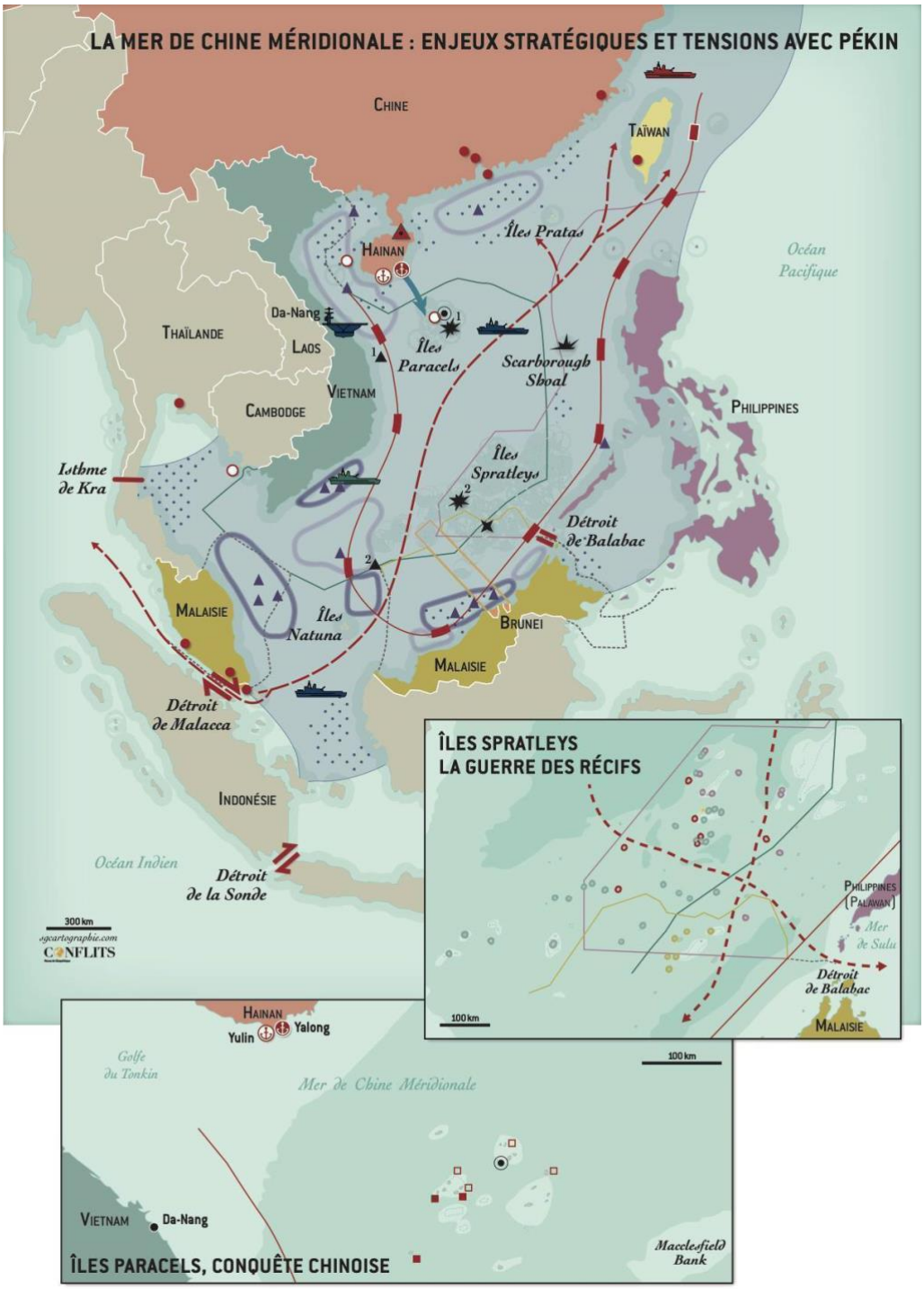
Face aux États-Unis, la menace antisatellite chinoise



par **Léo Henquinet – Conflits – publié le 2 août 2022**

https://www.revueconflits.com/face-aux-etats-unis-la-menace-antisatellite-chinoise/

Vecteurs balistiques, forces navales, systèmes de défense anti-missile, systèmes spatiaux… Alors que la montée en puissance de sa défense est structurellement tournée vers la dissuasion ou, le cas échéant, l'affrontement face aux États-Unis, en particulier sur le théâtre indopacifique, Pékin développe également des capacités antisatellites qui menacent les intérêts fondamentaux et la supériorité militaire de son adversaire, dépendants de l'exploitation des technologies et applications spatiales.

L'affirmation de la dimension spatiale

Le 23 mai 2022, le Président Joe Biden a déclaré que si la Chine venait à attaquer **Taïwan**, les États-Unis la défendraient militairement[1]. À l'heure où l'Europe a les yeux rivés sur la guerre russo-ukrainienne, cette déclaration souligne la place secondaire qu'occupe ce conflit pour Washington, et illustre une fois de plus que sa priorité est la lutte contre « l'ennemi systémique » chinois.

Néanmoins, la guerre d'Ukraine a mis en lumière ou attesté de l'efficacité de certains moyens ou méthodes dans la conduite de la guerre moderne : importance de la maitrise des airs, multiplication des effets par l'usage des drones, effets de la « brutalisation », utilisation tactique des couloirs humanitaires… Surtout, l'espace a été le théâtre de deux événements inédits, qui confirment l'émergence d'une nouvelle dimension du champ de bataille.

Le 15 novembre 2021, la Russie a détruit un de ses satellites au moyen d'un missile intercepteur *Nudol*, dans le cadre de la phase de développement de son système de défense antimissile balistique, dual[2]. Mais ce tir antisatellite s'inscrit dans une temporalité qui, rétrospectivement, est celle des préparatifs de l'invasion de l'Ukraine. Le choix de sa date a donc été motivé par la volonté de démontrer à ses adversaires, en particulier aux membres de l'OTAN, dont les intérêts économiques et la puissance militaire sont largement dépendants de l'utilisation de l'espace, que Moscou a pleinement intégré la dimension spatiale en tant que milieu de confrontation, et qu'elle pourrait, par l'espace, infliger des dommages considérables à ceux qui s'opposeraient militairement à sa politique[3]. Le 24 février 2022, jour du déclenchement de l'invasion russe, une cyberattaque a frappé des dizaines de milliers d'utilisateurs du satellite de télécommunications KA-SAT (du réseau satellitaire de la société américaine Viasat), rendant inopérants modems et terminaux. Les USA, l'Union européenne et le Royaume-Uni ont attribué cette attaque à la Russie[4]. Les services de sécurité et les autorités politiques ukrainiennes étaient utilisatrices du réseau Viasat[5], et ont vu leurs communications perturbées lors de cette première phase de la guerre, avant que des acteurs occidentaux, aux premiers rangs desquels Starlink[6], ne fournissent des moyens pour assurer la continuité et la résilience des capacités ukrainiennes[7]. D'autres cyberattaques de moindre ampleur visant des systèmes spatiaux russes et ukrainiens ont aussi été dénoncées. S'ajoute à cela une intense activité de brouillage des signaux *GPS*, non revendiquée, probablement réalisée par des systèmes russes comme le *Tirada-2S**[8]***.

S'il convient de relativiser le rôle de ces actions et la place de la dimension spatiale dans le déroulé du conflit, notamment parce que les deux belligérants présentent une asymétrie en termes de moyens et d'intérêts spatiaux et ont peu intégré les technologies et applications spatiales en soutien à leurs opérations conventionnelles, elle illustre néanmoins la confirmation de l'extension à l'espace du champ de conflictualité et le potentiel tactique et stratégique des opérations antisatellites.

Mais dans le cas du duel sino-américain, la dimension spatiale est un enjeu majeur, car l'accès et l'utilisation de l'espace sont des leviers et des attributs essentiels à la puissance politique, économique et militaire de Pékin et, surtout, de Washington. En effet, plus que toute autre puissance, la supériorité militaire des USA repose sur un appui inégalé des technologies et applications spatiales à ses forces armées conventionnelles et stratégiques.

La Chine est bien conscience de cette vulnérabilité des USA, mais aussi de sa propre nécessité de garantir la sécurité de ses intérêts dans l'espace, en particulier face aux intentions américaines d'assurer, si besoin par la force, la continuité de leur domination spatiale, c'est-à-dire de leur capacité à structurer les évolutions au sein du domaine spatial et à pouvoir en toute circonstance y garantir la prééminence de leurs intérêts, en vue notamment de perpétuer leur capacité à dominer les autres dimensions (terre, air, mer, cyber).

L'espace, théâtre de la confrontation croissante entre la Chine et les États-Unis

L'on assiste depuis le début des années 2000 à une montée en puissance des politiques de défense spatiale chinoises et américaines, et à l'affirmation de leur volonté de garantir (ou acquérir) la domination de l'espace par des moyens de défense active, voire par l'atteinte aux capacités adverses.

Washington a été à l'initiative de cette nouvelle « arsenalisation » de l'espace[9]. Après avoir fait la démonstration d'une supériorité technologique éclatante durant la Première Guerre du Golfe[10], reposant, entre autres, sur une utilisation inédite des technologies et applications spatiales en appui à la planification, à la conduite et au suivi des opérations, sa dépendance a dès la fin des années 1990 été identifiée comme une vulnérabilité majeure pour sa sécurité nationale et sa capacité de projection[11]. Émergent alors des politiques issues de concepts comme le *space control* et la *space dominance****[12]***, qui visent à prévenir toute menace sur ses intérêts spatiaux et à garantir sa domination spatiale, y compris par le déni d'accès aux moyens adverses[13].

Cette tendance s'articule avec la modernisation de sa défense antimissile balistique, jusqu'à prévoir, après le retrait du traité ABM en 2001 qui les prohibait, le déploiement d'une composante d'intercepteurs basés dans l'espace[14]. C'est la parité et la crédibilité des forces de dissuasion de l'ensemble des puissances nucléaires qui sont alors menacées par ces projets américains, ainsi que l'ordre pacifique prévalent dans l'espace. Car si des objets spatiaux conduisent des activités militaires, et si rien n'interdit le déploiement d'armements conventionnels dans l'espace, un équilibre de fait prévalait depuis la Guerre froide quant à la préservation de l'espace du champ de conflictualité, notamment quant à l'exclusion du déploiement des armes spatiales antisatellite et duales (à la fois *space-to-ground* et *space-to-space*).

Après deux essais en 2005 et 2006[15], la Chine a répondu en 2007 à l'approche unilatéraliste de la domination spatiale américaine en procédant à la destruction d'un de ses satellites en fin de vie au moyen d'un missile antisatellite, affirmant sa volonté et sa capacité à porter ou soutenir le conflit dans l'espace. Washington ne s'y est pas trompée et a détruit, presque un an jour pour jour après le tir chinois, un de ses satellites défectueux, également par un missile antisatellite.

Avant la mise en œuvre du « pivot asiatique »[16], puis la désignation explicite de la menace structurelle chinoise comme priorité stratégique, l'espace a donc été dès la décennie 2000 le motif d'une confrontation croissante, esquissant le duel entre les deux puissances majeures du début du XXIe siècle. Si la « guerre contre le terrorisme » et la lutte contre les « *rogue states* » vont provisoirement supplanter une menace chinoise déjà identifiée[17], les désillusions américaines au Moyen-Orient et, surtout, l'ampleur du développement économique, politique et militaire de Pékin, qui ne cache plus ni ses ambitions de puissance aux échelles régionales et globales, ni sa volonté d'évincer les USA de leurs positions asiatiques et, plus largement, de leur statut de première puissance mondiale, vont conduire Washington à réviser ses priorités stratégiques, et à faire de la question chinoise l'enjeu majeur de la perpétuation de sa domination du système international.

La confrontation croissante entre Chinois et Américains n'est pas sans conséquences sur la place de la dimension spatiale pour les USA. Car s'ils bénéficient de supériorité militaire certaine grâce à une exploitation sans commune mesure avec les autres États des moyens spatiaux, face à un adversaire conventionnel doté de moyens antisatellites, le risque est grand de le voir tenté de rétablir la parité, voire même d'obtenir l'avantage asymétrique en atteignant à la disponibilité ou à l'intégrité des systèmes spatiaux américains, et donc en menaçant les forces américaines d'évoluer dans un environnement partiellement ou totalement dégradé.

Pour mettre en œuvre ce levier de dissuasion et de supériorité militaire, Pékin a fait du développement de capacités antisatellites un axe majeur de sa politique de défense et de sa politique spatiale.

La montée en puissance des capacités antisatellites chinoises

Des moyens non-cinétiques adaptés à la nature du milieu spatial

Mais parce que la Chine est elle aussi dépendante, et de plus en plus, de l'espace pour son développement économique, son rayonnement politique et pour soutenir ses forces armées, elle ne se limite pas aux missiles antisatellites. Leurs effets se résument à la destruction de la cible, et l'attaque est facilement attribuable grâce aux moyens de reconnaissance, d'alerte précoce et de surveillance de l'espace. Surtout, les destructions cinétiques produisent un grand nombre de débris, qui risqueraient d'entrer en collision avec un ou des satellites et qui, selon leur taille, peuvent provoquer des dommages importants sur les composants impactés, voire la destruction du système. Plus de 1500 nouveaux débris spatiaux ont par exemple été détectés à la suite du tir antisatellite russe du 21 novembre 2021. Procéder à des tirs antisatellites pourrait donc compromettre la réputation internationale du pays et ses propres capacités à exploiter l'espace, car les débris spatiaux sont une menace majeure pour la sécurité et la durabilité de l'ensemble des activités spatiales, tous opérateurs confondus.

Eu égard au rôle des technologies et applications spatiales dans la garantie de la puissance militaire et de la crédibilité de la force de dissuasion des grandes puissances, un tir qui aurait des effets sur les systèmes étrangers menacerait même de conduire à l'escalade. C'est pourquoi règne depuis la Guerre froide un équilibre de fait entre les puissances spatiales quant au non-emploi des moyens cinétiques et à la maitrise du niveau de violence exercée au sein du domaine spatial[18].

Afin de pouvoir conduire des opérations antisatellites sans le remettre en cause, la Chine développe des armes couvrant l'ensemble du spectre des capacités antisatellites non-cinétiques, qui peuvent agir par gradation et produire des effets réversibles ou irréversibles, très complexe à suivre et à attribuer, car profitant de la « dimension grise » de l'espace[19] et pouvant être assimilée à des dysfonctionnements ou des accidents, ou se situer sous le seuil de conflictualité.

Des rapports ont fait état du développement, d'essais et de déploiements par la Chine de dispositifs de guerre électronique, de lasers à haute énergie (HEL), d'armes à micro-ondes, de forte puissance, de satellites de proximité et de moyens cyber dédiés à opérer face à aux systèmes spatiaux[20]. Ces armements, tout en minimisant les risques d'occasionner des débris spatiaux, s'articulent autour de deux types d'effets recherchés : la neutralisation partielle, temporaire ou totale du système visé, et la compromission ou la falsification du système et de ses données.

Les HEL ont des effets gradués selon la puissance mise en œuvre, allant de l'aveuglement d'un capteur (notamment ceux des satellites de reconnaissance) à la destruction des composants et des circuits électroniques d'un satellite. Bien que des contraintes techniques persistent quant à l'émergence, au moins à court terme, d'un arsenal crédible opérationnellement, Pékin a démontré que ses HEL terrestres étaient en mesure d'aveugler, et peut-être d'endommager les capteurs ou les composants des satellites, *a minima* en orbite basse. Dès 2006, un satellite de reconnaissance américain a ainsi été aveuglé[21]. Quant aux armes à micro-ondes, moins développées, elles produisent des interférences et des perturbations sur les composants et les circuits électroniques des satellites, qui peuvent aller jusqu'à leur neutralisation. Lasers et armes à micro-ondes visent directement le segment spatial du système satellitaire ciblé, contrairement aux systèmes de guerre électronique, qui affectent les flux de données entre le segment spatial, le segment sol et le segment utilisateur en émettant des signaux à très haute intensité, mais soumis à une forte dispersion, qui permettent donc de perturber ou dénier l'accès à des données et services spatiaux sur une zone donnée, notamment les réseaux de communications ou de géopositionnement.

Les satellites de proximité : l'action depuis l'espace

Les satellites de proximité sont capables de mener des opérations de proximité : « des manœuvres intentionnelles visant à rapprocher physiquement un satellite d'un autre objet en orbite, en vue de s'y amarrer ou de mener des opérations à ses abords »[22]. Outre les applications des services en orbite (maintenance, transfert d'orbite, amélioration des composants), les compétences d'approche et de manœuvre co-orbitale sont particulièrement exploitables à des fins militaires[23].

Car l'espace est un milieu dépourvu de souveraineté nationale, et pour lequel il n'existe pas de définition internationale des actes hostiles. Il est donc, en principe, parfaitement autorisé d'approcher d'un satellite étranger. Par ailleurs, le milieu spatial demeure un environnement relativement peu maitrisé en comparaison des autres dimensions et où des collisions accidentelles entre satellites sont, bien que très rare, parfaitement probables, et ce d'autant plus qu'il est de plus en plus investi par les activités humaines. Du reste, les moyens de distinguer avec certitude ce qui relèverait de la collision accidentelle d'une agression demeurent limités. En 2009, un satellite militaire russe et un satellite de télécommunication civil américain se sont accidentellement percutés, provoquant leur destruction[24]. La Russie avait alors exploité politiquement l'accident, en instrumentalisant le caractère dual du satellite

américain impliqué (son propriétaire, la société Iridium, effectuait essentiellement des prestations de services au profit des forces armées américaines) et en profitant de l'impossibilité de prouver avec certitude les causes exactes de la collision pour les lier au développement par Washington de satellites de proximité destinés à des usages militaires, et dénoncer ainsi la menace que les USA feraient peser sur l'ensemble des acteurs spatiaux.

Avec la multiplication du nombre de satellites manœuvrants et l'arsenalisation croissante de l'espace, un tel événement qui surviendrait aujourd'hui ne manquerait pas d'être empreint d'ambiguïtés encore plus fortes. Néanmoins, comme pour les missiles antisatellites, la destruction physique par une collision entre deux systèmes spatiaux produit de nombreux débris. L'emploi des capacités de manœuvre co-orbitale tend donc à être couplé à des systèmes embarqués de guerre ou d'écoute électronique, d'armes laser, d'armes chimiques, d'armes à micro-ondes ou à des moyens cinétiques non destructifs (filets, bras articulés), qui présentent l'avantage de pouvoir agir par gradation ou de produire des effets réversibles.

Équipes de moyens de défense passive (en particulier de moyens de surveillance de leur environnement) ou actifs, cinétiques ou non-cinétiques, les satellites de proximité, aussi appelés « satellites patrouilleurs » ou « butineurs », sortes de « sous-marins de l'espace »[25], peuvent ainsi profiter de la dimension grise de l'espace pour s'y mouvoir et mener des opérations très discrètes, complexes à caractériser et à attribuer, visant à espionner, leurrer, brouiller, compromettre, intercepter, endommager, ou détruire un satellite étranger.

Depuis la décennie 2010, de nombreuses opérations de proximité chinoises en orbite basse et en orbite géostationnaire (à environ 36 000 km d'altitude) ont été documentées[26]. Ont été rapportées des manœuvres de déplacement et de rapprochement en orbite, ainsi que des manœuvres complexes d'accrochage et de « remorquage » par des systèmes dotés de bras robotisés[27]. Si le plus grand secret entoure les capacités et missions précises de ces systèmes, il est probable qu'ils sont en phase d'expérimentation dans le cadre du développement de satellites de services en orbite et de capacités antisatellites, ou qu'ils assurent des missions de renseignement sur des satellites étrangers[28], à l'instar, par exemple, des approches du satellite-espion russe *Louch Olymp*, dont l'une des manœuvres à proximité d'un satellite franco-italien en 2017 a été rendue publique par Paris[29].

Bien qu'il n'y ait pas de preuves attestant de telles opérations réalisées par un satellite chinois, les démonstrations de son dynamisme et de ses progrès dans la manœuvrabilité des systèmes en orbite attestent de sa capacité à en exploiter la dualité et à « patrouiller » dans l'espace. Ils dotent Pékin d'une capacité à mettre en œuvre des moyens antisatellites directement depuis l'espace, qui exploite à la fois la dualité de leurs capacités, l'absence de cadre juridique et les limites de la connaissance du milieu spatial pour conduire des opérations très discrètes et complexes à attribuer.

Armes non-cinétiques et satellites de proximité participent donc l'hybridation de la conduite de la guerre, c'est-à-dire de la combinaison d'actions et moyens conventionnels et non-conventionnels dans les différents champs et dimensions, aussi bien contre des objectifs civils que des objectifs militaires.

Dans cette logique d'hybridation, la Chine a rassemblé en 2015 ses moyens spatiaux, électroniques, informationnels et cyber au sein d'une même branche de l'Armée Populaire de Libération, la « Force de soutien stratégique », illustrant sa volonté de faire du domaine

spatial un prolongement du champ de confrontation informationnelle, dans lequel les dimensions cyber et spatiale sont pleinement intégrées.

Un mode d'action antisatellite apparait alors particulièrement favorable au contre-espace chinois : la cybermenace.

La cybermenace chinoise : exploiter le continuum espace-cyberespace

Espace et cyberespace forment un *continuum*, dû à une double interconnexion entre ces deux dimensions[30]. Infrastructurelle, d'abord, les systèmes spatiaux étant une composante des infrastructures de télécommunications, et étant dépendants des technologies, réseaux et services informatiques pour interagir avec le sol ou d'autres systèmes spatiaux. Applicative, ensuite, les données spatiales transitant par des réseaux informatiques, et étant stockées, exploitées et valorisées à l'aide de systèmes informatiques.

Alors que la dimension cyber est aussi un milieu de confrontation militaire à part entière et que les cyberattaques sont très difficiles à attribuer, ce *continuum* tend également à favoriser la conduite d'opérations antisatellites produisant des effets tactiques ou stratégiques tout en préservant la dimension spatiale d'un conflit ouvert qui menacerait l'ensemble des puissances spatiales.

Atteintes à l'intégrité, à la disponibilité et à la confidentialité[31] peuvent être occasionnées par une cyberattaque contre les infrastructures au sol (antennes, stations, lignes de communication), les terminaux des utilisateurs, ou encore les antennes et logiciels des satellites (voire même leurs composants), créant « des dommages temporaires et réversibles, ou au contraire des destructions physiques et permanentes »[32]. Les attaquants pourraient par exemple prendre le contrôle du système de propulsion embarqué sur un satellite (outre les satellites de proximité, de plus en plus de satellites en sont équipés afin d'effectuer des corrections de trajectoire ou de position et prolonger ainsi leur durée de vie,) et le désorbiter ou occasionner une collision (volontaire ou accidentelle) avec un autre objet spatial, ou encore dégrader ou paralyser le réseau d'un opérateur militaire ou dual (comme pour le cas de la cyberattaque russe ayant frappé Viasat le 24 février 2022) .

À cet égard, le cas de la guerre d'Ukraine confirme l'importance de l'appui et des attaques cyber[33], et a même, comme nous l'avons évoqué, illustré le potentiel opérationnel de l'exploitation du *continuum* espace-cyberespace. La cyberattaque russe du 24 février s'inscrit dans un contexte dans lequel Russes, Ukrainiens et alliés mènent une activité offensive d'une ampleur inédite dans le domaine cyber, visant aussi bien des cibles économiques, symboliques, et militaires, afin « d'affecter le ressenti des populations et des forces armées, et, surtout, d'atteindre à la cohérence d'ensemble du dispositif de C2 (*Command and Control*) adverse »[34], notamment en compromettant ou en paralysant les communications et le partage d'informations entre les troupes et le commandement.

Nul doute qu'un conflit sino-américain verrait la démultiplication des cyberattaques antisatellites. Parce que les deux pays disposent de moyens très développés, mais aussi parce que, en particulier dans le cas des USA, leur puissance est bien plus dépendante de leurs moyens spatiaux et de leur domination dans le champ informationnel, ce qui accroit considérablement l'intérêt de les affecter, en particulier lors des phases préparatoires ou préalables à un engagement.

Pékin dispose de capacités avancées pour mener des cyberattaques face aux systèmes spatiaux. Le rassemblement en 2015 de ses moyens cyber, informationnels et spatiaux tend également à indiquer qu'à la différence des USA, elle a pleinement intégré au niveau stratégique, organisationnel et opérationnel la nature interdépendante de ces dimensions, afin non seulement de faciliter la conduite d'opérations multi-milieux et multi-champs par les armées chinoises, mais aussi, comme l'ont affirmé les autorités et les stratèges du pays[35], pour pouvoir cibler au mieux les réseaux au cœur des systèmes de C2 adverses, « centre nerveux du champ de bataille dans les conflits modernes »[36].

Par définition, qui plus est la concernant, il est très difficile de mesurer l'activité cyber-offensive de la Chine face aux systèmes spatiaux. Plus encore que les autres moyens antisatellites, lesquels s'appuient sur des programmes industriels, avec des infrastructures physiques, des essais, sa politique de cyberdéfense face aux systèmes spatiaux est un angle mort structurel des services de renseignements américains et alliés.

Aucune source ne fait mention de cyberattaque chinoise d'un système militaire américain, ce qui n'exclut en rien que des actions sous le seuil soient déjà menées[37]. D'autant que les cyberattaquants chinois s'intéressent depuis longtemps à l'industrie spatiale américaine (et occidentale), et ont donc travaillé à exploiter les failles de ces systèmes. Des sources ont en effet fait état de campagnes de cyberattaques contre des systèmes spatiaux attribuées à la Chine, surtout à des fins d'espionnage économique[38]. Le groupe de pirates chinois « *Putter Panda* », lié à l'Armée Populaire de Libération[39], spécialisé dans les attaques ciblant les technologies de défense américaines, a notamment été identifié dès 2014 comme visant particulièrement le secteur spatial, et capable de disposer d'un « fort degré de contrôle » sur le système victime[40].

Les preuves des capacités chinoises à infiltrer des réseaux satellitaires étrangers et la cyberattaque russe du 24 février 2022 laissent entrevoir les effets qui pourraient affecter la sécurité nationale américaine ou le déploiement de ses forces en cas de confrontation militaire entre les deux pays. Une paralysie, même partielle, du dispositif de C2 des armées américaines engagées sur un théâtre, en particulier à l'extérieur, les contraindrait à évoluer dans un environnement profondément dégradé. Nicolas Chaillan a d'ailleurs insisté sur l'avance technologique chinoise et la vulnérabilité des USA, et affirmé qu'à cet égard, ils n'auraient probablement pas les capacités de combattre face à Pékin avant une vingtaine d'années[41].

Dissuader dans l'espace, dissuader par l'espace.

Face à un adversaire lui aussi doté de moyens de conduire des opérations hybrides antisatellites, une posture de défense spatiale reposant sur la dissuasion nucléaire est peu crédible, non seulement parce que les effets des attaques subies pourraient être très complexes à caractériser et à attribuer, mais aussi parce qu'ils pourraient se situer sous le seuil de celles de nature à enclencher le dialogue dissuasif. La « dimension grise » du domaine spatial et la prépondérance des moyens hybrides, en plus de tendre à la multiplication des opérations antisatellites, réduisent donc *de facto* la portée de la dissuasion nucléaire étendue à l'espace[42]. D'autant qu'officiellement, certes non sans ambiguïtés, la doctrine nucléaire chinoise insiste sur le non-emploi en premier[43].

Pour pouvoir assurer la sécurité de ses intérêts spatiaux, la Chine assume donc une posture de défense active, qui « participe d'une forme de dissuasion par le châtiment »[44], en

développant et en démontrant des capacités à détecter, déjouer ou riposter à des actions hostiles. Elles pourraient aussi infliger des dommages potentiellement considérables aux puissances qui seraient tentées de s'opposer à elle militairement, en menaçant d'atteindre aux moyens spatiaux appuyant leurs forces armées, ou encore en ciblant des systèmes civils, et renforcent ainsi le pouvoir dissuasif de Pékin. Elles renvoient au concept de « dissuasion intégrée », « une forme de dissuasion « stratégique » intégrant tous types de capacités – en particulier des capacités non-nucléaires pouvant au besoin servir des finalités plus coercitives que dissuasives »[45].

Du reste, son arsenal antisatellite pourrait remettre en cause la crédibilité de la défense antimissile et de la force de dissuasion nucléaire américaine, qui repose largement sur l'utilisation des technologies et applications spatiales : satellites d'alerte précoce, de communication, de reconnaissance, d'écoute électronique, de positionnement… En visant ces systèmes, la Chine pourrait rétablir la parité des capacités stratégiques avec les USA, voire même acquérir l'avantage asymétrique en les paralysant, et ainsi maximiser son propre pouvoir dissuasif.

Malgré les limites que nous avons évoquées, les missiles antisatellites sont un moyen d'assurer *a minima* et à moindre cout une posture de dissuasion dans et par l'espace, étant en mesure de démontrer par gradation sa capacité et sa volonté d'y agir, via le développement ou les essais conduits dans le cadre des programmes liés à la modernisation de ses capacités balistiques et de ses systèmes de défense antimissile[46], ou dans le cadre de programmes de développement de missiles antisatellites dédiés. Cette dimension démonstrative est la principale utilité des missiles antisatellites, mais ne saurait suffire à assurer une posture dissuasive crédible, car la mise en œuvre de tels moyens menacerait d'atteindre à ses propres intérêts spatiaux, et de remettre en cause l'équilibre prévalent au sein du domaine spatial quant à la prépondérance des opérations conduites sous le seuil.

Au-delà des moyens antisatellites, les capacités de surveillance de l'espace sont aussi de nature à dissuader un adversaire de conduire des attaques antisatellites, en favorisant l'identification, la caractérisation et l'attribution d'une action hostile, qui risquerait de voir son auteur désigné (*naming*) et compromis sur la scène internationale (*shaming*) ou confronté au risque d'escalade. Alors que la surveillance de l'espace est un enjeu majeur pour l'ensemble des acteurs du domaine spatial, qui opèrent dans un milieu de plus en plus encombré et en proie à une contestation croissante, la Chine a impulsé une montée en puissance dans les systèmes terrestres et spatiaux de surveillance de l'espace[47]. USA mis à part, elle dispose aujourd'hui des capacités les plus avancées pour détecter et traquer les objets spatiaux. Elle multiplie les capteurs au sol (radars, télescopes, lasers) mais aussi en orbite, comme l'ont attesté les nombreux événements de rendez-vous orbitaux effectués depuis 2010 par des satellites de proximité, qui requièrent une connaissance précise de la situation spatiale, et qui peuvent eux-mêmes y contribuer s'ils sont équipés de dispositifs de surveillance de leur environnement.

Ce besoin de connaissance de l'environnement spatial est du reste renforcé par l'investissement croissant du gouvernement et des acteurs privés chinois dans les activités spatiales, scientifiques et civiles. Pour assurer la sécurité des missions et la durabilité de l'exploitation de l'espace, alors que celui-ci est en proie à un encombrement croissant, les opérateurs ont besoin de plus en plus de données, de plus en plus précises, sur la situation spatiale. C'est donc l'ensemble du programme spatial chinois qui alimente sa montée en

puissance dans le domaine de la surveillance de l'espace, dont la dualité est mise au service de sa capacité à dissuader l'adversaire de s'en prendre à ses intérêts spatiaux.

Sa volonté d'élargir l'éventail de ses capacités de contre-espace contribue aussi à faire de la surveillance de l'espace une priorité de sa politique de défense spatiale. Car la dualité des moyens de surveillance de l'espace ne s'arrête pas au pouvoir dissuasif du *naming and shaming*. Ils sont en effet essentiels à la mise en œuvre des armes antisatellites qui visent le segment spatial. Par exemple, eu égard à la très faible dispersion de leur faisceau, les armes laser requièrent des données très précises sur la position et la vitesse orbitale pour atteindre leur cible, qui transite à des centaines ou à des milliers de kilomètres d'altitude et à une vitesse de plusieurs dizaines de milliers de kilomètres par heure.

Les capacités chinoises de contre-espace sont donc un levier de dissuasion face aux puissances spatiales, et d'abord face aux USA, qui voient Pékin se doter de moyens à même de défendre passivement et activement ses intérêts spatiaux, mais aussi de leur infliger des dégâts économiques et militaires majeurs.

Elles sont aussi un levier d'effets tactiques et stratégiques, qui pourraient, en cas de conflit conventionnel, à l'instar de sa menace dans le champ de la dissuasion nucléaire, lui permettre de rétablir la parité dans les autres dimensions ou d'y obtenir la supériorité, en privant partiellement ou totalement l'adversaire de son appui spatial.

Une vocation opérationnelle : le cas de la mer de Chine

Outre ce potentiel dissuasif des armes antisatellites, leur utilité en cas de conflit impliquant les USA est évidente. Un théâtre en particulier, régulièrement qualifié de « poudrière », au cœur des tensions entre la Chine et son voisinage, mais aussi et surtout entre la Chine et les USA, pourrait voir la menace antisatellite chinoise mise en œuvre au niveau opérationnel : les mers de Chine.

Point chaud des tensions régionales et globales, la montée en puissance du contre-espace chinois participe de la remise en cause de l'équilibre géostratégique y prévalant. Elle s'inscrit dans une stratégie hybride menée à l'échelle régionale visant à l'accumulation de gains relatifs, notamment par la création de zones de contestations et de dénis d'accès[48] dans les espaces aériens et navals, et pourrait, comme nous l'avons évoqué, dissuader Washington de s'impliquer dans un conflit, ou permettre à Pékin de rétablir la parité ou d'acquérir l'avantage asymétrique si tel était le cas. Elle s'articule également à la volonté chinoise d'assurer la crédibilité de sa force de dissuasion nucléaire face aux USA, alors que la capacité de projection de ses sous-marins nucléaires lanceurs d'engins (SNLE) vers le Pacifique est non seulement contrainte par la géologie et la géographie politique sud-est asiatique[49], mais aussi exposé aux moyens de reconnaissance par satellite américain.

L'architecture de défense mise en place par les USA et ses alliés dans la région repose d'abord et avant tout sur la puissance navale américaine, incarnée par sa Septième flotte, qui y circule en permanence pour garantir *de facto* la liberté de navigation, et stationne dans le proche voisinage de Pékin (en Corée du Sud et au Japon). À l'échelle de l'Asie-Pacifique, les USA ont multiplié les points d'appui, et disposent de bases (à Guam) ou de facilités d'accès à certains ports (au Vietnam, en Thaïlande, en Australie et à Singapour) pour y stationner leurs bâtiments. Leur capacité à maitriser les airs est également capitale, et repose sur leurs forces aéronavales (la majorité des porte-avions américains est affectée au Pacifique) et sur les

Pacific Air Forces, elle aussi en station permanente dans la région (à Hawaï, au Japon et en Corée du Sud).

La politique de défense indopacifique des États-Unis comporte une forte dimension interalliée. Ses partenariats stratégiques vont des accords de défense (pour les cas du Japon, de la Corée du Sud, de l'Australie, de la Thaïlande et des Philippines) à la coopération militaire, au plan stratégique, matériel ou opérationnel, en particulier dans le domaine de la surveillance navale et aérienne, mais aussi à travers la conduite de patrouilles et d'exercices militaires communs[50]. S'ils sont d'ampleurs hétérogènes, ces partenariats et ces alliances voient leur portée opérationnelle conditionnée à l'interopérabilité entre les différentes armées, c'est-à-dire à leur capacité à coordonner leurs doctrines et leurs moyens pour mener des actions communes de manière cohérente.

Mais ces forces nationales, et celles des USA plus que toutes sont très dépendantes des technologies et applications spatiales pour la planification, la conduite et le suivi des opérations. Et Pékin est bien consciente de leur vulnérabilité vis-à-vis de la menace antisatellite.

Conjuguant sa militarisation croissante de la zone et la montée en puissance de sa défense spatiale, et dans la logique de sa stratégie hybride d'accumulation de gains relatifs, elle a notamment déployé des dispositifs terrestres et navals de guerre électronique visant à brouiller ou falsifier (*spoofing*) les flux de données des réseaux satellitaires. En avril 2018, des images satellites ont démontré qu'elle avait placé dans l'archipel des Spratleys des équipements de brouillage de système GNSS, en particulier du *GPS*. Le 15 novembre 2019, le *MIT Technology Revew* a publié une enquête faisant état de mystérieuses perturbations du *GPS* dans le port de Shanghai, mêlant *jamming* et *spoofing*, non sans s'interroger sur leur origine[51]. Des événements similaires ont aussi été signalés en 2019 dans les ports de Dalian, Tianjin, Rizhao, Quanzhou et Fuzhou[52], le long d'une grande partie de son pourtour littoral.

Leur mise en œuvre pourrait fortement bouleverser les forces navales et aériennes américaines (et alliées) déployées en mers de Chine, elles dont la navigation repose en partie sur l'utilisation du *GPS*, de même que le ciblage et le guidage de leurs missiles et, plus largement, les capacités de localisation, de suivi, de coordination et de synchronisation des actions de l'ensemble des unités et systèmes d'armes dans les différentes dimensions. L'on imagine le désarroi d'un commandant de vaisseau américain croisant en mers de Chine et qui serait dans l'impossibilité de connaitre ses coordonnées de géopositionnement ou celles des autres bâtiments, ou confronté à des signaux falsifiés qui lui fourniraient des données inexactes.

Des rapports évoquent aussi le développement de dispositifs de brouillages destinés à affecter les réseaux de télécommunications satellitaires[53], et qui devraient probablement être déployés prioritairement pour opérer dans la région. Ils présenteraient l'avantage de pouvoir brouiller les signaux reçus par les terminaux d'une zone dédiée, sans devoir passer par des attaques contre le segment spatial, et donc de contourner la masse des satellites de communication déployés par les USA. Théâtre lointain, ces derniers sont essentiels pour assurer une liaison sécurisée et continue entre les armées et avec le commandement, et sont, avec les moyens de géopositionnement, au cœur de l'architecture du C2 américain.

Outre ses systèmes dédiés à la surveillance de l'espace, les bâtiments d'essais et de mesures des classes *Yuanwang* croisent en *quasi*-permanence dans les mers de Chine, et leurs radars peuvent détecter et suivre des objets aérospatiaux (missiles, satellites), au moins en orbite

basse, et favoriser ainsi la mise en œuvre de mesure de contre-espace. Ils peuvent par exemple identifier les satellites de reconnaissance survolant la région, et les désigner à des moyens antisatellites dédiés à l'attaque du segment spatial, notamment aux lasers à haute énergie.

Car affecter les capacités de reconnaissance et d'écoute électronique par satellite des USA procurerait à la Chine un avantage tactique ou stratégique certain, en les privant (au moins partiellement) de leurs moyens d'observation du théâtre ou de ses activités, en particulier des mouvements de sa flotte et des évolutions de son dispositif de défense sol-air et mer-air, en partie mobile.

C'est donc la continuité ou à la cohérence du dispositif américain de C4ISR (*Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance*), son système de collecte, de traitement et de dissémination de l'information, qui seraient, à des échelles locales, voire même régionales, menacées par les armes antisatellites chinoises, au risque de rendre l'armée américaine « sourde, aveugle et muette » s'il était déstabilisé ou paralysé.

Les modalités de mise en œuvre de l'interopérabilité de forces étrangères coalisées renforcent encore cette dépendance à l'espace, car du géopositionnement aux communications par satellite, c'est une large part des capacités de transmission, de coordination et de synchronisation interalliées qui mobilise des moyens spatiaux partagés ou intégrés. C'est particulièrement le cas du *GPS*, largement utilisé par les armées ayant noué des partenariats de défense avec les USA. Du reste, comme la guerre d'Ukraine nous l'a montré, si d'aventure un conflit en mers de Chine venait à survenir et que les USA se refusaient à s'impliquer directement, ses systèmes spatiaux qui fourniraient un appui à ses alliés seraient des cibles stratégiques pour Pékin.

Bien qu'ils agissent avec discrétion et soient le fruit de programmes très opaques, les satellites de proximité, les armes à énergie dirigée et les dispositifs de guerre électronique ont une signature physique, et, bien que le milieu extra-atmosphérique, « dimension grise », demeure un espace beaucoup moins maitrisé que les autres dimensions, leurs déploiements voire leur mise en œuvre peuvent être observés.

Au niveau opérationnel, le défi pour la Chine est donc de pouvoir combiner précision, masse et mobilité pour mettre en œuvre des moyens en mesure d'atteindre les cibles d'intérêt tactique ou stratégique, d'atteindre à la redondance des capacités américaines découlant de l'ampleur de sa présence dans l'espace, tout en étant capables de dissimuler ou protéger ses capacités antisatellites, qui seraient naturellement menacées en cas de conflit de haute intensité.

Conclusion

À la croisée de sa politique globale de montée en puissance militaire et de ses ambitions technologiques et politiques, lesquelles sous-tendent son investissement massif dans les activités spatiales[54], duales, la Chine développe, et déploie même, des armes antisatellites en mesure d'assurer une posture de défense active dans l'espace, mais aussi d'atteindre à des intérêts économiques et sécuritaires fondamentaux des USA. Ce dynamisme alimente la perception américaine d'une vulnérabilité à ce que des analystes ont désigné sous le nom de « Pearl Harbour spatial »[55], autrement dit à une frappe en premier dans l'espace

potentiellement « décapitante », et participe du pouvoir dissuasif de Pékin, mais aussi à nourrir une course aux armements spatiaux entre Chinois et Américains.

Comme l'illustre le cas de la militarisation des mers de Chine, la dimension spatiale est pour Pékin un milieu de confrontation à part entière, par laquelle elle pourrait menacer une puissance militaire américaine encore largement supérieure[56] d'acquérir l'avantage asymétrique, au moins au niveau tactique. Mais parce que la Chine est elle aussi dépendante des technologies et applications spatiales, ses capacités antisatellites demeurent contraintes par la nécessité d'en maitriser le seuil d'emploi. C'est pourquoi cette montée en puissance s'inscrit pleinement dans l'hybridation de la guerre, où la confusion des limites entre état de guerre et état de paix, guerre régulière et guerre irrégulière[57], technologies civiles et technologies militaires, tend d'abord à favoriser « l'action hybride aérospatiale »[58]. Elle s'insère plus particulièrement au sein d'une stratégie de déni d'accès et d'interdiction multi-milieux et multi-champs, en visant à obtenir des effets dans les autres dimensions, interdépendantes des moyens spatiaux, en contestant l'accès à leur service.

En cas de conflit avec une autre puissance spatiale, eu égard aux avantages tactiques et stratégiques de la domination spatiale, l'inconnue demeure quant au risque de voir les belligérants abaisser le seuil d'emploi de l'ensemble des moyens antisatellites, et faire de l'espace circumterrestre un milieu en proie à un conflit ouvert. Néanmoins,

BIBLIOGRAPHIE

Articles scientifiques

BARNET, Todd. United States National Space Policy, 2006 & ; 2010. *Florida Journal of International Law*. 2011, p. 277-292.

BRUSTLEIN Corentin, « La Chine et l'avènement de la « dissuasion stratégique intégrée » », *Revue Défense Nationale*, 2018/7 (N° 812), p. 32-36.

COSTE Jean-Charles, « De la guerre hybride à l'hybridité cyberélectronique », *Revue Défense Nationale*, 2016/3 (N° 788), p. 19-23.

EISENHOWER Susan, « Défense spatiale : ambitions et ambigüités américaines », *Politique américaine*, 2005/3 (N° 3), p. 11-24.

LECOINTRE François, « L'espace au cœur des opérations militaires modernes », *Revue Défense Nationale*, 2020/10 (N° 835),

LOGSDON John, « Le *leadership* américain et l'espace : la recherche de la puissance et de la gloire », *Hermès, La Revue*, 2002/2 (n° 34), p. 65-78.

MAIRE, Christian. (décembre 2021). Réflexions sur l'essai anti-satellite russe du 15 novembre 2021. *Fondation pour la Recherche Stratégique*. Note de la FRS n°41/21.

MAULNY Jean-Pierre, SCHNITZLER Gaspard, « Puissance militaire : la Chine, ennemi public numéro un des États-Unis ? », *Revue internationale et stratégique*, 2020/4 (N° 120), p. 21-26.

PENET Luc, « Rôle de l'action aérospatiale dans la guerre hybride », *Revue Défense Nationale*, 2021/HS4 (N° Hors-série), p. 95-106.

ROCHE Nicolas, « Chapitre 11. L'espace et la cyberdéfense : enjeux de sécurité, régulation et dissuasion », dans : *Pourquoi la dissuasion*. sous la direction de ROCHE Nicolas. Paris cedex 14, Presses Universitaires de France, « Hors collection », 2017, p. 435-484.

SCHAEFFER Daniel, « Les mers de Chine dans la relation Chine-États-Unis », *Outre-Terre*, 2013/3 (N° 37), p. 367-391.

SOURBèS-VERGER Isabelle, « Mythes et réalités de l'espace militaire », *Hermès, La Revue*, 2002/2 (n° 34), p. 169-182.

SOURBèS-VERGER Isabelle, « La Chine dans l'espace et le rêve chinois », *Monde chinois*, 2020/4 (N° 64), p. 16-35.

SOURBèS-VERGER Isabelle, « L'espace, lieu particulier des rivalités politiques et technologiques », *Revue Défense Nationale*, 2022/6 (N° 851), p. 73-78.

STEININGER Philippe, « Maîtriser l'air, maîtriser l'espace : comme un bégaiement de l'histoire », *Stratégique*, 2019/3 (N° 123), p. 205-214.

STEININGER Philippe, « Janvier 1991, une tempête dans le désert consacre la puissance aérienne », *Revue Défense Nationale*, 2021/8 (N° 843), p. 26-31.

STEININGER Philippe, « Demain, la guerre des étoiles ? », *Revue Défense Nationale*, 2022/3 (N° 848), p. 94-98.

THIBOUT Charles, « La voie technologique du conflit sino-américain », *Revue internationale et stratégique*, 2020/4 (N° 120), p. 59-70.

Articles en ligne

Aquilina, V. (17 septembre 2021). *Le service en orbite dans la nouvelle course à l'espace. De la réparation de satellites à l'exploitation des ressources spatiales*. areion24.news. Disponible sur : https://www.areion24.news/2021/09/17/le-service-en-orbite-dans-la-nouvelle-course-a-lespace-de-la-reparation-de-satellites-a-lexploitation-des-ressources-spatiales-2/

Harris, M. (15 novembre 2019). *Ghost ships, crop circles, and soft gold : À GPS mystery in Shanghai*. MIT Technology Review. Disponible sur : https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

Joe Biden promet de défendre Taïwan en cas d'invasion chinoise. (23 mai 2022). La Croix.com. Disponible sur : https://www.la-croix.com/Monde/Joe-Biden-promet-defendre-Taiwan-cas-dinvasion-chinoise-2022-05-23-1201216472

Louvet, B. (1 février 2022). *La Chine opère une manœuvre impressionnante en orbite géostationnaire*. Sciencepost.fr. Disponible sur : https://sciencepost.fr/satellite-chine-orbite-geostationnaire/

Maurin, A. (juillet 2022). La dimension spatiale du conflit en Ukraine : de la compétition à la confrontation ? *La note du CESA – Hors-série Ukraine, 8*. Disponible sur : https://fr.calameo.com/cesa/read/006940288556eefb66758

Mielcarek, R. (20 août 2017). *Les mystérieuses activités des « sous-marins de l'espace»*. RFI.fr. Disponible sur : https://www.rfi.fr/fr/hebdo/20170818-mysterieuses-activites-sous-marins-espace-militarisation-defense-satellite-orbite

Reuters. (11 octobre 2021). *La Chine a gagné le combat de l'intelligence artificielle-ancien chef des logiciels du Pentagone*. Challenges.fr. Disponible sur : https://www.challenges.fr/high-tech/la-chine-a-gagne-le-combat-de-l-intelligence-artificielle-ancien-chef-des-logiciels-du-pentagone_784315

Seibt, S. (8 avril 2022). *L'espace, nouvelle frontière de la guerre informatique ?*. France24.com. Disponible sur : https://www.france24.com/fr/%C3%A9co-tech/20220408-l-espace-nouvelle-fronti%C3%A8re-de-la-guerre-informatique

Senecal, S. (25 mars 2009). *La communisation sur la collision entre deux satellites américain et russe en février 2009*. Ecole de Guerre Economique. Ege.fr. Disponible sur : https://www.ege.fr/infoguerre/2009/03/analyse-de-la-collision-entre-deux-satellites-americain-et-russe-en-fevrier-2009

Seydtaghua, A. (15 mai 2022). *Starlink en Ukraine, le joli coup d'Elon Musk*. LeTemps.ch. Disponible sur : https://www.letemps.ch/opinions/starlink-ukraine-joli-coup-delon-musk

Untersinger, M. (15 mars 2022). *L'Ukraine reconnaît « une énorme perte de communication » après la cyberattaque contre le satellite KA-SAT*. Le Monde.fr. Disponible sur : https://www.lemonde.fr/pixels/article/2022/03/15/l-ukraine-reconnait-une-enorme-perte-de-communication-apres-la-cyberattaque-contre-le-satellite-ka-sat_6117632_4408996.html

Untersinger, M. (10mai 2022). *Guerre en Ukraine : la Russie accusée d'être derrière la cyberattaque ayant visé le réseau du satellite KA-SAT*. Le Monde.fr. Disponible sur : https://www.lemonde.fr/pixels/article/2022/05/10/guerre-en-ukraine-la-russie-accusee-d-etre-derriere-la-cyberattaque-ayant-vise-le-reseau-du-satellite-ka-sat_6125513_4408996.html

Wolf, J. (28 octobre 2011). *China key suspect in U.S. satellite hacks : commission*. Reuters.Com. Disponible sur : https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028

Rapports

Accenture. (juin 2022). *Global Incident Report : Russia-Ukraine Crisis | June 10* (Nº 16).

Center for strategic international studies. *Space threat assessment 2020*. Washington, mars 2020. 80 p.

U.S. Defense Intelligence Agency. (2019). *Challenges to security in space*. 46 p.

U.S. Defense Intelligence Agency (2019). *China Military Power*. 125 p.

Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. 237 p.

Notes

Vidéo

Europe 1. (25 juin 2022). *Ukraine : « La guerre a commencé dans l'espace » , déclare le Général Michel Friedling* [Vidéo]. YouTube.com. Disponible sur : https://www.youtube.com/watch?v=c6s4jjCGO_g

[1] *Joe Biden promet de défendre Taïwan en cas d'invasion chinoise*. (23 mai 2022). La Croix. Disponible sur : https://www.la-croix.com/Monde/Joe-Biden-promet-defendre-Taiwan-cas-dinvasion-chinoise-2022-05-23-1201216472

[2] « à la fois antisatellite et anti-missile ».

MAIRE, Christian. (2021, décembre). Réflexions sur l'essai anti-satellite russe du 15 novembre 2021. *Fondation pour la Recherche Stratégique*. Note de la FRS n°41/21. p. 18.

[3] Europe 1. 25 juin 2022. *Ukraine : « La guerre a commencé dans l'espace » , déclare le Général Michel Friedling* [Vidéo]. YouTube. https://www.youtube.com/watch?v=c6s4jjCGO_g

[4] Untersinger, M. (10 mai 2022). *Guerre en Ukraine : la Russie accusée d'être derrière la cyberattaque ayant visé le réseau du satellite KA-SAT*. Le Monde.fr. Disponible sur : https://www.lemonde.fr/pixels/article/2022/05/10/guerre-en-ukraine-la-russie-accusee-d-etre-derriere-la-cyberattaque-ayant-vise-le-reseau-du-satellite-ka-sat_6125513_4408996.html

[5] Untersinger, M. (15 mars 2022). *L'Ukraine reconnaît « une énorme perte de communication » après la cyberattaque contre le satellite KA-SAT*. Le Monde.fr. Disponible sur : https://www.lemonde.fr/pixels/article/2022/03/15/l-ukraine-reconnait-une-enorme-perte-de-communication-apres-la-cyberattaque-contre-le-satellite-ka-sat_6117632_4408996.html

[6] Starlink est la constellation de satellites de communications de la société américaine SpaceX. Elle est constituée de plusieurs milliers de satellites.

[7] Seyftaghia, A (15 mai 2022). *Starlink en Ukraine, le joli coup d'Elon Musk*. Le Temps.ch. Disponible sur : https://www.letemps.ch/opinions/starlink-ukraine-joli-coup-delon-musk

[8] Maurin, A. (juillet 2022). La dimension spatiale du conflit en Ukraine : de la compétition à la confrontation ? *La note du CESA – Hors-série Ukraine, 8*. Disponible sur : https://fr.calameo.com/cesa/read/006940288556eefb66758

[9] A la différence de la « militarisation » de l'espace, qui englobe l'ensemble des activités spatiales remplissant des fonctions militaires, l'arsenalisation » de l'espace désigne plus

spécifiquement le développement et le déploiement d'armes *ground-to-space* et *space-to-ground*.

[10] STEININGER Philippe, « Janvier 1991, une tempête dans le désert consacre la puissance aérienne », *Revue Défense Nationale*, 2021/8 (N° 843), p. 30.

[11] SOURBèS-VERGER Isabelle, « L'espace, lieu particulier des rivalités politiques et technologiques », *Revue Défense Nationale*, 2022/6 (N° 851), p. 78.

[12] BARNET, Todd. United States National Space Policy, 2006 & ; 2010. *Florida Journal of International Law*. 2011. p. 278.

[13] LOGSDON John, « Le *leadership* américain et l'espace : la recherche de la puissance et de la gloire », *Hermès, La Revue*, 2002/2 (n° 34), p. 76.

[14] SOURBèS-VERGER Isabelle, « Mythes et réalités de l'espace militaire », *Hermès, La Revue*, 2002/2 (n° 34), p. 178.

[15] Center for Strategic International Studies. *Space Threat Assessment*. Mars 2020. p. 11.

[16] SCHAEFFER Daniel, « Les mers de Chine dans la relation Chine-États-Unis », *Outre-Terre*, 2013/3 (N° 37), p. 383.

[17] La Commission Rumsfeld, chargée en 1999 « d'évaluer l'organisation et la gestion des activités spatiales comme soutien à la sécurité nationale », a insisté sur le dynamisme du programme spatial chinois.

EISENHOWER Susan, « Défense spatiale : ambitions et ambigüités américaines », *Politique américaine*, 2005/3 (N° 3), p. 14.

[18] « Le ressort de cette retenue résidait dans le lien très fort entre spatial et nucléaire. ».

STEININGER Philippe, « Demain, la guerre des étoiles ? », *Revue Défense Nationale*, 2022/3 (N° 848), p. 95.

[19] LECOINTRE François, « L'espace au cœur des opérations militaires modernes », *Revue Défense Nationale*, 2020/10 (N° 835), p. 15.

[20] Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. p. 34.

[21] Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. p. 57.

[22] Aquilina, V. (17 septembre 2021). *Le service en orbite dans la nouvelle course à l'espace. De la réparation de satellites à l'exploitation des ressources spatiales*. areion24.news. Disponible sur : https://www.areion24.news/2021/09/17/le-service-en-orbite-dans-la-nouvelle-course-a-lespace-de-la-reparation-de-satellites-a-lexploitation-des-ressources-spatiales-2/

[23] LECOINTRE François, « L'espace au cœur des opérations militaires modernes », *op.cit.*, p. 14.

[24] Senecal, S. (25 mars 2009). *La communisation sur la collision entre deux satellites américain et russe en février 2009*. Ecole de Guerre Economique. Disponible sur : https://www.ege.fr/infoguerre/2009/03/analyse-de-la-collision-entre-deux-satellites-americain-et-russe-en-fevrier-2009

[25] Mielcarek, R. (20 août 2017). *Les mystérieuses activités des « sous-marins de l'espace»*. RFI.fr. Disponible sur : https://www.rfi.fr/fr/hebdo/20170818-mysterieuses-activites-sous-marins-espace-militarisation-defense-satellite-orbite

[26] Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. p. 35.

[27] Le 22 janvier 2022, le satellite Shinjian-21 s'est amarré à un satellite chinois en orbite géostationnaire et l'a remorqué à environ 3000 kilomètres plus haut, avant de se repositionner sur l'orbite géostationnaire.

Louvet, B. (1 février 2022). *La Chine opère une manœuvre impressionnante en orbite géostationnaire*. Sciencepost.fr. Disponible sur : https://sciencepost.fr/satellite-chine-orbite-geostationnaire/

[28] Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. p. 35.

[29] ACHILLEAS Philippe, MARéCHAL Jean-Paul, « Éditorial. L'espace : la « nouvelle frontière » de la Chine », *Monde chinois*, 2020/4 (N° 64), p. 11.

[30] STEININGER Philippe, « Maîtriser l'air, maîtriser l'espace : comme un bégaiement de l'histoire », *Stratégique*, 2019/3 (N° 123), p. 209.

[31] BORTZMEYER Stéphane, SOUISSI Mohsen, SCHAFER Valérie, « Cybermenaces, enjeux et sécurité », *Flux*, 2019/4 (N° 118), p. 61.

[32] ROCHE Nicolas, « Chapitre 11. L'espace et la cyberdéfense : enjeux de sécurité, régulation et dissuasion », dans : , *Pourquoi la dissuasion*. sous la direction de ROCHE Nicolas. Paris cedex 14, Presses Universitaires de France, « Hors collection », 2017, p. 468.

[33] Accenture. (2022, juin). *Global Incident Report : Russia-Ukraine Crisis | June 10* (Nº 16).

[34] COSTE Jean-Charles, « De la guerre hybride à l'hybridité cyberélectronique », *Revue Défense Nationale*, 2016/3 (N° 788), p. 21.

[35] U.S. Defense Intelligence Agency. (2019). *Challenges to security in space*. p. 9.

[36] U.S. Defense Intelligence Agency. (2019). *China Military Power*. p.46.

[37] Selon Nicolas Chaillan, premier responsable de la sécurité logicielle pour l'armée de l'air américaine et la *Space Force* entre 2019 et 2021, « la plupart du temps ces tentatives d'attaques sont classifiées ».

Seibt, S. (8 avril 2022). *L'espace, nouvelle frontière de la guerre informatique ?* France24.com. Disponible sur : https://www.france24.com/fr/%C3%A9co-tech/20220408-l-espace-nouvelle-fronti%C3%A8re-de-la-guerre-informatique

[38] En 2007 et en 2008, des cyberattaques ont provoqué de courtes pannes de deux satellites américains. La Commission d'examen des questions économiques et de sécurité entre les États-Unis et la Chine du Congrès américain a suspecté la responsabilité de la Chine, sans être en mesure d'en apporter la preuve.

Wolf, J. (28 octobre 2011). *China key suspect in U.S. satellite hacks : commission*. Reuters.Com. Disponible sur : https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028

[39] CrowdStrike Global Intelligence Team. Mai 2014. *CrowdStrike Intelligence Report: PUTTER PANDA.* p. 18.

[40] *Ibid.* p. 49.

[41] Reuters. (11 octobre 2021). *La Chine a gagné le combat de l'intelligence artificielle-ancien chef des logiciels du Pentagone*. Challenges. Disponible sur : https://www.challenges.fr/high-tech/la-chine-a-gagne-le-combat-de-l-intelligence-artificielle-ancien-chef-des-logiciels-du-pentagone_784315

[42] ROCHE Nicolas, « Chapitre 11. L'espace et la cyberdéfense : enjeux de sécurité, régulation et dissuasion », dans : , *Pourquoi la dissuasion*. sous la direction de ROCHE Nicolas. Paris cedex 14, Presses Universitaires de France, « Hors collection », 2017, p. 476.

[43] BRUSTLEIN Corentin, « La Chine et l'avènement de la « dissuasion stratégique intégrée » », *Revue Défense Nationale*, 2018/7 (N° 812), p. 33.

[44] STEININGER Philippe, « Demain, la guerre des étoiles ? », *Revue Défense Nationale*, 2022/3 (N° 848), p. 97.

[45] BRUSTLEIN Corentin, « La Chine et l'avènement de la « dissuasion stratégique intégrée » », *Op.cit.*, p. 34.

[46] PERONO Pierre-Stanley, JALUZOT Marine, TOURAINE Patrice, *Les nouveaux enjeux de l'espace*. VA Éditions, 2021.

[47] Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. p. 58.

[48] SCHAEFFER Daniel, « Les mers de Chine dans la relation Chine-États-Unis », *op.cit.*, p. 383.

[49] SCHAEFFER Daniel, « Les mers de Chine dans la relation Chine-États-Unis », *op.cit.*, p. 369.

[50] SCHAEFFER Daniel, « Les mers de Chine dans la relation Chine-États-Unis », *op.cit.*, p. 380.

[51] « Personne ne sait qui est à l'origine de cette usurpation d'identité, ni quel pourrait être son objectif final. Ces navires pourraient être des cobayes involontaires pour un système de guerre électronique sophistiqué[…] Mais une chose est sûre : une guerre électronique invisible se joue à Shanghai sur l'avenir de la navigation, et le *GPS* est en train de perdre. ».

Harris, M. (15 novembre 2019). *Ghost ships, crop circles, and soft gold : À GPS mystery in Shanghai*. MIT Technology Review. Disponible sur : https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

[52] Center for strategic international studies. *Space threat assessment 2020*. Washington, mars 2020. p. 16.

[53] Secure World Foundation. *Global Counterspace Capabilities : An Open Source Assessment*. Avril 2021. p. 53.

[54] THIBOUT Charles, « La voie technologique du conflit sino-américain », *Revue internationale et stratégique*, 2020/4 (N° 120), p. 63.

[55] SOURBèS-VERGER Isabelle, « La Chine dans l'espace et le rêve chinois », *Monde chinois*, 2020/4 (N° 64), p. 30.

[56] MAULNY Jean-Pierre, SCHNITZLER Gaspard, « Puissance militaire : la Chine, ennemi public numéro un des États-Unis ? », *Revue internationale et stratégique*, 2020/4 (N° 120), p. 22.

[57] TENENBAUM Élie, « Guerre hybride : concept stratégique ou confusion sémantique ? », *Revue Défense Nationale*, 2016/3 (N° 788), p. 33.

[58] PENET Luc, « Rôle de l'action aérospatiale dans la guerre hybride », *Revue Défense Nationale*, 2021/HS4 (N° Hors-série), p. 100.