L'espace : la frontière finale de la cybersécurité

Matthias POPOFF
Analyste Marché
CyberInflight

Les questions de cybersécurité appliquées au domaine spatial ne sont pas nouvelles, mais elles ont pris une nouvelle tournure depuis le début des années 2020. Cette prise de conscience s'est progressivement constituée vers la deuxième moitié des années 2010, où la croissance de l'économie spatiale à travers le phénomène du New Space a conduit au développement d'une nouvelle génération d'acteurs privés au sein du secteur spatial. Cette croissance rapide a rapidement introduit des problématiques de cybersécurité dans son sillage.

Au cours des années 1990, il était coutume de percevoir l'évolution des différents programmes spatiaux de la NASA à travers la règle « *pick three* » en référence au slogan « *Faster, Better, Cheaper* » de Daniel GOLDING alors directeur de l'agence. Cette règle stipulait que les facteurs de vitesse, d'efficacité et de coûts d'un programme spatial ne pouvaient être tous les trois atteints simultanément. Le New Space peut affirmer remettre en cause ce paradigme en introduisant des programmes peu coûteux, très rapides et très efficaces. Cependant, la question de la cybersécurité est trop souvent absente. Cette situation amène à imaginer un nouveau paradigme où la cybersécurité joue comme un facteur à part entière, on parlerait alors de « *pick four* ». Un programme pourrait alors être rapide, peu coûteux, efficace mais pas sécurisé. De fait, la cybersécurité implique des coûts supplémentaires, du temps additionnel pour l'implémenter correctement et a un impact non négligeable sur les performances des systèmes spatiaux (énergie, place, poids). S'il est à rappeler qu'il ne s'agit nullement d'une loi scientifique (et que l'exemple de la constellation Starlink démontre qu'il est possible de combiner les quatre facteurs), le « *pick three/four* » souligne les problématiques de priorité du domaine spatial quand il s'agit de cybersécurité.

La jonction du cyber et du spatial au carrefour des compétences

L'un des problèmes principaux concernant l'arrivée de nouveaux acteurs cyber, qu'ils soient institutionnels ou économiques, est d'aborder le domaine spatial sans prendre en compte ses particularités. Le secteur spatial se caractérise par la diversité de ses infrastructures et surtout le caractère unique du milieu dans lequel elles sont déployées, c'est-à-dire : l'espace extra-atmosphérique. On y retrouve plusieurs segments connectés à des milliers de systèmes disposés sur plusieurs orbites. Au sein de ce secteur, les données constituent la raison pour laquelle des systèmes sont envoyés en orbite. Il s'agit d'un marché des données, par les données et pour les données. Sécuriser les données ainsi que les systèmes qui les collectent ou

les font transiter devient dès lors une nécessité et une priorité. Il en ressort que la sécurisation des différentes composantes du secteur spatial ne s'effectue pas toujours selon les mêmes contraintes que les autres domaines. Certes, les contraintes de poids, de taille et d'énergie sont présentes dans d'autres domaines (voitures autonomes, etc.), mais l'espace extra-atmosphérique est un domaine à part entière. La sensibilisation aux questions cyber a pris un retard considérable en comparaison des autres domaines. La guerre en Ukraine a en ce sens fortement contribué à faire évoluer les mentalités.

Le spatial à l'épreuve de la guerre en Ukraine

Le 24 février 2022, quelques heures avant que les premiers chars russes n'entrent en Ukraine, une cyberattaque de grande ampleur touchait le réseau satellitaire de l'opérateur américain Viasat, dont dépendait l'armée ukrainienne pour certaines de ses capacités critiques. Plusieurs dizaines de milliers de modems furent neutralisés jusqu'en Europe de l'Ouest. Cette attaque a constitué un tournant majeur en matière de cybersécurité spatiale. Les initiatives se sont depuis démultipliées à différents niveaux sans pour autant permettre au secteur d'atteindre un bon niveau de résilience et de maturité face aux cybermenaces. L'implication directe de nombreuses entreprises spatiales privées au sein du conflit ukrainien a abouti à une hausse exponentielle du nombre de cyberattaques.

Au-delà du conflit en Ukraine, la croissance des cybermenaces à l'encontre du secteur spatial a notamment été soulignée à travers les *Pentagon Leaks*. Parmi les nombreux documents qui ont fuité, certains évoquaient la mise en place d'armes cyber par la Chine qui seraient destinées aux systèmes spatiaux et à leurs infrastructures. La multiplication des actions offensives entraîne une course aux armements. Les Etats et les entreprises établissent des initiatives dans le but de développer et d'assurer le niveau de cybersécurité des systèmes spatiaux et surtout de maintenir la viabilité de capacités souveraines dans l'espace extra-atmosphérique.

L'état de l'art de la cybersécurité spatiale

Il existe aujourd'hui un écart important entre les Etats-Unis et l'Europe concernant le niveau de maturité face aux menaces. Un bon indicateur pour évaluer le niveau de maturité d'un écosystème face aux menaces cyber est la date d'établissement d'un ISAC (*Information Sharing Center*). Le Space ISAC américain a été créé en 2019 et commence tout juste à entrer dans sa pleine phase opérationnelle. De son côté, la commission européenne a annoncé début avril 2023 le lancement de travaux préliminaires en vue de l'établissement d'un ISAC européen supervisé par EUSPA (European Union Agency for the Space Programme). Cet écart n'est pas surprenant étant donné que les Etats-Unis, première puissance spatiale à l'échelle mondiale et centre de gravité du développement des TIC (Technologies de l'Information et de la Communication), ont été les premiers visés par les cyberattaques. De fait, la puissance étatique la plus exposée est également celle qui a le plus à perdre et donc le plus à défendre.

Les initiatives visant au renforcement de la résilience des systèmes spatiaux et de leurs infrastructures aux Etats-Unis ont connu une nette croissance à partir du milieu des années 2010. Aujourd'hui, il existe une solide base juridique au sein de l'écosystème américain (Framework SPARTA, SPD-5, CMMCv2, ...) ainsi que de nombreuses initiatives de recherche soutenues et financées par l'Etat américain, telles que la compétition Hack-A-Sat.

De l'autre côté de l'Atlantique, les initiatives en matière de cybersécurité spatiale ont réellement commencé à monter en puissance à partir de l'attaque de Viasat. L'éclatement du cadre européen entre les agences spatiales nationales, l'ESA, EUSPA, ainsi que les différentes forces armées, n'a pas aidé à accélérer la mise en place d'un socle solide.

Néanmoins, plusieurs programmes sont mis en place et tendent à apporter une réponse face aux défis. On peut notamment citer le programmes ARTES (*Advanced Research in Telecommunications Systems*) mais également la constellation IRIS2 dont l'un des axes principaux est la cybersécurité. Ces programmes illustrent une volonté certaine de rattrapage, mais traduisent également un état réactif plus qu'actif de la part des décideurs à différentes échelles.

La place du cyberspatial dans la conduite des opérations

Le cyber est désormais au cœur des opérations spatiales des forces armées. Lors de son intervention à l'événement CyberSatGov, le Colonel John Smail de l'US Space Force (USSF) avait déclaré que : « L'espace est unique dans la mesure où il dépend réellement du cyberespace. Les autres domaines de guerre ne sont pas en permanence dans le cyberespace ». Les opérations cyber font partie des sept disciplines de la puissance spatiale définies par l'USSF. Cette intégration étroite s'effectue en parallèle d'une dépendance toujours plus forte des infrastructures terrestres vis-à-vis des systèmes spatiaux. A ses débuts, le spatial revêtait une fonction stratégique par sa place vitale dans les stratégies nucléaires des deux blocs. Les années 1980 et la guerre du Golfe en 1991 a fortement contribué à intégrer le spatial dans la conduite opérationnelle des opérations militaires. La guerre en Ukraine a signé une nouvelle étape de cette évolution avec une intégration inédite du spatial jusqu'au niveau tactique. De fait, le spatial appuie chaque infrastructure et composante d'un pays, d'une société ou d'une économie. Dans ce contexte, chaque système spatial non sécurisé représente une potentielle faille qu'il convient de sécuriser afin d'éviter une perte brutale de capacité.

Le récent phénomène économique du New Space, qui se caractérise par une forte croissance du secteur privé au sein du secteur spatial, ne doit pas faire oublier que l'espace reste un milieu intrinsèquement politique.

Dans cet écosystème en pleine évolution, la conclusion peut être tirée qu'« il n'y a pas de puissance spatiale sans cyberpuissance ».