3i3s
le département de cybersécurité satellitaire et spatiale sort de terre

par : Dr Isabelle Tisserand
Vice-présidente du département cybersécurité de 3i3s
Institut Indépendant International pour les solutions satellitaires et spatiales

Biographie.
Isabelle Tisserand est docteur de l'Ecole des Hautes Etudes en Sciences Sociales, anthropologue expert en sécurité et défense. Spécialiste de la protection des patrimoines stratégiques, elle est également enseignante, auteur de plusieurs livres, et Capitaine de corvette de la réserve citoyenne de la Marine nationale.

Les enjeux de la cybersécurité satellitaire et spatiale sont colossaux en matière de sécurité et de défense des populations. La constellation de réseaux de satellites est vitale pour soutenir les activités humaines et participe, lorsque tout fonctionne au mieux, à l'équilibre global de la défense, de l'économie et de la vie sociale présente et future des individus.
L'industrie n'a jamais été aussi florissante dans le domaine de l'aérospatial, mais de nouveaux risques pèsent sur ses patrimoines (la collision des satellites avec des débris ou autres objets spatiaux, le hacking, les armes anti-satellitaires, les conduites inappropriées, etc.), raison pour laquelle il est nécessaire d'innover en matière de cybersécurité globale. La promotion de cette adaptation se fonde sur l'usage des technologies certes, mais aussi et surtout sur les sciences humaines et sociales, parce que le capital spatial est composé des patrimoines matériel, informationnel, mais surtout humain.

L'écosystème satellitaire.
L'écosystème satellitaire est composé de satellites artificiels, eux-mêmes composés de charges utiles sélectionnées en fonction des missions, de plateformes permettant d'assurer certaines fonctions : fourniture d'énergie, contrôle thermique, propulsion, orientation et communication.
L'usage des satellites nécessite des moyens de support au sol dont les centres de contrôle pour leur surveillance, les réseaux de stations terrestres, les centres de collectes et les centres de traitement des données collectées par leurs charges utiles.

Près de 1300 satellites ont été répertoriés fin 2015. Le rapport « *Satellite Manufacturing and Launch Services, 6th Edition* », annonce une croissance de 600% dans les dix années à venir pour les satellites non-géostationnaires.
Secteur d'activité en perpétuelle évolution, le domaine satellitaire répond certes aux besoins d'innovation mais aussi à l'arrivée de nouveaux opérateurs1.

Statut et fonctions des services satellitaires.

Les satellites sont des systèmes d'information spatiaux que l'on peut parfaitement intégrer au parc des infrastructures sensibles et critiques à protéger et à défendre2. En ce sens, les lois, les règlements et les pratiques de défense propres aux Opérateurs d'Importance Vitale, doivent être appliqués. Nous pensons ici et en France, à la Loi de Programmation Militaire, aux directives de sécurité, aux politiques de protection des patrimoines publiées par les États et par les entreprises privées.
Les usages des satellites sont incontournables et indispensables en matière de maîtrise des risques climatiques et naturels, alertes précoces, météorologie, télédétection3, navigation, reconnaissance géographique, exploration, observation, géolocalisation, surveillance, applications militaires, télémédecine, transactions financières, accès à l'Internet, télécommunications.
Le développement des projets industriels et scientifiques associés aux emplois qu'ils génèrent et liés aux missions spatiales d'exploration, d'exploitation des ressources spatiales (météorites), d'essaimage humain sur des exoplanètes, s'appuient fondamentalement sur leur utilisation.

Mais ces systèmes restent vulnérables. Plusieurs types d'attaques de satellites par hacking sont courants. Par exemple, le « *Jam* » est comparable à une attaque DDoS qui permet de « spammer » le signal et les ondes radio d'un émetteur ou d'un récepteur, d'encombrer de manière exponentielle les flux d'émissions d'informations de façon à ce que le signal ne puisse plus atteindre sa destination initiale. Le « *Eavesdropping* » permet à un hacker

1 https://www.giiresearch.com/report/ns236928-global-satellite-manufacturing-launch-markets-2nd.html#top

2http://nasasearch.nasa.gov/search?utf8=%E2%9C%93&affiliate=nasa&query=satellites&commit=Search

3 http://www.satimagingcorp.com/satellite-sensors/

d'entendre, de voir les transmissions et d'utiliser les données interceptées. Le « *Hijacking* » consiste à utiliser illicitement un satellite. La prise de contrôle permet de modifier le signal et de le remplacer par un autre. Des informations envoyées par l'Internet via un satellite peuvent donc être détournées, copiées, volées, truquées. « *Les attaques au sol* » de centres de contrôles peuvent majorer des attaques spatiales, et avoir des impacts immédiats sur les activités humaines économiques, scientifiques, politiques et sociales. N'oublions pas, également, les techniques de hacking social et psychologique qui permettent d'obtenir des informations auprès d'acteurs clés - personnels impliqués dans les programmes de gestion des satellites -, afin de construire des attaques supportées par des technologies.

Pour une stratégie de cybersécurité globale des patrimoines spatiaux.

Les mesures de sécurité et de défense des patrimoines spatiaux font partie des programmes de protection des infrastructures nécessaires au fonctionnement des satellites. La stratégie doit être globale : les mesures de prévention (sûreté, sécurité, défense, cybersécurité, cyberdéfense) doivent être appliquées sur terre et dans l'espace et pour l'ensemble des patrimoines cités.

Toutes les infrastructures terrestres doivent être parfaitement sécurisées physiquement, administrativement, techniquement et surtout humainement. Ce dernier point est de plus en plus développé dans les méthodologies internationales et trop peu en Europe.

Physiquement, les stations de contrôle et tout ce qui permet d'assurer leur fonctionnement doivent être protégés par des limites infranchissables pour qui ne serait pas autorisé à accéder à ces sites, avec des codes d'accès, des caméras, des enregistrements des entrées, des activités et des sorties.

Administrativement et juridiquement, les organigrammes doivent être précis, l'accès et l'utilisation des sites et de ses objets doivent faire l'objet de règlements communiqués aux personnels, quelles que soient leurs fonctions.

Techniquement, seule la redondance technologique des stations au sol, des réseaux électriques et des *hardware* et *software* à bord des satellites, peuvent permettre d'éviter les interruptions de service. Le chiffrement est également une parade robuste pour éviter le hacking.

Techniquement, le piratage qui utilise les interceptions électroniques à distance peut également être évité, grâce aux techniques de brouillage des signaux émis par les stations de contrôle.

Du point de vue comportemental, la protection doit être assurée par des agents de sécurité rigoureusement sélectionnés et formés au plus haut niveau. Cette mesure doit concerner tous

les acteurs impliqués dans les projets. Ainsi, tous les personnels doivent faire l'objet de dépistages préventifs en termes de risques comportementaux pouvant avoir une incidence sur la sécurité des fonctionnements satellitaires et des centres de contrôles. Ils doivent être sensibilisés, formés et entraînés aux risques physiques, psychologiques, techniques et sociaux inhérents aux patrimoines spatiaux stratégiques ; aux plans de continuité d'activités et de résilience ; au maintien en condition opérationnel, à l'interopérabilité entre opérateurs. Enfin, l'ensemble du dispositif de sécurisation doit aussi pouvoir bénéficier du renseignement au sens large, car il procure une connaissance qui permet l'anticipation.

La compétition satellitaire.

A peu près 1300 satellites sont exploités par 80 pays et organisations différentes. Les dépendances satellitaires sont sujettes au risque de compétition qui peut engendrer de graves conflits lorsqu'elle s'appuie sur l'usage de cyberattaques et d'armes anti-satellitaires. Le Brésil et l'Inde4 travaillent sur ce thème, tout comme la Russie et la Chine qui, de fait, challengent la dominance américaine.

En ce sens, la gouvernance est un sujet actuel primordial, notamment pour l'Europe qui détient des capacités et des patrimoines significatifs distribués de manière très sporadique dans le monde (sites, projets, équipes, agences, laboratoires). Il y a d'une part, un bénéfice à promouvoir l'autonomie de la cybersécurité et de la protection des services spatiaux, en prévenant les risques géopolitiques et, d'autre part, une difficulté a à adopter une politique internationale, du fait de la coexistence complexe qui existe entre les affaires mondiales et les gouvernances multilatérales5.

La cartographie des risques et des réponses, en termes de sécurité et de défense, est connue et commune à tous. Mais la concertation entre les pays est complexe du fait que les décideurs ne partagent pas forcément les mêmes approches quant aux principes politiques et stratégiques.

Une politique de base, commune aux pays européens impliqués dans les programmes spatiaux, représenterait un premier effort salutaire, permettant de développer des principes communs et le partage d'approches et de méthodes. Il existe déjà des codes de conduite mais ils ne suffisent pas6.

---

4 https://www.geospatialworld.net/wp-content/uploads/2016/05/Draft-NGP-Ver20120ammended_05May2016.pdf

5 Space security for Europe, Issue, report N°29, July 2016. Rapporteurs : Massimo Pellegrino, Gerald Stang.

6 Lucia Marta. Code of conduct on space activities : unsolved critiques and the question of its identity. FRS note 26/2015, December 2015.

A ce propos, la France montre actuellement l'exemple en adoptant et en promouvant la directive européenne de sécurité (DNIS)7. En effet, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) prévoit le renforcement de ses capacités nationales de cybersécurité, afin d'établir un cadre de coopération entre États membres pour le renforcement de la cybersécurité d'opérateurs issus de secteurs clés, et de certaines plateformes numériques.

Bien que cela ne concerne encore que le patrimoine informationnel, le nouveau concept d'Opérateurs de Services Essentiels (OSE) publié dans la directive laisse espérer qu'une politique globale de cybersécurisation des trois patrimoines cités, se développera dans un avenir proche.

La gouvernance opérationnelle.

Une gouvernance spatiale, si elle veut faire l'objet de politiques efficaces, ne doit pas s'éloigner de la pratique de terrain. La recherche d'excellence, en matière de gouvernance opérationnelle et de cybersécurité satellitaire et spatiale, doit s'appuyer sur les RETEX (retours d'expériences) et la recherche scientifique.

De nombreux thèmes doivent être étudiés pour l'équilibre des besoins et un bon niveau de garantie de fonctionnement du parc satellitaire : outre la sécurité spatiale et sa gouvernance locale et globale, il est nécessaire de travailler à la robustesse de la fiabilité, la flexibilité, l' « abordabilité » (en termes de coûts), la disponibilité et la durabilité des patrimoines.

Cette approche nécessite une coopération évidente entre le monde civil et le monde militaire, différents acteurs tels que décideurs, chercheurs, ingénieurs, etc. et par conséquent différentes disciplines scientifiques.

Soulignons que 2016 est une année particulièrement critique pour la sécurité spatiale européenne du fait de projets vitaux (Copernicus8, Galiléo9). C'est une année au cours de laquelle le développement des affaires spatiales est en nette progression, qu'il s'agisse de projets scientifiques relatifs à l'essaimage humain interplanétaire, de projets industriels et commerciaux. Tout cela démontre que la dimension économique des programmes spatiaux est forte et totalement assujettie à la cybersécurité globale, quels que soient les programmes et les pays.

---

7 https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

8 http://www.developpement-durable.gouv.fr/IMG/pdf/Seminaire_ImST_060913_Copernicus.pdf

9 https://galileo-mission.cnes.fr/

La bonne santé économique des différents acteurs du marché et les partenariats de financements publics et privés sont des conditions indispensables pour relever les prochains défis qui sont pour l'essentiel et comme nous l'avons dit, la concertation des approches en matière de sécurité par les gouvernements avec la publication d'un cadre légal unifié, les politiques de sécurité et de défense globales, les politiques industrielles, l'accroissement des marchés, le développement de nouvelles applications, le management du trafic satellitaire et spatial, l'éducation des citoyens aux usages satellitaires et spatiaux dont ils ont et auront besoin, les projets d'exploration extra-planétaire.

Autre défi de l'année 2016, Philippe Boissat, fondateur de 3i3s, ingénieur spécialiste des satellites, Senior Advisor Aerospace & Defense Europe & United State of America chez Deloitte, a demandé la création du département de cybersécurité dans les programmes spatiaux dont la dimension humaine est fondamentale. En effet, les personnels du domaine évoluent dans un milieu spécifique car spatial et international, ouvert et sans limite lorsque l'on songe par exemple aux activités de recherche et de développement. Cette population professionnelle interculturelle et interdisciplinaire, ouverte d'esprit et ouverte sur le monde, aborde la cybersécurité d'une façon particulière que nous avons étudiée, et la communication, pour plus de cybersécurité dans leurs réflexes, doit être adaptée à leurs profils et à leurs activités.

Les sciences humaines et sociales cohabitent par conséquent de manière cruciale avec les sciences technologiques en termes de recherche dans le département de cybersécurité de 3i3s. Nos analyses et nos réponses stratégiques permettent, entre-autres, de soutenir les fondamentaux de l'espèce humaine que sont l'exploration, son développement et son adaptation pour sa continuité.

Enfin, nous observons que la nature de certains services satellitaires - notamment en matière de prévention de crises majeures pour la protection de la planète Terre et de ses populations -, nous engage à une analyse profonde de l'évolution naturelle de « La pensée de défense », en nous défiant régulièrement sur les principes de dissuasion et de paix.

Contactez nous sur le site http://3i3signature.com/

Notre équipe est là pour vous conseiller et pour vous aider à entretenir l'*aerospace spirit*