par le temps moyen requis pour sa restauration (MTTR) qui est d’approximativement 37 heures pour la constellation GPS.
* **Probabilité d’occurrence** : Occasionnel – la probabilité d’occurrence d’une panne satellite est de l’ordre de trois fois par an en considérant une constellation GPS composée de 24 satellites. En effet, la probabilité d’occurrence d’une panne, par satellite GPS et par heure, est officiellement inférieure à . Il n’est à l’heure actuelle pas possible d’estimer cette probabilité pour la constellation Galileo qui n’est à l’heure actuelle pas totalement opérationnelle.
* **Exemples** : Panne d’horloge satellite GPS.   
  Une panne d’horloge majeure s’est produite le 1er janvier 2004 à bord du satellite GPS PRN23 et son signal a été quand même transmis pendant plusieurs heures. L’information de mauvaise santé contenue dans le message de navigation du satellite, en vue de son utilisation par les récepteurs pour écarter les mesures correspondantes du calcul de la solution de navigation, n’a été reçue que plusieurs heures après le début de l’incident.

Menace de type 2 : Défaillance mineure d’un satellite

Des défaillances mineures de satellites peuvent également se produire, elles ont un effet bien plus modéré sur le modèle nominal d’erreur qui est de l’ordre de quelques dizaines de centimètres. Ces pannes mineures peuvent avoir de multiples origines : biais inter-fréquences, mauvaise qualité de signal (distorsions et déformation du signal, incohérences entre code et porteuse), ou un biais d’antenne.

* **Gravité :** Mineure – biais d’erreur faible (dizaines de centimètres) sur les informations de position et de temps fournies par les récepteurs GNSS
* **Zone :** Large – mondiale
* **Durée :** Longue (plusieurs jours) – ces défaillances sont plus difficiles à détecter et peuvent ne pas être corrigées pendant une très longue période.
* **Probabilité d’occurrence :** Occasionnel – la probabilité d’un tel évènement est considérée comme du même ordre qu’une panne majeure de satellite

Menace de type 3 : Panne de constellation

Une panne de constellation est caractérisée par une panne majeure qui affecte plusieurs satellites en même temps. Ce type de panne est souvent causé par une mauvaise mise à jour du segment sol ou une constellation dégradée.

* **Gravité** : Grave – des biais d’erreur très important peuvent apparaitre sur les informations de position et de temps fournies par les récepteurs GNSS
* **Zone :** Large – mondiale
* **Durée :** Limitée
* **Probabilité d’occurrence :** Eloigné
* **Exemples** : Anomalie du GPS ayant affecté la communauté mondiale des utilisateurs de l’heure GNSS le 26 janvier 2016[[20]](#footnote-21).   
  Des utilisateurs et des entreprises ont fait l’expérience de problèmes de synchronisation et de datation GNSS après que le 26 janvier 2016, 15 satellites GPS aient diffusé des signaux de synchronisation entachés d’une erreur de 13 microsecondes par rapport aux spécifications de l’ordre de 30 nanosecondes. Le dysfonctionnement a commencé lorsque le processus de mise hors service de l'ancien satellite GPS SVN 23 a affecté le logiciel du segment sol, puis le bon fonctionnement des autres satellites de la constellation GPS. Même si le problème a été résolu en 6 heures, les impacts étaient encore visibles 12 heures après la fin de l’incident. Les opérateurs de télécommunications dépendants du GNSS et sans systèmes de secours résilients ont été impactés par cette anomalie.

#### Naturelle

Menace de type 4 : Evènements solaires extrêmes

* **Gravité** : Critique - Anomalies de fonctionnement des satellites avec possibles répercussions critiques sur le fonctionnement des récepteurs GNSS sans moyen de détection pour l’utilisateur
* **Zone** : Large – mondiale
* **Durée** : Longue – les périodes de tempête solaires peuvent s’étaler sur plusieurs mois
* **Probabilité d’occurrence** : Eloigné
* **Exemples** : Tempêtes solaires d’octobre/novembre 2003   
  Des anomalies de fonctionnement liées à ces tempêtes ont été observées sur les 2/3 des satellites de la NASA[[21]](#footnote-22).

### Signal (Segment Utilisateur)

#### Intentionnelle

##### Le brouillage

Menace de type 5 : Brouillage fixe à des fins de protection de la vie privée ou d’actions illégales

* **Objectif** : Perturbation du fonctionnement de tous les récepteurs GNSS sur une zone donnée afin d’empêcher l’utilisation de moyens de surveillance (drone, etc.)
* **Profils d’attaquants** :
* VIP du monde du sport/spectacle : protection contre les moyens d’observation intrusifs mis en œuvre par des paparazzis
* Groupes criminels organisés / Groupes terroristes : protection contre les moyens de surveillance mis en œuvre par les forces de police.
* **Gravité** : Grave - Perte totale de l’information GNSS fournie par les récepteurs concernés
* **Zone** : Limitée/Etendue
* **Durée** : Limitée/longue en fonction du type d’action illégale à protéger ou du temps nécessaire pour faire arrêter les émissions dans le cas des VIPs
* **Probabilité d’occurrence :** Fréquent
* **Exemples** : Utilisation d'équipements électroniques pour soutenir le trafic de drogue  
  Un gang a comparu devant un tribunal britannique en décembre 2017[[22]](#footnote-23) pour son implication dans des activités illégales, notamment le trafic de drogue. Dans le cadre de ses actions, le gang a mis en œuvre des techniques de contre-surveillance électronique sophistiquées, incluant le brouillage GNSS, pour échapper aux forces de l’ordre. L'équipement utilisé était un générateur de signaux multifonction destiné à perturber la réception des signaux GNSS, WiFi, 3G et 4G.

Menace de type 6 : Brouillage embarqué à des fins de protection de la vie privée ou d’actions illégales

* **Objectif** : Perturbation du fonctionnement d’un récepteur GNSS par son utilisateur afin d’empêcher un report de position vers un système de suivi et/ou de contrôle (traçage).
* **Profils d’attaquants** :
* Individus (mal informés ou malveillants). Des employés (mécontents ou malhonnêtes) peuvent également avoir recours à ce type de brouillage pour perturber le fonctionnement des organismes ou entreprises dans lesquels ils travaillent.
* Groupes criminels organisés : sont susceptibles d’utiliser des brouilleurs embarqués destinés à perturber le fonctionnement des « traceurs » mis en œuvre pour la protection de voitures de luxe ou de biens de valeur par exemple.
* **Gravité** : Grave – perte totale de l’information GNSS fournie par les récepteurs concernés qui ne peut donc pas être reportée vers les systèmes de suivi, de contrôle ou de « traçage ».
* **Zone** : Restreinte – plusieurs dizaines à plusieurs centaines de mètres en horizontal autour du véhicule, et plus en vertical
* **Durée** : Courte/Limitée – durée d’un trajet
* **Probabilité d’occurrence** : Fréquent
* **Exemples** : Mesures effectuée au cours du projet STRIKE 3 (Horizon 2020)[[23]](#footnote-24)   
  Au cours de ce projet, un réseau international de surveillance des interférences GNSS a été déployé. Un grand nombre de ces mesures a été réalisé à proximité de voies de circulation. L’objectif était d’évaluer l’ampleur du problème du brouillage dans le monde. Des stations de surveillance ont été installées dans 23 pays à travers le monde. Plus de 450 000 signaux d'interférence GNSS ont été relevés et analysés : environ 73 000 ont été identifiés comme ayant un impact majeur sur les équipements GNSS, quand 59 000 d'entre eux ont été identifiés comme ayant été émis par des brouilleurs de signaux.

Menace de type 7 : Brouillage embarqué à des fins de non-paiement de frais d’utilisation d’un service

* **Objectif** : Perturbation du fonctionnement d’un récepteur GNSS par son utilisateur afin d’éviter le paiement de frais d’utilisation d’un service
* **Profils d’attaquants** : Individus (mal informés ou malveillants)
* **Gravité** : Grave - Perte totale de l’information GNSS fournie par les récepteurs concernés
* **Zone** : Restreinte – plusieurs dizaines à plusieurs centaines de mètres en horizontal autour du véhicule, et plus en vertical
* **Durée** : Limitée /Longue (en fonction du type de service)
* **Probabilité d’occurrence** : Probable - pourrait devenir plus importante en fonction du développement des services correspondants
* **Exemples** : Voir la menace de type 8 : Mesures effectuée au cours du projet STRIKE 3 (Horizon 2020)

Menace de type 8 : Brouillage à des fins militaires

* **Objectif** : Perturbation sans discrimination du fonctionnement des moyens GNSS militaires utilisés sur un champ de bataille ou dans les infrastructures d’importance vitale d’une nation ennemie
* **Profils d’attaquants** : Nations
* **Gravité** : Critique - Perte totale de l’information GNSS fournie par les récepteurs concernés pendant une longue durée
* **Zone** : Etendue
* **Durée** : Longue – plusieurs jours voire plusieurs semaines
* **Probabilité d’occurrence** : Eloigné – Ce type de perturbation est coûteux à mettre en œuvre et a surtout été observé dans des zones de guerre ou dans des pays avec des régimes autoritaires. Cependant, la possibilité de sa mise en œuvre aux frontières de l’UE ne peut pas être totalement écartée.
* **Exemples** : Brouillages du GPS par la Corée du Nord depuis 2010[[24]](#footnote-25)   
  Selon les responsables du renseignement sud-coréen, le brouillage périodique des signaux GPS observé sur une grande partie de leur territoire est généré par des brouilleurs de forte puissance positionnés à la frontière nord-coréenne. Plusieurs centaines d’aéronefs et de navires ont subi des perturbations du fonctionnement de leurs équipements GNSS pendant ces périodes.

##### Le leurrage

Menace de type 9 : Leurrage ciblé d’équipements non critiques

* **Objectif** : Perturbation du fonctionnement d’un récepteur GNSS sans autre objectif que de démontrer la faisabilité d’une technique de leurrage
* **Profils d’attaquants** : Pirates (amateurs ou professionnels)
* **Gravité** : Critique - fourniture d’informations erronées par les récepteurs GNSS correspondants
* **Zone** : Restreinte – plusieurs dizaines de mètres
* **Durée** : Courte
* **Probabilité d’occurrence** : Occasionnel - Toutefois les techniques de leurrage démontrées pourraient être reprises par d’autres pirates plus mal intentionnés (voir menace de type 9)
* **Exemples** : Récentes conférences DEF CON   
  la DEF CON est une convention de hackers qui se tient chaque année à Las Vegas aux États-Unis. La première s'est déroulée en juin 1993. Des participants à de récentes conférences ont démontré la faisabilité du leurrage des informations GNSS utilisées dans des Smartphone, un drone[[25]](#footnote-26) et un serveur NTP[[26]](#footnote-27).

Menace de type 10 : Leurrage ciblé d’équipements critiques

* **Objectif** : Perturbation du fonctionnement de récepteurs GNSS afin de provoquer le dysfonctionnement de systèmes impliqués dans des activités d’importance vitale.
* **Profils d’attaquants** : Groupes terroristes / Pirates (amateurs ou professionnels)
* **Gravité** : Critique - fourniture d’informations GNSS erronées à des systèmes les utilisant pour réaliser d’autres fonctions
* **Zone** : Limitée
* **Durée** : Courte à longue en fonction des systèmes ciblés
* **Probabilité d’occurrence** : Eloigné - pourrait devenir plus importante en fonction de la disponibilité de produits grand public en mesure de générer les types de leurrage adéquats.
* **Exemple** : Expérimentation[[27]](#footnote-28) de leurrage sur des Tesla Model S et Model 3 électriques et semi-autonomes.  
  Des essais en grandeur réelle ont montré qu'avec un matériel peu coûteux et un logiciel open source, il était possible de tromper le récepteur GNSS d’un modèle de véhicule Tesla en moins d'une minute. Les signaux de leurrage émis ont affecté la cartographie, les calculs de puissance et les systèmes de suspension de la voiture rendant impossible l'utilisation correcte du système semi-autonome de la voiture. Le véhicule a réagi aux signaux de brouillage en ralentissant et en activant le clignotant droit comme s’il se situait à 150 m de la sortie alors qu’il en était à 5 km. Le conducteur a dû reprendre le contrôle manuel afin d’éviter que la voiture ne quitte la route.

Menace de type 11 : Leurrage à des fins militaires

* **Objectif** : Perturbation du fonctionnement des moyens GNSS militaires ennemis utilisés sur un champ de bataille
* **Profils d’attaquants** : Nations
* **Gravité** : Critique – Dégradation de l’information GNSS fournie par les récepteurs concernés : perte totale ou fourniture d’informations PNT erronées difficile à détecter pour le récepteur
* **Zone** : Etendue
* **Durée** : Longue – plusieurs jours voire plusieurs semaines
* **Probabilité d’occurrence** : Eloigné - ce type de perturbation, coûteux à mettre en œuvre, a été observé dans certaines zones de guerre. La possibilité de sa mise en œuvre aux frontières de l’UE ne peut pas être totalement écartée.
* **Exemples** : Leurrage du GPS par les forces Russes en Syrie[[28]](#footnote-29).   
  Le conflit en Syrie a été utilisé par les forces Russes pour y tester leurs équipements militaires, y compris ceux de guerre électronique. Des signaux de leurrage du GPS ont en particulier été émis et ont perturbés le fonctionnement de drones militaires américains. Bien que les signaux émis imitaient ceux transmis par les authentiques satellites GPS, ils ne transportaient aucune information de navigation valide. Les récepteurs GPS ciblés par ce leurrage accrochaient les signaux GPS sans être en mesure de calculer des solutions de navigation valides, et étaient donc rendus inutilisables. Les signaux de leurrage étant beaucoup plus puissants que les signaux GNSS authentiques reçus des satellites, ils représentaient également une menace directe pour la sécurité de l'aviation commerciale à portée des transmissions.

Menace de type 12 : Leurrage pour la protection de VIPs du monde politique

* **Objectif** : Perturbation du fonctionnement des moyens GNSS utilisés sur une zone où séjournent ou transitent des VIPs
* **Profils d’attaquants**: Nations
* **Gravité** : Critique - Dégradation de l’information GNSS fournie par les récepteurs concernés : perte totale ou fourniture d’informations PNT erronées difficile à détecter pour le récepteur
* **Zone** : Limitée
* **Durée** : Longue – plusieurs jours voire plusieurs semaines
* **Probabilité d’occurrence** : Eloigné - Ce type de perturbation, coûteux à mettre en œuvre a toutefois été observé à plusieurs reprises dans des zones ou séjournaient certains chefs d’Etat en dehors de la zone Union Européenne.
* **Exemples** : Leurrage du GPS lors des déplacements du chef de l’Etat Russe.   
  Une corrélation étroite entre des déplacements du chef de l'Etat Russe et des événements de leurrage du GNSS a été mise en évidence dans une étude[[29]](#footnote-30) réalisée par le C4ADS (Center for Advanced Defense Studies). Cet organisme de recherche utilise des techniques d'analyse de données sophistiquées pour enquêter sur les problèmes de sécurité et les conflits mondiaux.

##### Les modifications ionosphériques

Menace de type 13 : Essais nucléaires dans l’espace

* **Objectif** : Démonstration des effets d’une explosion atomique dans l’espace.
* **Profils d’attaquants** : Nations
* **Gravité** : Critique – Susceptible de mener à la destruction de satellites par le rayonnement induit, sans distinction de type et de fonction
* **Zone** : Large (dans l’espace et au sol)
* **Durée** : Longue – les effets de tels essais peuvent perdurer le fonctionnement de satellites pendant plusieurs mois
* **Probabilité d’occurrence** : Improbable - en raison de la très grande portée des explosions nucléaires dans l’espace, il a été démontré qu’il était presque impossible d'éviter des dommages collatéraux sur un grand nombre de satellites, y compris ceux du pays à l’origine de l’explosion.
* **Exemples** : Essais nucléaires réalisés par les Etats Unis et l’Union Soviétique. Plusieurs de ces tests ont été effectués à haute altitude par les États-Unis et l'Union soviétique entre 1958 et 1962[[30]](#footnote-31). L’Opération Argus conduite par les Etats Unis durant l’été 1958 avait pour objectif d’injecter des particules chargées dans la magnétosphère et d’évaluer les possibles effets sur les ogives et les radars soviétiques. Le test réalisé par les états unis le 9 juillet 1962 a révélé l'impact destructeur de l'impulsion électromagnétique produite par une explosion nucléaire. Située à plus de 1 300 kilomètres du site d'essai, l'île hawaïenne d'Oahu a subi une surtension qui a détruit de nombreux appareils électriques.

#### Non intentionnelle

Menace de type 14 : Leurrage causé par le dysfonctionnement ou la mauvaise configuration d’un équipement

* **Profils d’attaquants** : Propriétaires d’équipements radioélectriques et électroniques
* **Gravité** : Critique - Fourniture d’informations erronées par les récepteurs GNSS situés à proximité d’un équipement mal configuré ou présentant des dysfonctionnements
* **Zone** : Restreinte
* **Durée** : Courte à longue en fonction du délai de détection et de localisation de la source de l’émission
* **Probabilité d’occurrence**: Occasionnel à l’échelle du territoire national
* **Exemple 1** : Dysfonctionnement d’un simulateur lors d’une conférence ION GNSS.   
  Lors de la conférence ION GNSS + 2017, les smartphones de certains des participants ont montré des comportements anormaux. Alors que certains n'étaient pas du tout affectés, d'autres équipements ne pouvaient plus envoyer de messages (SMS, e-mails, etc.), et affichaient un emplacement incorrect situé en Europe, ainsi qu’une date trois années dans le passé. La source de leurrage a été identifiée comme étant un simulateur GNSS exposé sur un stand, qui ne fermait pas correctement ses ports de sortie inutilisés. Même s'il ne s'agissait pas d'une attaque sophistiquée et intentionnelle, mais simplement d'une émission accidentelle et que le simulateur n’était pas équipé d’antennes, cela a eu des répercussions très importantes, certains smartphones ont affiché un emplacement et une heure incorrects jusqu'à 1 heure et demie après la fin de l'événement tandis que d’autres nécessitaient un redémarrage pour pouvoir fonctionner.
* **Exemple 2** : Incident de leurrage non intentionnel lors du salon automobile de Genève[[31]](#footnote-32)  
  En mars 2019, le Salon international de l'automobile de Genève a été confronté à un incident de leurrage. La plupart des équipements de navigation des voitures de la salle d'exposition se sont mis à afficher un emplacement et une date incorrects (Buckingham en 2036). Bien que cette perturbation du signal GNSS n'était pas générée de façon intentionnelle et n'ait pas créé de problème majeur sur le Salon, certains observateurs ont souligné le fait que ce type de perturbation reste toutefois susceptible de produire des accidents de la route pour les véhicules semi-autonomes, plus dépendant des signaux GNSS.
* **Exemple 3 :** Incident de leurrage sur l’aéroport d’Hanovre (Allemagne)[[32]](#footnote-33)[[33]](#footnote-34)  
  En 2010, sur l'aéroport de Hanovre, les récepteur GPS de plusieurs avions de ligne se sont accrochés sur les signaux émis par un répéteur GPS installé à l’intérieur d’un hangar dont les portes étaient restées ouvertes. Des positionnements GPS erronés ont été pris en compte par les systèmes avioniques pendant les phases de roulage, déclenchant des alarmes et des alertes liées à une mauvaise localisation du seuil de piste. Ces répéteurs GPS sont des équipements utilisés pour recevoir une couverture satellite à l'intérieur d’un bâtiment, par exemple pour effectuer des tests.

Menaces de brouillage causé par :

**Type 15 : Dysfonctionnement d’un équipement**

**Type 15 bis : Non-conformité d’un équipement**

**Type 15 ter : Utilisation non conforme d’un équipement**

**Type 15 quater : Parasites électromagnétiques d’un équipement radioélectrique**

**Type 15 quinquies : Test d’équipements industriels**

* **Profils d’attaquants** : Propriétaires d’équipements radioélectriques et électroniques
* **Gravité** : Critique - Perturbation du fonctionnement du récepteur GNSS. Dégradation forte de la précision jusqu’à perte de fourniture d’information de temps et de position.
* **Zone** : Restreinte à limitée en fonction du type de dysfonctionnement et d’équipement concerné
* **Durée** : Courte à longue en fonction du délai de détection et de localisation de la source de l’émission
* **Probabilité d’occurrence** : Occasionnel – l’utilisation croissante des équipements radios augmente la probabilité de brouillage dans la bande GNSS

#### Naturelle

Menace de type 16 : Phénomènes de scintillation récurrents

* **Gravité** : Significative - Dégradation des informations de position fournies par les récepteurs GNSS pouvant être générée par une diminution du nombre de satellites utilisables à un instant donné et par une dégradation du rapport signal/bruit des signaux reçus. Elle peut conduire à des sauts de phase du récepteur et à la dégradation de ses performances générales.
* **Zone** : Large - plusieurs milliers de kilomètres généralement situés dans les régions à environ ~ 15 ° de chaque côté de l'équateur géomagnétique ainsi que dans les régions polaires
* **Durée** : Limitée
* **Probabilité d’occurrence** : Probable - La fréquence d'occurrence globale de la scintillation augmente non seulement avec une activité solaire élevée, mais suit également certains modèles saisonniers. En général, la scintillation est plus active autour des équinoxes.
* **Exemples** : Sans objet

### Récepteur (Segment Utilisateur)

#### Intentionnelle

Menace de type 17 : Leurrage des couches applicatives

* **Objectif** : Agir sur certaines fonctions d’un équipement afin de contrôler les informations fournies par sa fonction de positionnement ou de datation/synchronisation
* **Profils d’attaquants** : Pirates (amateurs ou professionnels)
* **Gravité** : Critique - utilisation d’informations PNT erronées par les équipements concernés
* **Zone** : Restreinte à large - plusieurs équipements répartis dans le monde entier peuvent être ciblés par une même attaque
* **Durée** : Longue - jusqu’à la suppression des éléments de code correspondants dans les équipements concernés
* **Probabilité d’occurrence** : Occasionnel – les menaces de cyber sécurité sont en augmentation constante
* **Exemple** : Leurrage de l’information de position utilisée par le jeu « Pokémon Go »   
  Au plus fort de la période d’engouement pour le jeu « Pokémon Go », étaient alors disponibles en ligne des applications de leurrage ayant pour but de contrôler les données de positionnement des smartphones et ainsi tromper l’application.

#### Non intentionnelle

Menace de type 18 : Mauvaise prise en compte des Secondes Intercalaires

* **Gravité** : Critique - impossibilité d’acquisition des signaux GNSS par les récepteurs concernés. Certains récepteurs peuvent cesser de fonctionner et nécessiter un redémarrage.
* **Zone** : Large – Des récepteurs répartis dans le monde entier peuvent être potentiellement touchés.
* **Durée** : Limitée
* **Probabilité d’occurrence** : Occasionnel.
* **Exemple** : Erreur de conception logicielle d’équipements aéronautiques.   
  En juin 2019, certains récepteurs GPS ont rencontré des problèmes de fonctionnement qui ont entraîné des retards sur certains vols civils[[34]](#footnote-35). Ces problèmes étaient liés à la mauvaise prise en compte d’une seconde intercalaire par les récepteurs GNSS de certaines marques qui a provoqué leur arrêt.

### Synthèse de la caractérisation

Le tableau ci-dessous fournit une synthèse des menaces caractérisées ci-dessus.

Tableau 9: Synthèse et caractérisation des menaces sur le GNSS

| Indice menace | Menace | Gravité pour le récepteur GNSS | Zone | Durée | Probabilité d’occurrence | Responsable |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Panne majeure d’un satellite** | Significative | Large | Limitée | Occasionnel | N/A |
| **2** | **Défaillance mineure d’un satellite mineure** | Mineure | Large | Longue | Occasionnel | N/A |
| **3** | **Panne de constellation** | Grave | Large | Limitée | Eloigné | N/A |
| **4** | **Evènements solaires extrêmes** | Critique | Large | Longue | Eloigné | N/A |
| **5** | **Brouillage fixe à des fins de protection de la vie privée ou d’actions illégales** | Grave | Limitée/ Etendue | Limitée/ Longue | Fréquent | VIP (monde du sport/spectacle) / Groupes criminels organisés / Groupes terroristes |
| **6** | **Brouillage embarqué à des fins de protection de la vie privée ou d’actions illégales** | Grave | Restreinte | Courte/ Limitée | Fréquent | Individus (mal informés ou malveillants) / Employés / Groupes criminels organisés |
| **7** | **Brouillage embarqué à des fins de non-paiement de frais d’utilisation d’un service** | Grave | Restreinte | Limitée/ Longue | Probable | Individus (mal informés ou malveillants) |
| **8** | **Brouillage à des fins militaires** | Critique | Etendue | Longue | Eloigné | Nations |
| **9** | **Leurrage ciblé d’équipements non critiques** | Critique | Restreinte | Courte | Occasionnel | Pirates (amateurs ou professionnels) |
| **10** | **Leurrage ciblé d’équipements critiques** | Critique | Limitée | Courte/ Longue | Eloigné | Groupes terroristes / Pirates (amateurs ou professionnels) |
| **11** | **Leurrage à des fins militaires** | Critique | Etendue | Longue | Eloigné | Nations |
| **12** | **Leurrage pour la protection de VIPs du monde politique** | Critique | Limitée | Longue | Eloigné | Nations |
| **13** | **Essais nucléaires dans l’espace** | Critique | Large | Longue | Improbable | Nations |
| **14** | **Leurrage causé par le dysfonctionnement ou la mauvaise configuration d’un équipement** | Critique | Restreinte | Courte/ Longue | Occasionnel | Propriétaires d’équipements radioélectriques et électroniques |
| **15** | **Brouillage causé par le dysfonctionnement d’un équipement** | Critique | Restreinte/ Limitée | Courte/ Longue | Occasionnel | Propriétaires d’équipements radioélectriques et électroniques |
| **15 bis** | **Brouillage causé par la non-conformité d’un équipement** | Critique | Restreinte/ Limitée | Courte/ Longue | Occasionnel | Propriétaires d’équipements radioélectriques et électroniques |
| **15 ter** | **Brouillage causé par l’utilisation non conforme d’un équipement** | Critique | Restreinte/ Limitée | Courte/ Longue | Occasionnel | Propriétaires d’équipements radioélectriques et électroniques |
| **15 quater** | **Brouillage causé par des parasites électromagnétiques d’un équipement radioélectrique** | Critique | Restreinte/ Limitée | Courte/ Longue | Occasionnel | Propriétaires d’équipements radioélectriques et électroniques |
| **15 quinquies** | **Brouillage causé par le test d’équipements industriels** | Critique | Restreinte/ Limitée | Courte/ Longue | Occasionnel | Propriétaires d’équipements radioélectriques et électroniques |
| **16** | **Phénomènes de scintillations récurrents** | Significative | Large | Limitée | Probable | N/A |
| **17** | **Leurrage des couches applicatives** | Critique | Restreinte/ Large | Longue | Occasionnel | Pirates (amateurs ou professionnels) |
| **18** | **Mauvaise prise en compte des Secondes Intercalaires** | Critique | Large | Limitée | Occasionnel | N/A |

# Contremesures en cas de menaces GNSS

Les contremesures pouvant être mises en place en prévision ou en présence d’une dégradation ou d’une perte GNSS peuvent prendre des formes diverses et être appliquées aussi bien au niveau technique qu’organisationnel par les opérateurs de systèmes dépendants de l’utilisation du GNSS.

## Contremesures techniques

Au niveau technologique, des moyens de redondance et des équipements indépendants du GNSS (par exemple un serveur de temps se reposant sur le signal horaire radio ou une horloge atomique) peuvent être installés par les opérateurs afin d’assurer la continuité en cas de perte du GNSS. De plus, il existe diverses contremesures spécifiques permettant de rendre les récepteurs GNSS plus robuste en cas de brouillage ou de leurrage du GNSS. Ces contremesures peuvent être classées parmi diverses catégories :

* **Détection** : diverses techniques permettent détecter mais aussi de caractériser une menace pesant sur le GNSS. Ces moyens de détection peuvent exploiter les données disponibles tout au long de la chaine de réception et de traitement d’un récepteur GNSS (surveillance des caractéristiques du signal GNSS comme la puissance ou le doppler, surveillance de l’horloge, utilisation d’algorithmes d’intégrité comme RAIM). Ils peuvent aussi se reposer sur l’utilisation de services GNSS renforcés comme le PRS ou l’OS-NMA de Galileo ou de services d’augmentation du signal GNSS comme EGNOS.
* **Atténuation** : ces techniques ont pour objectif d’atténuer les effets d’une potentielle menace sur le GNSS comme un brouillage ou un leurrage. Elles peuvent se baser sur des méthodes de traitement du signal comme le filtrage dans les domaines fréquentiel et temporel. Ces méthodes de filtrage permettent d’atténuer la puissance d’un signal indésirable détecté dans la bande de fréquence du GNSS. Il est aussi fréquent d’utiliser des capteurs supplémentaires lors de l’estimation de la position de la vitesse et du temps (PVT) via l’emploi d’algorithmes d’hybridation. Ces capteurs peuvent être des centrales inertielles, des caméras, des radars ou des odomètres par exemple.
* **Annulation** : certaines méthodes permettent d’annuler complétement de potentiels signaux d’interférence ou de leurrage. Ces méthodes se reposent généralement sur l’utilisation de réseaux d’antennes CRPA (Controlled Reception Pattern Antenna) capables de manipuler leurs diagrammes de réception et de créer des nuls aux angles d’où proviennent les signaux indésirables.
* **Evitement** : les techniques d’évitement peuvent se reposer sur l’utilisation des différentes constellations (Galileo, GPS, Beidou, GLONASS) et bandes de fréquences GNSS disponibles afin de contourner une potentielle menace GNSS. Les moyens d’évitement englobent aussi l’émission de lois et de réglementation sur l’utilisation des fréquences GNSS.

## Contremesures procédurales – Rôle de l’ANFR

L’Agence Nationale des FRéquences (ANFR) est un établissement public de l’Etat ayant pour mission la planification, la gestion et le contrôle du spectre radioélectrique en France. L’ANFR assure notamment le contrôle de l’utilisation des fréquences radioélectriques et le traitement des brouillages qui lui sont signalés sur le territoire national. L’Agence garantit ainsi l’usage de ces fréquences avec un minimum de perturbations.

l’ANFR est particulièrement impliquée dans la lutte contre les brouillages du GNSS et le risque de prolifération de brouilleurs illicites. Dans ce cadre elle intervient pour la localisation et l’identification des origines des émissions occasionnant des brouillages préjudiciables.

Si la détection d’un brouillage du GNSS n’empêche pas les préjudices potentiellement associés de se produire, elle est essentielle, notamment pour les utilisateurs professionnels du GNSS, car elle constitue la première étape indispensable à sa résolution. Par ailleurs, elle permet la mise en place de mécanismes de résilience adaptés.

La détection d’un brouillage par une victime peut nécessiter l’installation sur ses sites d’équipements spécifiques afin d’optimiser ses capacités de détection. Cette détection doit se prolonger d’un signalement à l’ANFR permettant à l’Agence d’intervenir pour résoudre le brouillage en localisant sa source et en identifiant ses auteurs. Le cas échéant, des sanctions peuvent être appliquées car un brouillage par utilisation d’un brouilleur ou d’un équipement non conforme est une infraction pénale soumise à des peines allant jusqu’à 6 mois de prison et 30 000 euros d’amende. Par ailleurs, l’ensemble des signalements contribue à mieux mesurer l’ampleur des phénomènes de brouillage à l’échelle nationale et ainsi à renforcer la connaissance nécessaire au maintien des moyens adéquats de protection et de défense.

Le traitement d’un brouillage GNSS, suite à son signalement à l’ANFR (environ 2 000 signalements de tous types de brouillages par an), est mené sur le terrain par des agents assermentés et habilités. Ces agents sont équipés de matériels techniques sophistiqués permettant la recherche, l’identification et la localisation de la cause du brouillage. Dans certaines situations, un dispositif de détection peut être installé sur un site adapté pendant la durée nécessaire à la caractérisation du brouillage, notamment dans le cas d’un brouilleur GNSS embarqué dans un véhicule. Une fois l’équipement et le responsable du brouillage identifiés, l’ANFR formule des préconisations pour faire cesser ce brouillage. L’Agence peut appliquer une taxe d’intervention de 450€ (loi de finances) et rédiger un procès-verbal transmis au procureur de la république pour poursuite en justice ; les brouillages et les utilisations de fréquences sans l’autorisation nécessaire étant soumis à des sanctions pénales lourdes (L. 39-1 du code des postes et communications électroniques). Ainsi, la détection et le signalement des brouillages du GNSS permet d’élever le niveau global de sécurité, réduisant les risques liés aux évènements redoutés identifiés à travers cette étude.

Les agents de l’ANFR mènent leurs investigations techniques sur site en se déployant à partir de six services régionaux (Toulouse, Villejuif, Donges, Aix-Marseille, Lyon, Nancy), du Centre de Contrôle International (Rambouillet), ou depuis ses antennes Antilles-Guyane et La Réunion-Mayotte. L’ANFR est également présente notamment pour des missions de contrôle du spectre en Nouvelle-Calédonie et en Polynésie française. La figure suivante présente les différentes directions du contrôle du spectre de l’ANFR.

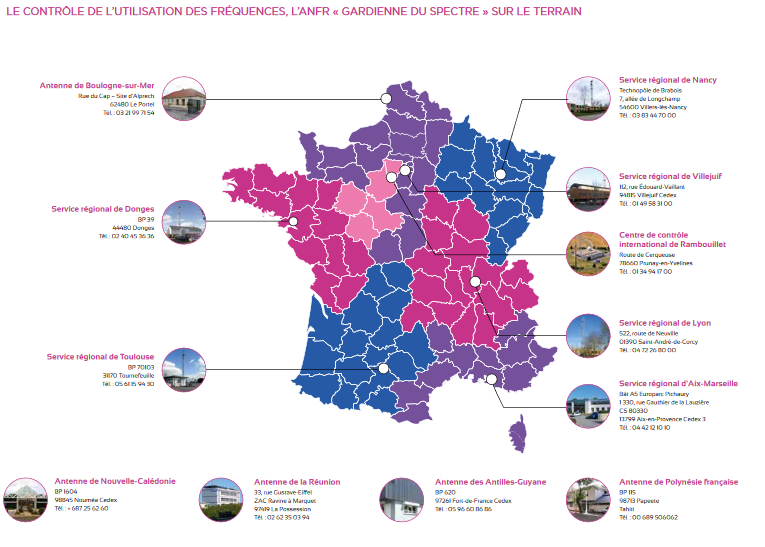


Figure 6 : Organisation de la direction du contrôle du spectre de l’ANFR

Pour finir, l’ANFR met également en place des actions pédagogiques pour lutter contre le risque de prolifération de brouilleurs GNSS[[35]](#footnote-36). Une plaquette et une affiche sont disponibles en français et en anglais sur son site Internet. Par ailleurs, un mailing très large a été effectué auprès d’entreprises qui géolocalisent leur flotte pour les sensibiliser au risque des brouillages du GNSS. Enfin, des interventions réussies de détection de brouilleurs GNSS illicites ou d’autres cas de brouillages non intentionnels du GNSS sont régulièrement relatés dans sa newsletter[[36]](#footnote-37), [[37]](#footnote-38), [[38]](#footnote-39), [[39]](#footnote-40), [[40]](#footnote-41), [[41]](#footnote-42).

Etudes d’impact GNSS par secteur

1. Energie
2. Gestion de l’eau
3. Finance
4. Métrologie
5. Météorologie
6. Communications électroniques, audiovisuel et information
7. Spatial
8. Industrie
9. Transport aérien
10. Transport maritime et fluvial
11. Transport routier
12. Transport ferroviaire
13. Information géographique

Abréviations et Sigles

0-9

3GPP 3rd Generation Partnership Project

A

ADF Automatic Direction Finder

ADMS Advanced Distribution Management System

ADP Aéroports de Paris

ADR Accord for Dangerous goods by Road

ADS-B Automatic Dependent Surveillance-Broadcast

ADSL Asymmetric Digital Subscriber Line

AEMF Autorité Européenne des Marchés Financiers

AIPCR Association Internationale Permanente des Congrès de la Route

AIS Automatic Identification System

AIV Activité d’Importance Vitale

AMDAR Aircraft Meteorogical Data Relay

AMF Autorité des Marchés Financiers

ANFR Agence Nationale des FRéquences

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information

AOT Autorités Organisatrices de Transport

API Application Programming Interface

ARCEP Autorité de Régulation des Communications Electroniques et des Postes

ATC Air Traffic Control

ATM Asynchronous Transfer Mode

AtoN Aid to Navigation

B

BDT BeiDou Time

BIPM Bureau International des Poids et Mesures

BRGM Bureau des Recherches Géologiques et Minières

BSC Base Station Controller

BTS Base Transceiver Station

BVLOS Beyond Visual Line Of Sight

C

C4ADS Center for Advanced Defense Studies

CA Carrier Aggregation

CAM Cooperative Awareness Messages

CAS Commercial Authentication Service

CDMA Code Division Multiple Access

CEN Comité Européen de Normalisation

CENELEC Comité Européen de Normalisation ELECtrotechnique

CGCS2000 China Geodetic Coordinate System 2000

CLUG Certifiable Localisation Unit with GNSS in the railway environment

CME Coronal Mass Ejections

CNES Centre National d’Etudes Spatiales

CNIL Commission Nationale de l’Informatique et des Libertés

CNR Compagnie Nationale du Rhône

COLREGs Convention on the International Regulations for Preventing Collisions at Sea

COGIC Centre Opérationnel de Gestion Interministérielle des Crises

CoMP Coordinated Multi-Point

CPL Courant Porteur en Ligne

CRE Commission de Régulation de l’Energie

CRNA Centre en Route de la Navigation Aérienne

CSG Centre Spatial Guyanais

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CSSPF Conseil Supérieur du Service Public Ferroviaire

CSTDMA Carrier Sense Time Division Multiple Access

CT2 Cordless Telephone generation 2

CWDM Coarse Wavelength Division Multiplexing

D

DAB Digital Audio Broadcasting

DARS Digital Audio Reference Signal

DECT Digital Enhanced Cordless Telecommunications

DENM Decentralized Environmental Notification Messages

DER Distributed Energy Resources

DFR Digital Fault Recorder

DME Distance Measuring Equipment

DNSA Direction des Services de la Navigation Aérienne

DoS Déni de service (Denial of Services)

DR-SF Diffusion Restreinte-Spécial France

DREAL Directions Régionales de l’Environnement, de l’Aménagement et du Logement

DROM-COM Départements et Régions d’Outre-Mer et Collectivités d’Outre-Mer

DSI Direction des Systèmes d’Information

DSP2 Directive sur les Services de Paiement

DWDM Dense Wavelength Division Multiplexing

E

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité

EGNSS-R European GNSS Navigation Safety Service for Rail

eICIC enhanced Inter-Cell Interference Coordination

eMBMS Evolved Multimedia Broadcast Multicast Services

EMC ElectroMagnetic Compatibility

EMI ElectroMagnetic Interference

EMS Energy Management System

EPSF Etablissement Public de Sécurité Ferroviaire

ERA European union agency for RAilways

ERDF Électricité Réseau Distribution France

ERTMS European Rail Traffic Management System

ETCS European Train Control System

ETL Equipement de Télésignalisation

ETRS89 European Terrestrial Reference System

ETSI European Telecommunications Standards Institute

F

FACTS Flexible Alternating Current Transmission System

FARN Force d’Action Rapide du Nucléaire

FDD Frequency-Division Duplexing

FDMA Frequency Division Multiple Access

FEVAD Fédération E-commerce et Vente A Distance

FM Frequency Modulation

FMS Flight Management Système

FNAUT Fédération Nationale des Associations d’Usagers des Transports

FNTR Fédération Nationale des Transports Routiers

FttH Fiber to the Home

FRMCS Future Rail Mobile Communications System

G

GEO Geostationary Earth Orbit

GLONASS Global Orbiting Navigation Service System

GLONASST GLONASS Time

GNSS Global Navigation Satellite System

GONTRAND GestiON Temps Réel d’un RéseAu National de Distribution

GOVSATCOM GOVernmental SATellite COMmunications

GPRS General Packet Radio Service

GPS Global Positioning System

GRAVES Grand Réseau Adapté à la VEille Spatiale

GRD Gestionnaire du Réseau de Distribution

GSM Global System for Mobile communications

GSM-R Global System for Mobile communication – Railways

GST Galileo System Time

GTRF Galileo Terrestrial Reference Frame

H

HAS High Accuracy Service

HNSE Horizontal Navigation System Error

HTTPS HyperText Transfer Protocol over TLS

I

IALA International Association of the marine aids to navigation and Lighthouse Authorities

ICE Intercontinental Exchange

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IFREMER Institut Français de Recherche pour l'Exploitation de la Mer

IGS International GPS Service

IGSO Inclined GeoSynchronous Orbit

IHM Interface Homme Machine

ILS Instrument Landing System

ION Institute of Navigation

IIoT Industrial Internet of Things

IoT Internet of Things

IP Internet Protocol

IPGP Institut de Physique du Globe de Paris

IRIG Inter-Range Instrumentation Group

IRS Inertial Reference System

IRU Inertial Reference Unit

IRU International Road and transport Union

IS-XX Interim Standard-XX

ITRS International Terrestrial Reference System

L

LEO Low Earth Orbit

LNAV Lateral NAVigation

LNE Laboratoire National de métrologie et d’Essais

LOFAR LOw Frequency ARray

LPV Localizer Performance with Vertical guidance

LRNS Long Range Navigation Systems

LTBF Laboratoire Temps-Fréquence de Besançon

LTE Long Term Evolution

M

MAN Metropolitain Area Network

MASS Maritime Autonomous Surface Ship

MEO Medium Earth Orbit

MiFID Market in Financial Instrument Directive

MiFIR Market in Financial Instrument Regulation

MILSAT MILitary SATellite

MMS Multimedia Messaging Service

MTTr Mean Time To Repair or Mean Time To Recover

MUNIN Maritime Unmanned Navigation through Intelligence in Networks

N

N/A Non Applicable

NASA National Aeronautics and Space Administration

NAVAIDS Navigational Aids

NAVWAR NAVigation WARfare

NB-IoT NarrowBand Internet of Things

NenuFAR New extension in Nançay upgrading LOFAR

NPL National Physical Laboratory

NPSS Narrowband Primary Synchronisation Signals

NSSS Narrowband Secondary Synchronisation Signals

NTP Network Time Protocol

NYSE New York Stock Exchange

O

OACI Organisation de l'aviation civile internationale

OCXO Oven Controlled X-tal(Crystal) Oscillator

OHI Organisation Hydrographique Internationale

OICA Organisation International des Constructeurs Automobiles

OMI Organisation Maritime Internationale

OMM Organisation Météorologique Mondiale

ONERA Office National d’Etudes et de Recherches Aérospatiales

ONF Office National des Forêts

OP Observatoire de Paris

OS-NMA Open Service Navigation Message Authentication

OTAN Organisation du traité de l'Atlantique nord

OTDOA Observed Time Difference Of Arrival

P

P25 Projet 25

PAS Publicly Available Specification

PBN Performance Based Navigation

PCL Pilot Controlled Lighting

PDH Plesiochronous Digital Hierarchy

PHS Personal Handy-phone System

PLC Programmable Logic Controller

PMR Professional Mobile Radio

PMU Phasor Measurement Unit

PNT Positionnement, Navigation et Temps

PPE Programmation Pluriannuelle de l’Energie

PPK Post Processed Kinematic

PPP Precise Point Positionning

PPS Pulse Per Second

PRC Primary Reference Clock

PRP Parallel Redundancy Protocol

PRTC Primary Reference Time ClockPRS Public Regulated Service

PTP Precision Time Protocol

PVT Positions, de Vitesse et de Temps

PZ90 Parametry Zemli 1990

R

RAN Radio Access network

RATP Régie Autonome des Transports Parisiens

RBC Radio Block Center

RDMA Remote Direct Memory Access

RDS Radio Data System

REGINA Réseau GNSS pour l’IGS et la Navigation

RENAG REseau NAtional GNSS

REVOSIMA REseau VOlcanologique et SIsmologique de MAyotte

RFI Radio Frequency Interferences

RFI Radio France Internationale

RFID Radio Frequency Identification

RGF93 Réseau Géodésique Français 1993

RGP Réseau GNSS Permanent

RGPD Règlement Général sur la Protection des Données

RGS Référentiel Général de Sécurité

RID Règlement concernant le transport International ferroviaire des marchandises Dangereuses

RNAV Area navigation

RNP Required navigation performance

RTC Réseau Téléphonique Commuté

RTCM Radio Technical Commission for Maritime services

RTCP Réseau Téléphonique Commuté Public

RTE Réseau de Transport d’Electricité

RTK Real Time Kinematic

RTU Remote Terminal Unit

S

SAIV Secteurs d’Activité d’Importance Vitale

APRR société des Autoroutes Paris-Rhin-Rhône

SAS Système d’Alerte et de Sauvegarde

SATCOM SATellite COMmunications

SBAS Satellite-Based Augmentation System

SCADA Supervisory Control And Data Acquisition

SCHAPI Service Central d’Hydrométéorologie et d’Appui à la Prévision des Inondations

SCTV Système pour Coordination, Traitement et Visualisation

SDES Service de la Donnée et des Études Statistiques

SDH Synchronous Digital Hierarchy

SDMA Space Division Multiple Access

SEC Secondary Equipment Clock

SEDIF Syndicat des Eaux D’Ile de France

SEL Single Event Latch-up

SEU Single Event Upset

SHEM Société Hydroélectrique du Midi

SHOM Service Hydrographique et Océanographique de la Marine

SGAM Smart Grid Architecture Model

SGG Smart Gas Grid

SIC Systèmes d’Informations Client

SIG Systèmes d’Information Géographique

SIL Security Integrity Level

SIP Session Initiation Protocol

SiS Signal in Space

SMF Sondeur Multi-Faisceaux

SMR Surface Movement Radar

SNCF Société Nationale des Chemins de fer Français

SNTP Simple Network Time Protocol

SOLAS Safety Of Life At Sea

SONEL Système d’Observation du Niveau des Eaux Littorales

SONET Synchronous Optical NETwork

SSR Secondary Surveillance RADAR

SSU Synchronisation Supply Units

STARS Satellite Technology for Advanced Railway Signalling

STM Service de Transport Maritime

SURF-IA SURFace Indication and Alerting

SYRTE SYstème de Références Temps-Espace

T

T&S Timing & Synchronisation

TAI Temps Atomique International

TCXO Temperature Compensated X (Crystal) Oscillator

TC RT Technical Committee Rail Telecommunications

TDD Time Division Multiplex

TDMA Time Division Multiple Access

TEDS TETRA Enhanced Data Service

TETRA Terrestrial Trunked Radio

THF Trading Haute Fréquence

TIA Telecommunications Industry Association

TLS Transport Security Layer

TMA Terminal Manoeuvring Area

TNT Télévision Numérique Terrestre

TSN Time Sensitive Network

TT&C Telemetry, Tracking & Control

TWSTFT Two-way satellite time and frequency transfer

U

UE Union Européenne

UHD Ultra High Definition

UIT/ITU Union Internationale des Télecommunications / International Telecommunication Union

UTC Temps Universel Coordonné

UTE Union Technique de l’Electricité

UTM Unmanned aircraft systems Traffic Management

UMTS Universal Mobile Telecommunications System

UWB Ultra WideBand

V

VHF Very High Frequency

VLAN Virtual Local Area Network

VNAV Vertical NAVigation

VNF Voies Navigables de France

VoIP Voix sur IP

VOR VHF Omnidirectional Range

W

WAM Wide Area Multilateration

WAMPACS Wide Area Monitoring Protection and Control System

WCDMA Wideband Code Division Multiple Access

WGS 84 World Geodetic System 1984

WIOD World Input–Output Database

WLAN Wireless Local Area Network

WPAN Wireless Personal Area Network

X

XO X (Crystal) Oscillator

Z

ZIP Zone d’Inondation Potentielle

Suivi des éditions

| Version | Date | Description | Auteurs |
| --- | --- | --- | --- |
| Initiale | 22/10/2021 | Version initiale pour recueil des commentaires du CNRS | Aurélien FOURNET, FDC  César EL-BEZ, FDC  Franck MANGIN, FDC |

1. Report on Road User Needs and Requirements, GSA, 01/07/2019 [↑](#footnote-ref-1)
2. https://www.gsa.europa.eu/sites/default/files/uploads/technology\_report\_2020.pdf [↑](#footnote-ref-2)
3. https://www.gps.gov/systems/gps/performance/accuracy/ [↑](#footnote-ref-3)
4. https://www.researchgate.net/publication/228936470\_GNSS\_Status\_and\_perspective#pf3 [↑](#footnote-ref-4)
5. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OS-SDD\_v1.1.pdf [↑](#footnote-ref-5)
6. https://gssc.esa.int/navipedia/index.php/Galileo\_Performances#cite\_note-Galileo\_OS\_SDD-1 [↑](#footnote-ref-6)
7. https://directory.eoportal.org/web/eoportal/satellite-missions/content/-/article/cnss [↑](#footnote-ref-7)
8. http://www.csno-tarc.cn/en/system/introduction [↑](#footnote-ref-8)
9. Failure Modes and Models for Integrated GPS/INS Systems, Umar Iqbal Bhatti and Washington Yotto Ochieng, Imperial College London [↑](#footnote-ref-9)
10. https://www.spaceweatherlive.com/fr/aide/que-sont-les-eruptions-solaires.html [↑](#footnote-ref-10)
11. Etude TIMING IA - CE – 2019 [↑](#footnote-ref-11)
12. Etude TIMING IA - CE – 2019 [↑](#footnote-ref-12)
13. 1st Interim Meeting TIMINGIA Minutes [↑](#footnote-ref-13)
14. https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/ [↑](#footnote-ref-14)
15. Above Us Only Stars, C4ADS report [↑](#footnote-ref-15)
16. https://www.defensenews.com/home/2015/08/02/electronic-warfare-what-us-army-can-learn-from-ukraine/ [↑](#footnote-ref-16)
17. Brief analysis on the dependency on GPS of EU critical infrastructures: Focus on Timing & Synchronisation aspects, SpaceTech Partners, 2019 [↑](#footnote-ref-17)
18. https://www.arcep.fr/fileadmin/cru-1624346775/user\_upload/nos-sujets/5G/nossujets-5G-01.PNG [↑](#footnote-ref-18)
19. https://www.arstechnica.com/tech-policy/2020/05/millions-of-gps-devices-at-risk-from-fcc-approved-5g-network-military-says/ [↑](#footnote-ref-19)
20. https://www.chronos.co.uk/files/pdfs/pres/2017/Impact\_of\_GPS\_UTC\_Anomaly\_Event\_of\_January\_2016\_on\_the\_Global\_Timing\_Community.pdf [↑](#footnote-ref-21)
21. http://www.unoosa.org/pdf/icg/2016/nepal-workshop/4-21.pdf [↑](#footnote-ref-22)
22. https://www.c4reports.org/aboveusonlystars

    https://www.dailymail.co.uk/news/article-5168725/Brutal-sophisticated-Scottish-gang-snared.html#ixzz51zm7yOKJ [↑](#footnote-ref-23)
23. http://gnss-strike3.eu/ [↑](#footnote-ref-24)
24. https://www.nytimes.com/2016/04/02/world/asia/north-korea-jams-gps-signals.html [↑](#footnote-ref-25)
25. https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEF%20CON%2023%20-%20Lin-Huang-Qing-Yang-GPS-Spoofing.pdf [↑](#footnote-ref-26)
26. https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEF%20CON%2025%20-%20Karit-ZX-Security-Using-GPS-Spoofing-To-Control-Time.pdf [↑](#footnote-ref-27)
27. https://www.prnewswire.com/il/news-releases/tesla-model-s-and-model-3-prove-vulnerable-to-gps-spoofing-attacks-as-autopilot-navigation-steers-car-off-road-research-from-regulus-cyber-shows-300871146.html [↑](#footnote-ref-28)
28. Above Us Only Stars, C4ADS report [↑](#footnote-ref-29)
29. https://www.c4reports.org/aboveusonlystars [↑](#footnote-ref-30)
30. https://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space [↑](#footnote-ref-31)
31. https://www.secureworldexpo.com/industry-news/geneva-auto-show-gps-spoofing-stunt [↑](#footnote-ref-32)
32. GMCA 641613 White Paper - Ref. Ares(2016)6664714 - 28/11/2016 - <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ae828e15&appId=PPGMS> [↑](#footnote-ref-33)
33. https://www.regulus.com/blog/top-10-gps-spoofing-events-in-history [↑](#footnote-ref-34)
34. <https://www.ainonline.com/aviation-news/business-aviation/2019-06-11/pilots-oems-dealing-collins-gps-issue> [↑](#footnote-ref-35)
35. https://www.anfr.fr/controle-des-frequences/brouillages/les-brouilleurs-dondes/les-brouilleurs-gps/ [↑](#footnote-ref-36)
36. <https://www.anfr.fr/controle-des-frequences/brouillages/les-enquetes-de-lanfr/actualite/actualites/les-enquetes-de-lanfr-la-cle-qui-rendait-invisible-mais-qui-a-ebloui-les-gardiens-du-spectre/> [↑](#footnote-ref-37)
37. https://www.anfr.fr/controle-des-frequences/brouillages/les-enquetes-de-lanfr/actualite/actualites/les-enquetes-de-lanfr-une-box-internet-brouille-les-equipements-gps-et-galileo-dun-industriel/ [↑](#footnote-ref-38)
38. https://www.anfr.fr/controle-des-frequences/brouillages/les-enquetes-de-lanfr/actualite/actualites/courrier-aux-entreprises-qui-geo-localisent-leur-flotte-de-vehicules/ [↑](#footnote-ref-39)
39. https://www.anfr.fr/controle-des-frequences/brouillages/les-enquetes-de-lanfr/actualite/actualites/laction-de-terrain-de-lanfr-pour-debusquer-des-brouilleurs-gps-genant-le-guidage-des-avions/ [↑](#footnote-ref-40)
40. https://www.anfr.fr/controle-des-frequences/brouillages/les-enquetes-de-lanfr/actualite/actualites/brouilleurs-gps-lanfr-sensibilise-aux-dangers/ [↑](#footnote-ref-41)
41. https://www.anfr.fr/controle-des-frequences/brouillages/les-enquetes-de-lanfr/actualite/actualites/brouillage-a-nantes-lanfr-a-resolu-un-grave-brouillage-a-laeroport/ [↑](#footnote-ref-42)