F-35, M-Code et PRS : la neutralité suisse à l'épreuve des satellites

Le conflit en Ukraine révèle l'importance cruciale de la guerre électronique, dont l'un des piliers est constitué par les systèmes de positionnement et de navigation PNT (Position, Navigation, Timing), qui reposent sur des constellations satellites. Or, en cas de guerre électronique, ces signaux peuvent être brouillés, trompés… ou coupés. Comment garantir notre indépendance dans un monde où le ciel est devenu un champ de bataille numérique ?

La guerre électronique et les PNT

De tous temps, la connaissance du terrain a été décisive pour les armées. Connaître le terrain, savoir précisément où sont positionnées les unités, est un prérequis pour décider des opérations et constitue un avantage décisif. Les cartes d'Etat-Major, la carte Dufour sont des exemples bien connus, qui permettaient un positionnement précis avec boussole.

De nos jours, la localisation se fait par des systèmes de positionnement et de navigation (PNT) qui se basent largement sur les systèmes globaux de navigation par satellites (GNSS):

- GPS (USA)
- Galileo (Europe)
- GLONASS (Russie)
- BeiDou (Chine)

Nous utilisons tous quotidiennement la partie civile de ces GNSS. Pourtant, en cas de guerre électronique nous ne pourrions pas nous y fier car ils sont bien trop faciles à brouiller, voire à tromper en nous fournissant un faux positionnement (ce qu'on appelle le spoofing).

C'est pour cette raison que les Etats qui contrôlent ces GNSS ont développé des versions militaires de leurs systèmes: le M-Code américain, basé sur le GPS, et le PRS de l'Union Européenne, basé sur Galileo. Ces versions militaires sont conçues pour résister au brouillage (*jamming*), à la falsification (*spoofing*) et pour fonctionner même en cas de crise grave (catastrophe, guerre, cyberattaque, etc.).

Les GNSS militaires: dépendance stratégique

La Suisse ne dispose pas (encore ?) des accès à ces systèmes GNSS militaires. Notre pays bénéficie d'une participation au programme Galileo, mais n'a pas encore conclu un accord pour le service PRS. Sans cela, ni les autorités suisses ni ses forces armées ne peuvent exploiter le signal crypté PRS destiné à des usages sécurisés. C'est d'ailleurs également le cas de la Norvège, qui héberge pourtant deux stations au sol pour Galileo destinées à soutenir la surveillance PRS (Svalbard et Troll Station dans l'Antarctique). La Norvège, en revanche, a accès au M-Code.

Cependant, l'achat du F-35 par la Suisse nous ouvre potentiellement la porte au M-Code américain. À ma connaissance, aucune communication officielle n'a encore confirmé si nous avons demandé ou obtenu l'accès complet au M-Code, mais cela est probable voire nécessaire pour une utilisation opérationnelle conforme aux capacités du F-35, qui intègre nativement un récepteur GPS militaire M-Code, indispensable pour sa navigation de précision, son guidage de munitions et sa résilience aux brouillages GNSS.

L'achat du F35 par la Suisse rend l'accès au M-Code techniquement indispensable.

Même si cela n'est pas automatique, il est très probable que nous obtenions l'autorisation des autorités américaines (dans le cas contraire, nos futurs F-35 voleraient en mode dégradé). Cela placerait la Suisse dans le cercle des nations alliées de confiance des Etats-Unis, sans pour autant rejoindre l'OTAN.

La dépendance au système américain est cependant problématique sur le plan politique. Il suffirait en effet d'une décision unilatérale du président américain pour couper les accès au M-Code, ce qui peut se faire d'un simple clic. De plus, le simple fait d'être intégré, de facto, dans le cercle des nations alliées des Etats-Unis est parfaitement contraire à notre principe fondamental de neutralité.

Sur le plan politique, il serait bien plus intéressant pour la Suisse d'avoir accès au PRS de l'UE, avec qui nous partageons les mêmes valeurs et le même agenda. Mais les choses paraissent à ce jour beaucoup plus compliquées, même si nous participons au programme Galileo.

Alternatives au M-Code et au PRS

Les alternatives existent cependant, même si elles sont encore moins robustes que les accès aux GNSS militaires. Les systèmes PNT n'utilisent pas seulement les GNSS, qui peuvent être indisponibles (tunnels, sous-sols) ou brouillés. Ils utilisent également d'autres sources. Par exemple, des systèmes gyroscopiques, les signaux radio, des signaux d'opportunité comme les réseaux 4G et 5G, l'IA, etc…

De plus, beaucoup de récepteurs GNSS offrent une redondance au niveau des constellations (GPS, Galileo, Glonass, Beidou) et peuvent ainsi recouper les informations de plusieurs systèmes. Il y a aussi de simples senseurs inertiels qui augmentent la capabilité pendant une certaine durée (comptée en minutes ou dizaine de minutes).

Plusieurs solutions permettent aujourd'hui de combiner intelligemment ces sources pour renforcer la fiabilité. Les chercheurs travaillent activement sur des moteurs d'intégrité sophistiqués (*Integrity Engines*) qui vérifient en temps réel la fiabilité des données, détectent les erreurs, les brouillages ou les falsifications, et garantissent une localisation sûre, même dans un environnement hostile.

Un enjeu crucial

Il est d'autant plus critique pour notre pays de disposer de solutions PNT robustes que ces technologies sont désormais omniprésentes. C'est le cas du domaine des transports civils, bien entendu. Mais également des services financiers qui utilisent une fonction discrète mais essentielle fournie par les GNSS: le temps exact, à la nanoseconde, qui permet d'horodater les transactions à haute fréquence. Les réseaux électriques en dépendent également pour détecter les anomalies et prévenir les coupures. Et ce ne sont que des exemples parmi d'autres.

En cas de guerre électronique, comme en sont actuellement victimes les pays baltes par exemple, l'arrêt du PNT paralyserait notre société numérique (arrêt des réseaux mobiles, perte de position pour les ambulances ou les trains, erreurs dans les bourses, pannes électriques). Le PRS européen a d'ailleurs également été conçu pour les services gouvernementaux comme la police, les secours, les ambassades, les infrastructures etc...

C'est pour ces raisons que notre politique concernant les systèmes PNT doit être positionnée très haut dans la liste de nos priorités. Elle ne concerne pas seulement les aspects militaires, mais tous les aspects de notre vie économique.

Gilbert Bapst
Vouvry

Scientifiques sur le terrain près du centre spatial d'Andøya au nord de la Norvège pour tester des équipements PNT de pointe (mesures de jamming et spoofing). Crédit: Gutec AB – reproduction autorisée

Besoins pour la Suisse : accès à services PNT sûrs et fiables		
M-Code (GPS) - USA	**PRS (Galileo) - UE**	**PNT indépendant**
Accès futur grâce à l'achat du F-35 ? Non confirmé	Négociation pour PRS pas encore entreprises	Sans utilisation de GNSS sécurisés (M-Code ou PRS)
La Suisse ne participe pas au programme américain: dépendance scientifique et politique totale par rapport aux USA. Problématique pour la neutralité	La Suisse participe au programme Galileo : compatible avec la neutralité	Développement et acquisition de solutions PNT indépendantes. Totalement compatible avec la neutralité
Risques de perdre les accès : élevés	Risques de perdre les accès : négligeables	Risques de perdre les accès : nuls

Accès aux GNSS sécurisé : situation actuelle et alternative pour la Suisse