iesd
Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III

MARS 2021

Les cybermenaces
Un nouvel enjeu pour la sécurité spatiale

Benoît Wagner

POLICY PAPERS

Analyse technico-capacitaire

A propos de l'IESD

L'Institut d'études de stratégie et de défense (IESD) est une structure de recherche universitaire créée en 2018 et spécialisée dans le champ des études stratégiques. Soutenu par l'Université de Lyon (UdL), l'IESD appartient à la **faculté de droit de l'université Jean Moulin – Lyon III**. L'institut accueille une équipe multidisciplinaire de chercheurs lyonnais et extérieurs (droit, science politique, gestion, économie, sociologie, histoire), et fédère autour d'elle un réseau d'experts, de chercheurs, de doctorants et d'étudiants spécialisés dans l'étude des interactions conflictuelles contemporaines.

L'IESD a reçu le **label « Centres national d'excellence défense » de la DGRIS** (Ministère des armées), dans le cadre d'un programme de recherche intitulé « *L'interconnexion des capacités stratégiques hautes (puissance aérienne, espace, nucléaire, défense anti-missiles) : conséquences politiques et opérationnelles des couplages capacitaires de haute intensité dans les espaces homogènes et les Contested Commons* ».

Directeur de l'IESD : **Olivier Zajec** ; maître de conférences en science politique habilité à diriger les recherches (HDR), faculté de droit, Université Jean Moulin-Lyon 3 (Université de Lyon)

Site web : https://iesd.univ-lyon3.fr/
Contact : iesd.contact@gmail.com

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08

POLICY PAPERS

Analyse technico-capacitaire

Benoît Wagner, « Les cybermenaces, un nouvel enjeu pour la sécurité spatiale », Policy Paper de l'IESD, coll. « Analyse technico-capacitaire », n°2, mars 2021.

Résumé

Pendant longtemps les réflexions sur la sécurité spatiale se sont focalisées sur des attaques de nature cinétique ou d'origine électromagnétique. Avec l'expansion du cyberespace, le secteur spatial a dû prendre en considération de nouvelles menaces et de nouveaux types d'acteur. Dans un contexte de préoccupation croissante des puissances spatiales quant aux risques de militarisation armée de l'espace, cette note esquisse du point de vue stratégique et juridique un panorama des principaux enjeux liés aux cybermenaces visant les systèmes spatiaux.

Abstract

For a long time, space security issues have focused on kinetic or electromagnetic attacks. With the expansion of cyberspace, the space sector had to consider new threats and new types of actors. In a context of growing concern among space powers about the risks of weaponization of space, this paper written from a strategic and legal perspective outlines an overview of the main issues related to cyber threats to space systems.

A propos de l'auteur

Benoît Wagner est doctorant au centre Alexandre Koyré de l'EHESS sous la direction d'Isabelle Sourbès-Verger et au LORIA (Laboratoire lorrain d'informatique et ses applications) sous la direction de Didier Fass. Ses recherches, financées par l'Agence Innovation Défense, portent sur les aspects stratégiques et juridiques de la défense des systèmes spatiaux français face aux cybermenaces.

Table des matières

Les cybermenaces, un nouvel enjeu pour la sécurité spatiale

La *Stratégie spatiale de défense*[1] publiée en 2019, à la suite des réflexions amorcées par la *Revue stratégique de défense et sécurité nationale* de 2017, rappelle que la sécurité des activités spatiales est un enjeu majeur pour la France dans la mesure où les systèmes spatiaux jouent un rôle essentiel pour notre société. Dans le domaine militaire, les moyens spatiaux servent d'appui aux opérations, avec des capacités d'observation que fournissent les satellites Hélios 2, Pléiades et maintenant CSO (composante spatiale optique). Mais aussi avec des capacités de télécommunications (Syracuse III et bientôt Syracuse IV) pour la mise en place de certaines liaisons de données tactiques et des capacités d'écoute qui seront bientôt disponibles avec CERES (Capacité d'Ecoute et de Renseignement Electromagnétique Spatiale). A travers la fonction PNT[2] que l'on peut retrouver dans les systèmes de navigation ainsi que dans les systèmes d'informations et de communication qui nécessitent une précision très fine telle que la plateforme Scorpion[3]. Enfin le spatial sert également pour l'alerte avancée[4], et la défense antibalistique, c'est-à-dire la surveillance des tirs et des activités d'essais de missiles balistiques, composante essentielle de la dissuasion nucléaire.

Dans le domaine civil, on retrouve également une fonction observation de la Terre destinée à la cartographie (Spot 6 et 7), à la production de données météorologiques (Calipso) et à l'analyse des risques naturels, climatiques et environnementaux (Pléiades, Sentinel 6 …). Une fonction télécom (internet, téléphonie, télévision par satellite) qui étend considérablement le cyberespace. Une fonction GNSS (global navigation space system)/PNT (Galileo) particulièrement importante, puisqu'elle permet à la fois à la géo-navigation et la synchronisation de différents réseaux tels que les réseaux numériques, bancaires et financiers ainsi que de distribution d'énergie. Les satellites assurent également la réalisation de missions scientifiques.

Les systèmes spatiaux représentent donc un enjeu stratégique qui nécessite une protection adéquate pour garantir une appréciation de situation indépendante et une liberté d'action souveraine. C'est notamment vrai dans un contexte où il semble y avoir une préoccupation renouvelée pour la militarisation de l'Espace et un droit international peu adapté aux nouveaux enjeux, augmentant de fait l'insécurité dans le cadre des activités spatiales.

Il n'existe pas de définition précise de la sécurité spatiale. Cependant, selon Jean Combacau, on peut distinguer deux aspects de la sécurité. Un premier de nature militaire que l'on relie traditionnellement à la sécurité individuelle des Etats, c'est-à-dire « *une situation dans laquelle [l'Etat] s'estime à l'abri de toute menace ou de toute entreprise mettant en cause son indépendance, son intégrité territoriale, le libre exercice de ses compétences, et qui le met en mesure de poursuivre librement son développement politique, économique et social* »[5]. De ce point de vue, on peut selon certains spécialistes français du domaine, tel que F. Gaillard-Sborowsky, I. Sourbès-Verger, I. Facon, X. Pasco, P. Achilleas, définir la sécurité spatiale comme correspondant à « *toutes les mesures visant à garantir la paix internationale en prévenant toute situation qui, depuis l'espace ou dans l'espace, est de nature à affecter la sécurité individuelle d'un État* »[6] . Le second aspect con-

[1] Ministère des armées, 2019, » *La stratégie spatiale de Défense »,* Rapport du groupe de travail « Espace ».

[2] Fonction du GNSS, positioning, navigation and timing.

[3]Le système SCORPION (synergie du contact renforcée par la polyvalence et l'infovalorisation) est un système de combat et de commandement de l'armée de terre, lancé en 2018, qui vise à mettre en cohérence les capacités des groupements tactiques interarmes en fédérant les plateformes et les combattants autour d'un unique système d'information et de communication. Il devrait être déployable en 2021 pour un premier GTIA, puis en 2023 pour équiper une première brigade.

[4] Après la réussite du démonstrateur SPIRALE en 2014, le développement du programme a pris du retard.

[5] J. Combacau, S. Sur, *Droit international public*, Paris, Montchrestien, 2010, p. 617.

[6] F. Gaillard-Sborowsky, I. Sourbès-Verger, I. Facon, X. Pasco, P. Achilleas, 2016, Sécuriser *l'espace extra-atmosphérique, éléments pour une diplomatie spatiale*, volume d'annexes, Fondation pour la recherche stratégique.

cerne la sécurité spatiale non-militaire. La législation française définit la sécurité comme « *un ensemble des dispositions destinées à maîtriser les risques dans le but d'assurer la protection des personnes, des biens et la protection de la santé publique et de l'environnement* »[7]. Cette définition se focalise donc plutôt sur la gestion des risques liés à l'environnement spatial tels que les débris ou les risques accidentels, sans tenir compte des actes de malveillance. On préférera donc, pour éviter les confusions, le terme de *sûreté spatiale* (qui correspond à *« space security »* en anglais) plutôt que *sécurité spatiale* (*« space safety »*) pour désigner les menaces volontaires ou les actes de malveillance visant les systèmes spatiaux ou les activités spatiales.

Les différents agissements récents des puissances spatiales ont tendance à renforcer l'hypothèse du regain d'intérêt pour la militarisation de l'espace. Ces deux dernières années ont vu, entre autres, la création de la *Space Force* aux Etats-Unis, la création d'un nouveau commandement dédié aux activités spatiales en France et la création une agence spatiale de défense indienne. On notera aussi l'essai du tir antisatellite (ASAT) de l'Inde de mars 2019, qui s'est pourtant toujours positionnée comme une puissance spatiale pacifique en privilégiant les programmes civils plutôt que militaires, ainsi que des tirs effectués par la Russie en 2020[8].

De plus, la directive 5 du mémorandum de la *Space policy* publié le 4 septembre 2020 par la Maison Blanche, rappelle que le secteur spatial n'échappe pas aux cyberattaques, aussi bien dans leurs modalités que dans leurs buts, allant des offensives étatiques[9] pouvant franchir le seuil de l'agression armée, jusqu'aux simples actes criminels[10]. La *Stratégie Spatiale de Défense* de 2019 mentionne ainsi explicitement que « *les attaques cybernétiques sur les parties logicielles des différents segments des capacités spatiales figurent parmi les menaces les plus probables […] allant [même] pour les plus graves jusqu'à la perte de contrôle des charges utiles, voire de la plateforme, réduisant celle-ci à l'état de débris* »[11].

Comme pour la « sécurité spatiale » il n'existe pas une définition précise des cybermenaces. En revanche, le livre blanc de droit international appliqué aux opérations dans le cyberespace[12] définit une cyberattaque comme une « *action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux données ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support* »

En outre, on pourrait définir les *cybermenaces* comme étant *la possibilité d'agression de la part d'un Etat ou d'acteurs non-étatiques, envers les intérêts d'un État (y compris les intérêts socio-économiques), concrétisée par une capacité et une volonté de nuire et menée au travers du cyberespace*.

A l'heure où l'on constate le renforcement de la thématique de la militarisation de l'Espace, et la perception croissante des cyberattaques comme l'un des types d'attaques les plus probables, leur place comme nouvel enjeu de la sûreté spatiale devient une question incontournable.

---

[7] Article 1, de l'arrêté du 31 mars 2011 relatif à la réglementation technique en application du décret n° 2009-643 du 9 juin 2009 relatif aux autorisations délivrées en application de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales.

[8] L'acronyme ASAT désigne les armes anti-satellites. Seuls quelques Etats disposent de ces capacités à savoir les Etats-Unis, la Russie, la Chine, l'Inde.

[9] On peut donner par exemple de l'Estonie en 2007 ou le cas de Stunext en 2010 (l'arrêt des centrales nucléaires iraniennes par *Worm* d'initiative israélienne et américaine).

[10] A l'instar du *ransomware* subi par la ville d'Atlanta aux États-Unis ; Bergounhoux, Julien, 24 avril 2018, « La ville d'Atlanta devra payer encore au moins 9,5 millions de dollars pour se remettre d'un ransomware », Usine digitale. https://www.usine-digitale.fr/article/la-ville-d-atlanta-devra-payer-encore-au-moins-9-5-millions-de-dollars-pour-se-remettre-d-un-ransomware.N684529

[11] *Stratégie spatiale de défense*, 2019, Rapport du groupe de travail « Espace », Ministère des Armées, p.25.

[12] *Livre blanc sur le droit international applicable aux opérations dans le cyberespace*, septembre 2019, Ministère des Armées.

Dans cette note, nous tentons d'esquisser un panel des enjeux et des difficultés que produisent les cybermenaces et les cyberattaques dans le cadre de la sûreté des activités spatiales. La focale principale portera sur les effets qu'elles engendrent sur le spectre de la menace pour la sécurité spatiale mais aussi sur l'insuffisance des dispositions internationales pour réguler les cyber-opérations dans le cadre des activités spatiales. Nous essaierons, ce faisant, de détacher l'analyse de la vision dominante marquée par les préoccupations et les approches américaines.

Un élargissement du spectre de la menace pour la sûreté spatiale

Pour comprendre en quoi les cyberattaques élargissent le spectre de la sûreté spatiale, (en anglais *« space security »*), il faut d'une part s'intéresser au changement qu'elles opèrent dans la typologie de la menace déjà existante et, d'autre part, étudier ce que ces changements produisent sur les acteurs impliqués dans le champ de la sûreté spatiale.

Un changement de typologie de la menace

Traditionnellement, lorsque l'on décrit les systèmes spatiaux, on distingue trois segments qui les composent. Le segment sol tout d'abord, qui regroupe les stations sol pour la récupération des données fournies par les satellites et les stations de maintien à poste[13] et de manière plus générale toutes les infrastructures au sol. Le segment espace ensuite, c'est-à-dire le milieu où orbite le satellite, et le satellite lui-même. Enfin, le segment liaison qui fait la jonction entre le segment sol et le segment espace ou entre les satellites eux-mêmes, en d'autres termes les faisceaux émis ou reçus par les satellites.

Historiquement, les armes anti-satellites ont vu le jour pendant la Guerre Froide, et plus spécifiquement dans le contexte de la dissuasion nucléaire. Il s'agissait principalement de priver l'adversaire de sa capacité d'observation et d'alerte afin d'optimiser l'efficacité de des armes nucléaires. Dès le début des années 60 et jusqu'au début des années 70, les Américains et les Soviétiques commencent à réfléchir à des moyens de défense anti-missiles qui seront ensuite transformés en armes anti-satellites, ainsi qu'à des satellites intercepteurs. Ces différents types d'armes entrent habituellement dans la catégorie des armes cinétiques[14].

À ce stade quelques remarques s'imposent concernant les armes cinétiques et leurs usages. D'une part, leur mise en œuvre est complexe du fait des contraintes de mécanique céleste qui rendent le « *hit to kill* » particulièrement difficile à maîtriser[15]. D'autre part, ce type d'ASAT[16] a une discrétion limitée, puisqu'il reste détectable par des dispositifs d'alerte avancée ou des capacités d'observation du ciel (radar). On notera également que leur développement coûte relativement cher et que les possibilités qu'offrent ces armes en termes d'options stratégiques sont extrêmement limitées, puisqu'elles se réduisent à la destruction de l'engin spatial ou de la station au sol. Enfin, leurs tirs risquent d'être confondus avec celui de missiles balistiques, avec les conséquences que cela peut entrainer.

Après la courte période de détente des accords SALT/ABM[17] de 1972 et de 1979 signés par Nixon et Brejnev pour limiter la production d'armes balistiques, ce qui incluait les ASAT, un regain d'intérêt apparaît pour celles-ci jusque dans les années 90. Les deux puissances spatiales vont alors dévelop-

[13] Ensemble des opérations visant à maintenir un satellite sur une orbite donnée, celle obtenue à l'issue de la mise à poste (passage de l'orbite initiale fourni par le lanceur, à l'orbite qu'exige la mission du satellite).

[14] CICDE, 19 juillet 2010, *Utilisation de l'espace à des fins de défense et de sécurité nationale,* Réflexion doctrinale interarmées, Ministère de la Défense, RDIA-2010/004_ESPACE (2010), N° 197/DEF/CICDE/NP du 19 juillet 2010, p.20.

[15] C'est d'ailleurs pour cette raison que toutes ces armes sont munies de charge explosive, bien qu'elles soient incluses dans la catégorie des armes cinétiques.

[16] Armes anti-satellites

[17] Strategic Arms Limitation Talks/ Anti-balistic missile

Voir : Paul B Stares, *Space and National* Security, Brooking press 1987.

per de nouveaux systèmes d'armes plus discrets basés sur des moyens de guerre électronique[18]. Ils peuvent être employés, soit depuis le sol, soit directement depuis le segment espace, par le biais de certaines antennes de satellite qui peuvent se voir modifiées afin de produire du bruit destiné à brouiller les liaisons satellitaires[19]. On peut également distinguer une sous-catégorie dans les moyens de guerre électronique : les armes à énergie dirigée. Leur but est de provoquer des échauffements successifs ou des surcharges électromagnétiques, soit par des *lasers* (Light Amplification by Stimulated Emission of Radiation), soit par des *masers* (Microwave Amplification by Stimulated Emission of Radiation) qui émettent un faisceau cohérent de micro-ondes. Il faut également mentionner les capacités d'écoute de certains satellites ou moyens au sol, qui n'entrent pas directement dans la catégorie des ASAT, mais qui représentent néanmoins une menace d'origine électromagnétique pour les satellites.

Ces nouveaux systèmes d'armes basés sur des moyens de guerre électronique viennent étendre la gamme et l'efficacité des options stratégiques disponibles puisqu'ils permettent d'espionner, de perturber, d'interrompre temporairement ou définitivement les services fournis par un satellite ou une station au sol, et sont extrêmement difficiles à esquiver[20]. En revanche, ils sont complexes à utiliser. Dans le cas des armes à énergie dirigée, il faut une ligne de visée directe et une certaine durée de maintien sur la cible, ce qui est difficile à obtenir étant donné que la vitesse moyenne d'un satellite est d'environ 7 à 8 km/s. Cela ajoute donc des contraintes supplémentaires pour la gestion de l'énergie et la dissimulation des attaques. De plus, leur coût de développement est plutôt élevé.

Plus récemment, on a pu voir émerger une nouvelle catégorie de menace : les cyberattaques. Contrairement à ce que l'on a pu observer plus haut pour les autres types de menaces, les cyberattaques n'élargissent pas seulement les options stratégiques disponibles, mais viennent transformer la façon de penser la sûreté spatiale. A cet égard, on retiendra deux cas particulièrement intéressants. Le premier concerne les attaques perpétrées en 2015 par le groupe cybercriminel Turla[21]. Ce groupe est connu entre autres pour avoir exploité les failles des réseaux satellitaires afin de dissimuler le transfert de données résultant de leur campagne d'espionnage visant des ambassades, des administrations et des entreprises, en utilisant les liaisons descendantes qui sont souvent peu protégées[22].

Le second cas concerne l'expérience menée en 2016 par le professeur Todd Humphrey, de l'université du Texas, qui réussit une expérience de détournement d'un yacht privé, en usurpant un signal GPS[23]. Ces exemples nous apprennent deux choses. D'une part, que les cyberattaques peuvent servir à dévoyer les systèmes spatiaux, c'est-à-dire en faire des usages pour lesquels ils ne sont pas prévus (ce qui n'était pas possible avant). D'autre part, qu'il est désormais possible de cibler principalement l'utilisateur, ce qui implique de devoir le traiter différemment du segment sol. D'un point de vue stratégique, l'utilisateur devient en quelque sorte une partie intégrante du système spatial mais qui diffère des trois autres segments. Les cybermenaces font donc apparaître un 4e segment. On notera d'ailleurs que ce n'est pas le cas lorsqu'il s'agit d'armes cinétiques ou à énergie dirigée, puisque l'utilisateur n'est atteint que par ricochet.

[18] Selon le glossaire du CICDE (à jour de 2015) la guerre électronique est toute : « *action militaire destinée à exploiter le spectre électromagnétique, qui englobe la recherche, l'interception et l'identification des émissions électromagnétiques, l'emploi de l'énergie électromagnétique, y compris l'énergie dirigée, pour diminuer ou prévenir l'emploi par l'ennemi du spectre électromagnétique* ».

[19] Cela vaut aussi bien pour les liaisons qui contiennent les données fournies par le satellite, que celles qui servent à l'opérer.

[20] Les liaisons optiques (LASER), commencent à être utilisées et sont beaucoup plus difficiles à intercepter ou à brouiller.

[21] Ce groupe est supposément relié à la Russie.

[22] S. Tanase, 9 septembre 2015, « *Satellite Turla: APT Command and Control in the Sky* », Kaspersky website, https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/

[23] Nous avons décidé volontairement de ne pas faire entrer l'usurpation de signal GPS dans la catégorie de la guerre électronique ; voir : B. Wagner, « Différencier les cyberattaques des attaques relevant de l'environnement électromagnétique », (en cours de soumission à la *Revue de défense nationale*).

A ces nouveaux aspects, il faut ajouter les attaques qui ciblent le segment liaison et plus particulièrement les données, qui peuvent être altérées par le biais des attaques *man-in-the-middle*[24]. Les cyberattaques peuvent également servir à réaliser des attaques plus classiques contre le segment sol ou espace (espionnage, perturbation, interruption temporaire ou définitive). De plus, elles ont l'avantage d'être plus discrètes puisqu'un tir de missile reste détectable par des moyens de surveillance, ce qui est également le cas des manœuvres potentiellement suspectes ou inamicales dans le segment espace. Les cyberattaques ont également l'avantage d'être plus faciles à mettre en œuvre étant donné que l'on peut s'affranchir de la plupart des complications liées à la mécanique céleste, à l'exception de celles qui concernent la captation des liaisons satellites. Elles sont aussi plus difficiles à retracer (cf. *infra*) et moins onéreuses, ce qui induit nécessairement des conséquences sur la typologie des acteurs du champ de la sûreté spatiale.

Une émergence de nouveaux acteurs potentiels dans le champ de la sûreté spatiale

Les cyberattaques transforment en profondeur la façon de penser la sûreté spatiale parce que, d'une part, elles modifient la typologie des menaces (supra), d'autre part, parce que les acteurs du champ de la sécurité spatiale s'en trouvent affectés. Comme nous l'avons déjà évoqué les ASAT relevant des catégories cinétiques et de guerre électronique, sont difficiles à mettre en œuvre et nécessitent un savoir particulier. Ce type d'ASAT a également des coûts de développement très élevés, aussi bien du point de vue financier que technique, si bien que seuls les Etats possédant des capacités spatiales ou balistiques pouvaient avoir accès à ce type d'armement. Cela réduisait considérablement le champ des agresseurs potentiels. De même, que les cibles restaient assez limitées puisqu'il s'agissait principalement de conflits entre Etats. Or, dès le début des années 2000, le phénomène « *New Space* » modifie le champ des acteurs de la sûreté spatiale.

Le « *New Space* » peut être caractérisé par l'augmentation rapide du nombre et de la diversité des acteurs privés liés au monde du numérique, dans le contexte de libéralisation du secteur spatial. Cette libéralisation produira deux impacts. Le premier aura pour effet l'accroissement des acteurs du secteur spatial aussi bien étatiques que non-étatiques et aura pour conséquence la multiplication des cibles disponibles. Soit en portant atteinte directement à une entreprise, soit à une organisation internationale, soit aux intérêts d'un Etat (y compris économiques) en visant un secteur d'activité dépendant des technologies spatiales.

Le second se traduira par une extension considérable du cyberespace, c'est-à-dire *« [l']espace de communication constitué par l'interconnexion mondiale d'équipements de traitements automatisés de données numériques »*[25]. En effet, les technologies spatiales sont nécessaires aux géants du numérique pour étendre leurs activités en fournissant plus largement des possibilités d'accès à internet à haut débit, ainsi que les applications qui en découlent[26] ; ce que l'espace, par le biais des super-constellations voire des méga-constellations de satellites (plus d'un millier de satellites) peut leur procurer. Mais cela aura aussi pour conséquence d'importer les acteurs évoluant dans le cyberespace ainsi que leurs logiques d'action.

En effet, la gamme des acteurs du cyberespace étant plus variée que celles du spatial, puisqu'il ne s'agissait que d'Etats jusqu'à présent, les acteurs de la sûreté spatiale doivent désormais composer

[24] L'ANSSI définit l'attaque *man-in-the-middle* comme une « catégorie d'attaque où une personne malveillante s'interpose dans un échange de manière transparente pour les utilisateurs ou les systèmes ».

Dans ce cadre, il est intéressant de préciser que la connexion est maintenue, soit en substituant les éléments transférés, soit en les réinjectant.

[25] Glossaire de l'ANSSI, site web de l'ANSSI, consulté le 1er avril 2020.

https://www.ssi.gouv.fr/entreprise/glossaire/

[26] X. Pasco, 2017, *Le Nouvel âge spatial. De le Guerre Froide au New Space*, CNRS éditions

avec des agresseurs potentiels répondant à d'autres logiques que celles des Etats, ce que s'efforce de faire l'ESEC[27] le nouveau centre de l'ESA basé à Redu, en Belgique[28]. Il faut également prendre en compte les Etats ne possédant aucune capacité spatiale ou de faibles capacités balistiques et qui peuvent dorénavant devenir des attaquants potentiels par le biais du cyberespace et de l'interconnexion qu'il produit avec les technologies spatiales.

A cela, s'ajoutent les possibilités de dissimulation, voire de fausse attribution, qu'offre le cyberespace et qui rendent particulièrement difficile l'identification de l'auteur ou du commanditaire de l'attaque, contrairement à un tir de missile qui reste identifiable ou de la quantité restreinte d'Etats possédant des moyens de guerre électronique suffisamment performants pour porter atteinte à un système spatial donné.

Parmi ces nouveaux acteurs, on peut aussi distinguer des acteurs non-étatiques tels que les cybercriminels, comme l'illustre le cas de Turla (cf. *supra*). Mais aussi des groupes de cyber-terroristes, même s'il n'y a aucun cas d'acte de sabotage identifié jusqu'à présent dans la littérature[29]. Cependant, on peut observer que le cyber-terrorisme se manifeste principalement par des actions de communication ou propagande. Au moins un cas a déjà pu être recensé concernant le secteur spatial, l'action perpétrée par les Tigres du Tamouls qui ont utilisé les réseaux d'Intelsat pour diffuser des messages non-autorisés de propagande au Sri-Lanka[30].

On mentionnera aussi la possibilité de devoir lutter contre des cyber-mercenaires. Ou encore des groupes d'hacktivistes qui pourraient s'inscrire à la fois dans une logique de propagande ou de dévoiement de technologie pour camoufler leurs réseaux de communication, même si aucun cas n'a encore été répertorié officiellement.

Tout cela contribue à créer des rapports asymétriques dans un milieu où les interactions restaient du fait des puissances spatiales. De plus, cette irruption de nouveaux acteurs vient renforcer la difficulté d'attribution des attaques. Il devient donc très complexe de savoir si l'attaque est l'œuvre d'un Etat, d'un acteur non-étatique ou d'Etat dissimulé derrière un acteur non-étatique comme ce pourrait être le cas de Turla.

Les cyberattaques ont donc provoqué un changement rapide de typologie de la menace et une mutation des acteurs du champ de la sûreté spatiale. Cette transformation rapide aura pour conséquence de rendre un certain nombre de dispositions internationales peu adéquates et de laisser place à une nouvelle source d'insécurité dans la pratique des activités spatiales.

Une insuffisance des dispositions internationales pour réguler les cyber-opérations accroissant l'insécurité dans le cadre des activités spatiales

L'insuffisance des dispositions internationales peut s'expliquer par une complexification des situations juridiques, ainsi que par des tentatives de régulations qui ont échoué ou qui se sont révélées inefficaces face aux nouvelles difficultés engendrées par les cyberattaques dans les activités spatiales, ce qui accroit l'insécurité dans leur pratique.

Une complexification des situations juridiques rendant l'application du droit délicate

Les cyberattaques offrent un certain nombre d'avantages, comme nous avons déjà pu l'esquisser plus haut, notamment en termes d'anonymat, mais lorsqu'on les combine avec les spécificités du spatial, les situations juridiques deviennent extrêmement complexes à carac-

[27] ESEC: ESA European Space security and Education Center.

[28] L. Del Monte, G. Naja, 2017, « Hack-my-sat : cyber threats and digital revolution in space », in : European Space Programs and digital challenge, Laurence Nardon (ed), IFRI, p.65-74

[29] D. Ventre, 2011, *Cyberespace et acteurs du cyberconflit*, Lavoisier Hermès, p.155

[30] D. Housen-Couriel, 2015, « Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses », Law & Cyber Warfare, p.120

tériser. Une situation juridique est un ensemble de faits que le droit doit prendre en considération pour y attacher une ou des conséquences juridiques. Or, en droit international, pour établir la responsabilité d'un Etat, il est nécessaire de démontrer qu'un fait internationalement illicite[31] a été commis par un Etat, ou bien qu'un un préjudice lui a été infligé[32], ainsi qu'un lien de causalité entre les deux éléments précédemment cités. Cela nous renvoie donc au problème de l'attribution et de l'identification des qualités de l'auteur de l'attaque[33]. On notera également, le problème de la « pluri-localisation » du préjudice ou du fait internationalement illicite. Cela pourrait se traduire entre autres, dans le cas du fait internationalement illicite, comme une violation du principe de diligence[34], lorsqu'un groupe opère depuis un territoire étranger (même si cela est limité à une obligation de moyen).

Le problème de la « pluri-localisation » devient encore plus complexe lorsqu'il s'agit d'identifier la nature directe du préjudice. En effet, la particularité des technologies spatiales fait qu'il peut être difficile de qualifier le préjudice direct, notamment lorsqu'un satellite fournit des services qui ne sont disponibles que par le biais d'un système spatial étranger. Le cas du système GPS dont dépendent de nombreux Etats en plus des Etats-Unis, en est un exemple. De même, que pour des raisons de coûts de fabrication, de plus en plus de satellites duaux sont produits, qu'ils soient civils et militaires ou en coopération comme c'est le cas d'Athéna-Fidus (satellite franco-italien). Dans ce type de cas, il extrêmement difficile de déterminer si c'est la composante militaire ou civile ou encore quel est l'Etat visé.

Dans le même ordre d'idée, lorsque le litige implique une personne de droit privé, tel qu'un cybercriminel, il faut prendre en compte le cas des délits complexes. Autrement dit, les délits dont les différents éléments matériels sont « pluri-localisés » et qui rendent l'application du droit extraordinairement compliquée en raison de l'ubiquité que peuvent offrir à la fois le cyberespace et les systèmes spatiaux. On admet, en général, pour fonder la compétence de la juridiction, soit le critère du « lieu du fait générateur » du dommage, soit le « lieu du dommage ». Sans même entrer dans les subtilités du droit international privé, on peut très vite se rendre compte des difficultés que cela engendre.

Concernant le critère du « lieu du fait générateur », il n'est pas aisé d'y recourir puisqu'il implique possiblement le lieu de conception du délit, mais aussi dans notre cas : le satellite qui voit ses services altérés ou encore le serveur qui est à l'origine de l'attaque ou dans un cas encore plus complexe plusieurs serveurs ne se trouvant pas dans un même Etat, comme ce fut le cas de Turla, où au moins une vingtaine de serveurs ont pu être recensés par la société d'antivirus Kaspersky.

Concernant le critère du « lieu du dommage », il est tout aussi complexe à établir d'autant plus que l'article VIII du *Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes* de 1967, dispose que l'Etat d'immatriculation « *conserve sous sa juridiction et son contrôle* » l'engin spatial. Or, si l'engin spatial d'un Etat A fournit un service à un Etat B ou à une multitude d'autres Etats, comme c'est le cas du GPS (supra), quel est le lieu du dommage qu'il

---

[31] L'article 2 du projet d'article de la Commission du droit international (CDI) dispose que *« il y a fait internationalement illicite de l'État lorsqu'un comportement consistant en une action ou une omission: a) est attribuable à l'État en vertu du droit international ; et b) constitue une violation d'une obligation internationale de l'État ».*

[32] L'article 31§2 du projet d'article de la CDI précise que *« le préjudice comprend tout dommage, tant matériel que moral résultant du fait internationalement illicite de l'Etat ».*

[33] De celle-ci dépend la qualification, ou non, de « fait internationalement illicite », puisqu'il faut que l'auteur soit susceptible d'engager l'Etat en plus de la violation de l'obligation de droit international.

[34] Dans l'affaire de 1928 Ile de Palmes, le juge Max Hubert, définit comme corollaire de la souveraineté, le principe de diligence, c'est-à-dire l'obligation de protéger à l'intérieur du territoire le droit des autres Etats, en particulier le droit à l'intégrité et l'inviolabilité de leurs territoires.

faut retenir et par conséquent quel droit devons-nous appliquer[35]?

A cela, il faut ajouter le problème de l'obtention de la preuve, lorsque le fait internationalement illicite est commis depuis un territoire étranger tiers au conflit. Par exemple, un Etat A qui subirait un préjudice risque de se heurter à la souveraineté d'un Etat C, si l'attaque menée par un Etat B passe par l'Etat C pour camoufler ses opérations ou par une multitude d'Etats.

Ces différents aspects démontrent la difficulté à appliquer le droit, d'autant plus que la préservation des intérêts d'une des parties peut s'opposer au traitement des différends par des juridictions. Le domaine de la preuve en est encore un parfait exemple. En effet, rendre une preuve publique peut s'avérer problématique[36], puisque dans le cadre de la justice internationale « *c'est en définitive au plaideur qui cherche à établir un fait qu'incombe la charge de la preuve* »[37], ce qui peut donner, de manière implicite, des indices sur les capacités techniques d'un Etat. De plus, en dévoilant une cyber-opération, il existe un risque que les failles soient exploitées par d'autres acteurs le temps que celles-ci soient corrigées, comme ce fut le cas pour WannaCry ou Eternal Blue[38].

Dans la même logique de difficulté d'application du droit on pourra mentionner, la question de la souveraineté et de son corollaire, le recours à la force. D'une part, elle implique de devoir affiner le concept à la fois dans le cas d'un système spatial, ce qui implique les quatre segments et les services fournis par le satellite et non pas uniquement le cas d'un engin spatial, puisque cette question trouve une réponse assez rapidement dans l'article VIII du traité précédemment cité. D'autre part, il n'est pas sûr qu'y répondre soit opportun. La résolution 3314 de 1974 définit l'agression armée (qui est la condition *sine qua none* pour invoquer la légitime défense au sens de l'article 51 de la charte des Nations-unis) comme « *l'emploi de la force armée par un Etat contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre Etat, ou de toute autre manière incompatible avec la Charte des Nations unies* ». Or, préciser ces concepts dans un texte juridique pour caractériser avec finesse les atteintes à la souveraineté reviendrait à déterminer implicitement un seuil d'agression et donc a contrario un niveau d'acceptation de l'agression.

C'est pourquoi il est nécessaire de se doter assez rapidement d'instruments de régulation. D'ailleurs, on a pu observer ces dernières années plusieurs tentatives qui allaient dans ce sens, mais qui se sont heurtées à de nombreux blocages.

Des tentatives de régulations insuffisantes pour assurer la sûreté des activités spatiales

Il existe plusieurs tentatives de régulation concernant aussi bien le spatial que le cyberespace pour essayer d'assurer la viabilité de leurs activités respectives. Mais comme on a pu le voir précédemment les situations juridiques étant particulièrement complexes, il est difficile de s'accorder sur de nouvelles dispositions internationales, notamment parce que ces situations ne répondent pas uniquement à des logiques juridiques. Dans notre cas, on s'intéressera davantage aux dispositions relatives au cyberespace, puisque la plupart des textes concernant les activités spatiales (civiles et militaires), ont été pensés ou rédigés avant que les cyberattaques ne soient véritablement devenues la préoccupation des Etats, ce qui a pour conséquence que la plupart de ces textes se focalisent principalement sur les questions d'armes en orbite ou d'armes cinétiques.

De manière générale, lorsque l'on étudie les différentes initiatives qui ont pour objectif de réguler la militarisation de l'espace ou les cyber-

[35] Il existe un certain nombre d'autres principes en droit international privé pour essayer de résoudre les conflits de droit applicable mais nous ne les aborderons pas dans cet article où nous nous contentons de faire un état des lieux des problèmes que les cybermenaces et cyberattaques peuvent engendrer.

[36] F. Delerue, 2020, *Cyberoperations and international law*, Cambridge University Press, p.108

[37] CIJ, 1984, Activités militaires et paramilitaires au Nicaragua, §101

[38] Ibid.

opérations, on s'aperçoit que la mise en place de nouveaux traités est extrêmement complexe avec parfois des positions inconciliables. Le cas de la Conférence du désarmement en est un bon exemple avec la position américaine qui consiste d'une part à refuser tout nouveau traité ou instrument ayant potentiellement une valeur contraignante et, d'autre part, les positions russes et chinoises qui veulent des normes contraignantes limitant la militarisation de l'espace. Mais l'on peut s'apercevoir également que l'application des règles du droit international public général reste un sujet sensible, non pas sur le fond mais sur leurs modalités. Un bon exemple est l'échec de la 5e session de l'UNGGE[39], à la suite du rejet de la Chine, de la Russie et de Cuba, en raison de la question de la légitime défense, des contre-mesures et de l'application du droit des conflits armés au cyber-opérations[40]. Ces positions montrent à quel point le sujet de la régulation est central et sensible.

On peut également remarquer que le recours à la *soft law*[41] reste peu satisfaisant, non pas dans le sens où elle ne produit pas d'effet contraignant, puisqu'il n'est pas rare d'y avoir recours pour inciter les Etats à adopter un comportement souhaité, notamment par la pression politique qu'elle peut exercer, surtout si de nombreux Etats y souscrivent. Mais plutôt parce que les nombreuses initiatives entreprises ont du mal à aboutir. Le code de conduite pour les activités menées dans l'espace extra-atmosphérique, (que l'on désignera ci-après par *code de conduite*) qui est une initiative européenne, dont l'idée était de contourner les blocages de la conférence du désarmement, en est un exemple. Dès le départ, le *code de conduite* n'était pas prévu pour être contraignant. En revanche, l'ambition était de pouvoir déboucher soit sur des normes juridiquement contraignantes, soit sur un traité, mais aucun des deux objectifs n'a réellement été atteint. La première version datant de 2004, avait pour intérêt d'essayer de poser un certain nombre de définitions, telles que « antisatellite » et « armes spatiales ». Cependant, les versions suivantes s'en abstiendront pour faciliter le consensus[42] et s'axeront davantage sur les questions de bonnes pratiques et de transparence. L'émergence du *Code de conduite* a été compliquée notamment en raison de nombreuses divergences entre Etats européens. Depuis 2010, malgré l'approbation thématique de l'UE, aucun texte juridiquement contraignant n'a pu émerger en raison de plusieurs blocages dès qu'il s'agit de statuer sur la question des armes spatiales.

A cela, il faut ajouter les productions de groupe d'experts, à l'instar du manuel de Tallinn pour les cyber-opérations qui n'a pas de valeur normative, mais qui exerce néanmoins une certaine influence auprès de nombreux experts, notamment parce qu'il sert d'ouvrage de référence[43]. Cependant même si le manuel de Tallinn à une influence incontestable, il reflète principalement une vision OTAN-centrée, voire anglo-saxonne du droit concernant les opérations cyber et ne pourra que difficilement servir de base à la production d'un instrument de régulation universel. Dans le même ordre d'idée, on peut souligner l'initiative du manuel de Milamos[44] pour le droit spatial, de

[39] United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) est une commission de l'assemblé générale des Nations Unies, fondée en 2004 et qui a pour objectifs de produire des normes pour responsabiliser le comportement des Etats dans le cyberespace.

[40] Selon ces objecteurs, l'application de la légitime défense ou des contre-mesures n'aurait que pour effet de renforcer la position des Etats déjà dominant au détriment des plus petits Etats.

[41] La soft law peut être définit comme l'ensemble des *« normes incertaines en raisons du fait soit de leur contenu, soit de leur inclusion dans une source non susceptible de créer des obligations juridiques* », en d'autre termes ce sont des textes de droit non contraignant.

P. Dallier, M. Forteau, A. Pellet, 2009, Traité de droit international public, LGDJ, 8e édition, p.427.

[42] W. Rathgeber, N-L Remuss, K-U Schrogl, 2009, *La sécurité de l'espace et le code de conduite européen pour les activités menées dans l'espace extra-atmosphérique*, Forum du désarmement, UNIDIR, p.39.

[43] F. Delerue, novembre 2017, « *Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber opérations* », CEIS.

http://francoisdelerue.eu/wp-content/uploads/2020/01/20171129_NP_F-Delerue_Analyse-Manuel-Tallinn-2-0.pdf

[44] Manual on International Law Applicable to Military Uses of Outer Space.

l'université de McGill et qui est en cours de production depuis 2016.

De plus, la plupart de ces initiatives prennent relativement peu en compte le cas des personnes de droit privé, qui sont de plus en plus nombreuses comme nous l'évoquions dans la première partie. Toutefois, il est intéressant de noter l'initiative de Microsoft qui a proposé une série de normes de comportement, en matière de cybersécurité pour les États, puis qui fut complétée en 2016, pour l'industrie des TIC[45].

Ces différents cas démontrent la difficulté de parvenir à un accord pour assurer la viabilité des activités spatiales face aux cyber-opérations. Néanmoins les problèmes de cybersécurité-spatiales semblent devenir une question davantage préoccupante, puisque l'on a pu voir récemment des projets du COPUOS[46], traitant de la viabilité à long terme des activités spatiales, s'intéresser au sujet[47].

Les cyberattaques opèrent donc une mutation profonde des questions de sûreté spatiale, tant sur le plan de la typologie de la menace, qu'en ce qui concerne la présence des acteurs dans le champ de la sécurité spatiale. Parallèlement à cela, les dispositions juridiques existantes semblent avoir du mal à assurer la sûreté spatiale face aux nouveaux enjeux que produisent les cyberattaques. A cela s'ajoutent des blocages sur la production de nouveaux instruments juridiques, liés en partie à des considérations géopolitiques, ce qui a pour effet de renforcer l'insécurité juridique dans le cadre des activités spatiales.

Néanmoins, au sein du droit spatial on peut observer une accélération de la demande normative en ce qui concerne la sûreté et la sécurité spatiale, ce qui est signe de la volonté de nombreux Etats de vouloir limiter la militarisation de l'espace extra-atmosphérique et d'assurer la viabilité des activités spatiales. Une volonté qui reste encore insuffisante.

***

Je remercie chaleureusement M. Sébastien Bombal, chef du pôle stratégie du commandement de la cyberdéfense (COMCYBER) pour les échanges que nous avons eu et le temps qu'il m'accordé ainsi que l'ICETA Eric Pfannstiel, adjoint au chef du bureau préparation de l'avenir du Commandement de l'Espace (CDE) pour ses commentaires.

[45] F. Delerue, *op.cit*, p.23

[46] Committee on the Peaceful Uses of Outer Space.

[47] Committee on the Peaceful Uses of Outer Space, 8-17 June 2016, *Updated set of draft guidelines for the long-term sustainability of outer space activities,* Fifty-ninth session Vienna, United Nations, p.15.
https://www.unoosa.org/res/oosadoc/data/documents/2016/aac_105l/aac_105l_301_0_html/AC105_L301E.pdf

Bibliographie

Ouvrages

J. Combacau, S. Sur, *Droit international public*, Paris, Montchrestien, 2010

P. Dallier, M. Forteau, A. Pellet, 2009, « *Traité de droit international public* », LGDJ, 8e édition,

F. Delerue, 2020, *Cyberoperations and international law*, Cambridge University

O. Kempf, 2015, « *Introduction à la cyberstratégie »,* 2édition, Economica

X. Pasco, 2017, « *Le nouvel âge spatial : de la Guerre Froide au New Space* », CNRS éditions, Paris

L. Peyrefitte, 1993, « *droit de l'espace* », Précis Dalloz, Dalloz

D. Ventre, 2011, *« Cyberespace et acteurs du cyberconflit* », Lavoisier Hermès,

Articles de périodiques

L. Del Monte, G. Naja, 2017, « *Hack-my-sat : cyber threats and digital revolution in space* », in : European Space Programs and digital challenge, Laurence Nardon (ed), IFRI

D. Housen-Couriel, 2015, « *Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses* », Law & Cyber Warfare,

X. Pasco, 2011, « Des *initiatives européennes pour la sécurité dans l'espace*, » AFRI, volume XII

Dictionnaire et glossaires

CICDE, 16 décembre 2013, « *Glossaire interarmées de terminologie opérationnel »,* amendé en 1 er juin 2015.

J-P de la Cotardière, J-P Penot, 1993, « *Dictionnaire de l'espace* », Larousse

Rapports et expertises

Chatham House, David Livingstone and Patricia Lewis, September2016, » *Space, the Final Frontier for Cybersecurity ? »*, International Security Department

CICDE, 19 juillet 2010, *Utilisation de l'espace à des fins de défense et de sécurité nationale,* Réflexion doctrinale interarmées RDIA-2010/004_ESPACE(2010), N° 197/DEF/CICDE/NP du 19 juillet 2010, p.20

F. Delerue, novembre 2017, « *Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber opérations* », CEIS

F. Gaillard-Sborowsky, I. Facon, X. Pasco, I. Sourbès-Verger, P. Achilleas, 2016, *Sécuriser l'espace extra-atmosphérique, éléments pour une diplomatie spatiale*, rapport final, Fondation pour la recherche stratégique

F. Gaillard-Sborowsky, I. Facon, X. Pasco, I. Sourbès-Verger, P. Achilleas, 2016, *Sécuriser l'espace extra-atmosphérique, éléments pour une diplomatie spatiale*, volume d'annexes, Fondation pour la recherche stratégique

M. L. Psiaki, T. E. Humphreys and B. Stauffer, août 2016 "*Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies*," in IEEE Spectrum, vol. 53, no. 8, pp. 26-53

W. Rathgeber, N-L Remuss, K-U Schrogl, 2009, « *La sécurité de l'espace et le code de conduite européen pour les activités menées dans l'espace extra-atmosphérique* », Forum du désarmement, UNIDIR

Stratégie spatiale de défense, 2019, Rapport du groupe de travail « Espace », Ministère des Armées

Revue stratégique de cyberdéfense, 12 février 2018, SGDSN

Contact : iesd.contact@gmail.com

Site : https://iesd.univ-lyon3.fr/

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08