Les atteintes aux systèmes de navigation satellitaires et le risque cyber

La navigation maritime et la manutention portuaire, comme bien d'autres secteurs d'activité, dépendent de systèmes de positionnement par satellite. Le réseau américain GPS (*Global Positioning System*), autrefois connu comme seul système en opération, fait aujourd'hui partie d'un grand nombre de systèmes satellitaires dédiés à la fourniture de signaux de localisation et de détermination du temps pour des services civils, militaires[1] et commerciaux. Cet ensemble de systèmes constitue les *Global Navigation Satellite Systems (GNSS)*. Ils regroupent les systèmes à portée universelle comme GLONASS qui appartient à la Russie, le BeiDou, à la Chine, le Galileo, à l'Europe et plusieurs systèmes régionaux. Tous ces systèmes émettent des signaux qui sont captés par des récepteurs installés à bord des navires ou à terre pour des missions diverses.

Mais les signaux émis sont généralement considérés comme étant faibles[2], et sont par conséquent vulnérables. Ils peuvent notamment être bloqués, endommagés ou compromis par toute sorte de menaces[3].

Par ailleurs, le GPS en particulier, fait l'objet d'une hyperconnectivité qui accroit le risque de déni de service compte tenu de l'augmentation de la surface d'exposition au risque[4], contribuant ainsi à de nombreux brouillages et leurrage de son signal.

L'organisation américaine *Center for Advanced Defense Studies* (*C4ADS)*, spécialisée dans l'analyse de données relatives aux problèmes de sécurité et de sûreté transnationaux, aux conflits globaux et au crime organisé[5], dans un rapport publié le 26 mars 2019[6], a fait état de

[1] Spirent, Fundamentals of GPS threats, how the growing threats to satellite navigation signals can impact your critical systems, and what to do about it, https://www.spirent.com/-/media/white-papers/positioning/fundamentals-of-gps-threats.pdf, p.2.

[2] Les cyber-spécialistes affirment que le problème des systèmes GPS et autres systèmes GNSS réside dans la faiblesse de leurs signaux, qui sont transmis à une distance de 12 500 km au-dessus de la Terre et peuvent être perturbés par des dispositifs de brouillage peu coûteux et largement disponibles : v. Jonathan Saul, Cyber threats prompt return of radio for ship navigation, https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT .

[3] Spirent, *Fundamentals of GPS threats*, préc. p.1.

[4] Observatoire du monde cybernétique, juin 2018, p.9.

[5] Olivier Chapuis, Brouillage et leurrage du GPS : le rapports de l'Organisation américaine C4ADS qui accuse la Russie, https://voilesetvoiliers.ouest-france.fr/equipement-entretien/electronique-embarquee/gps/brouillage-et-leurrage-du-gps-le-rapport-de-l-organisation-americaine-c4ads-qui-accuse-la-russie.

[6] https://www.c4reports.org/aboveusonlystars

9883 cas de leurrage des signaux GPS ayant affecté 1311 navires entre février 2016 et novembre 2018. Dans ce rapport, tous les cas de leurrage recensés sont rattachés à des considérations milliaires.

Pourtant, les activités civiles sont tout aussi vulnérables. En plus des impacts qu'elles peuvent avoir sur la navigation maritime, les atteintes aux *GNSS* constituent-elles des cyber menaces ? Et quand elles sont orchestrées par certains États, ne doivent-elles pas entrer dans la catégorie des risques de guerre?

Une grande variété de menaces

Deux grandes catégories de menaces affectent les *GNSS*. Il y a d'un côté des phénomènes naturels qui peuvent perturber les signaux émis par les différents systèmes satellitaires de positionnement. C'est en effet le cas des éruptions solaires, phénomène qui se caractérise par une interférence électromagnétique provoquée par les éruptions du soleil et d'autres activités solaires et qui dissipe les signaux émis par les satellites dans l'espace[7]. Il y a ensuite le phénomène d'obscuration au cours duquel les satellites ne sont plus suffisamment visibles et les signaux émis n'atteignent plus la surface de la terre et donc les récepteurs installés sur les navires. Dans ces deux cas, les systèmes embarqués perdent les signaux ou enregistrent des signaux erronés qui affectent la précision de la localisation des utilisateurs[8]. La deuxième catégorie de menaces rassemble celles des atteintes qui sont causées par les activités humaines, intentionnellement ou non. On peut mentionner le brouillage des signaux qui peut être le fait d'une surconnexion, mais aussi un acte délibéré dans une intention malveillante. La malveillance humaine peut aussi conduire au leurrage des signaux émis par les différents systèmes satellitaires.

Le brouillage consiste en une tentative de dégrader et de perturber la connectivité par une interférence dans les signaux émis par les *GNSS*[9]. Il implique une perturbation des signaux émis qui peut se détecter immédiatement par une perte de service sur les récepteurs. Ceux-ci ne sont plus en mesure de les capter. Le leurrage, beaucoup plus dangereux, introduit une information erronée ou fausse pour l'utilisateur du signal qui croît avoir une information valable[10]. Dans le cas du leurrage, les récepteurs captent bien des signaux, qui ne sont plus cependant ceux émanant des satellites. Normalement, les signaux émis par les systèmes de navigation satellitaires sont captés par des récepteurs à bord des navires. Ces signaux leur permettent de calculer la position réelle des navires qu'ils communiquent ensuite au système d'identification automatique qui assure la communication avec les autres intervenants. En cas de leurrage, des transmetteurs imitent les systèmes de navigation satellitaires en diffusant de faux signaux. Les récepteurs embarqués reçoivent ces signaux qui faussent alors le calcul de la position du navire et donc sa localisation et les informations inexactes sont ensuite communiquées à toute la chaine[11].

Impacts des atteintes aux signaux *GNSS* sur la navigation maritime

Les atteintes aux signaux émis par les *GNSS* ont des impacts sur la navigation maritime. Les navires victimes de leurrage peuvent être amenés à passer en mer plus de temps que prévu, et

[7] Spirent, *Fundamentals of GPS threats*, préc. p.6.
[8] Idem.
[9] David Livingstone and Patricia Lewis, *Space, the Final Frontier for Cybersecurity*?, Chatham House, RINA, 2016, p. 16.
[10] G. Goavec-Merou, J.-M Friedt, F. Meyer, *Leurrage du GPS par radio logicielle*, OSU Theta, Observatoire de Besan ̧con, 16 septembre 2018 , p. 1.
[11] C4ADS, *Exposing GPS spoofing in Russia and Syria*, Report, 2019, p. 7

engendrer par conséquent des frais supplémentaires pour les armateurs ou transporteurs. Des scénarios plus dangereux peuvent être envisagés. En effet, le leurrage peut conduire les navires à des positions totalement inattendues, ces derniers perdant systématiquement leur trajectoire sans que les équipages s'en aperçoivent[12].

Par ailleurs le brouillage ou le leurrage des GNSS, empêchant les systèmes embarqués de déterminer la position exacte du navire et celles des navires environnants, peuvent entrainer des collisions entre eux ou provoquer bien d'autres accidents.

De plus, compte tenu de la dépendance accrue à l'égard de la navigation par satellite, en particulier le GPS, le réflexe des équipages à revenir aisément aux moyens de navigation traditionnels à la suite d'un brouillage de signaux peut avoir été affecté, parce que les compétences ne sont plus utilisées quotidiennement et ne relèvent plus des habitudes[13]. Dans certaines situations, même quand l'équipage est informé du brouillage des signaux, la préparation psychologique n'empêche pas qu'il soit confronté à des difficultés. Le système de visualisation des cartes électroniques pourrait ne plus être à jour et le fonctionnement des systèmes d'information et de communication pourrait être paralysé même si l'équipage parvient à reprendre le contrôle du navire. Dans ces conditions, de graves accidents pourraient survenir.

Même si aucun des cas relevés par l'organisation américaine *C4ADS* n'a véritablement entraîné d'accidents maritimes majeurs, l'organisation souligne toutefois que le leurrage des signaux émis par les *GNSS* constitue une menace réelle pour la navigation maritime.[14]

Les atteintes aux *GNSS*, menaces cyber ou risques de guerre?

Aux termes d'une définition proposée par l'association des professionnels de la réassurance en France, le cyber risque désigne toute atteinte à des systèmes électroniques et/ou informatiques sous le contrôle d'une entreprise ou de ses prestataires, consécutive à un acte malveillant, une erreur humaine, des problèmes techniques ou un évènement naturel ou accidentel et entraînant des dommages pour l'entreprise[15] et/ou ses partenaires commerciaux.

Les atteintes aux signaux *GNSS*, qu'elles soient naturelles ou provoquées par l'homme, intentionnellement ou non, affectent les systèmes électroniques à bord des navires, destinés à capter ces signaux. Soit, ils sont défaillants, étant dans l'impossibilité de capter des signaux brouillés ; soit, ils fonctionnent normalement mais sont alimentés par de faux signaux. Dans ces deux cas, et dans bien d'autres, il en résulte un risque pour le navire : perte de temps en mer, risque de collision, d'échouement, d'égarement... L'atteinte n'a pas directement porté sur les systèmes électroniques embarqués mais elle aboutit à les rendre défaillants.

Les atteintes aux signaux *GNSS* constituent sans doute des menaces cyber quelle qu'en soit la cause. Elles prennent des formes différentes selon les cas. Ainsi des brouillages ou leurrages peuvent être perpétrés à des fins civiles contre des activités civiles. Mais dans des zones de conflits armés, des États ou des groupes armés pourraient aussi utiliser ces mêmes attaques

[12] Alain Grant, Paul Williams, Nick Ward, Sally Basker, préc.

[13] Selon une expérience menée par la General Lighthouse Authority pour illustrer les impacts du brouillage du GPS sur la navigation maritime : Alain Grant, Paul Williams, Nick Ward, Sally Basker, préc.

[14] Frédérick Auvray, les brouillages du signal GPS toujours actifs en méditerranée orientale, Le marin, 8 avril 2019 : https://www.lemarin.fr/secteurs-activites/shipping/33961-les-brouillages-du-signal-gps-toujours-actifs-en-mediterranee.

[15] Association des professionnels de la réassurance en France, in « Etude sur les cyber risques », juin 2016, p. 16.

pour créer des avantages militaires avant ou pendant un conflit[16]. Dans ce cas, les atteintes aux signaux *GNSS* constituent un acte de guerre, qui demeure avant tout une cyber attaque.

Le leurrage est particulièrement considéré comme faisant partie du monde de la cybercriminalité et de la guerre électronique[17].

Les risques cyber dans le secteur maritime prennent ainsi une tournure qui ne fait que compliquer les problématiques déjà délicates posées au sujet de l'assurance des risques cyber.

ADAM ASSURANCES - 33, Allées de Chartres – 33000 Bordeaux

www.adam-assu-mar.com

Le Lab – Recherches et innovations en assurances maritimes et transports
En partenariat avec
le Centre de droit maritime et océanique, Nantes
et le Centre de recherche et de documentation européennes et internationales, Bordeaux

Patrice A. EDORH-KOMAHE
pedorh-komahe@adam-assu-mar.com

Publié le 25 avril 2019

[16] Patricia Lewis, David Livingstone, *The cyber threat in outer space*, Bulletin of the Atomic scientist, 2016.
[17] Chris Lo, *GPS spoofing: what's the risk for ship navigation?* https://www.shiptechnology.com/features/ship-navigation-risks/.