La cybersécurité dans l'espace

Le cyberespace et l'espace extra-atmosphérique présentent de nombreuses similitudes. Ces deux domaines ouverts, partagés, étendus, transfrontaliers et intangibles sont de plus en plus interconnectées du fait de la numérisation, qui expose les satellites, les stations sol et les terminaux utilisateurs aux menaces cyber. Il est essentiel de comprendre les liens entre l'espace et le cyberespace afin de mieux protéger les équipements spatiaux dont les sociétés dépendent.

Par Clémence Poirier

Deux satellites dans l'espace juxtaposés sur un fond de lignes de code de programmation.
Image générée à partir de DALL-E Open AI

Le 24 février 2022, quelques heures avant l'invasion de l'Ukraine, une cyberattaque a visé le réseau satellitaire KA-SAT de Viasat, utilisé par les forces armées ukrainiennes. Destinée à empêcher l'Ukraine de s'appuyer sur les capacités spatiales pour répondre à l'invasion, l'attaque a également touché des infrastructures critiques et des milliers de particuliers à travers l'Europe. Cet événement a mis en lumière la vulnérabilité des systèmes spatiaux aux menaces cyber.

Les satellites, comme tout objet numérique, peuvent être piratés. Mais comme il s'agit d'une technologie qui n'est pas forcément visible dans la vie quotidienne du grand public, il est facile d'oublier à quel point les sociétés en dépendent. Rien qu'aux États-Unis, l'impact économique d'une interruption des services GPS pourrait atteindre 1 milliard de dollars par jour. Une cyberattaque contre un satellite peut entraîner des perturbations majeures dans les marchés financiers, les transports routiers, les prévisions météorologiques, les connexions internet, les réseaux électriques, le contrôle aérien et les opérations militaires, le tout simultanément.

Si cette menace n'est pas nouvelle, elle a été renforcée par la numérisation des systèmes spatiaux et de l'espace dans son ensemble. Aujourd'hui, beaucoup de satellites intègrent des composants logiciels et sont connectés à internet. En outre, la plupart des processus de conception, de fabrication, d'essai, de lancement et d'exploitation reposent sur des technologies numériques. Par exemple, la première connexion Bluetooth avec un satellite a été établie à une distance de plus de 600 km. Ces engins spatiaux peuvent donc être assimilés à de coûteux ordinateurs en orbite, piratables au même titre que n'importe quel autre appareil connecté. Cette tendance a mené à un élargissement de la surface d'attaque, qui désigne tous les points d'entrée pouvant être exploités par un attaquant pour perturber, endommager, désactiver ou prendre le contrôle d'un satellite.

Le caractère intrinsèquement hostile de l'espace (éloignement par rapport à la Terre, rayons cosmiques, températures extrêmes, radiations, etc.) crée un ensemble unique de défis politiques, juridiques, techniques et commerciaux dans un secteur qui a longtemps fait abstraction des menaces cyber. De surcroît, la cybersécurité ne se limite pas aux satellites en orbite, mais couvre

également la chaîne d'approvisionnement et les segments sol, spatial et utilisateur tout au long de leur cycle de vie, ce qui ajoute davantage de complexité.

Cette analyse examine l'évolution du secteur des télécommunications et du paysage des menaces dans l'espace, les cybermenaces auxquelles les systèmes spatiaux sont exposés, ainsi que les questions politiques, réglementaires et commerciales qui en découlent. Pour finir, elle fournit un aperçu de la manière dont la Suisse pourrait tenter de remédier à ces vulnérabilités.

Militarisation et arsenalisation de l'espace

La militarisation de l'espace désigne l'utilisation du spatial pour la conduite d'opérations militaires sur Terre. Elle a commencé dans les années 1950, en parallèle des avancées réalisées dans le domaine des missiles balistiques et des armes nucléaires. Dans les années 1990, le débat sur la militarisation de l'espace s'est recentré sur les aspects opérationnels. Les satellites sont devenus des outils essentiels au déroulement des opérations militaires sur Terre. Depuis 2022, les discussions sur la militarisation sont davantage axées sur la commercialisation, les belligérants s'appuyant sur des services privés plutôt que sur des systèmes appartenant à l'armée.

L'arsenalisation de l'espace fait référence au positionnement ou à l'utilisation d'armes en orbite. Il s'agit d'un phénomène émergent qui reste latent, mais n'est pas encore totalement concret. Le stationnement d'armes dans l'espace n'est pas interdit par le droit international. Seul le déploiement d'armement de destruction massive l'est, en vertu du traité sur l'espace extra-atmosphérique de 1967.

La fusion cyber-espace

Le secteur des télécommunications a considérablement évolué au cours des deux dernières décennies. Aujourd'hui, les systèmes spatiaux font partie intégrante de l'infrastructure numérique au sens large. Si l'essentiel du trafic internet passe par les câbles sous-marins et la fibre terrestre, la place des satellites dans les activités web augmente progressivement depuis cinq ans. Ce phénomène s'explique par la transformation du marché des télécommunications. Auparavant, les services de radiodiffusion et de télédiffusion directe, notamment, étaient assurés par un petit nombre de satellites géostationnaires. Avec l'arrivée des grandes constellations commerciales en orbite basse, le marché a évolué vers la fourniture de services internet haut débit, y compris pour la connexion directe aux appareils (e.g., smartphones, ordinateurs).

> La plupart des incidents ne visent pas le satellite en orbite, mais les stations au sol ou les terminaux utilisateurs.

Par ailleurs, les satellites sont de plus en plus intégrés dans les systèmes de télécommunication terrestres, notamment les réseaux mobiles 5G et 6G. On peut s'attendre à ce que leur place dans l'infrastructure web continue de s'accroître, y compris au-delà de la Terre. Par exemple, la NASA et l'ESA sont en train d'élaborer des normes dans le cadre du projet LunaNet, qui vise à mettre en place un réseau internet sur la Lune.

Le paysage des menaces

Le paysage des menaces dans l'espace a évolué. Ce dernier est aujourd'hui encombré. L'orbite terrestre concentre actuellement quelque 9 000 satellites opérationnels, 100 millions de débris d'environ 1 millimètre de diamètre, 500 000 d'une taille allant de 1 à 10 centimètres et 30 000 de plus de 10 centimètres. L'espace est également devenu un terrain de concurrence où évolue un nombre croissant d'acteurs publics et commerciaux. Il s'agit aussi d'un lieu contesté. Les États ont observé une hausse des essais de missiles antisatellites (Chine en 2007, Inde en 2019, Russie en 2021), des manœuvres hostiles et des missions d'inspection avec des tentatives d'écoutes (Luch-Olymp), mais aussi le lancement de projectiles (Kosmos-2523) et le déploiement d'avions spatiaux à haute manœuvrabilité (X37-B), sans oublier l'introduction de nouvelles postures offensives et défensives dans les doctrines militaires.

Le paysage des cybermenaces dans l'espace a également évolué. Au tout début de l'ère spatiale, les menaces électroniques entre les systèmes soviétiques et américains constituaient le principal risque. À partir des années 1980, les risques d'attaque électronique et d'interception de données satellitaires par des pirates ou des amateurs, ainsi que les interférences dans la diffusion par satellite dans le cadre de la guerre froide (avec la diffusion illégale de propagande, par exemple) ont été au centre des préoccupations. À partir des années 1990, la télédiffusion par satellite a connu un essor, mais aussi une hausse des piratages. Les années 2000 ont été marquées par un accroissement des attaques de type «leurrage» (spoofing) émanant d'acteurs non étatiques ainsi que par des cyber attaques parrainées par un État-nation, ciblant principalement le segment sol. Depuis les années 2010, les cyberattaques ne cessent d'augmenter en volume et en complexité. Provenant d'un ensemble hétérogène d'acteurs, elles visent des systèmes étatiques et commerciaux sur toute la surface d'attaque.

Aujourd'hui, le paysage des menaces se caractérise par une meilleure compréhension de la dépendance des sociétés et des armées à l'égard de l'espace, qui fait des satellites des cibles intéressantes. À cela s'ajoute la montée de l'hacktivisme avec de nombreux groupes prenant parti dans des conflits armés (à l'image de Killnet, qui a visé Starlink dans le contexte de la guerre en Ukraine). Désormais, les entreprises spatiales sont régulièrement la cible de groupes criminels. Lockbit s'en est ainsi pris à SpaceX et Boeing, par exemple. Jusqu'à présent, les conséquences de ces attaques ont généralement été temporaires et réversibles. La plupart des incidents ne visent pas le satellite en orbite, mais les stations au sol ou les terminaux utilisateurs.

Le nombre de cyberattaques ciblant des systèmes spatiaux a explosé ces derniers temps. Il est toutefois difficile de fournir des chiffres précis. Cela s'explique par le fait que la plupart des entreprises spatiales étaient auparavant des sociétés de défense, qui pensaient que la sécurité passait par l'obscurité. Afin d'empêcher toute exploitation malveillante, elles évitaient de communiquer des informations, de signaler les attaques ou de divulguer des données sur leur organisation ou leurs systèmes. Elles n'avaient d'ailleurs aucune obligation légale de notifier les incidents aux autorités ou à leur clientèle.

Des entreprises et des chercheurs ont tenté de recenser les cyberattaques contre les systèmes spatiaux: les résultats de leur travail illustrent bien l'évolution du paysage des menaces. La base de données de Pavur et Martinovic dénombre 113 attaques entre 1957 et 2022. La société d'intelligence économique CyberInFlight fait état de 337 cyberattaques depuis les années 1970, dont 90 en 2023 et 30 au cours du seul mois de janvier 2024. Les disparités dans

les chiffres sont dues au manque d'informations accessibles publiquement et à des divergences dans les méthodologies. En outre, il s'agit probablement d'estimations basses, car toutes les attaques ne sont pas signalées. Les méthodes et les données varient encore plus au niveau national. La NASA a déclaré 1 785 incidents cyber pour la seule année 2020 (y compris les pertes et les vols d'équipements).

Les spécificités de l'espace

Contrairement aux menaces cinétiques, les cyberattaques contre les systèmes spatiaux peuvent affecter la stabilité stratégique dans l'espace. Si celle-ci a pu se maintenir au fil des ans, c'est parce que l'accès à l'espace, aux technologies spatiales et aux capacités antisatellites (ASAT) était limité. De plus, les ASAT cinétiques peuvent être surveillées et attribuées par n'importe quel pays doté de capacités radar, ce qui empêche tout déni plausible. Par ailleurs, ces armes créent généralement des débris spatiaux qui touchent les autres satellites en orbite sans faire de distinction. Les cybermenaces constituent un changement de paradigme à plusieurs titres. D'une part, les capacités cyberoffensives sont facilement accessibles à tous. Ensuite, les cyberattaques sont difficiles à attribuer et un déni plausible est toujours possible. Enfin, les cyberattaques contre des systèmes spatiaux ne génèrent pas de débris et n'ont donc pas de répercussions sur l'assaillant, ce qui peut favoriser les comportements irresponsables dans l'espace comme dans le cyberespace. En outre, de nombreuses infrastructures critiques ont besoin d'une connectivité satellite pour fonctionner. Une seule cyberattaque contre un appareil spatial peut impacter le fonctionnement de plusieurs secteurs essentiels en même temps.

Questions politiques

Jusqu'en 2019, les politiques publiques du monde entier ont largement occulté les cybermenaces pesant sur les systèmes spatiaux. Des chercheurs ont attiré l'attention sur cet angle mort, suggérant que les risques cybernétiques étaient trop simplifiés et mal compris, et que les stratégies spatiales et cyber étaient incompatibles entre elles. Depuis, les pays ont progressivement intégré ces menaces dans leurs politiques publiques.

Afin de s'adapter à l'évolution du paysage des menaces, les principales puissances spatiales ont alors commencé à compléter leurs politiques spatiales par des stratégies de défense. La France a ainsi publié en 2019 sa stratégie spatiale de défense, qui reconnaît les cybermenaces touchant les systèmes spatiaux et les considère comme l'une des menaces les plus probables. En 2019, l'Italie a adopté sa stratégie de sécurité nationale pour l'espace afin de répondre aux menaces intentionnelles et non intentionnelles, y compris les menaces cyber. Le Royaume-Uni a promulgué en 2022 une stratégie spatiale de défense, qui met en évidence le pouvoir de nuisance des cybermenaces sur la capacité du pays à conduire des opérations militaires. Elle souligne également le développement de capacités cyber par des adversaires potentiels qui pourraient cibler des équipements spatiaux britanniques. En règle générale, cependant, ces documents prévoient peu de mesures spécifiques pour contrer les cybermenaces, hormis l'adoption d'une posture controffensive (France, Italie), l'intégration du spatial dans les exercices cyber (Royaume-Uni), le durcissement (France) ou la préservation des capacités à opérer dans un environnement dégradé (France).

> Une seule cyberattaque contre un appareil spatial peut impacter le fonctionnement de plusieurs secteurs essentiels en même temps.

Les États-Unis ont adopté en 2020 la directive 5 sur la politique spatiale, qui définit les principes généraux de cybersécurité pour les systèmes spatiaux. Selon la doctrine Space Power de l'US Space Force, les opérations cyber sont un volet essentiel des opérations militaires spatiales pour conserver la «dominance spatiale». L'armée américaine détaille ensuite cette approche pour les actions tant défensives qu'offensives dans ses documents doctrinaux.

Les puissances spatiales émergentes dont les capacités sont plus évoluées dans le domaine cybernétique que dans le secteur spatial, telles que l'Estonie ou Israël, ont décidé de faire de la cybersécurité un pilier de leurs politiques spatiales et de l'utiliser comme un tremplin pour développer leurs programmes spatial.

La cyberattaque contre le satellite de Viasat avant l'invasion de l'Ukraine a constitué un signal d'alarme pour les responsables politiques européens. La boussole stratégique, la politique de cyberdéfense et la stratégie spatiale pour la sécurité et la défense de l'UE considèrent toutes les menaces cyber pesant sur les systèmes spatiaux comme des risques importants, pernicieux et probables. Celle-ci recommande la prise en compte de la sécurité dès le stade de la conception, l'intégration systématique des normes de cybersécurité, l'échange de bonnes pratiques entre entités commerciales, une surveillance de la sécurité de tous les programmes spatiaux de l'UE et l'intégration de mesures de cybersécurité dans une nouvelle législation spatiale.

Questions réglementaires

Les cadres réglementaires pour la cybersécurité dans l'espace restent limités en Europe. Parmi les États européens, onze ont adopté des législations spatiales, mais aucune d'entre elles n'intègre de mesures de sécurité informatique juridiquement contraignantes.

Au niveau de l'UE, en 2022, la directive SRI 2 a reconnu que l'espace était un secteur de haute criticité et demandé aux «opérateurs d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui fournissent de services spatiaux» de mettre en œuvre des mesures de cybersécurité et des mécanismes de signalement plus stricts. Comme il s'agit d'une directive, elle doit être transposée dans les législations nationales. Toutefois, presque aucun pays européen ne l'a fait à ce jour. De plus, son champ d'application peut encore faire l'objet d'interprétations. Par exemple, on peut se demander si les «infrastructures terrestres» englobent également les segments utilisateur et spatial. En outre, les mesures énoncées par la directive SRI 2 restent très générales et ne sont pas nécessairement adaptées aux spécificités des systèmes spatiaux. Le secteur aura probablement besoin d'un appui pour assurer sa mise en œuvre.

L'UE est également en train d'élaborer une législation spatiale qui devrait intégrer des mesures de cybersécurité. En parallèle, plusieurs États membres de l'UE ont commencé à actualiser leurs législations spatiales nationales pour y inclure des dispositions cyber, mais attendent d'abord l'introduction du texte de l'UE. La présentation du projet de loi de l'UE était initialement prévue en mars 2024, mais elle a été reportée à l'été 2024 au plus tôt.

Il est important de noter que l'élaboration de normes de cybersécurité spécialement applicables aux systèmes spatiaux a été relativement lente et laborieuse. Les standards de cybersécurité classique sont

généralement inadaptés et ne tiennent pas compte des spécificités des systèmes spatiaux et de l'environnement orbital. Certaines entités (telles que le Comité consultatif pour les systèmes de données spatiales) n'ont développé que récemment des normes spécifiques pour les systèmes spatiaux, qui doivent encore être adoptées par l'ensemble du secteur.

Questions techniques

La cybersécurité n'est pas la même sur Terre que dans l'espace. Dès qu'un engin spatial est lancé, il devient impossible d'y accéder et de retirer ou remplacer ses composants en cas de vulnérabilité ou de dysfonctionnement. Si les services en orbite pourraient permettre de réaliser de telles opérations, ce marché n'est pas encore parvenu à maturité. Le satellite ne peut être débranché comme on le ferait avec un ordinateur sur Terre.

L'élaboration de normes de cybersécurité spécialement applicables aux systèmes spatiaux a été relativement lente et laborieuse.

En outre, la puissance de calcul à bord d'un engin spatial est limitée. L'utilisation de longues clés de chiffrement peut donc s'avérer contraignante, car elle risque d'épuiser la source d'énergie limitée du satellite.

La numérisation des systèmes spatiaux accroît leur vulnérabilité aux menaces cyber conventionnelles, ce qui appelle à mettre en œuvre des protocoles de cybersécurité traditionnels. Dans le même temps, les spécificités de ces systèmes font apparaître les limites des mesures de sécurité informatique classiques. Par exemple, le chiffrement VPN de bout en bout, très répandu sur les ordinateurs sur Terre, n'est pas adapté aux satellites, car leur trop grande distance par rapport à la Terre entraîne la perte de paquets de données.

Questions commerciales

Dans l'industrie, les opérateurs ont longtemps négligé la cybersécurité, car les opérateurs (et la clientèle) privilégiaient la latence et l'efficacité. Aujourd'hui, les grandes entreprises spatiales semblent avoir pris conscience des menaces cyber. La difficulté se situe plutôt du côté des start-ups, car elles préfèrent souvent se concentrer sur les spécificités de leur mission ou n'ont pas les ressources nécessaires pour intégrer la cybersécurité.

Des initiatives visant à faire face aux menaces cyber ont été mises en place par l'industrie tels que les centres de partage et d'analyse d'informations pour le spatial (Space ISAC). Ils permettent ainsi de partager des renseignements, des vulnérabilités, et autres informations avec les membres et les agences gouvernementales. L'UE a ainsi décidé de créer un ISAC spatial en 2023. Les questions liées à sa gouvernance restent toutefois à préciser, notamment quant à l'intégration potentielle d'entités européennes non communautaires, telles que la Suisse, la Norvège ou le Royaume-Uni.

La demande de cybersécurité spatiale est en hausse. Cette situation crée un marché émergent composé de nouvelles entreprises spécialisées dans ce domaine, de sociétés informatiques traditionnelles qui tentent de se faire une place dans le secteur spatial et de grandes entreprises spatiales qui cherchent à y commercialiser des services de cybersécurité. Le secteur devrait générer 33,2 milliards de dollars au cours des dix prochaines années et offrir ainsi des opportunités à des pays innovants tels que la Suisse.

Enjeux pour la Suisse

Comme beaucoup d'autres pays européens, la Suisse ne possède pas de satellites souverains. Elle mène toutefois des activités spatiales, comme l'illustre le lancement en mars 2024 de trois satellites belges transportant des charges utiles de renseignement d'origine électromagnétique pour l'armée suisse. Le pays reste donc vulnérable aux cybermenaces. Environ 160 entreprises suisses participent à la chaîne d'approvisionnement spatiale et le fonctionnement de plusieurs secteurs critiques de l'économie repose sur des services satellitaires étrangers (banques, transports, logistique, forces armées, etc.). En définitive, leur fonctionnement dépend de mesures de sécurité mises en œuvre par des acteurs étrangers.

Cette question a attiré l'attention des responsables politiques en 2021, incitant le Conseil fédéral à publier un rapport sur les risques cyber dans l'espace à la demande du Parlement suisse. En mai 2024, le comité sur la politique de sécurité du Conseil national, s'appuyant sur les conclusions du rapport de 2021, a déposé une motion invitant le Conseil fédéral à renforcer la coopération avec l'UE dans le domaine spatial, au vu de l'importance grandissante que celui-ci revêt en matière de politique de sécurité. La motion traite toutefois de l'espace en général et ne se concentre pas sur la cybersécurité spatiale.

La politique spatiale 2023 évoque brièvement la possibilité de cyberattaques contre des satellites. Elle ne prévoit toutefois aucune mesure pour garantir la cybersécurité dans le secteur spatial suisse. Les autres politiques publiques n'abordent pas le sujet. Sur le plan juridique, la Suisse ne possède pas encore de législation spatiale, mais est en train d'en élaborer une. Il reste à voir si elle intégrera la cybersécurité.

Perspectives

L'évolution du paysage des menaces doit s'accompagner d'une meilleure compréhension des risques cyber et des mesures visant à protéger les équipements spatiaux et le large éventail de services qu'ils offrent à la société. Les prochains défis en matière de cybersécurité spatiale consisteront à combler le manque de compétences et d'informations, à élaborer un cadre juridique adapté et à déterminer le moyen le plus efficace de mener des opérations cyber dans l'espace et d'y répondre.

Voir le site thématique du CSS pour en savoir plus sur la cybersécurité.

Clémence Poirier est Senior Researcher dans le Cyberdefence Project au sein de l'équipe «Risk and Resilience» au Center for Security Studies (CSS) à l'ETH de Zurich.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH de Zürich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Éditrice: Névine Schepers
Relecture: Clémence Poirier
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

Les relations de Pyongyang avec Moscou et Pékin No 342
Comparaison des politiques d'infrastructures critiques No 341
La coopération entre l'Europe et l'Indopacifique No 340
Risques nucléaires et mesures de réduction No 339
Enjeux de la sécurité des connaissances No 338
La réduction stratégique des risques au-delà des puces No 337

ISSN: 2296-0228; DOI: 10.3929/ethz-b-000676386