Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2022)
Heft: 3

Artikel: Cyberespace et espace
Autor: Ventre, Daniel
DOI: https://doi.org/10.5169/seals-1044745

Deuxième édition de l'exercice militaire spatial (AsterX) international organisé à la Cité de l'Espace, à Toulouse, le 4 mars 2022.

Cyber

Cyberespace et espace

Daniel Ventre

Docteur en Science Politique, chercheur au CESDIP (Centre de Recherche sur le Droit et les Institutions Pénales, UMR 8183), CNRS

La conquête spatiale a véritablement démarré avec le lancement du satellite Sputnik par l'URSS en 1957. Depuis lors l'espace est devenu un lieu de concurrence entre les grandes puissances mais aussi de coopération (station internationale), un milieu dont l'utilisation est désormais indispensable au fonctionnement de nos sociétés. L'informatisation du monde est contemporaine de cet investissement de l'espace, débutant elle aussi dans les années 1950. Leurs histoires respectives sont liées. Chronologiquement, mais plus encore. Sans informatique il n'aurait guère été possible d'envoyer engins et hommes dans l'espace. Les satellites, « ordinateurs dans l'espace »[1], sont autant de pièces essentielles à l'infrastructure de communication planétaire, civile et militaire. Ils sont une pièce maîtresse de la guerre moderne, des systèmes de communication qui sous-tendent la mise en œuvre de la guerre réseau centrique (Network Centric Warfare) depuis les années 1990, des systèmes C4ISR. Ces dernière années la militarisation des deux domaines (espace et cyberespace) s'est accélérée, principalement au sein des grandes puissances. La prise en compte de l'étroite interdépendance qui lie les deux domaines impacte les cadres doctrinaux et stratégiques dont nous proposons ici une première lecture en nous intéressant plus spécifiquement à l'approche américaine.

I – Définir les objets

Pour le Département de la Défense américain l'espace est « la zone au-dessus de l'altitude à laquelle les effets atmosphériques sur les objets aériens deviennent négligeables [...] la zone entourant la Terre à des altitudes égales ou supérieures à 100 kilomètres (54 milles marins) au-dessus du niveau moyen de la mer ». [2] La ligne de Karman en est donc la frontière.

Le cyberespace est quant à lui un *« domaine global au sein de l'environnement informationnel et qui est constitué des réseaux interdépendants d'infrastructures de technologies de l'information, des données qui y résident, des réseaux de télécommunication, des systèmes informatiques, des processus embarqués et des contrôleurs »* (JP 3-12)[3]. Plus pratique sans doute que cette énumération est le désormais modèle à trois niveaux : *« le cyberespace peut être décrit en termes de 3 couches interdépendantes : le réseau physique, le réseau logique, le niveau des individus (JP 3-12) ».*

Les deux domaines sont militarisés et font l'objet d'un renforcement des moyens qui leur sont alloués, en raison de leur fonction essentielle au maintien de la sécurité nationale et des capacités de défense.

Le budget américain alloué en 2019 au programme spatial militaire a été augmenté de manière significative (+8%)[4] ; le Président Trump a annoncé le 18 juin 2018 la création d'une Space Force dont la mission sera de protéger les Etats-Unis d'attaques provenant de l'espace ; la nouvelle agence spatiale SDA (Space Development Agency), créée en mars 2019 s'est fixée pour mission de renouveler

[1] Brian Weeden, Current and future trends in Chinese counterspace capabilities, Proliferation Papers, Ifri, Novembre 2020, 44 pages, Paris, https://www.ifri.org/sites/default/files/atoms/files/current_and_future_trends.pdf

[2] Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-14, Space Operations, 10 avril 2018, modifié le 26 octobre 2020, 96 pages, Etats-Unis.

[3] Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-12, Cyberspace Operations, 8 juin 2018, 104 pages, Etats-Unis

[4] Le budget américain alloué au spatial militaire est de 9,3 milliards en 2019 : 4,8 milliards pour les satellites, 2,4 pour les véhicules de lancement, 2,1 milliards pour l'entretien et les programmes classifiés. La part du spatial ne représente toutefois que 1,3% du budget global de la défense américaine, qui s'élève à 686 milliards en 2019. Source : Arthur Kremski, La nouvelle doctrine américaine du Space Power, La note du CERPA, novembre 2018, 1 page.

l'approche des déploiements satellitaires en mettant sur orbite 1'000 nouveaux satellites d'ici 2026 (l'objectif étant notamment de disposer d'une nouvelle architecture de communications sécurisées, plus performante en termes de débits, couvrant une plus grande surface).

La militarisation du cyberespace s'est accélérée au tournant de la décennie 2010, avec la création du cyber commandement américain et progressivement dans de nombreux pays une reconnaissance et normalisation de l'existence de capacités cyber-offensives dans plusieurs Etats. La dimension « cyber » est au cœur de toutes les opérations militaires, quel que soit le lieu de projection des forces américaines. Des opérations offensives dans le cyberespace font désormais partie de la panoplie usuelle de l'action militaire et d'agences de renseignement.

II – A propos de l'interdépendance des domaines et leurs interactions

Mais ce qui nous intéresse ici n'est pas tant le développement individuel de chacun de ces espaces, marqué par la militarisation et l'arsenalisation, que leurs interactions, leurs relations, leur interdépendance, qui auront inévitablement un impact sur la pensée militaire (doctrine), politique (stratégies, diplomatie, droit international), et sur la dimension bureaucratique (organisation).

Cette interdépendance est exprimée à maintes reprises dans les documents officiels.

- « Le cyberespace, tout en faisant partie de l'environnement informationnel, est dépendant des domaines physiques que sont l'air, la terre, la mer, et l'espace » (JP 3-12) ;
- « La relation entre l'espace et le cyberespace est unique en ce que virtuellement toutes les opérations spatiales dépendent du cyberespace, et qu'une pat significative de la bande passante du cyberespace ne peut être délivrée que par des opérations spatiales, qui offrent une option de connectivité globale essentielle pour les opérations du cyberespace » (JP 3-12) ;
- « Les opérations dans l'espace permettent de nombreuses cyber opérations, et le contrôle des segments des systèmes de l'espace requiert l'utilisation du cyberespace » (JP 3-14).

Pour tenter d'identifier les multiples points du cyberespace et de l'espace qui se croisent nécessairement et attestent de cette interdépendance des deux domaines, nous mobilisons la notion de « système spatial » qui nous paraît plus utile que la définition même de l'espace, car elle décrit un système technologique composé de 3 segments, définis comme suit :

- Le segment « sol » est constitué des stations et technologies au sol utiles aux ressources du segment spatial, les équipements terrestres, les capteurs ; il faut entendre « sol » de manière large, car cela inclut la dimension terrestre, maritime et aérienne, c'est-à-dire tout ce qui se situe en dessous de la ligne de Karman ;
- Le segment « lien » concerne la transmission du signal entre le sol et l'espace, ou entre éléments dans l'espace ;
- Le segment « espace » comprend les engins spatiaux opérationnels dans le domaine spatial.

Sur la base de ces segments et des 3 couches du cyberespace, nous proposons une matrice qui permet d'analyser les interactions entre espace et cyberespace. Le tableau suivant doit être lu en partant de chacune des trois couches du cyberespace vers chacun des trois segments de l'espace, chaque intersection répondant à la question : le cyberespace intervient-il sur ce segment de l'espace, si oui sous quelle forme ?

Les réponses apportées ici ne sont pas exhaustives mais illustrent à la fois la présence de l'informatique à tous les niveaux de l'espace et la possibilité qui en découle d'y réaliser des opérations offensives. La cybersécurité de l'espace dépend de celle de chacun de ses segments.

Cette interdépendance se traduit également dans l'organisation des forces de défense. L'US Space Force a besoin de compétences cyber et négocie avec le Cyber Command et l'Air Force la mise à disposition de personnels spécialisés (2021).[7] Les compétences cyber sont indispensables dans le domaine spatial que ce soit pour assurer le fonctionnement des communications satellites, le fonctionnement des systèmes SCADA, la cybersécurité des systèmes satellitaires et des stations au sol par exemple. Le Space Command de son côté envisage la création d'un centre cyber (Joint Cyber Center) pour favoriser les liens avec le Cyber Command[8] dans le but d'assurer la cybersécurité des satellites de communication et des stations au sol, en s'appuyant sur les technologies de pointe telles que l'IA.

III – Quelques remarques de nature politique et juridique

Le traité international des Nations Unies (Résolution 2222 du 19 décembre 1966)[9] ne définit pas explicitement l'espace. Il pose toutefois les conditions de son utilisation et quelques règles essentielles : il conçoit l'espace comme un « global commons » (article premier) et fait notamment interdiction d'y déployer en orbite des armes de destruction massive ; il insiste sur la nature pacifique du projet d'exploration et d'utilisation de l'espace. Le Traité n'interdit ni la militarisation ni l'arsenalisation de l'espace. Si les armes de destruction massive y sont interdites, d'autres capacités offensives, cybernétiques par exemple, peuvent y prendre place. Rappelons qu'aucun texte international de même nature n'existe pour le cyberespace. On observe bien dans de ce dernier les

[7] Meredith Roaten, JUST IN : Space Force Wants More Cyber Teams, 5 mars 2021, National Defense Magazine, https://www.nationaldefensemagazine.org/articles/2021/5/3/just-in-space-command-wants-more-cyber-teams

[8] Lauren C. Williams, Space Command moves for tighter cyber integration, 21 avril 2021, https://fcw.com/articles/2021/04/21/space-command-cyber-zero-trust.aspx

[9] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 1499th plenary meeting, 19 Décembre 1966, Version française : https://www.unoosa.org/pdf/publications/STSPACE11F.pdf

		3 segments de l'espace (outer-space)		
		Espace	*Liens (communication)*	*Sol*
3 couches du cyberespace	*Couche 3 (information, données, sens)*	Interception des communications	Interception des communications	Interception des communications
	Couche 2 (logicielle, applicative)	Fonctionnement logiciel des ordinateurs embarqués dans les objets spatiaux Cyberattaque[5] du sol vers l'espace, de satellite à satellite… Attaques par malware, intrusions, dénie de service, etc.	Chiffrement des données Sécurité des communications Interception des communications Command intrusion, Spoofing, jamming[6]	Fonctionnement logiciel des systèmes des équipements au sol Cyberattaque contre systèmes au sol. Attaques par malware, intrusions, dénie de service, etc.
	Couche 1 (physique, matérielle)	Ordinateurs embarqués dans les engins spatiaux Cyberattaques visant à saboter les systèmes (destruction des systèmes)	Technologies d'interception des communications (sur les câbles terrestres ou sous-marins…)	Ordinateurs des stations et équipements de communication au sol Cyberattaques visant à saboter les systèmes (destruction des systèmes)

Tableau : Où et comment espace et cyberespace se rencontrent-ils ?

[6] Les cyberattaques sont des menaces intentionnelles (au même titre que les armes antisatellites, le brouillage, les attaques lasers) qui s'ajoutent aux menaces d'origine humaine non intentionnelles (débris), et aux menaces d'origine naturelle (activité solaire par exemple). JP 3-14. L'infrastructure ou système spatial est particulièrement vulnérable et exposé aux cyberattaques, au point que ces menaces seraient bien plus importantes que celles que font peser des armes cinétiques. Sandra Erwin, DoD Space Agency : cyber attacks, not missiles, are the most worrisome threat to satellites, SpaceNews, 14 avril 2021, https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/

[7] Les opérations de type jamming et spoofing et plus généralement les opérations menées contre le segment « lien », peuvent être considérées comme relevant uniquement du spectre électromagntique, donc de la guerre électronique et non de la dimension cyber proprement dite.

efforts des Etats pour y développer un arsenal spécifique et en faire un espace d'affrontement. Rien ne semble donc s'opposer à ce que l'espace soit un domaine de la cyber conflictualité à part entière.

L'utilisation pacifique de l'espace, qui est l'une des perspectives inscrites dans le Traité de 1966, pourrait ainsi sembler largement compromise par les initiatives de quelques grandes puissances dans l'espace (militarisation, développement d'armes pour l'espace, tests de destruction de satellites, création de commandements de l'espace) et par la généralisation, à l'échelle de la planète, de politiques de cyberdéfense agressives et du recours à des actes de violence dans le cyberespace.

Des études s'intéressant au statut juridique de ces deux espaces affirment que la communauté internationale serait en train de s'orienter vers la création de mécanismes de régulation ou de gouvernance en dehors du système des Nations Unies.[10] Ces futurs arrangements internationaux seraient élaborés par les principales puissances technologiques et scientifiques. Une hypothèse intéressante considère que la cyberguerre est au centre de ce processus : en brouillant les distinctions juridiques de l'espace et du cyberespace, l'intégration des systèmes spatiaux aux infrastructures du cyberespace qui vise à atteindre les objectifs fixés dans les doctrines de cyberguerre stratégique aurait pour effet de fusionner les domaines de gouvernance de l'espace et du cyberespace, via des accords spécifiques, hors des mécanismes juridiques conventionnels des Nations Unies. Quels que soient les cadres et formes qu'adopteront les régulations des deux espaces, leur interdépendance fonctionnelle se reflètera inévitablement dans leurs statuts juridiques.

D. V.

[10] Larry Martinez, Is There Space for the UN? Trends in Outer Space and Cyberspace Regime Evolution, European Space Policy Institute, Perspectives, n°56, 7 pages, Janvier 2012