



Les risques et les alternatives à la géolocalisation pour les armées

Dans les domaines de la défense et de la sécurité, les capacités de positionnement par satellite (GNSS) représentent un atout indispensable pour la géolocalisation et la synchronisation des systèmes. Utilisées dans un très grand nombre d'équipements, elles ont revêtu un caractère indispensable pour l'exécution de certaines missions. Cette dépendance comporte toutefois des risques qui constitueraient de réelles menaces à la sécurité nationale de nombreux États. C'est pourquoi les armées recherchent des méthodes pour remédier au problème.

La vulnérabilité des systèmes de géolocalisation

L'augmentation du nombre d'incidents liés aux systèmes de navigation par satellite depuis le début des années 2000 démontre clairement la réalité des menaces que font peser ces réseaux. Ces potentielles menaces peuvent être de différentes natures : des cyberattaques, des armes antisatellites ou encore des risques de collision liée aux débris spatiaux. Des actions de guerre électronique peuvent également couper les communications et brouiller les signaux sur un large spectre par le biais de la transmission d'un signal soit plus puissant soit identique¹ aux signaux transmis par les satellites *GPS*. De plus, les menaces naturelles comme les éruptions solaires peuvent gravement endommager certains satellites.

Plus concrètement, en 2003, à la veille du début de l'opération *Iraqi Freedom*, la société russe *Aviaconversiya*² a fourni aux forces armées irakiennes des dispositifs capables de brouiller les signaux *GPS* jusqu'à une distance de 200 km à la ronde. Toutefois, l'impact de ces brouilleurs sur les opérations n'a pas été significatif car des frappes de coalition ont neutralisé les sites. Cependant, les méthodes de brouillage se perfectionnent et plus récemment, d'importantes activités de brouillage réussies ont été reportées en Corée du Sud³ en 2016, en Norvège lors de l'exercice *ZAPAD 2017*, ou encore en mer Noire le 24 juin 2017⁴.

La recherche de la redondance dans les capacités de navigation

Afin de contrer les menaces sécuritaire et économique, les Américains ont créé le comité exécutif national du *PNT* (*Positioning, Navigation and Timing*) et entamé en 2008 le développement d'un système de navigation maritime à longue portée appelé *eLoran* (*Enhanced Long-Range Navigation*). En juin 2016, l'*US Navy* a simulé une panne *GPS* sur plusieurs semaines afin de continuer à expérimenter cette technique. En janvier 2018, l'*US Air Force* a conduit un exercice aérien interdisant l'usage du *GPS* ; les pilotes ont dû utiliser d'autres méthodes de navigation et de ciblage comme le radar *AESA* qui détecte les missiles et qui permet de s'orienter sur des distances plus courtes. L'*US Army* opte, quant à elle, pour l'utilisation de pseudolites qui permettent la modulation de la puissance des signaux en cas d'un éventuel brouillage ennemi. De plus, le Département de la Défense des États-Unis prévoit d'investir 5 milliards de dollars entre 2018 et 2022 dans le développement de la résilience du système *GPS* aux menaces extérieures.

Certaines innovations techniques permettraient également de s'affranchir des *GNSS* : les systèmes de navigation inertiels, la miniaturisation des horloges atomiques, ou des concepts d'appariement d'images radar, pourraient déboucher sur des capacités de navigation automatisées plus fiables. En 2013, via son programme *All-Source Positioning and Navigation* (*ASPN*), la *Defense Advanced Research Projects Agency* (*DARPA*) lance un système qui consiste à se positionner grâce aux signaux de télévision, de radio, ceux des antennes relais et même des dispositifs de brouillage adverses. Ce projet offre des solutions de navigation sur n'importe quelle plate-forme opérationnelle et dans tous les environnements.

*Le développement de dispositifs de détection de ces menaces, ainsi que les nouvelles techniques de positionnement seraient des solutions au problème. Leur usage pourrait mener les armées à se passer des systèmes *GPS* et à avoir un certain avantage sur leurs ennemis.*

Ces propos ne reflètent que l'opinion de l'auteur.

1 La transmission de signaux identiques à ceux transmis par les satellites *GPS* est une technique de leurrage.
2 *Aviaconversiya* est un fabricant russe de produits de contre-mesures électroniques.
3 Environ 1000 avions civils et 700 bateaux auraient été affectés par ces manœuvres de brouillage.
4 Il s'agit d'un cas de brouillage par usurpation à l'encontre de navires civils.