Maria LUCAS-RHIMBASSEN
Mémoire de complément d'études en droit de l'espace

RESILIENSIS SPATIALIS

Solutions contractuelles pour la résilience des infrastructures spatiales

Chaire SIRIUS
Université Toulouse 1 Capitole
Septembre © 2017

RESILIENSIS SPATIALIS

Solutions contractuelles pour la résilience des infrastructures spatiales

Auteure:
Maria Lucas-Rhimbassen, Attachée de recherche à la Chaire SIRIUS
(maria.lucas-rhimbassen@ut-capitole.fr**)**

Sous la supervision du Professeur Dr. Lucien Rapp,
Directeur de la Chaire SIRIUS (UT1)

Sommaire exécutif

Ce texte a pour but d'analyser l'importance de l'infrastructure de services dans un contexte de commercialisation du secteur spatial, à l'aube de l'entrée annoncée de l'intelligence artificielle, de l'internet des objets (IoT), de l'interconnectivité et du *"machine learning"*. Notre société devient dépendante presqu'en totalité de la qualité et de la fiabilité des plateformes et infrastructures assurant le bon fonctionnement des services. Celles-ci impliquent de façon importante l'infrastructure dite spatiale (satellites et autres objets). Cependant, ces infrastructures deviennent vulnérables face à des événements divers tels que les radiations cosmiques, tempêtes solaires, mais aussi face à des risques nouveaux, engendrés par l'homme: cyberattaques, interférences accidentelles ou intentionnelles, voire pire, sabotage. À l'heure actuelle, il y a un manque de dispositifs politiques et légaux, nationaux ou internationaux, qui puissent régir les actions à prendre face à ce type de risques. Les gouvernements ont beau créer des listes qui distinguent le niveau de priorité à accorder à certaines infrastructures jugées "critiques" ou "vitales", beaucoup de confusion obscurcit toutefois le statut des infrastructures spatiales. Certains les jugent critiques, d'autres non. Même ceux qui les jugent critiques ne vont pas toujours assez loin dans les détails. Ainsi, en raison des problématiques liées à la gouvernance, aux facteurs géopolitiques ou encore aux enjeux économiques, ces listes diffèrent de pays en pays, entraînant davantage de confusion et de tension sur la scène internationale, menant à des préoccupations au niveau de la sécurité. En effet, les autorités compétentes ainsi que les experts concernés étudient le problème de la vulnérabilité des infrastructures (spatiales) dans une perspective de sécurité, relevant de l'angle des processus (ou procédures) au détriment des résultats et objectifs (aboutissements). Ces derniers constituent en fait la continuité des services. Celle-ci est souvent illustrée par des histoires à succès impliquant des partenariats viables et

mutuellement bénéfiques, entre secteur public et privé, visant davantage le long-terme et en privilégiant continuité et assurabilité des services, et avec moins d'accent sur les régimes d'assurances en fonction des risques. On appelle cela "*mission assurance vs insurance*" et ce, à la lumière d'un choix stratégique s'enlignant sur le concept de résilience. Nous avons étudié ce concept fortement mis en avant, qui demeure néanmoins vague et mystérieux et nous montrerons comment la résilience peut fournir des solutions pratiques ainsi que faire profiter les parties prenantes grâce à un retour sur investissement non-négligeable, et même très important. Cependant, nous le concédons, ce terme très utilisé semble superflu pour certains, surtout dans le secteur spatial, mais pas seulement.

Ainsi, au niveau académique, on retrouve plus d'une vingtaine de définitions de ce concept, les unes plus citées que les autres, divisées dans deux grandes écoles de pensée, mais toutes deux demeurant dans une optique macro-. Notre défi est d'en concilier les différences tout en préservant les distinctions et de rassembler le tout au niveau micro-, plus pragmatique et concret, et d'en appliquer la résultante dans le secteur spatio-juridique, soit plus précisément dans le domaine des contrats. Nous avons déterminé ce besoin après avoir étudié des dizaines de clauses contractuelles existantes, les ayant classées selon une typologie évaluant leur apport vis-à-vis la résilience. Les résultats nous ont poussés à conclure à un besoin réel de clauses encadrant le concept en y apportant des lignes directrices pouvant rassurer le dialogue entre les parties prenantes et faire un pas de plus vers l'assurabilité, comblant ainsi, du moins en partie, le manque que nous avons constaté tant au niveau macro- que micro-juridique. Notre solution est de créer et de mettre en marche une multi-clause, basée sur un portfolio d'options et de variantes, encourageant les parties prenantes au contrat à opter pour une résilience suggérée et définie dans ladite clause. Le but est d'introduire la notion de résilience en droit des contrats, à commencer par le secteur spatial. Nous allons, en effet, formuler des recommandations en vue des conditions à rencontrer, suggérer une définition large et libérale et déterminer la pertinence et l'applicabilité de telles clauses. De plus, nous sommes en faveur de la mise sur pied d'un groupe de travail sur le sujet pour tester ce type de clause sur le terrain et l'itérer autant que nécessaire, tout en collaborant étroitement avec l'UNIDROIT en vue de l'élaboration de pratiques contractuelles reconnues au niveau international et ainsi inciter les autorités compétentes à en tenir compte et à s'en inspirer lors de la création ou la refonte de législations spatiales nationales.

À Marie Juneau

Pour sa résilience exemplaire à travers les générations et les étoiles

Tables des matières

Liste des figures

Une partie de notre problème est centrée sur l'effort d'introduire un contrôle extérieur pour un système-de-systèmes qui doit être maintenu par des forces internes en équilibre. Nous ne cherchons ni à reconnaître ni à nous interdire d'inhiber ces systèmes autorégulateurs de nos espèces desquels dépend la survie de ces espèces. Nous ne tenons pas compte de nos propres fonctions de rétroaction.

Et l'homme créa un Dieu,
Frank Herbert

Introduction

L'industrie spatiale est confrontée à un problème qui risque de prendre de l'ampleur. Les satellites deviennent vieillissants et tombent en panne, constituant ainsi une menace en orbite. Par exemple, 1 cubesat (mini-satellite) sur 7 a été perdu après le lancement d'une fusée Soyouz qui en transportait 72[1]. Des fois, les fabricants optent pour des assurances, d'autres fois non. D'une part, par exemple, l'opérateur du satellite Intelsat 33[2], dont les problèmes techniques lui racourcissent la durée de vie de 3.5 ans, a décidé de recourir à une prime d'assurances de 78 millions d'euros, car il perdait des clients. D'autre part, cet été, par exemple, SES Astra qui est le plus grand opérateur privé de satellites au niveau mondial, a encouru près de quarante millions de dollars de pertes au total à cause de deux satellites. Ceux-ci avaient rempli leur durée de vie programmée à une quinzaine d'années et continuaient à assurer des services de télécommunications, mais voilà qu'ils atteignent leurs limites. Pour mitiger les pertes, SES a lancé un satellite de remplacement pour l'un et et en ce qui concerne le 2^{e} satellite, qui avait perdu près du tiers de sa capacité, elle a redirigé les signaux vers de nouveaux transpondeurs sur d'autres satellites (appartenant ou non à SES). Dans ces deux cas, SES a préféré assurer la continuité du service en appliquant le principe de redondance des systèmes et de résilience du service au lieu de toucher à des primes d'assurances. De plus, en agissant ainsi, SES a voulu arrêter le montant des pertes s'élevant à 40 millions et empêcher la saignée qui aurait résulté en des pertes financières encore plus graves. Ainsi, le problème était qualifié de « temporaire » et tout devrait rentrer dans la normale avant la

[1] Voir l'article sur Space News à : http://spacenews.com/additional-cubesats-on-july-14-soyuz-flight-are-unresponsive/, consulté le 4 september 2017.
[2] Voir l'article sur Space News à: http://spacenews.com/intelsat-33e-propulsion-problems-to-cut-service-life-by-3-5-years/, consulté le 3 septembre 2017.

fin du trimestre[3]. Ce texte aidera les lecteurs à comprendre les mécanismes derrière ce choix stratégique et expliquera pourquoi l'assurabilité vs l'assurance, un principe juridique et commercial, doit être défendu par les juristes à travers le concept de la résilience, qui lui, provient d'autres disciplines, mais qui dicte la nouvelle tendance technique dans le secteur. En effet, nous dépendons de plus en plus des systèmes spatiaux, mais nous héritons aussi des leurs risques et vulnérabilités. Dans une société moderne et hautement connectée, nous dépendons de manière critique d'une vaste variété de systèmes qui assurent le bon fonctionnement de l'ensemble des infrastructures régissant notre quotidien, sur une base continue. Souvent, nous avons tendance à prendre pour acquis ce bon fonctionnent et à sous-estimer les conséquences de son éventuelle interruption. Ce problème s'aggrave à l'aube d'une recrudescence de nouveaux risques (par exemple, de nature informatique ou relevant de la chaîne d'approvisionnement). Dans cette optique, la face cachée des systèmes spatiaux est leur fragilité progressive, peu importe le niveau du "fractionnement" de la technologie destinée au secteur spatial, puisque celle-ci tombe rapidement en désuétude par rapport à celle destinée aux fins "terrestres". Cette symbiose va toutefois évoluer, car les interdépendances des interfaces et plateformes augmentent et alors, la vulnérabilité n'en sera que plus élargie. Cette situation alarmante oblige les experts du secteur à réétudier et à réévaluer les interactions entre infrastructures (systèmes spatiaux et infrastructures critiques sur Terre). Plusieurs scénarios divisés en modules sont établis pour permettre de mieux évaluer l'interopérabilité ainsi que les interconnections des conséquences en cascades, suite à plusieurs incidents. On compte les conséquences par centaines. Si un satellite est endommagé par un débris spatial ou fait l'objet d'une attaque cybernétique, le répertoire des impacts va inclure: brouillage du GPS, des chaînes de télévision, des moyens de télécommunications, d'internet, le chaos dans le système de paiement en ligne et du *e-trading*, des dysfonctionnements dans le secteur bancaire, pannes du réseau énergétique, isolement des forces armées déployées, désorientation des bateaux en mer, désorganisation

[3] Voir l'article sur Space News à http://spacenews.com/ses-loses-12-transponders-on-nss-806-satellite-says-impact-is-temporary/, consulté le 31 août 2017.

de la coordination des vols, pertes progressives des moyens de restauration et de retour à la "normale". Ce type d'événement peut durer de quelques secondes à plusieurs minutes, voire des jours ou semaines, sinon des mois. Le niveau de gravité est en corrélation directe avec la durée de l'évènement. Ainsi, la résilience de la société (d'une ville, d'un pays ou de la planète) est alors compromise, du moins sur le court ou moyen terme. L'économie globale risque gros car, même si certains services reposent sur des systèmes alternatifs (ex: internet par fibre optique et non par signal satellite), le très dense enchevêtrement des multiples systèmes interagissant ou se partageant la part du service affectera forcément l'ensemble, ce n'est qu'une question de durée, assez brève[4]. De ce fait, nous considérons qu'il est impératif de traiter du besoin d'autonomie résiliente des systèmes spatiaux et que nous intégrons cette discussion au contexte juridique, car à part les grands traités internationaux sur l'utilisation de l'espace extra-atmosphérique à des fins pacifiques[5], il y a un grand vide juridique dans le sujet qui nous préoccupe. Non seulement une gouvernance entrecroisée s'impose, allant au-delà des "mécanismes conventionnels"[6], mais il est nécessaire de se concentrer sur le droit commercial à l'échelle internationale, en raison de la transition du secteur spatial vers une privatisation et commercialisation poussées. De plus, fournir des solutions juridiques plus précises, mais flexibles, viendrait rassurer les différents acteurs des sous-secteurs concernés, car, selon eux, les distinctions légales demeurent "floues" et contribuent à une situation confuse causant des tensions entre les segments espace, sol et utilisateur. À ce jour, nous comptons des spécificités techniques permettant aux satellites d'être minimalement résilients grâce à une relative capacité d'auto-régénération (*self-heal*), en cas de détection de certaines anomalies données. Le satellite gèle alors ses fonctions et attend des instructions du segment sol (centre de contrôle), afin de mitiger les dégâts. Ceci

[4] Les détails d'un tel scénario peuvent être consultés dans les médias : http://www.bbc.com/future/story/20130609-the-day-without-satellites et http://www.telegraph.co.uk/culture/books/10785683/What-would-happen-if-satellites-fell-from-the-sky.html. (consulté le 13 juin, 2017)

[5] Nous nous référons au *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* (OST), de 1967, disponible sur le site web du *United Nations Office for Outer Space Affairs* (UNOOSA) : http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html, qui reste identique 50 ans après.

[6] Ibid.

est une solution partielle, pas toujours couronnée de succès et, puisque les instructions se font par le biais de reconfiguration du *software*, le système est à la merci des cyberattaques, surtout si des informations sensibles sont entre les mains de parties non autorisées. Ce risque est d'autant plus croissant dans un contexte de commercialisation. L'externalisation peut être farouche et la sous-traitance non contrôlée. Ces motifs nous poussent à parler de résilience maintes fois, sans nous contenter seulement de la mentionner, mais aussi de la décrire et à justifier son utilité dans le secteur et défendre le fait que ce n'est pas un simple "*buzzword*" du moment, qui risque de perdre tout son éclat demain. En effet, la résilience n'est bel et bien pas un produit du "*self-help*" qu'on applique à l'improviste. C'est, au contraire, un concept reconnu dans le monde académique et qui accumule une masse critique transversale et qui incite à des actions concrètes satisfaisant davantage ceux et celles qui trouvent que le "développement durable" relève plutôt d'un principe théorique conciliant. Puisque la résilience peut conduire à des mesures concrètes, chaque secteur (écologie, psychologie, ingénierie, management, etc.) qui s'en inspire ou qui l'invoque tend à l'adapter à ses besoins et à se l'approprier. Cela étant dit, un secteur en particulier manque à ce panorama et il s'agit de celui du droit, qui ne possède pas de mesure expresse ou implicite traitant de la résilience. Peut-être que la tradition selon laquelle le droit joue un rôle davantage réactif que proactif est à l'origine de ce manque et nous sommes déterminés à relever le défi et à prouver le contraire. La société actuelle dépend d'infrastructures essentielles, vitales et critiques, qui assurent les services de base comme la distribution énergétique, hydraulique, les réseaux de transport ou de communication, etc. En raison des progrès technologiques (internet et internet des objets (IoT), connectivité, intelligence artificielle (AI), *machine learning*, etc.) ces infrastructures se transforment et deviennent graduellement intégrées. Leur intégration passe maintenant par des systèmes en orbite, modifiant le paradigme selon lequel nous voyons les satellites isolés au-dessus des autres systèmes terrestres, au sommet d'une pyramide de hiérarchie technologique. En effet, ils font partie intégrante des autres infrastructures et une pensée linéaire ne rend pas justice à la réalité, du fait de la banalisation des interactions entre les interdépendances

fréquentes. Le grand schéma, soit le système des systèmes, ne permet plus d'isoler un système des autres car un autre s'en trouvera affecté et viendra altérer, à la longue, le fonctionnement de l'ensemble global des écosystèmes complexes. Nous voilà donc à la merci d'un éventuel "jour sans satellites". Pour ces raisons, nous préconisons l'approche de la résilience.

Notre méthodologie repose sur une revue de la littérature abordant le sujet dans les secteurs de l'écologie, de la psychologie, de la gestion du risque de la cybersécurité. Nous avons aussi étudié les différentes stratégies nationales et la jurisprudence pour situer l'état du droit en la matière, si applicable. Ensuite, nous avons analysé des *business cases* à succès, comme par exemple le cas *Paradigm*, qui privilégient l'assurabilité aux dépens des assurances. Ceci nous a conduits vers l'étude de contrats non classés et non confidentiels relevant du domaine spatial, ainsi qu'à leur tri en fonction de leur niveau de résilience. Nos découvertes sont catégorisées par type de clause dans un tableau et elles nous ont fortement aidés à identifier les éléments nécessaires à la rédaction de notre propre modèle de clause en vue de le tester sur le terrain et de recueillir l'avis des juristes, dans le domaine public et privé, afin de pouvoir par la suite, le soumettre à UNIDROIT et de créer un nouveau standard reconnu à l'international. Le texte se divise en plusieurs sous-parties et nous commençons tout d'abord par dresser le portrait d'une société hautement dépendante des infrastructures critiques, qui elles-mêmes reposent sur des interactions se répercutant au spatial. L'impact de la vulnérabilité de ceux-ci par rapport à de nouveaux risques suscite des inquiétudes parmi les juristes en droit de l'espace et nous y réagisssons par la solution résiliente que nous allons définir. Il sera possible aussi de constater qu'il existe plusieurs définitions regroupées dans deux grandes écoles de pensée et nous en dévoilerons les dichotomies: "*soft*" vs "*hard*", avant de les concilier grâce à notre prototype de clause. Le prochain défi sera d'en tester le potentiel et de partager les itérations avec notre auditoire.

1. Contexte: l'importance de l'infrastructure de services

1.1. L'ère de l'intelligence artificielle

Dans un contexte d'interconnectivité croissante des objets et de villes intelligentes, nous sommes témoins du terrain gagné par l'intelligence artificielle, au point où celle-ci vise à ne faire qu'un avec l'être humain et atteindre la "singularité"[7] (en transformant notre perception via la réalité augmentée) et, un jour peut-être, la technologie quantique, dont les fondements intriguaient même Einstein, qui les qualifiait de "*spooky*". Les prouesses technologiques transforment la situation actuelle sur Terre comme dans l'espace extra-atmosphérique. Les divers systèmes sont tellement imbriqués les uns aux autres que l'on parle maintenant de *systèmes des systèmes*, car les liens sont de plus en plus présents, et invisibles (signal, ondes, etc.), voire intangibles, ce qui peut nous faire oublier ces interactions. En tant que juristes, nous devons poser des questions et réfléchir quant à la direction et aux conséquences de ces avancées. L'interconnectivité augmentée se complexifie donc et il en surgit une vulnérabilité conséquentielle. C'est pourquoi il est opportun de se poser ces questions en ce moment. Quand il y a une cyberattaque, la société s'en retrouve abasourdie et paralysée. Quand des algorithmes du *trading* à haute fréquence ne fonctionnent pas comme prévu pendant des millièmes de secondes, le marché financier entier est au bord de l'écroulement. Imaginer alors la vulnérabilité et les conséquences de la société quand la singularité sera la cible de problèmes techniques, de *hacking* ou de logiciels malveillants. C'est en anticipant ce genre de problèmes que nous devons penser à développer la capacité autonome de divers systèmes à devenir résilients et à se régénérer et à s'adapter, ou vice-versa. Après le lancement d'un objet spatial, toute réparation est soit très délicate, soit impossible. Que dire alors de tous les systèmes qui en dépendent ainsi que du reste des infrastructures critiques sur lesquelles nous nous basons? De plus, non seulement les satellites risquent de ne pas fonctionner normalement, mais si la situation s'avère aggravée, ils risquent de devenir des débris spatiaux, hors de contrôle et de mettre en danger d'autres satellites, augmentant les risques

[7] *'The Singularity is Near'*, par Ray Kurzweil, New York: Penguin Group, 2005.

d'engendrer l'effet *Kessler*. Celui-ci décrit la multiplication exponentielle et irréversible des collisions avec des débris, rendant les orbites sursaturées. Étant donné les risques croissants de cyberattaques, ceci peut survenir rapidement. Malgré ce risque, on dénote une certaine inertie de la part des États en général, certains plus que d'autres, quand il s'agit de prendre des mesures efficaces pour mitiger, en amont, les dégâts potentiels. Ainsi, la situation hétérogène provoque de nouvelles tensions géopolitiques et fait couler beaucoup d'encre dans la communauté du droit spatial. Des pays comme les États-Unis et le Royaume-Uni reconnaissent le fait que les infrastructures spatiales sont critiques, mais ils n'évoquent pas de mesures précises relatives à leur protection, outre le besoin qu'elles soient désormais "résilientes". Or, qu'est-ce que cela signifie? Les définitions académiques de la résilience ne se retrouvent pas adéquatement représentées dans le secteur spatial, alors est-il légitime de se poser la question et d'entamer un dialogue? D'une part, les États-Unis ont une perception plus militaire et tactique de la résilience et l'ont divisée en six sous-catégories dont la dernière est la tromperie ("*deception*"). Cette approche préconise moins une intention constructive qu'une stratégie contribuant aux tensions et donc le terme de résilience se voit dénaturé et rattaché à des stratagèmes potentiellement conflictuels et c'est là un des problèmes de nuance majeurs, car la résilience, à la base, ne contient aucun élément associé à la tromperie. D'autre part, le Royaume-Uni fait recours maintes fois au terme dans sa politique et stratégie spatiales, sans toutefois se pencher en profondeur sur ce que cela implique concrètement. Mais y a-t-il besoin de le définir? Nous sommes d'avis que oui, pour justement prévenir la dénaturation permettant de remplir des missions contraires à l'essence-même de la résilience, qui, selon l'ONU, est une branche plus pragmatique du développement durable. Nous voulons aussi définir et défendre le concept avant qu'une utilisation trop large et non mesurée ne lui nuise. Notre objectif est de démontrer qu'il est possible d'appliquer la résilience au spatial et de relever le défi de protéger des systèmes difficilement accessibles. Ainsi serons-nous, peut-être, mieux équipés pour l'intelligence artificielle, le *machine learning* et la singularité, dans un futur proche, du moins au niveau juridique.

En effet, après la revue de la littérature et la recherche sur le terrain, nous entrevoyons la possibilité qu'en introduisant graduellement le concept de résilience dans les contrats spatiaux, nous inciterons le secteur privé à influencer le secteur public et qu'au final, une autoréglementation s'ensuive, à des fins durables. La résilience se caractérise par la régénération et l'adaptation, mais aussi par un retour d'expérience qui développe une sagesse rétrospective, du recul et de la prévoyance. Ces notions psychologiques trouveront un écho avec l'intelligence artificielle qui fait son entrée dans les systèmes. Ainsi, une approche transdisciplinaire du terme permettra des associations créatives et davantage de chances de ressources pour faire face aux imprévus. Nous estimons que le droit a un rôle initiateur et proactif à jouer dans ce contexte.

1.2. Dépendance croissante à l'égard des infrastructures de service

Le développement des infrastructures se fait à un rythme accéléré. Les projets de méga-constellations de petits satellites sont en compétition à savoir lequel sera le plus monumental, de l'ordre de centaines à des milliers de mini-satellites pour une interconnectivité plus dense, rapide et universelle. L'Agence Spatiale Européenne (ESA) nourrit des ambitions de village sur la Lune tandis que la NASA crée des plans pour une économie cislunaire « post ISS », et que le secteur privé veut aller sur Mars, comme le promet le magnat Elon Musk qui a l'intention de mourir sur la planète rouge après qu'il "réussisse" à nous y transporter par milliers. Ce coup médiatique inédit représente l'image spectaculaire dont s'est doté l'entrepreneuriat spatial (nommé *New Space*). Est-ce une véritable révolution, un feu de paille ou bien un nouveau lustre d'une économie spatiale n'ayant jamais cessé de se privatiser ? Peut-être que les poids lourds font face maintenant à de nouveaux entrants qui prêchent une innovation plus radicale qu'auparavant, bousculant l'ordre et le partage des appels d'offres et des soumissions. Cette externalisation[8] de moins en moins contrôlée en

[8] "*Space industrial war: Towards a risk of creeping takeovers in the global space industry*?'', par Dr. Lucien Rapp, et al. Acte de colloque, 5th Manfred Lachs Conference, McGill, 2016. Disponible à: https://www.mcgill.ca/iasl/events/mlc2016, consulté le 19.06.2017

raison de ses proportions, peut échapper à la réglementation en place et devenir une source de risques élevés. C'est un exemple qui témoigne du pouvoir des contrats et donc ce serait un excellent point de départ pour instaurer des standards de résilience pour éviter un "jour sans satellites[9]". Bon nombre d'activités de notre vie quotidienne dépend d'un fonctionnement ininterrompu des satellites: internet, transactions bancaires, télécommunications, GPS, coordination des avions, etc. Même si certaines activités ne sont pas concernées ou seulement de manière partielle, la forte complexité des interactions finit par rassembler le tout sous un toit spatial, qui se voit ainsi intégré à toutes les autres infrastructures critiques.

Figure 1 *L'Infrastructure spatiale: auspices universels ou intégrés aux infrastructures critiques? Interdépendances brisant les silos isolés*

1.3. La vulnérabilité croissante des infrastructures spatiales

Comme mentionné précédemment, les interdépendances ne cessent de s'ancrer. Celles-ci sont classées avec plus de précision dans le tableau ci-dessous[10]. Les liens les plus prononcés concernent les services GNSS/TIC-finance-transport-télécoms-défense-télédétection. Pour cette raison, le GNSS et son équivalent GPS sont considérés comme des infrastructures critiques.

[9] ''*If They Were A Day Without Satellites*…'', produit par Joseph Pelton, accessible à : https://www.clarkefoundation.org/2015/12/a-day-without-satellites/, consulté le 20.06.2017

[10] Un graphique compilé par la ROSA et la EURISIC Foundation (*EURISC Foundation - European Institute for Risk, Security and Communication Management*), disponible à: http://iaaweb.org/iaa/Scientific%20Activity/mamaia2015report.pdf, consulté le 12.11.2016

ICS/IC	Energy	ICT	Water	Food	Health	Finance	Defense, National Security	Administration	Transport	Chemical and Nuclear Industry
Remote Sensing	2	2	3	3	2	1	5	5	4	3
Communication	2	**6**	1	2	3	**5**	**6**	**5**	4	3
Meteorology	3	1	4	3	2	2	4	2	3	2
GNSS	4	**6**	4	4	4	**6**	**6**	**5**	**6**	**5**
Nanosatellites	1	2	2	2	1	1	2	2	1	1
Space stations	2	2	1	1	3	1	3	3	1	2
Rockets	1	1	1	1	1	1	5	2	4	1
Space Probes	3	3	1	1	3	3	3	3	2	1

1 The infrastructures are related but the interaction is of little importance
2 The interaction is important but only for a few of the CI components, leading to a diffuse and indirect dependece towards the SCI
3 The infrastructures interact strongly and in some cases it can be said that there is a degree of direct dependence of the CI on the SCI
4 The dependence of CI on SCI is important but does not represent a threat
5 CI is fully dependent on the SCI activity and its perturbation would cause a potential irremediable deterioration and a disruption of CI functions
6 Both infrastructures strongly interact and are dependent on each other, the disruption of one causing the disruption of the other

Figure 2: CI – SCI interaction (interaction from CRITSYS)

Figure 2 *Les interdépendances identifiées par la ROSA*

Ainsi, les satellites ne constituent plus une source de solutions pour une société moderne et interconnectée, mais une part du problème à cause de leur fragilité, surtout dans un contexte d'incertitude généré par l'externalisation et la sous-traitance. Les efforts de traçabilité dans la chaîne d'approvisionnement viendront-ils contrer les risques de sabotage latents intégrés aux micrologiciels (*firmware*)? Les nouveaux procédés d'endurcissement (*hardening*) viendront-ils fournir la robustesse et la redondance nécessaires à un système résilient? La cryptographie sera-t-elle efficace quand la sous-traitance érode lentement le secret industriel?

Il y a débat à savoir si ces menaces s'avèrent toutes vraies, mais nonobstant ce débat, les craintes, quant à elles, existent et se propagent dans la communauté spatiale, ce qui contribue à la dégradation des relations politiques. Ceci pousse les gouvernements à exiger

que leurs satellites soient de véritables forteresses, ce qui fait que les satellites militaires ou classés (*milsat* ou *govsat*) soient mieux équipés contre des attaques. Or, avec les satellites à usage double (*dual use*), signifiant usage militaire et commercial, la tâche est difficile. En effet, bien que les charges utiles (*payloads*) soient séparées, elles se partagent la même plateforme (*bus*). Nous verrons comment le réseau (*network*) qui relie tous ces systèmes devient à son tour de moins en moins étanche - prendre par exemple l'internet des objets connectés. C'est pourquoi la classification de risques est très importante et que les mesures de sécurité et de résilience doivent y être entièrement adaptées:

> *''Increasing the resilience of space systems can begin with the* ***hardening of both the space and ground segments against physical and cyber attacks, building redundancy into satellite constellations, or sharing capabilities with third parties to ensure backup service provision****. But effective protection of space assets requires embedding security considerations into* ***strategic, policy, technology and funding decisions*** *throughout all of the phases of space programmes,* ***from conception to operation. Extra care is required to futureproof big programmes with long lead times****. In order to develop a common understanding of space risks, and thus facilitate cooperation and integrated responses, the creation of a* ***common risk and resilience assessment methodology for European space infrastructures may be worth exploring.*** *In addition, rather than a separate framework for managing space risks,* ***infrastructure protection measures can be integrated, making use of existing critical infrastructure protection (CIP) efforts and strategies at national and European levels.*** *The existence of legislative and administrative frameworks for CIP at the EU level, with links to national frameworks, can help make the development and implementation of space security measures significantly easier.* ***In managing major space programmes, the security of the entire data life cycle has to be assured so that both programme partners and service users can be confident in the integrity, reliability, and security of the data.*** *An effort can be made at the European level to develop common principles for managing space data policies Nevertheless, in contrast to the national security strategies of some countries, such as the United States,* ***connections between space and security have not been central to most EU security documents"***[11]*. (Emphase ajoutée)*

Les systèmes spatiaux sont en train de changer du *hardware* traditionnel vers un amas de fournisseurs de services interconnectés, se caractérisant par un rôle plus important du *software*. Cet amas se doit de développer des capacités endogènes de régénération et

[11] Voir le rapport de l'institut *European Union for Security Studies*: "*Space security for Europe Report*", par Massimo Pellegrino et Gerald Stang, 2016, accessible à : http://www.iss.europa.eu/publications/detail/article/space-security-for-europe/. (Consulté le 11.03.2017) [Pellegrino]

d'adaptation face au danger. Une des étapes reliant ce genre de capacité à l'intelligence artificielle est la conscience de soi (*self-awareness*), l'un des piliers de la résilience.

> *"Architecture replacing traditional monolithic satellite by a spaceborne cluster of interconnected modules (…) operating on a common wireless network that allows them to share resources (services provided by space systems—data processing, data storage, and space-to-ground communication). Common infrastructure modules can be maintained, exchanged, and upgraded* ***independently from the payload modules. Fractionated architectures also offer greater resilience against cyberattacks because of the reconfigurable nature of the network. Real-time network management and fault tolerance can provide multiple routing paths around the cluster, including rapid and autonomous reconfiguration in the face of network degradation, component failure, or the addition or removal of resources***[12]*". (Emphase ajoutée)*

Les interdépendances qui rendent ces amas de plus en plus denses sont de nature cybernétique[13], mais quand les amas sont intégrés aux infrastructures critiques, la nature des interdépendances se complexifie et varie, allant de physique, géographique, logique à politique, procédurale, budgétaire et économique. La superposition de ces facteurs les rend opaques[14] et il est alors difficile de les cartographier[15]. Ainsi, des disciplines dédiées à mieux s'orienter sur cette dynamique ont fait surface. Par exemple, l'architecture de systèmes orientée sur les fournisseurs de services[16] (SOA), se dirige de plus en plus vers l'assurabilité et la sécurité de l'information (IASE), ce qui explique pourquoi la cybersécurité occupe une place incontournable dans le spatial, un environnement qui est maintenant devenu "contesté, congestionné et compétitif"[17].

> *"Service Oriented Architecture Resiliency (SOAR) defined as the continued availability and performance of a service despite negative changes in its environment is vital in a Service-Oriented Architecture (SOA). An SOA infrastructure must ensure that a service is highly available regardless of unpredictable conditions, such as sudden and significant degradation of network latency, increase in database response times, or degradation of dependant services. SOA lets increasing productivity, efficiency and business resilience, reduce costs and improve* ***IT alignment with business priorities. SOA allows creating architecture that is more flexible, responsive and easy to align with the needs of customers. Each transaction in an***

[12] *Achieving Mission Resilience for Space Systems*", par Jandria S. Alexander, dans *Aerospace Corporation's "CROSSLINK®"*, V13, No 1 (Spring 2012), disponible à : http://www.aerospace.org/crosslinkmag/spring2012/achieving-mission-resilience-for-space-systems/. (consulté le 13.02.2017). [CROSSLINK]

[13] "*Urban Resilience for Emergency Response and Recovery: Fundamental Concepts and Applications*", par Gian Paolo Cimellaro, Springer 2016. [Urban Resilience]

[14] Rapport ENISA sur la: "*Resilience of the Internet Interconnection Ecosystem" (Inter-X: Resilience of the Internet Interconnection Ecosystem Full Report*), April 2011, accessible à : https://www.enisa.europa.eu/publications/interx-report, accessed on 01.03.2017. [Inter-X]

[15] Ibid.

[16] Les systèmes spatiaux sont susceptibles à des cyberattaques, voir CROSSLINK, supra, note 12.

[17] Une expression utilisée par les États-Unis dans leur stratégie sur la sécurité : *US "National Security Space Strategy", Unclassified Summary*, 2010. Accessible à : < https://www.hsdl.org/?view&did=10828>. (consulté le 08.01.2017)

> ***SOA application may concern many separate web services. SOA can be built based on a middleware solution that integrates services throughout a network architecture. In order to support SOA applications a flexible, adaptive and agile network infrastructure*** *called Service-Oriented Network (SON) is used*[18]*."(Emphase ajoutée)*

Cette nouvelle architecture contient des éléments qui nous intéressent: flexibilité, adaptabilité et agilité, qui font tous partie du concept de la résilience, parallèle à la doctrine de robustesse et d'endurcissement[19]. Ces éléments sont particulièrement attirants dans un contexte commercial et contractuel qui recherche des notions similaires, car ils s'inscrivent dans la lignée de pensée de nouveaux modèles d'affaires et de gouvernance ; un cadre dans lequel nous voulons rajouter le droit par le biais de clauses qui guideront les parties à se

	THREAT				
TARGET	NON-INTENTIONAL	INTENTIONAL	EFFECT	MITIGATION MEASURES	PRIORITY
space infrastructure	space debris		physical damage	TCBMs, hardening, shielding, SST	high
	space weather		bugs, damage	SSA, software, monitoring	high
	unknown space phenomena		failure	redundancy, hardening, resilience, R&D	medium
		KEW/ASAT	partial/total destruction	international law, ITAR, rules, TCMBs, deterrence,	very low
		EMP (h alt nuc.)	destruction, Van Allen	international law, ITAR, rules, TCMBs, deterrence,	low
		DEW (energy)	signal disturbance, mechanical destruction	various	medium
		laser-based ASAT	sensors/mechanical damage	classified	high
		HPM ASAT (mcrw)	sensors blinded, receivers and electr. degr.	self-protecting devices	medium
		EW (E-war)	signal loss, satellite control loss	various	very high
		jammers	radarsat/satcom incapacitation	waveforms, nulling antennas, beamforming, jam	very high
		cyber attacks	transponder hijack, sat degr, info loss,	cryptography, secured softwae, process standard	very high
ground infrastructure	natural disaster		loss of comm w/ sat, ground segm disrupt	redundancy, hardening, physical security measures	medium
		physical attacks	loss of comm with sat, ground segment	redundancy, hardening, physical security measures	medium
		sabotage	loss of comm with sat, ground segment	hardening	medium
		cyber attacks	denial of service, info stolen/compromised	cryptography, authentif. proced., integrity checks	very high
		back doors	info compromised	cryptography, authentif. proced., integrity checks	high
data links	interference		denial of service/comms/radar systems	radio-f ooord at national/international, null ant,	medium
		jamming	denial of service/comms/radar systems	radio-f ooord at national/internatl, null ant, wvfrm,	high
		spoofing	wrong informatio prodided	cryptography, authentif. proced., integrity checks	medium
		cyber attacks	denial of service	cryptography, secure d software	very high
		interception	information compromised	cryptography, specific waveforms	high
technology/industry	tech transfer		3rd party space progr competition for	coordinate export control, space indusrtial policy	high
	supply shortage		no system deployed	space industrial policy	high
	lack of launch opportunities		satellite grounded	european launch policy, framework contracts	medium
	loss of industry know-how		no system deployed	space industrial policy, space R&D programmes	medium
	loss of spectrum and orbital resources		no system deployed	coordinaed Euposition at European and ITU levels	high
	new! Firmware, supply chain under stress		**hack**	**industrial policy**	**?**

Figure 3 *Les risques identifiés par le guide de la sécurité spatiale (Pellegrino, supra note 11) A noter que nous avons ajouté le dernier élément, suite à des discussions avec des représentants de l'ESA.*

[18] Rapport "*Enabling and managing end-to-end resilience*" — *ENISA,* 2011, disponible à : https://www.enisa.europa.eu/publications/end-to-endresilience. (consulté le 22.02.2017)

[19] Le cas sera discuté dans la section traitant des contrats.

prémunir de mesures efficaces à certains types de risques[20]. Ces risques concernent plusieurs segments de l'industrie spatiale, soit le segment spatial, du signal et de l'industrie. Cet écosystème complexe, qui lui-même fait partie d'un écosystème encore plus vaste, est une représentation appropriée des dimensions que peut prendre un système des systèmes et de ses pieds d'argile face aux dangers d'une attaque délibérée aboutissant à une guerre électronique (*E-war*). Ceci peut expliquer la prise de position tactique par le département américain de la Défense. Cependant, des connotations militaires potentiellement génératrices de tensions irréversibles risquent de desservir irrémédiablement le concept, étant donné que les enjeux sont bien trop interdépendants et critiques au niveau du *statu quo* mondial actuel.

2. Les problématiques: limites politiques des infrastructures de services

2.1. Les priorités gouvernementales divergentes autour des infrastructures critiques

Comme les infrastructures, l'interconnectivité et bon nombre d'autres services dépendent d'environ 1300 systèmes spatiaux. Il est impératif de trouver un moyen d'inciter les parties prenantes (donneurs d'ordre, fabricants, opérateurs, clients, etc.) de viser à la hausse les standards d'assurabilité des missions et services[21], pour maintenir le bon fonctionnement des autres infrastructures critiques[22], soit: les réseaux hydrauliques, de l'énergie, du transport, de la finance, de la nourriture, de la santé, des technologies de l'information, de l'industrie, de l'environnement, de l'administration civile, de la sécurité, de l'ordre public, de la recherche, de l'espace, et ainsi de suite[23]. Cette liste a été produite par la Commission

[20] Dans ''*Handbook on Space Security*'', édité par Kai-Uwe Schroegl, Springer 2015, [Handbook]
[21] Un nombre stipulé par la *Union of Concerned Scientists*, dans "*UCS Satellite Database*", disponible à : http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.VmXWlnYrLIV (consulté le 20.04.2017)
[22] Tel qu'élaboré dans la "*2008 Directive on European Critical Infrastructures*" (*Directive 2008/114/EC*), 'infrastructure' signifie un bien, un système, ou une partie essentielle au maintien des fonctions vitales de la société : sécurité, santé, économie, etc. Voir : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:jl0013. (consulté le 13.03.2017)
[23] La liste élaborée par la *European Union Agency for Network and Information* Security (ENISA) n'est pas utilisée par tous le pays membres. Voir le rapport de 2014 de l'ENISA sur les *"Methodologies for the Identification of Critical Information*

Européenne, dans son livre vert sur le "Programme Européen de Protection des Infrastructures Critiques" (EPCIP). Cependant les États membres ont leur propre liste, ce qui peut semer la confusion[24]. De plus, même si certains États comme le Royaume-Uni a ajouté le spatial sur la liste, il ne figure pas dans la section des mesures détaillées[25]. On se pose alors la question des conséquences d'une pensée linéaire qui tend à vouloir isoler les infrastructures en silos. Selon cette vision, il serait aisé d'isoler les risques inhérents au spatial (radiations, tempêtes spatiales, débris spatiaux, *e-war* dont certaines tactiques incluent: *targeted capability, general capability, assured disruption, forced transparency, silent erosion, digital media control*[26], pannes, sabotage, cyberattaques, etc.), or comme mentionné, cela serait loin de correspondre à la gravité de la réalité[27].

Les composantes spatiales ont intégré les discussions quand les secteurs public et privé ont réalisé l'importance du signal GPS et GNSS, sur lesquels reposent, grâce aux horloges atomiques, des services tels que la coordination des transports, des vols aériens, des chaînes d'approvisionnement, de *timing* des finances, etc. Les États-Unis ont alors compris l'utilité d'accorder une protection équivalente aux infrastructures critiques (CIP) au GPS, en 1997. Cette protection a ensuite été étendue, en 2002, aux satellites de télécommunications[28] et de services[29]. Cependant le défi qui consiste à cerner la complexité des interconnections transversales a été surmonté en 2006 quand la protection a inclu l'ensemble de l'infrastructure spatiale américaine avec le *National Infrastructure Protection Plan*. En 2010, ces initiatives ont permis à l'espace et à l'espace cybernétique de gagner en momentum

Infrastructure Assets and Services: Guidelines for Charting Electronic Data Communication Network", disponible à: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis. (consulté le 10.02.2017)

[24] Voir annexe 3.

[25] Tel que résumé dans le Cabinet anglais dans "*UK Cabinet Office Summary of the 2016 Sector Security and Resilience Plans",* produced by the Cabinet disponible à : www.gov.uk/government/organisations/cabinet-office (consulté le 11.02.2017)

[26] ''*From "Fortress to Resilience*", par Sandro Bologna, Alessandro Fasani and Maurizio Martellini, dans "*Cyber Security Deterrence and IT Protection for Critical Infrastructures*", édité par Maurizio Martellini, Springer, 2013.

[27] "*The Road to Resilience in 2050, Critical Space Infrastructure and Space Security*", par Liviu Muresan et Alexandru Georgescu, RUSI Journal, V 160 numéro 6, 2015. [Muresan]

[28] "*An Act to establish the Department of Homeland Security, and for other purposes*" ou *Homeland Security Act* (HAS), de 2002. Accessible à : < https://www.dhs.gov/homeland-security-act-2002>, consulté le 13. 06. 2017

[29] ''*The National Strategy For Homeland Security'',* d'octobre 2007. Accessible à : https://www.dhs.gov/national-strategy-homeland-securityoctober-2007, consulté le 14.05.2017

à travers *la National Security Strategy*[30]. De ce côté-ci de l'Atlantique, en Europe[31], ce genre de protection a été attribué en 2006 sous l'EPCIP[32], après l'adoption par la Commission Européenne des mesures de protection des infrastructures critiques, en 2004, à travers le continent[33]. Le spatial y a trouvé sa place en 2011, grâce à la Stratégie Spatiale Européenne[34]:

> *"Space infrastructure is critical infrastructure on which services that **are essential** to the smooth running of our societies and economies and to our citizens' security depend. It must be protected and **that protection is a major issue for the EU that goes far beyond the individual interests of the satellite owners**[35]". (Emphase ajoutée)*

Toutefois, le rôle de la Commission reste nébuleux[36] et la portée transnationale de l'EPCIP suscite un problème de gouvernance interétatique, freinant une mise en place fluide. En effet, malgré le principe de subsidiarité, les États membres peuvent voir l'EPCIP comme une intrusion à leur souveraineté, surtout en ce qui concerne un domaine hautement sensible et stratégique[37]. Les tensions ne font que s'accentuer quand nous y incluons le secteur privé. Des initiatives européennes comme la *European Union Agency for Network and Information Security*[38] (ENISA) ont étudié des plans de concertation du secteur public au regard de la cybersécurité[39], fortement ancrée dans le spatial. Les solutions mises en place et testées relèvent des partenariats publics-privés (PPP), mais avec des résultats mitigés et pour cause : les PPP mettraient le gouvernement dans une situation précaire de dépendance vis-à-

[30] ''*International CIIP handbook*'' de 2008/2009, par Brunner, E. M., & Suter, M. (2008) *Center for Security Studies*, (CSS), EHT Zurich, dans ''*Space as a Critical Infrastructure*'', by Markus Hesse and Marcus Hornung, cité dans le chapitre 10 de Handbook, supra, note 20.
[31] Ibid.
[32] Commission du 12 décembre 2006 sur le *European Programme for Critical Infrastructure Protection* (EPCIP), accessible à : https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure [COM(2006) 786 final – Official Journal C 126 of 7.6.2007]. Accessible à : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33260. consulté le 23.03.2017
[33] Pour plus de details, voir: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33259.
[34] 2006. 2008: *COUNCIL DIRECTIVE* 2008/114/EC, accessible à http://eur-lex.europa.eu/legal-ontent/EN/TXT/?uri=CELEX:32008L0114 du 8 décembre 2008 sur l'identification et la désignation d'infrastructures critiques européenne et le besoin d'améliorer leur protection. Consulté le 18.01.2017 [2008 Directive]
[35] ''*Critical Infrastructure*'' par by Markus Hesse and Marcus Hornung, chapitre 10 dans Handbook, supra, note 20, citant la *Commission of the European* Union (COM(2011) 152) : ''*Towards a space strategy for the European Union that benefits its citizens*'', accessible à : http://ec.europa.eu/enterprise/policies/space/files/policy/comm_pdf_com_2011_0152_f_communication_en.pdf, consulté le 13. 04. 2017
[36] Pellegrino, supra, note 11.
[37] En avril 2007, le Conseil a adopté les conclusions sur l'EPCIP dans lesquelles il réitérait que c'était la responsabilité ultime des États membres de gérer la protection à l'intérieur de leurs frontières tout en appréciant les efforts de la Commission de développer des procédures européennes d'identification des infrastructures critiques européennes (ECIs).
[38] ENISA, Art 114 sur le TFEU (*Treaty Functioning EU*), *Internal Mkt Regulation* (EC) No 460/2004 du Parlement et Conseil Européen, du 10 mars 2004, établissant l'ENISA (OJ L 077, 13/03/2004).
[39] Pour ce qui est des infrastructures critiques de l'information (CIIP).

vis le privé qui a des intérêts divergents du public, spécialement dans les secteurs sensibles et critiques. Ainsi, l'infrastructure critique de l'information, dont l'internet par exemple, est devenue une arène non seulement de communication, d'échanges et de solutions internationales, mais aussi de conflits nationaux, supranationaux et transnationaux[40]". Il est alors crucial, dans notre cas de trouver des solutions systémiques grâce à une approche holistique de la politique, de la technologie, de l'économie, de la gouvernance et du droit[41]. En présence d'une telle variété d'acteurs, la gouvernance adaptive fera place à la résilience via son mode de fonctionnement à objectifs multiples : ''*multi-objective reality when handling conflicts among diverse stakeholders and, at the same time, adapts this social problem to solve issues concerning dynamic ecosystems*[42]". Ce type de gouvernance a été reconnu dans l'Agenda 21 de l'ONU, dans les années 90, ce qui montre bien que ce n'est pas un concept tout nouveau. Depuis sa formulation, plusieurs pistes ont été étudiées conduisant à encourager le secteur privé à y participer et à trouver des moyens d'autorégulation. Une de ces pistes est la hiérarchie de l'ombre (soit le "*shadow hierarchy*"), qui consiste en une certaine « menace » de législation par le gouvernement, un agent de "méta-gouvernance", ou de contrôle indirect par rapport à l'auto-organisation[43]. Un style de réglementation caractérisée par des "mesures refuge" (''*safe harbor clause*") permettant à la Commission d'encadrer la protection des infrastructures critiques de l'information pourrait s'avérer efficace[44]. En effet, des

[40] "*Resilience governance and ecosystemic space: a critical perspective on the EU approach to Internet security*", par Mareile Kaufmann, dans *Environment and Planning D: Society and Space,* 2015, volume 33, pages 512 – 527. [Kaufmann, 2015]

[41] Pellegrino, supra, note 11.

[42] "*ADAPTIVE GOVERNANCE OF SOCIAL-ECOLOGICAL SYSTEMS''*, par FOLKE ET AL, dans *Annual Review of Environment and Resources*, Vol. 30:441-473, 21 novembre 2005.

[43] ''*Public-Private Partnerships and the Challenge of Critical Infrastructure Protection''*, par Andersson and Malm (2007), p. 140, dans ``*International CIIP Handbook*'', 2006, par Isabelle Abele-Wigert, Myriam Dunn, *Office for Official Publication of the European Communities*, 2006. [Dunn]

[44] "*The Evolution of Global Internet Governance: Principles and Policies in the Making*", par Roxana Radu, Jean-Marie Chenou, Rolf H. Weber, Springer 2014, citiant "*Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection*", par Myriam Dunn Cavelty, Manuel Suter, *International Journal of Critical Infrastructure*, V2-4, 2009. [Suter]. De plus, dans "*Protecting critical infrastructure in the EU. CEPS Task Force Report*", de décembre 2010, par Bernhard Hamerli et Andrea Renda, où l'on peut lire que ''*it is clear that when it comes to creating a trusted environment "[s]upranational PPPs may face a problem of size*", accessible à : https://www.researchgate.net/publication/48665286_Protecting_critical_infrastructure_in_the_EU_CEPS_Task_Force_Report_16_December_2010. Voir aussi "*The Governance of Network and Information Security In the European Union: The European Public-Private Partnership for Resilience* (EP3R)" dans Gaycken, Krueger, Nickolay (eds.), *The Secure Information Society*. Berlin: Springer Publ., 2012. [Gaycken]

principes de méta-gouvernance seraient appropriés au spatial étant donné la complexité des écosystèmes, incluant tout réseau d'information et de cybersécurité, deux domaines évoluant assez rapidement et qui requièrent une grande capacité d'adaptation. C'est pourquoi la gouvernance adaptive ("*adaptive governance*" ou AG) nous intéresse. La complexité multidimensionnelle des interdépendances nous laisse penser que la polycentricité serait un modèle de gouvernance à considérer pour optimiser le degré de résilience et contrer les facteurs de risques dans le spatial. Non seulement ce serait une solution de développement durable, mais aussi un gain financier sur le long terme, étant donné que le retour sur investissement rentabiliserait la logique : l'opinion publique, suite à un éventuel événement perturbateur (crise, désastre, cataclysme, etc.), peut mener à des actions gouvernementales destinées à réduire les pertes et à des actions de la part du privé pour mitiger les pertes de profitabilité. Ceci implique des mesures pour mitiger les coûts et, par conséquent, à rechercher des partenariats, mandats et incitatifs pour le développement futur et l'investissement industriel dans les infrastructures critiques. Ce schéma circulaire, influencé par la pensée systémique[45], représente une dynamique adéquate pour l'application de notions de résilience, qui peut ainsi générer du momentum polycentrique :

[45] ''*The Fifth Discipline: The Art & Practice of the Learning Organization*'', par Peter M. Senge, Doubleday and Currency, 1990.

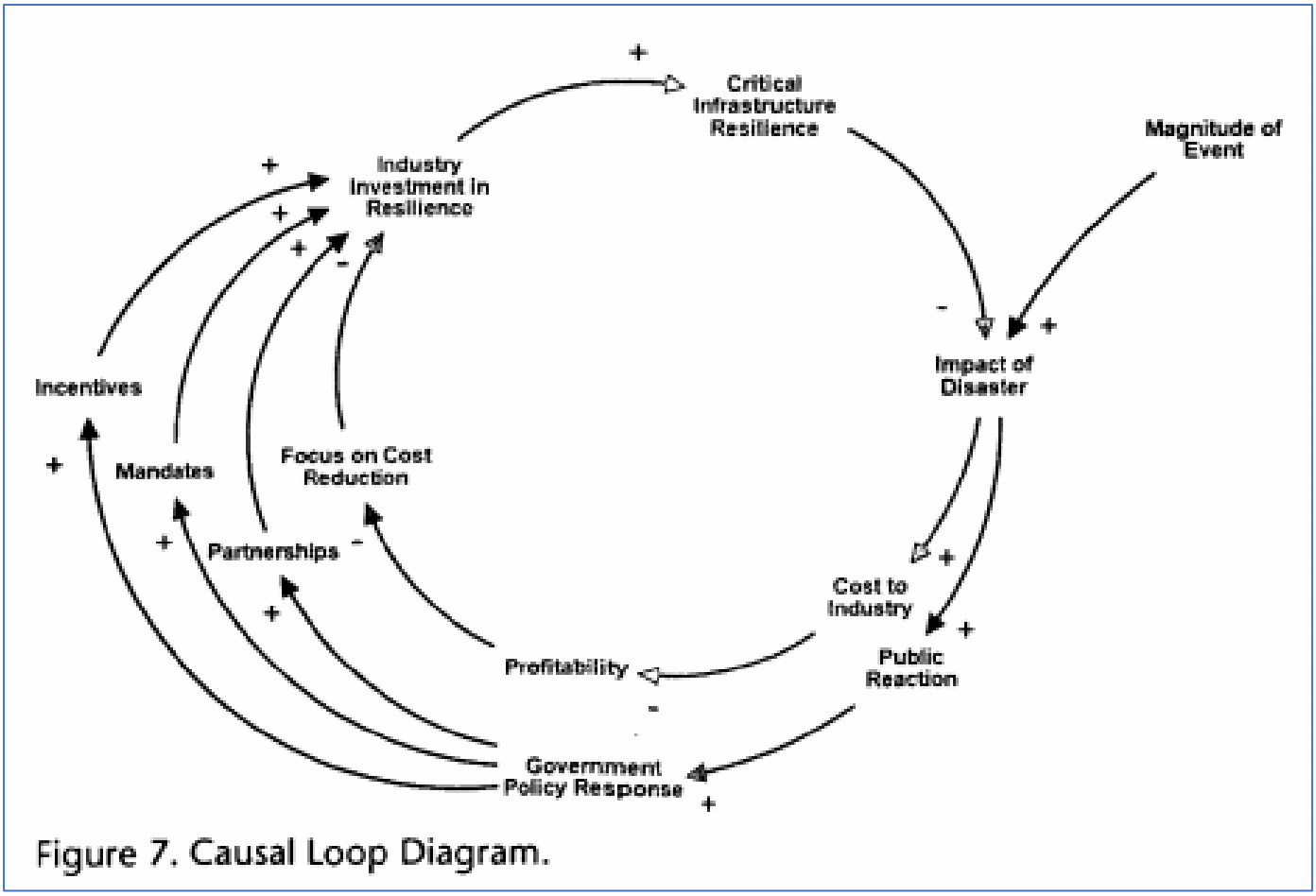


Figure 4 *Le retour sur investissement (Resilience Return on Investment "RROI") - Un argument impossible ? Homeland Security Review vol 7 no 1 Winter 2013: Resilience Return On Investment, an Impossible Argument? By Agrawal and Church*

2.2. La perspective de sécurité politique et commerciale à privilégier

En raison de l'absence de barrières nationales (sauf exception) dans le spatial et dans l'espace cybernétique, les interdépendances sont plutôt de nature transfrontalières[46] et transversales, ce qui donne de nouvelles dimensions aux conséquences :

> *''What does this dependency mean for resilience governance processes, especially given the global reach of space systems and the widespread reliance on a very low number of such assets? It means, mainly, that this* ***is a collective problem whose only solution lies in finding a collective approach to managing risks, vulnerabilities and threats. National efforts are welcome and likely to be the backbone of such efforts, given that the most resources and organizational capacities are devoted to Critical Infrastructure Protection efforts at national levels. However, an overreliance on individual efforts allows for the formation***

[46] 2008 Directive, supra note 34, art. 7.

> ***of gaps in security to which security decision makers will be blind, given informational asymmetries. Cooperation at near global levels is important for adequately gauging risks, for legitimizing a global approach to standards, commitments to sustainable practices that limit the creation of new debris and dispose of systems at the end of their lifespan etc. Neither should this be an exclusive effort on the part of spacefaring nations, though they do have a technological and financial advantage. It is important for all countries recognizing their dependence to support a framework which takes their needs and concerns into account. Issues of sovereignty, liability, stakeholder involvement and jurisdiction will complicate attempts at global governance, but the alternative is an uncoordinated mess of interests, ideas and bad incentives[47]"***. *(Emphase ajoutée)*

Ainsi, par effort collectif, les problématiques de souveraineté et de principe de subsidiarité surgissent. Cependant, cela peut aussi se traduire en un bon point pour la résilience, puisque cela encourage une approche distributive, polycentrique et de gouvernance décentralisée :

> *"According to ENISA and the Council of the European Union, the global nature of the Internet requires a holistic and systemic approach to network and cross-border information. (…) This means that distributed responsibilities are politically desired and considered effective only as long as they share certain universal standards… Efforts have been undertaken to accomplish exactly this harmonization, such as conducting exercises, devising a global code of conduct, supporting strategic cooperation, establishing a common language and standardizing the definition of gaps[48]".*

Cependant, en ce qui concerne le secteur spatial en Europe, nous rencontrons un défi politique supplémentaire, soit le principe de "juste retour", qui oppose l'Agence Spatiale Européenne et la Commission Européenne. En effet, les projets supervisés par l'Agence y sont soumis et les pays ayant le plus contribué financièrement se verront attribuer une participation plus substantielle. En revanche, ceci ne s'applique pas à la Commission. Comme certains projets sont soit chapeautés par les deux entités ou en importante interaction avec d'autres projets, la portée du juste retour est difficile à déterminer, ce qui peut générer de la discorde. La volonté politique *(political will)* s'en voit alors affectée, ce qui devient assez délicat, car elle est souvent un moteur considérable de mobilisation médiatique, de légitimité et de succès. Cette inconsistance ne réassure pas les parties prenantes à un partenariat spatial et une

[47] ''*CRITICAL INFRASTRUCTURE DEPENDENCY ON SPACE SYSTEMS*'', par Georgescu, Alexandru; Botezatu, Ulpia-Elena; Popa, Alina-Daniela; Popa, Stefan; Arseni, Stefan-Ciprian. *Scientific Bulletin "Mircea cel Batran" Naval Academy; Constanta,* 19.1 (2016): 527 [Georgescu].

[48] "Resilience, Emergencies and the Internet: Security In-Formation", par Mareile Kaufmann, Routledge, Jun 14, 2017. [Kaufmann, 2017]

solution d'harmonisation s'impose pour les projets à long terme, au niveau pan-européen. Dans cette optique, en ce qui concerne les infrastructures critiques spatiales, nous pouvons suggérer l'élaboration de la gouvernance adaptive transnationale.

Les aspects transnationaux[49] peuvent s'inspirer des notions provenant de deux volets de la résilience que nous empruntons à la division des infrastructures en 1) souples (*soft*) et 2) lourdes (*hard*). La souplesse encadrera le niveau organisationnel, soit l'adaptabilité et la polycentricité. Le volet "lourd" encadrera, quant à lui, ce qui relève davantage du monde technique et l'interopérabilité s'y rattachant[50]. Ceci peut être illustré par un exemple de l'une des composantes de la résilience : la redondance des systèmes. Le signal GPS est résilient en ce sens, puisque s'il voit son service dégradé pour cause de panne ou autre incident, le signal peut toujours être repris par son équivalent européen GALILEO et vice-versa[51]. Cependant, cette interopérabilité de services est à double tranchant, puisque la vulnérabilité peut être étendue si la redondance ne comporte pas un minimum de différences ou d'étanchéité. Ce risque devient d'actualité dans un contexte spatial de commercialisation et de recours fréquent à des composantes standard obtenues sur le marché (*commercial off the shelf* ou *COTS*). Pour cette raison, l'architecture spatiale se doit non seulement résiliente, mais créative tout en tenant compte des spécificités uniques du spatial :

> "***The criticality of space systems can no longer be ignored***, *and there is also the realization of the heavy dependence of previously mentioned critical infrastructures on space infrastructures, which provide command and control capabilities, information gathering, emergency response support and so on. For this reason, CIP precepts should be applied to critical space infrastructures (CSI) as well, identifying threats, mitigating vulnerabilities and minimizing disruptions.* ***However, policy and decision makers should not just transpose CIP from terrestrial to space systems, as this would ignore the risks inherent in the heavy interconnections between the two. Rather, space systems should be integrated in existing CIP frameworks with the full realization of their importance, triggering developments in the fundamentals of critical infrastructure protection efforts around the world*** *(…) The negative consequences are an increase in the exposure of critical terrestrial infrastructures*

[49] "*Realizing a New Global Cyberspace Framework Normative Foundations and Guiding Principles: Global Cyberspace Framework*", par Rolf H. Weber, Springer, 2014.
[50] Handbook, supra note 20.
[51] ''*Space Security Index 2016*'', du 2 novembre 2016. Section 3.4 sur *la DARPA The National Positioning, Navigation, and Timing Resilience and Security Act* de 2015 (the *DARPA The National Positioning, Navigation, and Timing Resilience and Security Act of 2015*), accessible à : https://www.congress.gov/bill/114th-congress/house-bill/1678. (consulté le 06.12.2017)

> *to the risk that space systems will be destroyed or will malfunction.* ***This places the entire system-of-systems at risk, because space systems have become an integral part of it, whether we consider them their own separate infrastructure or a component of each critical infrastructure sector in part. In truth, it is becoming difficult for decision makers and security experts to pinpoint where one infrastructure ends and another begins, because of the fluidity and the diffusiveness of modern infrastructure systems,*** *which are more than simply physical assets in a precise geographic location*[52]*". (Emphase ajoutée)*

Ce genre de spécificités, qui ne peuvent être simplement transposées du terrestre au spatial, oblige des organisations comme l'ENISA à étudier les spécificités relatives au monde cybernétique. Dans ce cas-ci, cela ne peut se faire sans inclure le secteur privé au processus par le biais des PPP, comme, par exemple, celui sur la Résilience Européenne (EP3R), de 2009 à 2013. Le processus permettait aux parties prenantes publiques et privées d'engager des discussions au sujet de prises de décisions stratégiques et de réglementation, de partager de l'information et ainsi de contribuer aux efforts de résilience. Toutefois, les résultats de cet exercice se sont révélés mixtes. L'effectif des participants et des organisateurs n'était pas constant, avec un taux de changement assez élevé, les objectifs étaient parfois exempts de précision, etc. De plus, les parties prenantes du privé espéraient une place privilégiée et plus rapprochée du cercle fermé des preneurs de décisions, pour y exercer davantage d'influence. Le nombre de participants n'étant pas idéal pour ce genre d'environnement[53], la motivation des acteurs concernés se voyait varier selon les incitatifs, parfois jugés non rentables. Ces leçons ont permis de fermer le cycle de l'EP3R et de passer à une nouvelle plateforme de collaboration, toujours axée sur le partage d'information : la *Network and Information Security* (NIS)[54].

En théorie, les points clé à retenir des PPP se résument dans le fait qu'ils sont: 1) utiles en temps de problèmes complexes; 2) adaptables selon le contexte et les circonstances; 3) une concession en faveur du privé en matière de prise de décision; 4) une incitation à

[52] Georgescu, supra, note 47.
[53] Gaycken, supra, note 44.
[54] La directive NIS de l'ENISA est accessible à: https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts, consulté le 19.06.2017

l'appropriation du projet de le degré de marge de manœuvre et propriété ou "*ownership*" accordé au privé et, 5) un exemple possible d'approche ''*bottom-up*''. Les avantages classiques sont l'alignement des objectifs et la création d'un lien de confiance accompagnant les efforts de baisse des coûts. Par contre, en réalité, malgré l'image d'un modèle idéal de gouvernance, les avantages espérés sont contradictoires[55], associant les PPP à une boîte de Pandore, offrant des solutions imprévisibles dans des secteurs en manque de ressources et de réglementation, comme les mesures nationales d'urgence et de gestion de crise. Souvent, dans ce type de secteur, les intérêts du public et du privé sont fondamentalement divergents à la source (sécurité vs efficacité, etc.) et le partenariat n'ira pas satisfaire les exigences tel quel, mais débouchera sur un compromis et la rentabilité risque alors l'emporter sur la qualité. Ceci est parfaitement applicable aux infrastructures critiques[56]. Pour ces raisons, des solutions transfrontalières s'imposent et nous visons les contrats ainsi que leur gestion.

Certes, outre les difficultés reliées au principe de subsidiarité ou de juste retour, le droit spatial connaît d'autres défis. Le droit en tant que tel est souvent relayé en arrière-plan, en coulisses, confiné à un rôle réactif et moins anticipatif. Dans le spatial, ce rôle est plus prononcé, puisque c'est un secteur sensible et stratégique, dont une grande partie est basée sur les fonds publics, donc du contribuable et alors le secteur se voit plus conservateur face au risque et donc aux avancées spectaculaires, pour ne pas entraîner un débat public non souhaité. Cette approche conservatrice trouve écho dans notre catégorie de résilience lourde (*hard resilience*) visant les aspects plus techniques. Celle-ci représente une approche conservatrice aussi du fait qu'elle vise le retour à un équilibre initial, approche privilégiée en génie. L'autre école de pensée de la résilience mise sur l'adaptation vers un équilibre nouveau, alternatif, et consiste donc en une approche progressive. Elle s'applique plutôt à l'aspect humain et organisationnel, souple, adapté aux sciences de la nature comme l'écologie et aux sciences sociales telles la psychologie, la gestion, etc. Au début, la résilience étudiait

[55] Dunn, supra, note 43.
[56] Suter, supra, note 44.

comment un système (ou un être vivant) surmontait un événement perturbateur exogène grâce à une capacité endogène[57] et s'adaptait pour trouver un nouvel équilibre (qu'il soit l'initial ou autre) tout en cultivant un retour d'expérience pour l'avenir. Par la suite, ce concept s'est vu divisé selon les besoins et nous avons hérité de ces deux grandes écoles de pensée, toutes deux utiles en leur sens, mais que nous souhaitons réunir à nouveau, de façon pragmatique. Ainsi, par exemple, pensons-nous, que le spatial devrait s'ouvrir à davantage de souplesse pour faire place à du progrès, permettre davantage de possibilités face à la résilience et à des solutions juridiques créatives et transversales :

> *"…systemic goals that are too narrowly focused on advancing the stability of political and economic goals; (2) monocentric (too centralized), unimodal (placing too much emphasis on uniform models) and fragmented structures of government; (3) inflexible methods that employ rules and legal abstractions and promote resistance to change; and (4) rational, linear, legal-centralist processes that assume away uncertainty. (…) traditional features of common law systems, such as stare decisis, checks and balances on government authority, judicial self-restraint, res judicata, and protection of individual rights and freedoms, also make the US legal system resistant to change[58]".*

En tenant compte de ces problématiques, nous comprenons pourquoi une plus grande souplesse juridique favoriserait des solutions innovatrices et des politiques plus détaillées par rapport à la résilience. En effet, elles expliquent la réticence des États à élaborer davantage sur le sujet. Par exemple, la *National Space Security Policy* de 2015[59] du Royaume-Uni mentionne plus de 34 fois le terme résilience, mais sans détailler en quoi elle consiste outre des généralités comme le besoin de la promouvoir, de l'élargir, de la renforcer, etc.:

> *"Objective 1: To make the United Kingdom more resilient to risks to space services and capabilities, including from space weather. This will be achieved by* ***increasing the resilience of space services to disruption from malicious (e.g. jamming) or natural (e.g. space weather) causes, and by reducing the vulnerability of essential infrastructure (e.g. transport and communications) to disruption to space services, or direct disruption caused by space weather****. In both cases we need a proportionate approach to* ***investing in resilience, balancing protective measures, such as encryption, hardening and resistance to jamming,***

[57] *"Some Thoughts on Resilience What do you mean, 'resilient'?"* par Dave Hodgson, Jenni L. McDonald, et David J. Hosken, dans *Trends in Ecology & Evolution*, Volume 30 : 9, p. 503 – 506.

[58] ``Law and Resilience: Mapping the Literature`` par Tracy-Lynn Humby, *Seattle Journal of Environmentl Law*, V4 Issue 1, 2014, accessible à : http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1032&context=sjel. (consulté le 20.02.2017) [Humby]

[59] Texte accessible à : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307648/National_Space_Security_Policy.pdf (consulté le 03.02.2017)

> ***with other means of promoting resilience, such as improved forecasting, alternative or fallback capabilities***. *Responsibility will rest largely with owners and operators of space services or with infrastructure owners and operators, with oversight provided by lead Government departments (…)". (Emphase ajoutée)*

Ensuite, le texte aborde le besoin d'en informer le public et (ce qui nous intéresse particulièrement) invite le secteur privé à y jouer un rôle fondamental:

> *"An improved understanding of our space security risks and dependencies across public and commercial sectors will allow the United Kingdom to build the right level of resilience for space capabilities and services.* ***It will also enable businesses, infrastructure sectors and other public and private sector bodies to exercise their responsibility to ensure that space resilience and space security considerations are incorporated in resilience, business continuity and security plans****". (Emphase ajoutée)*

Bref, un rôle opérationnel dont l'importance croît pour éventuellement se passer de l'intervention étatique : "*resilience can be enhanced through good partnership and information-sharing,* ***without the need for direct intervention by government*** *in areas that are the responsibility of infrastructure owners and operators*", pendant que le gouvernement étudiera des questions plus larges et transversales, notamment en ce qui a trait aux partenariats internationaux, surtout en ce moment d'incertitude attribuée au "*Brexit*". Étant donné la position prise par le R.-U. en ce qui concerne la résilience et le privé[60], il n'est pas surprenant que nous visions les contrats, pour aller plus loin dans cette ligne de pensée.

2.3. Le processus vs l'aboutissement

Dans notre division de la résilience en deux volets, nous nous sommes inspirés de la littérature pour établir un parallèle additionnel : 1) le volet souple recouvre le processus, tandis que et 2) le volet lourd, plus rigoureux, couvre l'aboutissement souvent technique de notre secteur et des infrastructures critiques et spatiales. Nous sommes d'avis que la réglementation mise davantage sur les processus et procédures et moins sur l'aboutissement. Or comme nous déterminons que les processus doivent s'ouvrir à la souplesse, il en va de même pour les politiques encadrantes. Ceci conduira les parties prenantes à se poser des questions par rapport aux buts recherchés d'un projet en question et mieux s'enligner sur

[60] ``*Contractual Governance: Institutional and Organizational Analysis*``, par Peter Vincent-Jones, Oxf J Leg Stud (2000) 20 (3): 317-351.

une mission et une vision (*outcome*) qui peuvent être souples, tout aussi bien que lourdes. Voici un exemple à la page suivante de vingt-cinq procédures d'approvisionnement (*procurement*), appelées "objectifs de sécurité", assez précises, plus ou moins souples, établies par l'ENISA en ce qui a trait aux infrastructures de l'information et à la cybersécurité, pour assurer la continuité des affaires et l'assurabilité de la mission. On peut voir que les mesures s'arrêtent à un certain niveau de superficialité et ne vont pas plus loin pour prendre du recul par rapport à un projet donné et surtout, ne parlent pas encore de résilience, même si quelques détails en font partie[61]. Nous constatons donc quelques premiers efforts procéduraux en ce sens, sur une base plus ou moins volontaire, donc souple et flexible. Nous voulons continuer dans cette dynamique grâce à une clause allant plus loin dans le micro-juridique et de permettre aux parties d'opter pour des degrés de résilience lors des négociations. La souplesse pourra entourer des clauses de négociation à l'amiable, de résolution de conflits, de clauses *"safe harbor"* etc., tandis que l'aspect lourd tournera plutôt autour de points précis (techniques) prévus dans les contrats. Nous visons donc les mécanismes juridiques du contrat tout comme les mécanismes plus techniques préconisant la résilience.

[61] Le rapport de l'ENISA Report: "*Security Guide for ICT Procurement: Security Guide for Electronic Communications Service Providers*", décembre 2014, accessible à: https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement. (consulté le 12.02.2017)

2.6 Business continuity management

SO19: Services continuity strategy and contingency plans

Security Risks
Weak or lack of service continuity strategy defined to guarantee the availability of service for the provider in case of an incident.
Security requirements
✓ The vendor shall ensure by tools, skills, resources or processes that services of the provider remain operational at all times, complying with the minimum level of service defined in the SLA and accepted by the provider. This can include, i.a.: – Spare parts[5] – Back up – Back up personnel to ensure critical functions are always maintained ✓ The vendor should provide complete documentation of business continuity processes. ✓ More specifically, the outsourcing service vendor should have a service continuity plan with a strong emphasis on potential failures of power supplies. This is very significant given that a failure of the power supplies can lead to a complete interruption of service for the provider. ✓ The vendor's business continuity plan should consider its dependencies of subcontractors ✓ The vendor should review its service continuity plan based on past incidents and past experience and revise it if necessary.

Figure 5 *ENISA Business Continuity Management Clause*

Au niveau européen ou international, le manque d'harmonisation des mesures d'intégration d'exigences de sécurité et de cybersécurité, de partage d'information[62], de réglementation, de définitions, d'évaluation de risques et de gouvernance corporative dans un environnement à parties prenantes multiples rend difficile le parcours de la résilience. Dans nos recherches, en ce qui concerne le secteur public, nous avons relevé beaucoup de défis, surtout en ce qui concerne son interaction avec le secteur privé. Cependant, nous avons trouvé des cas intéressants dans lesquels ces deux secteurs ont réussi à s'entendre et à générer des

[62] Le rapport de l'ENISA : ''*National Cyber Security Strategies (NCSSs)*'', 2013. accessible à : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map. (consulté le 12.02.2017)

solutions innovantes dans le but d'accroître l'assurabilité de la mission, ce qui a débouché sur des pistes propices à la résilience. En effet, le *business case* liant *Paradigm Secure Communications* (initialement faisant partie d'Astrium, EADS et maintenant d'Airbus) au ministère de la Défense britannique a donné suite à l'histoire couronnée de succès relative aux satellites militaires de communication (*milsatcoms*) *Skynet* 5[63], à travers un mécanisme semblable au PPP: le PFI (pour *Private Finance Initiative*), avec pour but le risque de transfert. Le résultat a été d'investir dans le lancement de deux satellites additionnels en 2006 et en 2007 (dont l'un devait servir de remplacement le cas échéant) et non dans des assurances supplémentaires. Le signal, l'infrastructure, le service et la rentabilité ont ainsi été optimisées en raison d'une plus grande capacité. En ce qui concerne les relations contractuelles entre les deux parties, il a été observé qu'une certaine flexibilité de négociation a conduit à une souplesse au niveau de l'entente de coordination. Les parties ont évalué le budget, les coûts et les flux de trésorerie avant de décider ensemble d'investir davantage dans l'assurabilité du service que dans les assurances. Ils ont donc opté pour la fabrication et le lancement de satellites supplémentaires.

Ces satellites avaient pour mission d'accroître la continuité du signal, mais ont aussi de générer de nouvelles opportunités d'affaires, prouvant ainsi que la résilience peut devenir rentable. C'est pour cette raison que nous nous concentrerons sur l'innovation des clauses contractuelles pour inciter le secteur à s'orienter vers un changement de "paradigme[64]" et à privilégier le long terme[65].

[63] "La Gestion des Risques dans le Cadre d'un PFI: L'Exemple de Paradigm au Royaume-Uni", par Francesco Giobbe and Jean-Claude Vechiatto, dans « Gestion et partage des risques dans les projets spatiaux », édité par L. Ravillon, Paris, Pedone, 2007, 11. [Ravillon, 2007].

[64] Filliale de l'EADS, maintenant Airbus, fabriquant des milsatcoms pour le Ministère anglais de la Défense. Accessible à : http://www.airbusgroup.com/airbusgroup/int/en/news-media/press-releases/Airbus-Group/Financial_Communication/2009/06/20090618_astrium_paradigm.html. (consulté le 23.03.2017)

[65] Clauses empruntées au *contrat Satellite Purchase Contract for In-Orbit Delivery - XM Satellite Radio Inc*. and Boeing Satellite Systems International Inc., accessible à : http://contracts.onecle.com/xm/boeing.sat.2001.05.15.shtml. (consulté le 28.01.2017) [XM Sat]

3. Résilience: un concept à introduire dans le domaine du droit

3.1. L'origine historique du concept

Jusqu'à présent, nous avons mentionné le terme à maintes reprises, mais sans entrer en détails, tout comme le font les diverses stratégies spatiales. Cependant, c'est ici que nous irons plus loin et entrerons dans l'étendue académique du terme. En ayant étudié les quelques vingt définitions les plus citées (que nous avons rajoutées à l'annexe 1), nous avons distingué deux courants de pensée : l'un progressif et l'autre conservateur, mais qui se partagent un tronc commun, soit plusieurs capacités dont celles d'absorber, de s'adapter et de se régénérer (ou se restaurer) tout comme l'indique le graphique ci-dessous:

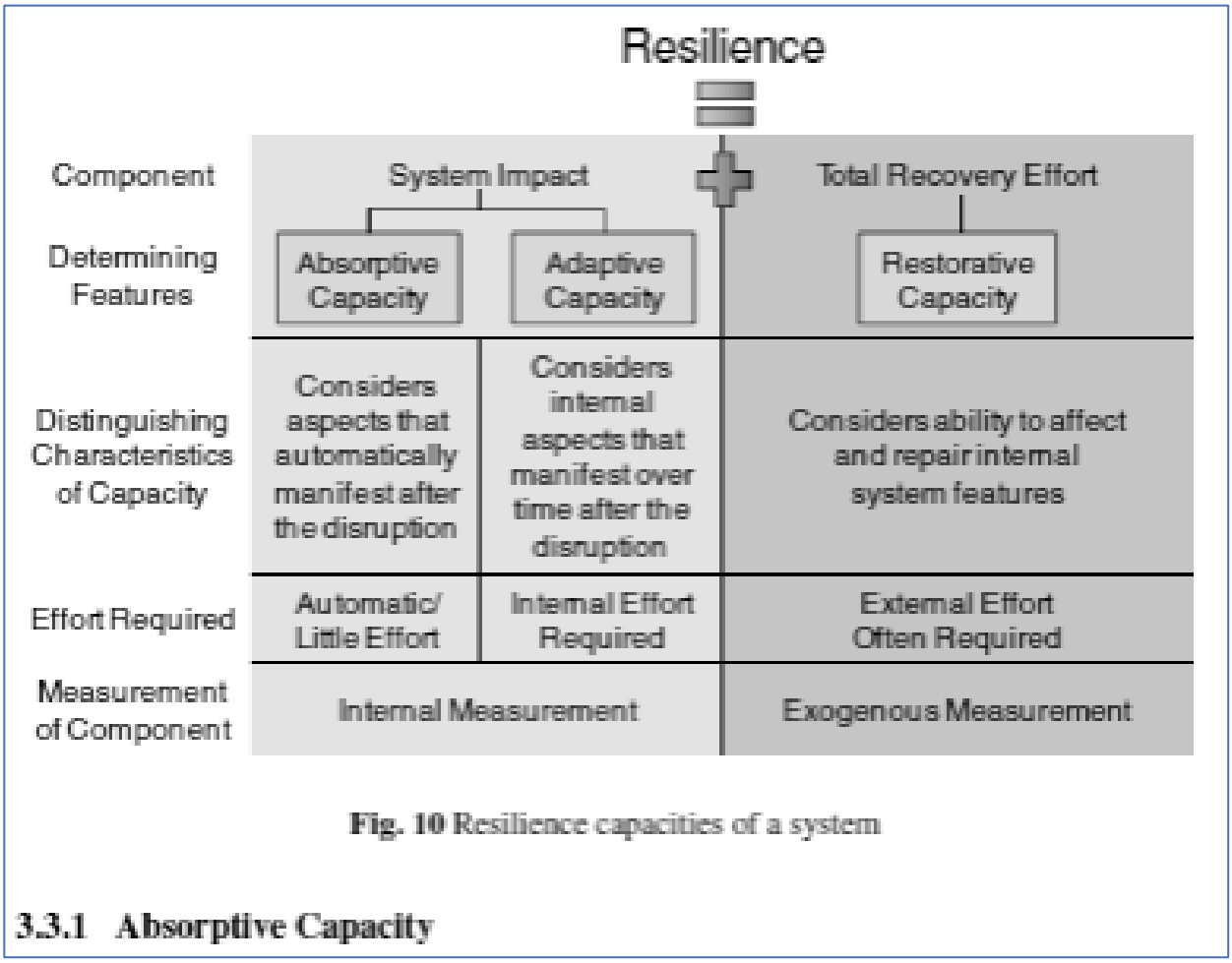


Fig. 10 Resilience capacities of a system

3.3.1 Absorptive Capacity

Figure 6 La capacité résiliente des systèmes

Profitant de cette ramification, nous avons trouvé très pertinente la superposition de l'infrastructure souple et lourde[66], puisque ces deux ramifications comportent de nombreux points communs, comme nous le montrons dans le tableau ci-dessous, synthétisant ces ressemblances :

Resiliensis Spatialis (Purpose: WHY)	
Paradigm Shift towards Long-Term Critical Space Infrastructures	
School of thought PROGRESSIVE (ADAPT)	*School of thought CONSERVATIVE (RESTORE)*
ECOLOGY, PSYCHOLOGY, BIOLOGY	*ENGINEERING*
SOFT RESILIENCE (process[67]: HOW)	*HARD RESILIENCE (outcome: WHAT)*
uncertainty, organization, governance	*precision, technological demands*
ORGANIZATIONAL CULTURE, CONTRACT MANAGEMENT	*CONTRACTUAL CLAUSES*

L'Agenda 2030 sur le développement durable rédigé par l'ONU fait référence à la résilience et appelle tous les États à l'appliquer dans divers aspects internes et externes de développement :

> *"will be implemented by all countries and stakeholders, acting in collaborative partnership and with the determination to take the bold and transformative steps that are urgently needed to shift the world on to a sustainable and* ***resilient*** *path[68]'. (Emphase ajoutée)*

[66] Projet RAMSES: ''*Climate change vulnerability and adaptation indicators. The European Topic Centre on Air and Climate Change (ETC/ACC)*'', pour la *European Environmental Agency* (EEA,) par Harley, M., Horrocks, L., Hodgson, N., van Minnen, J., 2008., Bilthoven,, N, dans WP 2: ''*Taxonomy of architecture and infrastructure indicators, D2.1: Synthesis review on resilient architecture and infrastructure indicators, Reference code: RAMSES*'' – D2.1RAMSES PROJECT Grant Agreement n° 308497, par James Kallaos, et al., accessible à : http://www.ramsescities.eu/fileadmin/uploads/Deliverables_Uploaded/28022014_deliverable_ramses_d2_1.pdf >, consulté le 21.01.2017)

[67] Voir annexe 5.

[68] ''*Coordination of space-related activities within the United Nations system: directions and anticipated results for the period 2016-2017*'' — *2030, Agenda for Sustainable Development Report of the Secretary-General*, UNCOPUOS, paragr. 83, avril 2016.

Les infrastructures figurent à l'objectif numéro 9 et cela encourage notre perception tournant autour de la nécessité de mettre l'emphase sur leur résilience et d'appliquer cela aux infrastructures spatiales critiques[69], d'un point de vue systémique[70] et transversal. Il faut se souvenir que l'architecture spatiale est en train d'évoluer techniquement vers un écosystème d'amas de fournisseurs interdépendants de services interconnectés[71], dans un contexte de privatisation. Ainsi, le rôle des contrats est en hausse et nous y voyons un angle avantageux pour entamer la proactivité du droit[72] et générer un standard de continuité dans un environnement d'incertitude[73]. Étant donné que la résilience souple traite d'auto-organisation (*self-organisation, self-awareness*, etc.) tout comme les lois souples ou le droit non-contraignant (*soft law*), nous considérons cet aspect particulièrement adéquat pour son rôle auprès de l'intelligence artificielle qui nourrit graduellement la notion de soi ("*self*"). Si l'on applique la résilience au concept de soi, cela signifie, en théorie, permettre à un système de se placer dans une situation donnée et d'adopter une stratégie appropriée de rétablissement, basée sur un *feedback*. En écologie, comme en biologie, tout un système de noyaux et de couches successives s'adapte et se régénère, illustrant ainsi cette fonction[74]. Ainsi peut-on s'en inspirer en ce qui a trait à la gouvernance adaptive.

3.2. Définition

Non seulement le spatial est un environnement à part en soi, mais pour des fins de discussion, nous allons faire référence à cet environnement dans une perspective de droit environnemental et d'écologie pour expliquer la pertinence d'une approche flexible. En effet,

[69] Muresan, supra, note 26
[70] Le système des systèmes se définit comme ''*individual infrastructures exist together in what is called a 'systems of systems' which is defined as a set of multiple, but independently operational systems that must interact effectively with one another to meet specific needs*'' tel qu'écrit dans "*Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*", par Kasthurirangan Gopalakrishnan et Srinivas Peeta, Springer, 2010.
[71] CROSSLINK, supra, note 12.
[72] En effet, "*adaptive management, cannot be implemented solely by agencies and executive planning and procedures; it requires the guidance of a legal principle and enforcement by the judicial branch*", comme l'écrit Lia Helena Monteiro de Lima Demange, dans "*The Principle of Resilience*", 30 Pace Envtl. L. Rev. 695 (2013), accessible à : http://digitalcommons.pace.edu/pelr/vol30/iss2/11f. (colsulté le 29.01.2017) [Monteiro]
[73] Kaufmann, 2015, supra, note 40.
[74] Dans CROSSLINK, supra, note 12, on peut lire que: ''*systems' self-awareness enables adaptation to a context and interpreting feedback accordingly in order to adopt a strategy which can later be shared*''.

d'après Holling (1973)[75], la résilience décrit en gros la capacité d'un écosystème d'absorber un choc, de s'adapter et de se rétablir ou d'évoluer, selon les circonstances. Avec le temps, l'interprétation la plus courante est celle conservatrice, d'un retour à un équilibre antérieur. Cette approche est généralement utilisée en génie et nous lui attribuons les facteurs d'une infrastructure lourde :

> *"Resilience can be perceived as a measure of ability to work through stress and recover to the same initial condition when the stress is removed. In telecommunications and information processing networks where the input conditions typically tend towards chaotic identifying the stable point to return to after a stress event has a degree of uncertainty. As such resilience is not a very straightforward item to define by requirements. Using the model for specifying detail requirements of preconditions, stimulus and response the precondition of resilience is the steady state, the stimulus is the load that leads to stress, and the response is (eventually) a return to the steady state. The problem from a requirements point of view is that if the initial response to stress is to stop but the eventual response is to restart in the same initial state this could be argued to be "resilient" but it is not as it is more correctly simply recoverable. A truly resilient network has to maintain operation throughout the stress event (i.e. availability should not be degraded) and also* ***return to a state as if unaffected by the stress when the stress is removed****.[76]" (Emphase ajoutée)*

La ramification dont nous nous servons, inspirée du projet RAMSES (voir note 63, supra) nous permet d'aller plus loin et de nous rapprocher du niveau organisationnel grâce à l'approche souple, inspirée de l'écologie et de l'interprétation de Holling se basant sur plusieurs équilibres possibles et états alternatifs[77]. Un écosystème peut perdre certaines fonctions mais continuer à fonctionner, en mode altéré, jusqu'à ce que d'autres fonctions et mécanismes se créent ou se refassent, avec de nouveaux systèmes remplissant des rôles identiques, similaires, alternatifs ou différents, selon l'approche d'adaptation sélectionnée[78]. Nous qualifions cette perspective de souple et progressive, qui encadre les processus en

[75] La résilience est une "*measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables*" tel que décrit dans "*Resilience and Stability of Ecological Systems*", par C. S. Holling, Annual Review of Ecology and Systematics, Vol. 4:1-23 (novembr 1973). [Holling]

[76] Rapport de l'ENISA sur ''*Ontology and Taxonomies of Resilience'',* accessible à : https://www.enisa.europa.eu/publications/ontology_taxonomies. (consulté le 12.01.2017)

[77] 1) l'approche selon laquelle la résilience conduit à un état antérieur (équillibre initial), tel qu'expliqué dans ''*A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities''* par Michel Bruneau, et al., *The Professional Journal of Earthquake Engineering Research Institut*e, V19 Issue 4, 2003, et 2) celle qui conduit à un état différent (nouvel équilibre), tel qu'explliqué dans ''*A Typology of Resilience: Rethinking Institutions for Sustainable Development''* par by John W Handmer and Stephen, dans *Organization & Environment* 9(4):482-511, décembre 1996.

[78] RAMSES, supra, note 66.

général, qu'ils soient systémiques ou organisationnels, puisqu'ils font face à l'incertitude[79], contrairement à l'approche conservatrice, qui elle, doit asseoir certains fondements de certitude et des paramètres concrets[80]. Les deux approches doivent fonctionner en symbiose, car l'une a besoin de l'autre pour atteindre un équilibre interne et une résilience spatiale par l'intermédiaire des contrats.

Hard infrastructure	Soft infrastructure
Resist	**Adapt**
Built	Social, economic, political
Focused	Comprehensive
Engineering/technical	Organizational
Industrial, operators	Institution, local authority
Quantifiable	Not (easily) quantifiable
Technological fix	Organizational fix
Structural measures	Non-structural measures
Outcome-based	Process-based
Sectoral	Non-sectoral

Table 2: Resilience characteristics for hard and soft infrastructures.

***Figure** 7 La taxonomie des indicateurs d'architecture et d'infrastructure, du projet RAMSES*

Comme mentionné, la notion de résilience comprend plus de vingt définitions[81], mais certains éléments les transcendent. Nous pouvons les résumer aux quatre R traditionnels de la résilience : 1) Robustesse[82] (capacité de résister) ; 2) Redondance (capacité de se reposer

[79] Ibid. Ceci se réfère à "*adaptability, responsiveness, ability to recover can be assessed with process-based indicators which monitor progress in implementation*" tel que décrit dans "*Towards indicators for resilient architecture and infrastructure*", par James Kallaos, Gaëll Mainguy, Annemie Wyckmans, Journal of Land Use, Mobility and Environment (TeMA), Vol 7 N 1, 2014.
[80] Ibid. Ici, nous faisons référence à la persistence, résistence et robustesse, pouvant être mesurées selon l'efficacité à retrouver l'équilibre initial.
[81] La vingtaine de définitions est compilée dans l'annexe 1.
[82] En génie, la résilience signifiait avant la capacité d'un matériel d'absorber de l'énergie dans un état de stress et de la libérer ensuite. In traditional engineering, resilience was the ability of a material to absorb energy under stress and release it later. Dans la théorie moderne des systèmes, cela signifie maintenant la capacité d'évoluer, soit la capacité d'un système de s'adapter graduellement alors l'environnement dans lequel il se trouve change (une approche empruntée à la biologie), tel que décrit par

sur un système alternatif) ; 3) ingéniosité à retrouver des Ressources (capacité à s'adapter de manière créative) et 4) Rapidité (capacité de se rétablir rapidement)[83]. De plus, quatre capacités proactives additionnelles viennent se superposer à ce portfolio : 1) capacité de faire face à des sources de menaces, qu'elles soient régulières ou irrégulières ; 2) capacité à surveiller la performance du système pour évaluer l'ampleur de l'impact (partial, total, intermittent, récurrent, etc.) ; 3) capacité d'anticiper les perturbations, pressions et conséquences (réponses automatiques, rétablissement à long terme, réparations, restauration, etc.) et, 4) capacité d'apprendre et de tirer des leçons à partir de l'expérience vécue[84]. Ceci nous interpelle, puisque la notion de soi est nécessaire à toutes ces capacités. Or, la notion de soi nous renvoie principalement à des disciplines comme la psychologie et alors nous comprenons qu'une approche transdisciplinaire et holistique s'impose :

> *"The 'self x' logic that regulates the ecosystem: to deal with the increasing complexity of systems and uncertainty of their environments, networking has turned to [the] self x concept that can be read as self-reconfiguration, self-optimizing, self-diagnosing, self-healing, self-protecting, self-organizing, self-forming, self-adapting or self-managing. Self x leverages wireline and wireless systems and provides transmission resiliency resulting in an autonomous behavior. The self x features and facilities relate to both hardware and software. All such solutions work with feedback loops that probe the whole infrastructure"*[85].

Appliquer le soi à la résilience et faire appel à la psychologie nous fait penser à l'interaction à venir entre la résilience et droit. Nous commençons avec les aspects micro et macro-juridiques. En effet, la notion de soi est cruciale. Elle est à la base de la résilience. Elle est indispensable à l'intelligence artificielle. Elle est essentielle à la survie d'un contrat. L'intelligence artificielle obéit aux lois de l'informatique, tandis que les contrats obéissent au droit. Nous pouvons étudier ces relations parallèles pour en trouver des éléments complémentaires et une approche transversale qui puisse répondre aux besoins d'un domaine

---

Kitano, H.: "*Systems Biology: A Brief Overview*''. Science, 295, 1662–1664 (2002) et Wagner, A.: ''*Robustness and Evolvability: A Paradox Resolved*''. ProcBiolSci, 275, 91–100 (2008).

[83] Les 4 R de Bruneau : ''*Overview of the Resilience Concept*'', par Michel Bruneau et Andrei Reinhorn, Actes du *8th U.S. National Conference on Earthquake Engineering,* avril 18-22, 2006, San Francisco, California, USA, accessible à : https://www.eng.buffalo.edu/~bruneau/8NCEE-Bruneau%20Reinhorn%20Resilience.pdf. (consulté le 13.12.2016)

[84] Inter-X, supra, note 11.

[85] Rapport ENISA : "*Enabling and managing end-to-end resilience",* p. 31, accessible à : https://www.enisa.europa.eu/publications/end-to-end-resilience/at_download/fullReport. (consulté le 03.01.2017) [End2End]

aussi complexe que le cyberspatial et de donner au droit et à l'autorégulation un rôle proactif légitime et valable sur le long terme.

	Legal Regulation	*Lex Informatica*
Framework	Law	Architectural Standards
Jurisdiction	Physical Territory	Networks
Content	Statutory/Court Expression	Technical Capabilities Customary Practice
Source	State	Technologists
Customized Rules	Contract	Configuration
Customization Process	Low Cost Moderate Cost Standard Form High Cost Negotiation	Off-the-Shelf Configuration Installable Configuration User Choice
Primary Enforcement	Court	Automated, Self-execution

Figure 8 *Le concept de* Lex Informatica *par Reidenberg. (*Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology , 76 Tex. L. Rev. 553 (1997-1998) Accessible à: http://ir.lawnet.fordham.edu/faculty_scholarship/42*)*

3.3 Les enjeux légaux: niveau macro-juridique vs niveau micro-juridique

Le développement durable dans le spatial occupe désormais une place importance sur le plan éthique depuis la création du groupe de travail sur la *Long-Term Sustainability* (LTS) à l'ONU, au *Committee on Peaceful Uses of Outer Space* (UNCOPUOS)[86]. Sans expressément se prononcer sur la résilience, le groupe jette les premières bases sur lesquelles nous pouvons formuler notre vision et justifier notre cause. De fait, une collaboration serait intéressante pour les fins de notre recherche. En effet, le développement durable est un concept plus large dans lequel nous insérons la résilience, un ingrédient opérationnel et essentiel :

> *"Since, among all definitions of resilience, according to Walker and Salt (2006) resilient systems are "sustaining ecosystems and people in a changing world" the resilience is intertwined with sustainability. Sometimes resilience is considered as one the indicators of sustainability. However the correlation between these two is more complicated. Moreover,*

[86] Le *United Nations Committee on Peaceful Uses of Outer Space* (UNCOPUOS), tenu par le *United Nations Office on Outer Space Affairs* (UNOOSA): http://www.unoosa.org/oosa/en/ourwork/topics/long-term-sustainability-of-outer-space-activities.html.

> *being resilient is essential to be really sustainable and they cannot be taken into account separately*[87]".

Le développement durable renvoie au développement qui rencontre les besoins du présent sans compromettre la capacité des générations futures à rencontrer leurs propres besoins[88] et il évolue en couches autour du noyau de l'équité intergénérationnelle[89]. En droit, cela nous intéresse particulièrement, puisque, d'un côté, l'équité est un pilier résilient, de la *common law*, car elle s'adapte selon la jurisprudence basée sur la *case law*, permettant aux juges de faire appel à leur bon sens selon les faits et les circonstances. Au début, l'*equity* évoluait en parallèle à la *common law* pour combler les manques de celle-ci en matière de flexibilité. D'un autre côté, la société a besoin d'adopter une obligation de diligence envers les générations futures et ainsi le principe d'équité intergénérationnelle fusionne le développement durable et le droit notamment grâce au droit environnemental. Comme la résilience nous vient de l'écologie et de la psychologie, nous pouvons donc continuer dans cette optique et créer une approche souple au niveau juridique, dans le domaine contractuel en raison de la commercialisation graduelle du spatial, nous inspirant de l'influence, du moins académique, du concept sur un nouveau type de gouvernance :

> *"Holling presented his findings on the **"multi-stable states**" he had discovered when applying his work to ecosystems. Contrary to the conventional belief that ecosystems oscillated around a single equilibrium, Holling discovered that ecosystems could "flip" between more than one stable state; they were both complex and adaptive and thus, characterized by surprise and inherent unpredictability.*
> (…)
> Aspects of law and governance marked deficient by legal commentators include incorrect understandings of the dynamics of natural systems; substantive goals that legitimize resource optimization; monocentric, uniscalar, and unimodal governing authority; and linear, front-loaded legal processes. On the other hand, law **and governance can enhance resilience by opting for a "systems view" of the object of regulation by enhancing monitoring, reflexivity, and information generation and diffusion; supporting multiscalar, polycentric,**

[87] "*Resilience Thinking: Sustaining Ecosystems and People in a Changing World*", par Brian Walker et David Salt, Island Press, 2012.
[88] "*Our Common Future*" Rapport par la *Brundtland Commission*, officiellement connue comme la *World Commission on Environment and Development* (WCED, 1987), accessible à: http://www.un-documents.net/wced-ocf.htm. Consulté le 13.06.2017
[89] Monteiro, supra, note 72.

> **and open governance; and by accommodating the adaptability of the legal system itself**[90]". (*Emphase ajoutée*)

La gouvernance adaptive a donc émergé de l'écologie et ouvre la voie à plusieurs perspectives quant à la gestion de changement d'écosystèmes à interdépendances complexes[91]. Ainsi, c'est un mode de gestion à niveaux multiples[92] qui inclut la réglementation, la politique, les débats, la négociation, la médiation, la résolution de conflit, les élections, les consultations ou protestations publiques, les processus de prise de décision, etc. Bref, beaucoup d'instances qui concernent un domaine aussi sensible que le spatial. De plus, comme celui-ci glisse vers une cybernétisation intense, nous prenons en compte la position de l'ENISA qui se prononce en faveur d'une gouvernance "hétérarchique" et "pluraliste". Celle-ci se définit comme:

> *"…a "third way" of ordering society, not through top-down state regulation or market self-regulation,* ***but through flexible regulations produced*** *through deliberation and cooperation amongst* ***a variety of stakeholders***[93]*". (Emphase ajoutée)*

Une telle approche est nécessaire pour faire face aux complexités transfrontalières propres au cyberspatial et comme nous avons déjà abordé le concept de polycentricité, nous soulignons ici leur similitude complémentaire :

> *"…involving systems in which "****political authority is dispersed to separately constituted bodies with overlapping jurisdictions that do not stand in hierarchical relationship to each other***[94]*". (Emphase ajoutée)*

La gouvernance adaptive et polycentrique destinée aux infrastructures spatiales critiques satisfait le niveau macro-légal de notre modèle. Ce niveau peut être considéré comme une première étape en étroite interaction avec l'étape subséquente qui traite du micro-légal : les contrats. En ce qui concerne la rédaction des clauses, nous pouvons nous inspirer du *Resilience Based Design* (RBD) qui consiste en une nouvelle manière de concevoir un système, en se concentrant sur les différentes capacités de la résilience en tant que balises :

---

[90] Humby, supra, note 58.
[91] "*Advancing adaptive governance of social-ecological systems through theoretical multiplicity*", par Timothy Karpouzoglou, Art Dewulf, Julian Clark, *Environmental Science & Policy* 57 (2016) 1–9.
[92] Un terme fréquemment utilisé par *le Stockhom Resilience Centre*. Voir: http://www.stockholmresilience.org/research/research-streames/stewardship/adaptive-governance-.html. (consulté le 12.12.2016)
[93] Humby, supra, note 58.
[94] Ibid.

> *The performance of an individual structure is not governed by its own performance, but it interacts heavily with the performance of other entities within the same community. Resilience based design (RBD) is a new fundamental way of looking at the problem, because interdependencies exists between the analyzed system and other structural and infrastructural systems. In this methodology, the building is not considered alone, but as a group of buildings using the "Portfolio Approach" which will allow regional loss analysis[95]".*

À travers cette perspective transversale, nous cernons le potentiel assez porteur de la résilience des infrastructures spatiales, au niveau juridique, que nous baptiserons ''*resiliensis spatialis*" tant sur le plan macro que micro et entamerons ainsi le vif du sujet : la clause. En RBD, tout comme en rédaction contractuelle, nous devons retrouver des indicateurs déterminant le seuil de résilience, de performance, d'incitatifs correspondants, etc. Or, à ce stade, nous rencontrons le problème des indicateurs quantitatifs et qualitatifs. Il y a débat entre plusieurs disciplines qui ne s'entendent pas sur les indicateurs. Le problème des indicateurs quantitatifs est qu'ils ne saisissent pas la variété et l'ensemble des enjeux et peut réduire, notamment en gestion de crise, des vies à des unités ou nombres sans aller plus loin. C'est pour cette raison que le qualitatif doit se développer davantage et produire des scénarios de plus en plus complexes, ce qui nous projette dans la problématique du *big data* et du *cloud security* pour stocker toutes ces données qui débouche sur le *quantum computing*, activement étudié par plusieurs États et entités de par le monde (États-Unis, Chine, Canada, Royaume-Uni, NASA, Google, D-Wave[96], Clyde Space, etc.). Une solution que nous proposons et d'appliquer notre ramification « *soft* **vs** *hard* » à « qualitatif (pour les scénarios) **vs** quantitatif (pour les coûts) ». Ces éléments sont très importants à un contrat et aux parties prenantes qui y négocient.

[95] "*Consideration of Resilience of Communities in Structural Design*", par Andrei M. Reinhorn et G. P. Cimellaro, dans ''*Performance-Based Seismic Engineering: Vision for an Earthquake Resilient Society*'', édité par M Fischinger, Chapitre: 27, Springer 2014. pp.401-421.

[96] Plus d'informations accessible à : https://ti.arc.nasa.gov/tech/dash/physics/quail/. Consulté le 20.03.2017. La cryptographie quantum est de nos jours testée à travers des signaux par satellite, par notamment les États-Unis, la Chine et le bientôt le Canada. Voir : http://www.ibtimes.co.in/global-quantum-communication-network-linking-computers-sensors-can-be-reality-thanks-china-731040. (consulté le 15.06.2017)

4. Solutions contractuelles pour la résilience de l'infrastructure spatiale

4.1. La résilience et les clauses contractuelles

Dans cette partie, nous nous allons traiter des différentes clauses contractuelles dans le spatial pour déterminer s'il existe en pratique des clauses définissant des standards de résilience ou des concepts similaires. Est-ce que les standards de qualité ou d'assurabilité du service représentent des indices potentiels de résilience? Nous allons ainsi étudier les mécanismes juridiques en place.

Nous ne pouvons parler de contrats dans le domaine du spatial sans mentionner quelques lignes sur la gestion des contrats (*contracts management*[97]), d'autant plus que c'est un domaine qui réunit différentes disciplines et ce, sur une période assez longue. UNIDROIT qualifie même ce genre de contrats de : "contrats à longue durée", nécessitant un plan directeur pour la gestion du programme, axé sur le long terme:

> *"This is especially important for satellite contracts where the* ***contract can be in effect for 18 to 20 years as the teams that conducted the negotiations are probably no longer involved in the contract*** *or even employed by the parties involved. No matter how detailed the contract documents are, there will be disagreements between the parties, but if these disagreements can be controlled and kept unemotional and practical, a satisfactory resolution will be found without resorting to the external remedies available to the parties as provided for in the contract*[98]*". (Emphase ajoutée)*

Dans notre cas, ils incluent la période précontractuelle (la phase d'approvisionnement et de soumissions, d'énoncé des travaux, des critères, etc.), puis la période de négociation contractuelle, d'exécution et de fin, toutes exigeant les termes les plus clairs et précis. Les parties prenantes participant à la rédaction des clauses doivent être présentes tout au long de la vie du contrat ainsi que suivre sa bonne exécution. Souvent celle-ci n'est surveillée de près que par les équipes techniques. Or il est important d'inclure les équipes juridiques et financières. C'est surtout le cas pour les ''*Service Level Agreements*'' (SLAs) qui ne comptent pas toujours les juristes à la table de négociation, ce qui est problématique et limite le rôle

[97] "*Contract Management*", par M. Elriz et P. Newman, Ch 20, dans *"Contracting for Space"*, éd. par LJ Smith and I. Baumann, Routledge, 2011. [Contracting for Space]
[98] Ibid.

proactif du droit spatial au niveau micro. Les SLAs proviennent des TIC[99] et sont adoptées dans le spatial étant donné sa cybernétisation. Ils décrivent la quantité et la qualité des standards de services et servent de base pendant les discussions entre acheteur et fournisseur et de référence pendant la vie du contrat ou lors d'une résolution de conflit. Ils peuvent contenir des listes techniques assez précises[100] et peuvent devenir un outil efficace et complémentaire au contrat[101], avec une incidence sur l'exécution contractuelle, malgré la nature généralement technique du contenu :

> *"During the negotiation phase, SLAs can be an excellent tool for helping the parties involved to improve their communications, to understand and reflect their mutual abilities and expectations, to clarify contractual responsibilities and thereby to bid the foundation for a long-term relationship. The SLA helps in structuring the discussions between customer and service provider about the details of the service, the requirements and expectations of the customer and the possible solutions the service provider can offer to meet these requirements and expectations. During the execution of the project, SLAs set the rules for constantly monitoring the quantity or quality of the service, for a fast resolution of technical problems and for measures to improve the service quality in the future. On this background, SLAs can also serve as a basis for effective dispute resolution[102]".*

Il faut néanmoins rester vigilant, car les SLAs peuvent entrer en compétition pendant la phase de négociation et il faut alors prendre le temps de les étudier en détail. Sinon, des superpositions contradictoires de SLAs différents peuvent entraîner de difficultés allant jusqu'à l'échec du programme[103]. En effet, il faut faire attention aux clauses concernant les services principaux et connexes (définis en détails), la durée, les standards de qualité, les indicateurs précis, méthodes et procédures, sanctions, etc.[104].

---

[99] "*The Use of Service Level Agreements in Space Projects*", by Ingo Baumann, dans "*Contracting for Space*", supra, note 97, p. 25.
[100] "*Performance and Warranty Articles in Space Industry Contracts*", par Ines Scharlach, dans "*Contracting for Space*", supra, note 97, p. 263. (Scharlach)
[101] Ibid, p. 305.
[102] Ibid, p. 304.
[103] Ibid. p. 310.
[104] Ibid.

Ainsi, les SLAs constituent une entente d'importance substantielle[105] et alors les fournisseurs visent un contenu aussi vague que possible possible, mais les que les acheteurs, au contraire, visent la précision exhaustive. Cette divergence peut donc être source de tensions, voire d'échec, si la rédaction n'est pas conforme et exacte. Les juristes ont, pour cette raison, un rôle inévitable, puisque ce document n'est pas exclusivement à caractère technique. Il a de fortes retombées économiques et juridiques ainsi que des incidences sur l'ensemble du projet.

La gestion de contrat, en tant qu'effort collectif, peut représenter une opportunité propice à l'exercice de la gouvernance polycentrique et contribuer à une culture organisationnelle adaptive et souple, introduisant ainsi des éléments de résilience. Cette souplesse correspond à la dynamique émergente de l'architecture orientée sur les services qui elle-même doit s'adapter aux changements des utilisateurs au sol tandis que les systèmes spatiaux impliquent des satellites en orbite difficile d'accès[106]. Dans cette optique, nous comprenons qu'une nouvelle gestion juridique de programme, de contrats, de SLAs, etc. s'impose[107] et que celle-ci comporte les divers éléments évoqués.

Dans le domaine spatial, la commercialisation renforce le droit privé dans le secteur et donc dans les contrats. Les contrats spatiaux ne sont pas nouveaux ni totalement différents en soi, mais l'agencement et l'adaptation de certaines clauses, souvent inspirées du secteur des TIC, les rend spécifiques à un environnement hautement technologique et à haut risque. Les parties prenantes à genre de contrat sont généralement les fabricants, les fournisseurs, les opérateurs, etc.), et l'objet implique l'infrastructure spatiale ainsi que les différents services (comme la production, le lancement, l'opération du satellite ou du signal, la vente, l'imagerie, la propriété intellectuelle, etc.). Les interdépendances entre les intérêts

[105] "*Export Control Issues in Space Contracts*", par Matthias Creydt and Kay-Uwe Horl, Ch 24, in "*Contracting for Space*", supra, note 97.
[106] Scharlach, supra, 100.
[107] "*Conclusions and Outlook*", L. J. Smith and I. Baumann, Ch. 34, in "*Contracting for Space*", supra, note 97.

nationaux, internationaux, institutionnels et commerciaux[108] de ces contrats nous ont poussés à analyser des dizaines de contrats concernés et à en évaluer les clauses préconisant l'assurabilité du service et à classer celles-ci dans un tableau qui ensuite nous aidera à rédiger un prototype de clause, puisque nous avons déterminé que les contrats ne contiennent pas suffisamment de clauses en ce sens. Ce faisant, nous en avons tiré des leçons et nous avons remarqué certaines discordances entre la pratique et l'académique. Par exemple, en théorie, il y a un certain débat autour des incitatifs de performance avant ou après le transfert de risque lors du lancement ou en orbite[109], mais ces incitatifs seraient devenus contre-productifs, puisque pris pour acquis[110]. Or, ils sont toujours présents dans la pratique et nous croyons que nous devons y recourir de façon modérée pour convaincre les parties prenantes à prendre en considération la clause qui doit être introduite graduellement afin que la gestion du changement se fasse de façon fluide.

Le droit contractuel occupe une place clé dans le spatial non seulement en raison de la privatisation, mais aussi du fait que le droit spatial se résumait, à l'époque, à quelques grands traités internationaux rédigés dans les années soixante, soixante-dix et quatre-vingt. En fait, le ''*Outer Space Treaty*'' (OST) de 1967, a cinquante ans et il ne comporte que 17 articles assez généraux pour encourager une grande adhésion. Il s'ensuivait que les spécificités et technicités étaient donc établies par réglementation nationale et par contrats cadres. Les États jugent maintenant que le droit spatial international comporte des lacunes ou ne satisfait pas leurs intérêts et alors décident de créer leur propre législation nationale, qui, le remarque-t-on, diffère selon leur interprétation de l'OST, de façon de plus en plus tranchante. Cette législation se rapproche des dispositions contractuelles, les encadrant graduellement, sachant que ces législations ont impliqué le secteur public et privé au

[108] "*Typology of Contracts in the Space Sector*", par Laurence Ravillon, dans ''*Contracting for Space*'', supra, note 97, p. 161.
[109] En France, ces incitatifs sont nommés: primes or clauses de performance or "d'intéressement en orbite".
[110] "La Prévention Contractuelle du Contentieux", par Julia Heinich, dans "Le Réglement des Différends dans l'Industrie Spatiale", actes de colloque, CREDIMI 2015, édité par Laurence Ravillon, Lexis Nexis, 2016.

processus de rédaction. Le secteur privé a donc eu son mot à dire et nous estimons que la résilience sera intégrée aux futurs processus de dialogue.

Ces législations, de plus en plus précises, affluent. Bien que la réglementation se fasse généralement en respect des grands traités, quelques dispositions divergentes, mais non sans importance, entraînent des tensions sur la scène internationale, car elles suscitent le débat entre experts qui craignent une future situation de ''*forum shopping*". La France a adopté une législation nationale en 2008, très précise, qui décrit en détail ce qui est requis des parties dans le secteur pour l'obtention de licences et d'autorisations, conformément aux exigences de l'article VI de l'OST de 1967. Les candidats à une licence doivent, par exemple, fournir aux autorités des garanties techniques, financières, professionnelles et morales et de prouver que 1) le projet est conforme à la réglementation et qu'il ne compromet pas les intérêts de la défense nationale française ou de ses engagements internationaux[111]; 2) que la vérification générale des personnes morales confirme une bonne gestion, un programme de contrôle de qualité, d'un programme de formation et de perfectionnement du personnel, le respect des normes internationales et l'absence de faillite; 3) la vérification technique du projet, soit la mise à disposition de documents aux autorités afin que celles-ci en vérifient les normes de sécurité, de la propriété, de la santé publique et environnementale, de prévention de risques, de plan de gestion de crise (nucléaire, débris spatiaux, collision, protection planétaire, etc.)[112]. Si ces mesures ne figurent pas dans les documents techniques ou dans les contrats, elles se retrouvent dans la loi. Ainsi, si le privé réussit à convaincre le secteur public de légiférer sur la résilience, si celle-ci ne sera pas stipulée dans le contrat, la loi la prévoira selon des standards génériques, ce qui poussera les parties co-contractantes à négocier leurs propres termes.

[111] Article 4.2 de la Loi française sur les Opérations Spatiales (LOS) du 3 juin, 2008. Accessible à : http://download.esa.int/docs/ECSL/France.pdf. (Consulté le 22.11.2016) [LOS]

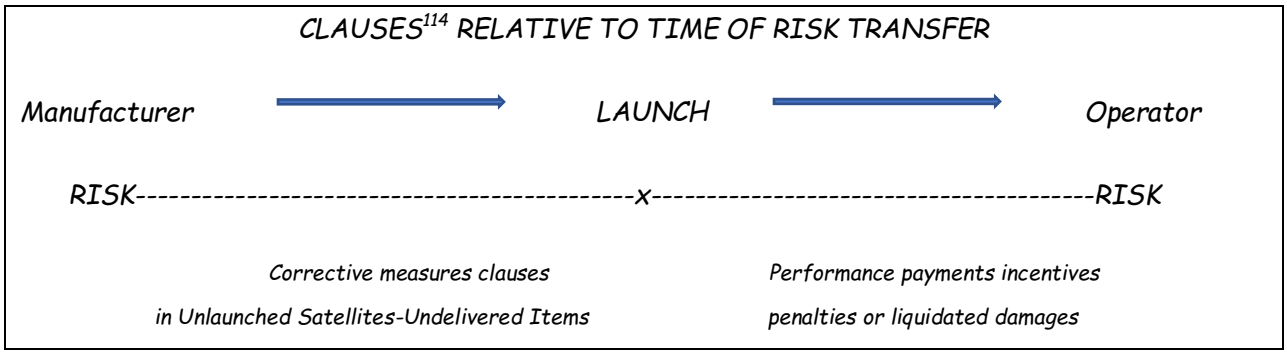
[112] "*Space Contracts: The Legal and Financial Liability Regime*", par Mireille Couston, dans "*Contracting for Space*", supra, note 97, pp. 321-322. (Couston)

Afin de déterminer le degré d'assurabilité et de continuité des services, missions et infrastructures spatiales, nous avons étudié plusieurs dizaines de clauses contractuelles, de notions théoriques, dispositions réglementaires et analyses de cas. Les clauses que nous avons sélectionnées pour étude, en raison de leur pertinence, sont celles afférant au transfert de risque, aux mesures correctives, aux incitatifs de performance et de paiement, de renoncement mutuel de recours (*cross-waivers*), d'obligation de réparation (*duty to correct*), de garanties, de force majeure, de solutions de rechange (*back-up solutions*), etc.

Nous abordons en premier les contrats d'achat de satellites. Ces contrats lient les fabricants (ex: Boeing, Lockheed Martin, Space Systems Loral, Orbital ATK, Airbus and Thalès Alenia Space) et les acheteurs (opérateurs, agences nationales, organisations internationales, clients privés, etc.), à travers un processus de soumissions. Cependant, l'architecture contractuelle est bien plus complexe en raison des fournisseurs et sous-traitants, car elle entre dans la catégorie de contrats de vente. De plus, comme la fabrication implique du personnel, de l'équipement, des installations et des services, celle-ci peut être classée comme contrat de prestation de services (maintenance, support technique, informations sur les fréquences et données géostationnaires, etc.) ; tendance à la hausse si l'on inclut l'architecture spatiale orientée vers les services. Finalement, nous retrouvons aussi les contrats de prestations de services en orbite, qui imposent un fardeau de risques plus lourd au fabriquant, en plus d'une clause de responsabilité en cas de défauts[113].

Selon la ligne du temps sur la page suivante, l'on peut mieux visualiser le processus de transfert de risque en ce qui concerne les opérations spatiales. Le scénario classique est celui du lancement de raquettes. Nous n'allons pas traiter des ballons stratosphériques, puisqu'encore très récents et dont le régime juridique reste encore à définir.

[113] En France France, selon l'article 1645 du Code Civil. (Revue française de droit aérien et spatial, p. 203, 1998).



Dans le cas des fusées, le risque est transféré lors du lancement tout juste après le point de non-retour. Le lancement en tant que tel doit faire l'objet de précisions qui déterminent exactement le moment du transfert de titre et de risque, pour prévenir toute ambiguïté, or dans les faits, ce n'est pas si simple. Pour ce qui est des contrats de satellites, le risque est transféré en orbite, après l'acception initiale et l'acceptation finale des services suite à la période de tests en orbite (*In Orbit Testing* ou *IOT*), période durant laquelle le client peut déjà commencer son activité commerciale:

> *"8.5 IN-ORBIT TESTING AND FINAL ACCEPTANCE OF SATELLITES.*
>
> *(a) IN-ORBIT TESTING.*
>
> *(1) Upon arrival of each Launched Satellite at its Specified Orbital Location, Contractor shall perform tests and analyses on such Satellite in accordance with the In-Orbit Test Plan, developed by Contractor and approved by Customer, pursuant to the requirements of Exhibit B (SOW) and Exhibit D (Test Plan Requirements) to determine whether and to what extent such Satellite meets the requirements set forth in such In-Orbit Test Plan.*
>
> *(2) For each Satellite, promptly upon completion of Pre-Eclipse In-Orbit Testing, Contractor shall conduct an in-orbit acceptance review and provide a documentation package setting forth the in-orbit test data required by, and in a condition fully conforming to, the requirements of Exhibit B (SOW) and Exhibit D (Test Plan Requirements). **"Initial Handover" of a Satellite shall occur upon completion of Pre-Eclipse In-Orbit Testing and provision of such In-Orbit Acceptance Test Review documentation package. Customer may begin commercial use of a Satellite upon Initial Handover of such Satellite**[115]. (Emphase ajoutée)*

[114] Voir annexe 5.1 pour le cas des contrats de satellites (acceptation initiale, finale et transfert en orbite de titre, risque).
[115] XM Sat, supra, note 65.

Des distinctions supplémentaires peuvent être prévues dans les contrats:

> *9. TITLE AND RISK OF LOSS*
>
> *9.1 TRANSFER OF TITLE.*
>
> *Transfer of title, free and clear of all liens and encumbrances of any kind, to each Deliverable Item (other than Satellites)* ***shall pass to Customer at Final Acceptance of such Deliverable Item. Transfer of title, free and clear of all liens and encumbrances of any kind, to each Satellite shall pass to Customer at the time of Initial Handover*** *of such Satellite, or, in the event of a Constructive Total Loss or Total Loss of such Satellite, at the time of such Constructive Total Loss or Total Loss, or, in the event such Satellite is placed in storage, as provided in Article 14.4 (Storage).*
>
> *9.2 TRANSFER OF RISK OF LOSS.*
>
> *Risk of loss or damage to each Deliverable Item shall pass to Customer at Final Acceptance of such Deliverable Item; provided, however, risk of loss or damage to each Satellite and its Launch Vehicle shall pass at Launch of such Launch Vehicle; provided, however, (x) in the event of a Terminated Ignition for a Satellite, risk of loss or damage for such Satellite and its Launch Vehicle shall revert to Contractor upon such Terminated Ignition and shall again pass to Customer upon the subsequent Launch of such Satellite and its Launch Vehicle, and (y) in the event a Satellite is placed in Storage, risk of loss or damage to such Satellite shall pass in accordance with Article 14.4 (Storage)*[116]*'. (Emphase ajoutée)*

Ce qui arrive après l'acceptation peut être résumé par l'exemple des clauses et conditions générales d'approvisionnement de l'ESA (*GCC*[117]), à la clause 20:

> *"CLAUSE 20: LIABILITY AFTER ACCEPTANCE*
>
> *After Acceptance of the Deliverable(s) by the Agency, the Agency shall have no claim against the Contractor and/or its Subcontractors and suppliers for any damage resulting from the use of the Deliverable(s) by the Agency. Furthermore, the Agency shall indemnify and hold the Contractor harmless and/or its Subcontractors and suppliers at whatever level for any such claims damages, losses and expenses (including legal fees and expenses) raised against it by a Third Party.* ***However, the Contractor shall indemnify and hold the Agency harmless against all claims, damages, losses and expenses (including legal fees and expenses) in case: a) such damage occurs to the Agency or a Third Party and arises from gross negligence or wilful misconduct on the part of the Contractor and/or its Subcontractors and suppliers at whatever contractual level; or b) the Parties agree at Contract conclusion***

[116] XM Sat, supra, note 65, art 9.

[117] La version de 2015 des GCC est accessible à : http://esamultimedia.esa.int/docs/LEX-L/Contracts/ESA_REG_002_rev2_new_Annex1_revised.pdf. (consulté le 17.04.2017) [GCC]

> ***that the items developed under the Contract shall be made available to consumers against commercial fee by the Contractor****. In case a Third Party brings such a claim against the Agency the Contractor shall be bound to join the Agency as co-defendant in the proceedings…". (Emphase ajoutée)*

Le transfert nous intéresse afin de déterminer quelles assurances s'appliquent et aussi qui serait responsable de la continuité de la mission afin de pouvoir établir quels seraient les besoins en termes de résilience, de contrôle de qualité et de responsabilité, tout en tenant compte des clauses de non-recours, car jusqu'au transfert, le fabricant maintient son devoir de réparation[118]:

> *"13.2 DUTY TO CORRECT.*
>
> *(a) Without limiting the obligations of Contractor or the rights of Customer under this Contract, prior to Launch of any Satellite or Delivery of any other Deliverable Item,* ***Contractor shall, at its expense, promptly correct any Defect related to any Deliverable*** *Item or component thereof that Contractor or Customer discovers during the course of the Work or from other spacecraft of a class similar to the satellites being built by Contractor, and notwithstanding that a payment may have been made in respect thereof, and regardless of prior reviews, inspections, approvals, or acceptances. This provision is subject to the right of Contractor to have any items containing a Defect returned at Contractor's expense to Contractor's facility for Contractor to verify and correct the Defect." (Emphase ajoutée)*

Une fois le titre et le risque transférés, le client doit, selon ses obligations contractuelles, verser des primes de performance ou appliquer des pénalités, dépendamment du service rendu[119]. Des exemples d'incitatifs et de services en orbite livrés à temps donnant droit à des primes se lisent comme suit:

> *"(e) If Contractor Launches both the first Satellite and the second Satellite on or before December 31, 2000, Customer shall pay Contractor an amount equal to Six Million Dollars ($6,000,000) (in addition to the Contract Price) on or before thirty (30) Calendar Days after Launch of the second Satellite[120].*

---

[118] Pour une clause complète sue les mesures correctives, voir : CORRECTIVE MEASURES IN UNLAUNCHED SATELLITES AND OTHER DELIVERABLE ITEMS (reprise de XM Sat, supra, note 65) à l'annexe 5.2.

[119] "*Long-term contract*" se réfère à un contrat dont l'éxecution se déroule sur une période qui implique une relation complexe entre les parties à travers le temps.(art 1.11 de l'UNIDROIT *Working Group on Long-Term Contracts Principles,* 2016, accesible à: http://www.unidroit.org.cloud.seeweb.it/english/governments/councildocuments/2016session/cd-95-03-e.pdf; http://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016. (consulté le 20.03.2017)

[120] XM Sat., supra, note 65, Art. 7 (e).

Ou encore:

> *12.2 IN-ORBIT PERFORMANCE INCENTIVES.*
>
> *Contractor represents that each Satellite will meet the criteria set forth or referenced in Article 12.3 (Calculation and Earning of Incentive Amounts) during the Orbital Design Life of each Satellite. To the extent any Satellite satisfies the criteria set forth or referenced in Article 12.3 (Calculation and Earning of Incentive Amounts), Customer shall pay Contractor Incentive Amounts, to be calculated as specified in Article 12.3 (Calculation and Earning of Incentive Amounts). The total aggregate amount of incentives paid by Customer to Contractor for any and all Satellites shall not exceed the Total Amount at Risk, plus interest thereon calculated pursuant to Article 12.6(b) of this Contract."*

Le devoir de réparation ne peut, pour l'instant, concerner que le *software*, car il s'agit de corriger des anomalies à distance. Celles-ci peuvent se faire au niveau informatique, mais impliquer aussi des opérations ayant un effet sur la structure d'un satellite, comme déployer des instruments ou changer leur angle pour permettre un fonctionnement en mode altéré, ou de configurer les systèmes de réserve, etc. Ainsi la résilience revêt un aspect majoritairement informatique et c'est pour cela qu'étudier les facettes de la cyber-résilience est important. Toutefois, cela peut aller plus loin dans le cas d'offres de services en orbite comme la réparation, ce qui pourra faire l'objet de nouveaux modèles d'affaires dans le futur. Les services en orbite se développent en ce moment pour ce qui est de la récupération de débris spatiaux. Il y a de l'innovation juridique à l'horizon, et nous nous demandons alors quel sera l'impact des clauses de non-recours dans une économie cislunaire à venir, ainsi que dans les contrats à long terme qui auront une période supérieure à l'heure actuelle. Les clauses de non recours mutuelles limitent les attentes de dommages-intérêts de nature pécuniaire, sauf en ce qui concerne les dommages causés au tiers (environnement, etc.) et, puisque le marché des assurances dans le domaine spatial est en difficulté, nous sommes d'avis que des obligations flexibles, de nature contractuelle, qui préconisent des mesures de résilience fourniraient une solution fort pertinente. Le renoncement mutuel de recours leur impose un standard tacite de qualité plus élevé. En effet, les *best efforts* (qui se définissent comme la diligence d'un professionnel prudent et raisonnable, procurant des

services de lancement ou de fabrication de lanceurs[121]) pour assurer la continuité du service : 1) engagent proactivement les parties à assurer une qualité réciproque et 2) constituent ainsi un terrain propice à la résilience[122], dans un environnement à haut risque. Cette dynamique fait en sorte que le renoncement de recours pousse vers des solutions contractuelles, de négociation et de responsabilité tacite de qualité. Au contraire, une dynamique coercitive (*police power*) favorisée par une menace assez présente de poursuites aurait dissuadé beaucoup d'acteurs à entrer sur ce marché risqué, ce qui ne cadre pas avec la privatisation et la concurrence graduelle dans le secteur. Nous considérons donc ce type de clause comme un pas vers la maturité, la flexibilité et la résilience.

Comme les contrats spatiaux ont de plus en plus pour objet les services, la résiliation ou la fin du contrat devient une option de moins en moins intéressante, en raison du nombre encore restreint d'acteurs et de fournisseurs dans le secteur qui puissent prendre le relais. Ceci explique l'importance accordée tant aux incitatifs qu'aux pénalités. Prenons par exemple les termes d'approvisionnement tels qu'établis par l'ESA dans ses *General Clauses and Conditions (GCC)*, à l'article 17, qui concernent les primes de performance ou encore les pénalités en cas de livraison tardive compromettant la mission, ou qui les mitige si le retard n'est pas dû à la négligence du co-contractant, ou encore permettant la résiliation en cas de non-livraison:

> *"17.1 Penalty*
> *17.1.1 Penalty for Late Delivery*
> *If the Contractor fails to comply with the Delivery date laid down in the Contract, it shall be liable to a penalty according to the scale of penalties attached hereto as Annex III, except where special provisions are made in the Contract. Penalties for late Delivery are due based on the mere fact of expiry of the time-limit and without formal notice, except when the Agency has formally renounced such penalties.*

[121] Ravillon, supra, note 63.

[122] En analysant ces clauses, nous devons mentionner que les provisions relatives aux assurances spatiales sont requises par la loi en ce qui concerne le fabriquant ou opérateur pour couvrir les préjudices causés aux tiers. L'assurance pour préjudice couvre une variété de dommages : design défecteux qui aurait put être corrigé lors de tests, mais observé seulement après lancement ; erreurs de la part de la station de contrôle conduisant à la perte de biens spatiaux ; tests inadéquats malgré l'adhésion aux normes industrielles, mauvaise performance mettant en jeu la mission, etc. Il n'y pas d'obligation de trouver la source de l'échec, mais d'enquêter et de dévoiler les résultats à l'autre partie. De plus, en ce qui concerne les satellites de secours (remplacement), la garantie d'exécution, par laquelle les parties prouvent en avoir les moyens, est obligatoire (pour le fabriquant et par le client). Cette clause s'appelle: ''*SECURITY FOR PERFORMANCE INCENTIVE PAYMENTS CLAUSES*''.

(…)
17.1.4 Objection to Penalties
The Contractor may object within thirty (30) Days from the date of receipt of notification. Failing such objection within this period, the Contractor shall be deemed to have accepted the penalties.
(…)
17.2 Performance related Penalties
A penalty scheme linked to performance may be introduced in the Contract. Such scheme ***shall be linked to the non-fulfilment of performance*** *parameters as specifically defined in the Contract.*
17.3 Incentives
In combination with a penalty scheme, an incentive scheme may be introduced in the Contract. Such ***scheme shall be linked to the fulfilment of contractual requirements including delivery dates and performance parameters as specifically defined*** *in the Contract". (Emphase ajoutée)*

Nous pouvons constater qu'une résiliation facilitée n'est pas la priorité.

En effet, la priorité est plutôt d'optimiser les chances de succès de la mission ainsi que l'assurabilité des services, ce qui requiert une bonne relation contractuelle entre les parties. Malgré ces efforts axés sur l'exécution contractuelle d'un programme, l'ESA, en tant qu'organisation intergouvernementale, se réserve le droit exclusif de résiliation unilatérale, puisque les décideurs sont les États membres qui, sous le couvert de la souveraineté, peuvent se retirer à tout moment, à condition de dédommager les co-contractants à hauteur du montant contractuel[123]". Ainsi, le pouvoir de résiliation subsiste. Celle-ci peut aussi survenir dans plusieurs éventualités comme en cas de force majeure[124], qui impose l'obligation de notification et le fardeau de la preuve sur la victime de l'événement. Selon les GCC et les exigences fixées par les États membres, si la victime n'a pas notifié l'ESA après trois mois, les parties peuvent soit renégocier le contrat, soit le résilier. Il est opportun de noter que les anciennes versions des GCC n'avaient pas de définition précise de la force majeure. Le terme était donc interprété différemment selon les juridictions, ce qui pouvait causer des

[123] "*Space Contracting within the Framework of the European Space Agency*", by Gunilla Stjernevi et Eleni Katsampani, dans "*Contracting for Space*", supra, note 97 p. 181.
[124] GCC, supra, note 117, Clause 33.

ambigüités. Alors, la nouvelle version spécifie clairement en quoi cela consiste. Nous y voyons un parallèle à faire avec la résilience pour réduire les confusions[125]. Ce qui a poussé l'ESA à y apporter des précisions est le fait que les co-contractants essayent de faire tourner les termes en leur faveur en jouant sur la clarté ou l'ambigüité. Pour un client, la force majeure doit être aussi claire et limitée que possible alors que pour le fabricant, elle aurait intérêt à rester vague et inclusive, pour se protéger. L'ESA a pris le parti de protéger la mission et donc de clarifier le terme.

Un autre exemple de priorité de la mission l'emportant sur le dédommagement pécuniaire, dans les GCC, se retrouve dans les diverses clauses de garanties, notamment les clauses 21.2, 21.3, et 21.4. Si une composante comporte un défaut, la partie dont elle provient n'est pas tenue de dédommager l'autre partie, mais doit remplir son obligation d'enlever, réparer et remplacer la pièce défectueuse, à ses propres frais, avant le lancement. De plus, ceci s'applique aussi aux défauts systématiques, présents dans d'autres composantes identiques, nonobstant le fait qu'elles soient ou non couvertes par le contrat:

> *"CHAPTER V WARRANTY CLAUSE 21: SCOPE OF WARRANTY*
>
> *21.1 The provisions set forth in the present chapter shall be applicable to all items contained in the Deliverables under the Contract with the exception of commercial, off-the-shelf, Third Party products, not integrated in the Deliverable(s). In this case the warranty of this product shall apply. The Contractor undertakes, within this warranty obligation, to remedy at its own expense and with due diligence any Defect which may appear in the Deliverables during the period stated in clause 22 below.*
>
> *21.2 The Contractor's warranty obligations for Deliverable hardware shall cover the cost incurred by the Contractor and/or its Subcontractors of removal and replacement or repair at the Contractor's option. The Contractor's warranty obligations for deliverable software shall cover the cost of correcting any Defect to the deliverable software. The warranty for both hardware and software Deliverables shall include the supply and updating of appropriate Documentation, as well as the cost of reinstallation and re-testing incurred by the Contractor*

[125] Par exemple, nous pouvons parler de la définition de force majeure dans IRIDIUM, 2010: "*Force Majeure means acts of God, acts of government (in its sovereign and not contractual capacity), acts or threat of terrorism, riot, revolution, hijacking, fire, strike (other than a strike involving the employees of Contractor, Customer or their respective Related Third Parties), embargo, sabotage, or interruption of essential services or supplies".* Pour plus d'informations, voir annexe 5.5 (*CONTRACT FOR LAUNCH SERVICES No. IS-10-008 Between Iridium Satellite LLC and Space Exploration Technologies Corp (Iridium 2010): 2.5 Primary and Backup Launch Site*, accessible à : http://investor.iridium.com/secfiling.cfm?filingid=1193125-11-81407&cik. (consulté le 02.02.2017) [Iridium]

and/or its Subcontractors. The warranty shall also cover all travel expenses, packing and transport charges incurred by the Contractor and/or its Subcontractors in connection with repair or replacement. If the Contract stipulates, in addition, a guarantee for protection and packaging, the warranty prescribed above shall operate from the date of expiry of the packaging guarantee.

21.3 If a Defect observed in the course of the warranty period is due to a technical or design error of a systematic nature within the Deliverable/ or part thereof, the provisions of this chapter shall apply to all identical, unlaunched Deliverables/or parts thereof. A Defect is considered as ***systematic if it can be demonstrated that the Defect will be reproduced in a Deliverable/or part thereof, if exposed to representative conditions as applied when the Defect was observed.***

21.4. The Contractor's liability under the provisions of this chapter shall not extend to:
a) Defects arising from the misuse of the Deliverables after Acceptance;
b) Defects in materials, assemblies or other supplies issued by the Agency for incorporation therein, provided always that the Contractor shall have properly exercised its duties as custodian of such items and shall have incorporated them in accordance with the requirements of the Contract;
c) compensation for damage resulting from the use of items covered by the Contract after Acceptance as per clause 20 above;
(…)[126] *(Emphase ajoutée)*

CLAUSE 22: WARRANTY PERIOD
22.1 The warranty for non-flight items shall run for a period of one (1) year from Acceptance by the Agency of the Deliverable(s) (hardware and software). The warranty for flight items shall run for a period of one (1) year from Acceptance by the Agency of the Deliverable(s) (hardware and software) or until lift-off, whichever is earlier.
22.2 Where Defects in items are remedied under the warranty, the warranty period shall be extended automatically by a period equal to that during which the Deliverables/or part thereof were not available to the Agency for their intended use. For Deliverables/or part thereof replaced, the warranty period shall recommence at the date of replacement. For Deliverable/or part thereof repaired or modified, the warranty period shall be prolonged automatically by a period equal to that during which the items were unavailable for their intended use.
22.3 In the event that, in addition to the nominal warranty stated herein, a post-launch warranty of Flight Systems (hardware and software) is required, conditions of such warranty will be specified in the Contract."

D'autres types de clauses de garanties sur le marché peuvent se lire comme suit:

"18.3 WARRANTIES FOR DELIVERABLE ITEMS.

[126] *GCC*, supra, note 117.

(a) SATELLITES.

Contractor represents that each Satellite furnished under this Contract shall be free from Defects other than Defects waived in writing by Customer. This representation shall begin on the date of Initial Handover of a Satellite and Customer's exclusive remedy for breach of this representation is set forth in Article 12 (In-Orbit Performance Incentive Payments).

(b) SATELLITE CONTROL SOFTWARE AND GROUND ENCRYPTORS.

Contractor represents and warrants that the Satellite Control Software and Ground Encryptors Delivered under this Contract shall be free from Defects other than Defects waived in writing by Customer. This warranty shall begin on the date of Final Acceptance of the respective Deliverable Item and run for one (1) year.

(…)

(f) SERVICES.

Contractor represents and warrants it will perform the Work in accordance with the highest professional standards of the commercial aerospace and satellite communications industry practice for work similar in type, scope, and complexity to the Work.

(…)[127]*".*

Nous pouvons voir que ces clauses garantissent surtout la qualité d'un produit ou service ainsi que l'obligation de réparation. Si toutefois cela ne suffit pas à rétablir l'exécution du programme, les parties sont libres de négocier ou éventuellement de résilier, mais ce faisant, elles ont encore la charge de s'entendre grâce aux clauses de résolution de conflit et d'arbitrage, le cas échéant[128]. Un contrat spatial peut durer plusieurs décennies et comporter un grand *turnover* au niveau du personnel qui ne sera donc pas nécessairement impliqué tout au long de la vie et de la gestion du contrat.

Un autre facteur donne plus d'ampleur au *turnover*. Il ne concerne plus seulement le personnel, mais aussi les parties prenantes comme les co-contractants et sous-traitants en raison de la privatisation graduelle en cours qui érode les monopoles traditionnels au profit de futurs regroupements privés. De plus, de nouveaux États joignent le cercle jusqu'ici assez

[127] XM Sat, supra, note 65.
[128] Voir annexe 7 : *GCC Clause 35 on Dispute Resolution.*

restreint des "puissances spatiales". Ainsi, le nombre d'États parties à un lancement (qui préparent le site de lancement, la charge utile et l'intégration du satellite au lanceur) s'accroît et d'autres pays que les États-Unis, la Russie, la Chine, le Japon, la France, l'Inde ou le Brésil convoitent cette possibilité. Bien que cela se fasse dans une ambiance de compétition, il existe des alliances interétatiques de plan B en ce qui concerne les sites de lancement, appliquant ainsi le principe de redondance des systèmes. Par exemple, la *Launch Services Alliance*[129] regroupe, depuis 2003, Arianespace et Mitsubishi Heavy Industries (et autrefois Boeing Launch Services qui a quitté en 2007) pour assurer la continuité des services de lancement si l'un des sites devient inopérant. Nous trouvons ce genre d'entente dans diverses clauses contractuelles de services de campagne de lancement alternatifs[130]:

> *"2.5 Primary and Backup Launch Site: The primary Launch Site for all Launch Services shall be VAFB and KWAJ is designated as the alternate Launch Site in the event of VAFB unavailability as provided for in this Section 2.5.*
>
> *2.5.1 Change of Launch Site* ***Not Attributable to Contractor****. No later than [***…***] months (or such shorter period that Customer may reasonably agree to in writing) prior to any scheduled Launch, Contractor shall (..) include in such notification: (i) the reasons for Launch Site or Launch Range unavailability; (ii) the duration of such Launch Site or Launch Range unavailability; and (iii) the next available Launch Opportunity at VAFB (to the best knowledge of Contractor at that time) and at KWAJ…*
>
> *2.5.2 Change of Launch Site* ***Attributable to Contractor****. No later than [***…***] months (or such shorter period that Customer may reasonably agree to in writing) prior to any scheduled Launch, Contractor shall (…) include in such notification: (i) the reasons for Launch Site or Launch Range unavailability; (ii) the duration of such Launch Site or Launch Range unavailability; and (iii) the next available Launch Opportunity at VAFB (to the best knowledge of Contractor at that time) and at KWAJ. Within [***…***] Fee associated with any Launch schedule adjustments as provided for in Section 6.2 shall apply to Contractor…*[131]*".*

Les contrats de lancement (*Launch Services Agreement* ou LSAs), constituent un contrat de service au niveau international et donc peut inclure plusieurs États[132]. Typiquement, il

[129] Pour plus de détails, voir : http://h2a.mhi.co.jp/en/news/past/2007/0424.html. (consulté le 04.02.2017)
[130] Iridium, supra, note 122. L'article 2.5 spécifie que ''*the primary Launch Site for all Launch Services shall be VAFB and KWAJ is designated as the alternate Launch Site in the event of VAFB unavailability as provided for in this Section 2.5*". Voir la versio en ligne à : http://investor.iridium.com/secfiling.cfm?filingid=1193125-11-81407&cik. (consulté le 03.03.2017)
[131] Ibid.
[132] ''Caisse Centrale de Réassurance v. Arianespace'', Cour d'appel, Paris, 2007, cité dans chapitre : ''Sommaire de Jurisprudence des Cours et Tribunaux'', par Mourre, A. et Pedone, P. Gazette du Palais, du 13 au 17 juillet, 44, dans Ravillon, supra, note 63.

comprend des définitions, délais, description du service à rendre (comme la préparation du site de lancement, du véhicule et des interfaces de la charge utile, la coordination d'un autre créneau de lancement en cas de report, etc.[133]), contrepartie, disposition en cas de retard, incitatifs, pénalité, coûts de remplacement, garanties, clauses de non-recours réciproques, assurances, force majeure, résiliation, arbitrage, loi applicable, confidentialité, entrée en vigueur, autorisations, etc.[134]. Ces clauses n'ont rien de nouveau en elles-mêmes, toutefois leur agencement et relation au standard de *best efforts* font place à l'innovation juridique, dans un environnement sensible et à haut risque. Celui-ci, rappelons-le, requiert des clauses de renoncement mutuel de recours afin de protéger les co-contractants et les sous-traitants contre les menaces potentiellement élevées de poursuite. Le renoncement est imposé par la loi quand il s'agit des LSAs et sujet à négociation entre co-contractants pour ce qui est des contrats de satellites (transpondeurs, etc.).

Ainsi, comme dans les contrats de lancement, les législations nationales (ex: la LOS ou la loi américaine de 1984 sur les lancements commerciaux, etc.) exigent des clauses de non recours. Ces clauses s'appliquent quand la faute n'est pas intentionnelle, ni due à la victime, ou encore si le contrat prévoit d'autres dispositions. Une clause de non recours se lit comme suit:

- *"In case of damages to a third party: in this scenario and when the damage has given rise to a compensation by the operator or to the application do the same guarantee it is provided that the liability of the participants to the operation or to the manufacture of the given object cannot be sought. The operator and the state thus abandon the possibly of any remedy[135].*
- *In case of damage to a person having participated in the operation or in the production of the space object concerned: in this case, the law stipulates that the liability of other persons cannot be sought. It is the principal of mutual waiver of liability among participants to a space operation[136]".*

[133] Ibid.
[134] Ibid, p. 164
[135] Couston, supra note 112, p. 326
[136] Ibid.

Par le passé, la jurisprudence n'imposait pas de telles clauses si elles n'étaient pas expressément stipulées dans le contrat, comme dans le cas *Intelsat v. Martin Marietta*. La loi, comme il était spécifié dans la license attribuée par l'autorité compétente au candidat, prévoyait que les clauses de renoncement mutuel de recours devaient être incluses dans le contrat, si les parties souhaitaient s'en prévaloir et que ce n'était pas à la loi de l'imposer:

> *"In the event that Martin Marietta fails to enter into, or fails to require other private party launch participants to enter into, waivers of claims required under this subparagraph (a), Martin Marietta shall indemnify and be responsible for any and all liability, loss or damage resulting from such failure[137]".*

Cependant, les choses ont changé depuis, et la loi américaine les impose bel et bien pour les activités liées au lancement et ainsi que pour les activités liées aux opérations sur satellites, sauf si, dans ce dernier cas, le contrat prévoit le contraire:

> *"SEC. 107. CROSS WAIVERS.*
> *Section 50914(b)(1) is amended to read as follows:*
> > *(1)(A) A launch or re-entry license issued or transferred under this chapter shall contain a provision requiring the licensee or transferee to make a reciprocal waiver of claims with applicable parties involved in launch services or re-entry services under which each party to the waiver agrees to be responsible for personal injury to, death of, or property damage or loss sustained by it or its own employees resulting from an activity carried out under the applicable license[138]".*

Idem pour la France:

> *"In the case of a damage caused by a space operation or the production of a space object to a person taking part in this operation or in that production, any other person taking part in the space operation or in the production of the space object having caused the damage and bound to the previous one by a contract cannot be held liable because of that damage, unless otherwise expressly stipulated regarding the damage caused during the production phase of a space object which is to be commanded in outer space or during its commanding in orbit, or in case of a wilful misconduct[139]".*

---

[137] *Martin Marietta Corp. v. Intelsat*, 763 F. Supp. 1327 (D. Md. 1991) U.S. District Court for the District of Maryland - 763 F. Supp. 1327 (D. Md. 1991) Mai 13, 1991, accessible à : http://law.justia.com/cases/federal/district-courts/FSupp/763/1327/1586244/. (consulté le 12.03.2017)

[138] ''*Commercial Space Launch Competitiveness Act*'', H.R.2262 - U.S, accessible à: < https://www.congress.gov/bill/114th-congress/house-bill/2262/text>. (consulté le 18.02.2017)

[139] LOS, supra, note 111, Title II, art. 20.

De plus, en Europe, les parties liées par contrat avec l'ESA sont aussi liées par des clauses de renoncement, tel que stipulé dans les clauses 18 et 19 des *GCC*:

> *"CHAPTER IV*
> *LIABILITIES CLAUSE 18: DAMAGE TO STAFF AND GOODS*
>
> *18.1 Inter-party cross-waiver of liability*
>
> *The Parties shall have no claim and no recourse against each other and against the other Party's Subcontractors, including the Agency's consultants and/or agents involved in the execution of the Contract: - for injuries to its employees (staff), including death, sustained by virtue of their involvement in the execution of the Contract. - for damages to goods owned by the Party (excluding items covered by clauses 11 and 12 above and Deliverable(s)), if the occurred damage arises from the execution of the Contract. 18.1.2 Exclusions from the cross-waiver of liability. The cross-waiver shall not be applicable in case a claim for injury to staff or damage to goods as described under 18.1 is based on gross negligence or wilful misconduct of the other Party. The cross-waiver of liability shall not be applicable to the claims listed below: a) claims for injuries to persons or damages to goods arising from testing using ESA owned testing facilities or ESA owned equipment, except for those covered by other specific arrangements; b) claims raised by the estate, family, survivors or subrogees (except when such claim is bound by the terms of this cross-waiver) or social security organization for bodily injury, other impairment of health or death of a staff involved in the execution of the Contract.*
>
> *(…)*
>
> *CLAUSE 19: LIABILITY FOR CONSEQUENTIAL DAMAGE DURING THE EXECUTION OF THE CONTRACT*
>
> *Except in case of gross negligence and wilful misconduct, the Parties shall not be liable towards each other for consequential damages sustained by the Parties arising from and during the execution of the Contract such as but not limited to:* ***losses of contract, income or revenue, profit, interests, financing, loss of customers, loss of availability and use of facilities, employees' productivity or loss of service of such persons, loss of opportunity, rental expenses****''. (Emphase ajoutée)*

Le niveau de risque dans l'industrie spatiale justifie ce genre de clause et ce, surtout pour ce qui concerne le lancement. En effet, pendant la campagne de lancement, plusieurs dangers de préjudice demeurent. Le satellite peut être détruit par le lanceur, l'opérateur ou le fabriquant peuvent endommager le site lors des préparations ou de l'intégration de la charge utile (*payload*) au reste de la plateforme (*bus*), le client peut encourir des pertes financières

en raison de retards, etc.[140], le tout devant être prévu dans le contrat, mais soumis au renoncement de recours. Ce renoncement résulte en des standards très stricts et une grande importance accordée aux *best efforts*, évalués par la coutume, la pratique et le secteur, car plutôt vagues. Cette interprétation flexible incite les parties à redoubler d'efforts et nous croyons alors qu'ils feraient de même pour la résilience, car notre définition se veut souple.

Pour ce qui est des opérations sur satellites, les contrats, qu'ils soient de location ou d'offre de services, l'opérateur (loueur ou prestataire), maintient un pouvoir sur le client en ce qui concerne les transpondeurs sur lesquels se base la transmission de données[141]. En effet l'opérateur peut interrompre le service au besoin pour diverses raisons:

> *"if the maintenance and the protection of the overall performance of the satellite requires the lessor to interrupt the lessee's use of the transponder, the lessor shall do so only to the extent necessary and for the shortest possible time or that the lessor shall have the right to suspend the lessee's access to the transponders and the Satellite in the event that the lessee breaches any of the operations procedures during such time as any breach continues[142]".*

Pour cette raison, les parties doivent négocier à l'avance leurs obligations et droits respectifs. En effet, elles doivent négocier les dispositions à prendre en cas de service interrompu et les crédits générés par un service dégradé en vue d'obtenir l'accès aux transpondeurs de rechange sur le satellite en orbite ou les droits relatifs à une rotation de transpondeurs (*back-up switching rights*), selon le créneau négocié sur la liste de priorité de clients. D'autres détails doivent être négociés, comme la résiliation prématurée, le remboursement ou l'ajustement financier par rapport à différentes circonstances.

Comme mentionné, les contrats concernant les opérations sur satellites ont tendance à être moins touchés par le renoncement (*cross-waivers*) prévu par la loi, à moins qu'il ne soit stipulé

[140] "*Specific Clauses of LSAs*", par Claude-Alain du Parquet, dans "*Contracting for Space",* supra, note 97, p. 387.
[141] On s'y réfère comme contrats de satellites.
[142] « Le partage des risques dans les contrats de location des transpondeurs », par E. Loquin, dans Ravillon, supra, note 63.

dans le contrat, mais ils contiennent des mesures de redondance favorisant la continuité du service grâce aux *back-up switching rights*, moyennant une contrepartie financière:

> *"5. TYPES OF SERVICE FULLY PROTECTED SERVICE (If Applicable)*
>
> *"Fully Protected" transponders, in the event of failure, shall be restored using spare equipment that may be available on the satellite at the time of failure, or on a comparable transponder on the same satellite, or on another SKYNET satellite then in orbit, pursuant to Paragraph 7 ("RESTORATION OF A FULLY PROTECTED FAILED TRANSPONDER") hereof, except where the failure is caused by the actions or inaction's of Customer not pursuant to directions of SKYNET. Fully Protected transponders are not preemptible.*
>
> *NON-PREEMPTIBLE SERVICE (If Applicable)*
>
> *"Non-Preemptible" transponders are not protected in the event of failure, and are not subject to preemption (non-preemptible) to restore any other customers protected service*[143]*.*
>
> *(…)*
>
> *7. RESTORATION OF A FAILED TRANSPONDER FULLY PROTECTED TRANSPONDER (If Applicable)*
>
> *In the event any Fully Protected transponder provided hereunder fails, pursuant to Paragraph 6 ("TRANSPONDER INTERRUPTION OR FAILURE") hereof, and if SKYNET unable to restore service on the affected transponder by switching in spare equipment that may be available on the satellite at the time of such failure, then SKYNET shall restore such service either (1) on a transponder of the same frequency band, having the same or greater bandwidth and the same power as the failed transponder, on the same satellite or (2) on a transponder of the same frequency band, having the same or greater bandwidth, the same or different power, the same or greater EIRP, and substantially equivalent domestic footprint, but no less than the same number of States included in the failed transponder footprint, on a nother SKYNET satellite then in orbit. Such transponder will then become the Fully Protected Transponder*[144]*".*

Assurer la disponibilité des transpondeurs et réduire les interruptions de service est essentiel. Ainsi, tout le réseau de GPS ou de GALILEO prévoit des satellites de réserve sur chaque orbite[145]. Ceci est un bel exemple de début d'assurabilité de la continuité du service

---

[143] ''*Transponder Service Agreement between Califa Entertainment Group Inc. and Loral SpaceCom Corp concerning Skynet transponder Service*'', 1999, accessible à : http://contracts.onecle.com/playboy/loral.transponder.1999.02.08.shtml. (consulté le 23. 03.2017)

[144] Ibid.

[145] ''*GALILEO: A CONSTELLATION OF NAVIGATION SATELLITES*'', accessible à : http://m.esa.int/Our_Activities/Navigation/Galileo/Galileo_a_constellation_of_navigation_satellites (consulté le 24.03.2017)

et de résilience grâce à des systèmes de redondance et des mesures négociées contractuellement[146]. Le cas de GALILEO est d'autant plus intéressant en ce sens que son modèle d'affaires contient deux segments de clients: ceux liés par contrat et les tiers. Le co-contractants obtiennent un service (images précises) en échange d'une contrepartie et le tiers peut bénéficier gratuitement d'une grande panoplie de données (*open data*) issue d'une infrastructure et d'un système des systèmes spatial plus résilient, sur le long terme.

À travers notre étude, nous avons donc analysé des dizaines de clauses et de cas dont nous avons ressorti des éléments de résilience, comme la redondance, la rapidité, la capacité à trouver des ressources et la robustesse, toutes liées à la continuité de service grâce aux pouvoirs internes d'adaptation des systèmes à différents chocs et impacts externes. Nous avons répertorié plusieurs clauses jugées d'intérêt et nous avons évalué leur incidence sur l'adaptation et la continuité. Moins d'un quart de ces clauses vont dans ce sens et nous y voyons alors un grand besoin.

Nous considérons comme à haut niveau de résilience les clauses qui assurent la bonne exécution d'une mission ou d'un service (*mission assurance*) et pour cette raison nous avons établi que la majorité des clauses entrent dans une catégorie inférieure (niveau moyen ou faible) dont celles de primes de performance, de pénalités, de garanties, de responsabilité ou de résolution de conflits, parce que ces clauses ne concernent l'objet du contrat que jusqu'à acceptation et non la suite et ce, toujours sous la protection de *cross-waivers* et d'assurances. Finalement, nous avons classé comme faible la clause de force majeure, puisque : 1) elle fait référence au dédommagement et non à l'assurabilité du service et 2) elle peut servir d'échappatoire aux co-contractants dans un domaine à haut risque. Le risque spatial est bien plus élevé que sur Terre, alors il faudrait peut-être revoir la force majeure traditionnelle et l'adapter au secteur (ex : "force majeure spatiale"), d'autant plus que la traçabilité des sources de préjudices dans l'espace demeure assez compliquée.

[146] "*Specific Aspects and Characteristics of Satellite Capacity Agreements in the Satellite Communication Business*", par Oliver Huth et Rafael Roelandt, dans "Contracting for Space", supra, note 97, p. 32.

Level of Resilience				
Clause	***N/A***	***Low***	***Medium***	***High***
IN-ORBIT TESTING			X	
SUPPORT SERVICES AFTER ACCEPTANCE				X
TITLE/RISK TRANSFER		X		
INITIAL/FINAL ACCEPTANCE			X	
INITIAL/FINAL HANDOVER			X	
LIABILITY AFTER ACCEPTANCE			X	
DUTY TO CORRECT			X	
IN-ORBIT (IO) PERFORMANCE INCENTIVE				X
SECURITY FOR PERFORMANCE INCENTIVE			X	
PENALTIES			X	
FORCE MAJEURE		X		
WARRANTIES		X		
HARDSHIP		X		
INSURANCE			X	
DISPUTE RESOLUTION/ARBITRATION			X	
BACK-UP LAUNCH SERVICES				X
CROSS-WAIVERS				X
LIABILITY DURING EXECUTION			X	
LIABLITY AFTER EXECUTION			X	
PROTECTED TRANSPONDERS				X

4.2. Les conditions à rencontrer

(i). La flexibilité: l'objectif relatif vs absolu

La résilience ne constitue pas une fin en soi, mais un moyen incitant au progrès dans l'économie spatiale grâce à l'assurabilité de la mission et du service, sur le long terme. Pour

l'instant, les infrastructures spatiales demeurent fragiles et précaires. Les stations spatiales ne durent pas plus que deux ou trois décennies, tout comme les satellites qui sont programmés pour durer de moins en moins, etc. Ceci ne favorise pas l'essor tant attendu de l'humanité dans un contexte cislunaire et interplanétaire, qui nécessite plus de certitude au niveau des infrastructures sur le long terme, ainsi que de leur interaction avec l'ensemble des infrastructures critiques. Pour le moment, tant que la résilience contractuelle fait ses premiers pas en tant que pionnière, elle doit demeurer souple inciter le secteur privé et public à jouer le jeu en tant que volontaires et collaborer à son élaboration, jusqu'à ce qu'elle gagne en masse critique et puisse être négociée librement par les parties. La rendre absolue est impossible car elle risquerait alors de succomber à l'inertie et de se figer, tombant dans l'oubli après avoir éloigné les intéressés pour cause d'exorbitance.

(ii). Caractère mesurable

Il faut trouver les bons indicateurs pour que la souplesse soit négociable : ni trop large ni trop limitée. Ceux-ci doivent former une bonne combinaison entre données quantitatives et qualitatives, mais pour ce faire, il faut d'abord aller sur le terrain et impliquer les parties à un exercice de *brainstorming*, basé sur les besoins et réalités du marché, qui demeure assez conservateur en raison des risques du secteur. Pour cette raison, nous formulons la recommandation qui consiste à se réunir dans des groupes de travail, incluant des professionnels de la recherche, du privé et du public (qu'ils soient juristes ou gestionnaires) et de participer à un processus d'idéation, de test, de *feedback* et d'itération. Nous avons décelé quelques pistes au préalable et les avons rajoutées à notre modèle de clause, avant de les tester avec des partenaires potentiels.

(iii). Nature incitative

Ces indicateurs doivent inciter les parties à opter pour davantage de résilience, selon leur capacité et selon le déroulement de la négociation. Une solution efficace serait un portfolio d'options et alternatives en ce sens, avec, à ce stade, une approche ''*pay what you can*''. Si

les premières étapes rencontrent un succès graduel, le niveau de résilience pourra alors gagner en importance, mais elle doit encore faire ses preuves et nous en sommes conscients. Le portfolio pourrait consister en plusieurs alternatives à négocier, contenant divers degrés de résilience. Par exemple, un niveau A toucherait aux fonctions essentielles et un niveau B à celles de nature plutôt accessoire. Chaque niveau serait accompagné d'indicateurs, de jalons importants, buts, mesures concrètes, termes légaux, etc. Des exemples intéressants de portfolio de services de configuration et de stratégies résilientes existent sur le marché technique des TIC (ex: IBM[147], Cisco, etc.), mais au niveau technique. Pour cette raison, nous ne recherchons pas de clauses techniques ou détaillées, mais plutôt larges et inclusives, préconisant une approche résiliente, qui se reflétera dans les documents techniques connexes et SLAs complémentaires.

4.3. Prototype d'une clause modèle

Notre prototype consiste en un préambule pour la mise en contexte, des définitions de quelques aspects clé de la résilience, la clause elle-même ainsi que les dispositions d'implémentation, le tout dans une perspective souple et ouverte à la négociation entre parties.

1) PRÉAMBULE :

"Tandis que :
- Les services commerciaux ayant pour relais une infrastructure – dans la mesure où celle-ci consiste en un segment spatial (satellites ou éléments de satellites), en un segment sol ainsi qu'en fréquences du signal – et les services requis pour les opérations concernées augmentent considérablement à travers ces dernières années ;

[147] Les services de résilience sont accessibles sur le site internet de IBM: http://www-935.ibm.com/services/us/en/it-services/business-continuity/?S_PKG=-&cm_mmc=Search_Google-_-GTS_GTS+Resiliency+Services-_-WW_EP-_-+resiliency_Broad_-&cm_mmca1=000000XA&cm_mmca2=10000924&mkwid=64ef2059-c348-4e93-a1eb-4baa58fc5b18|449|98528&cvosrc=ppc.google.%2Bresiliency&cvo_campaign=000000XA&cvo_crid=181716604725&Matchtype=b&cm_mmca7=9055221&cm_mmca8=kwd-74293200791&cm_mmca9=64ef2059-c348-4e93-a1eb-4baa58fc5b18&cm_mmca10=181716604725&cm_mmca11=b (consulté le 20 août 2017)

- La qualité de ces services, dont certains contribuent à la survie de l'humanité, impliquera la résilience des infrastructures spatiales qu'ils utiliseront, ce qui en constituera des infrastructures critiques, puisque la dépendance de ces services s'accentuera ;

- La résilience des infrastructures spatiales deviendra ainsi une exigence majeure pour les services fournis aux clients, puisqu'un nombre grandissant de services terrestres dépendront de la qualité et de la complétude d'une liaison par satellite ;

- L'engagement pris par un opérateur d'infrastructure spatiale qui est de fournir une infrastructure résiliente est en voie de devenir un élément différentiateur dans les années à venir en ce qui concerne divers services ayant pour relais les satellites ;

- En ce qui concerne les clauses prévues dans divers contrats dans le secteur spatial et des activités spatiales, précédemment identifiées, aucune d'elles ne couvre de point particulier relatif à la résilience d'une infrastructure spatiale ;

- Les clauses les plus pertinentes d'entre elles ne traitent dans l'objet du contrat que de manière indirecte la résilience à travers la réparation ou la maintenance préventive ou évacuent le problème à travers la force majeure ; aucune d'entre elles ne traite directement de la résilience et n'établit aucun incitatif ou sanction qui puisse assurer le fait que la résilience des infrastructures spatiales soie garantie ;

- Cet échec résulte en des dispositions légales qui concernent les processus (soft resilience) uniquement, au détriment des aboutissements (hard infrastructure) – comme illustré dans le cas de Paradigm Secure Communications (assurabilité vs assurance) – ce qui complexifie le problème au lieu de contribuer à sa résolution.

2) DÉFINITION

La clause provisoire est basée sur les éléments suivants :

- La résilience est un engagement explicite de la part de l'opérateur d'une infrastructure spatiale, soumis à un régime d'incitatifs et de pénalités ;

- La résilience est un objectif relatif, enclenché par les facteurs suivants :

> *- la perte d'une fonction essentielle de l'infrastructure spatiale,*
>
> *- à la suite d'un événement ou série d'événements affectant le hardware, le software ou le firmware de l'infrastructure spatiale et que,*
>
> *- la capacité spontanée de l'infrastructure de réduire l'ampleur et la durée des effets dudit événement et / ou de retourner instantanément ou dans un court délai à des conditions d'opérations stables, impliquant un nombre limité de dégradations objectivement acceptables.*

- La résilience est mesurable, comportant différents niveaux de résilience proposés par l'opérateur dans ses spécificités et sélectionnées par le client ;

- La résilience peut ainsi constituer un argument de vente de services pour l'opérateur, ainsi qu'un avantage concurrentiel, dans la mesure de sa responsabilité contractuelle vis-à-vis le client, ce qui en fait un incitatif;

- Le client d'un opérateur d'infrastructure spatiale choisit le niveau de résilience auquel il s'attend concernant l'infrastructure qu'il utilise.

3) SUBSTANCE :

La clause provisoire se lit comme suit :

CLAUSE RELATIVE À LA RÉSILIENCE

I. Le fournisseur, sujet aux sanctions et incitatifs décrits, s'engage à prendre toutes les précautions et mesures requises pour garantir le niveau de résilience sélectionné et, plus particulièrement, de procéder au design, à la fabrication, à l'approvisionnement, à sous-traiter, assembler, opérer, fournir, maintenir, suivre de près (…) le [système satellitaire / le lanceur / le répéteur / le signal (…)], sujets à ce contrat, de manière à ce que, dans l'éventualité d'un événement ou d'une combinaison d'événements modifiant le cours normal des fonctions essentielles relevant du hardware, software ou firmware :

- *l'ampleur et la durée des effets en soient réduites spontanément et que,*
- *le [système satellitaire / lanceur / répéteur / signal (…)] retourne quasi-instantanément à une condition d'opérations stable, impliquant des dégradations objectivement acceptables.*

4) INTERPRÉTATION ET IMPLÉMENTATION :

II. Aux fins d'interprétation et d'implémentation de cet article :

- La "résilience" se réfère à la capacité endogène d'un [système satellitaire / lanceur / transpondeur / signal …], faisant face à un événement ou série d'événements, de modifier ses fonctions essentielles pour :

- *réduire spontanément l'ampleur et la durée des effets et,*
- *de retourner quasi-instantanément à une condition d'opérations stable, impliquant des dégradations objectivement acceptables.*

- la ou les "fonction(s) essentielle(s)" signifie la ou les fonction(s) [système satellitaire / lanceur / transpondeur / signal …], correspondant au niveau de résilience, décrit dans l'annexe ci-dessous (Annexe "Résilience" – que les parties auront négocié préalablement)

- le "degré de "résilience" renvoie au niveau de résilience sélectionné par le client, niveau correspondant aux fonctions essentielles du [système satellitaire / lanceur / transpondeur / signal …], tels que décrites dans l'annexe ci-dessous (annexe "Résilience").

- les "événements ou série d"événements" se réfèrent à des événements ou séries d'événements affectant le:

- hardware […]

- software […]

- firmware […]

- les "conditions stables" sont définies par les indicateurs ci-dessous (à prévoir) *[…]*

- "spontanément" signifie la capacité de réagir avec ses propres moyens ou moyens accessoires et de procéder à l'implémentation programmée ou activée aussitôt l'événement ou la série d'événement survenus ;

- "instantanément" signifie à l'intérieur de quelques secondes, minutes ou heures, selon le niveau de résilience sélectionné contractuellement par les parties ;

- les "dégradations objectivement acceptables" sont énumérées ci-dessous (à déterminer)

[…]© [148]

Ce modèle de clause résume la plupart des thèmes abordés au cours de ce texte et nous formulons l'hypothèse, qu'à long terme, il incitera les acteurs du spatial à adopter ce genre de portfolio et à évoluer en ce sens, en assurant la continuité des missions et services tout en innovant leur modèle d'affaires pour faire de la résilience un nouveau service critique en soi, que ce soit dans un contexte de privatisation ou de (cyber) sécurité spatiale[149]. Avec cette première clause provisoire, nous nous donnons pour objectif d'aller sur le terrain et d'entamer un dialogue ouvert avec le secteur tant public que privé et de partager les résultats dans des travaux ultérieurs.

[148] Clause rédigée par la Chaire SIRIUS, Toulouse, avril 2016.

[149] En septembre 2015, le Bureau du Secrétaire américain de la Défense a publié un livre blanc intitulé "*Space Domain Mission Assurance: A Resilience (Disaggregation, Distribution, Diversification, Protection, Proliferation and Deception)*" qui se résume ainsi : "*As we have noted previously, all of these resilience measures, along with reconstitution and defensive measures, and alternate/cross domain abilities may be used individually and collectively to achieve warfighting mission assurance. Resilience is but one contributor to that equation. But we believe it is a critical component to define at the system level, in the control of the system designer, analyst, and operational commander to help drive those requirements that cannot be addressed through resilience alone. The National Space Policy, the National Security Space Strategy, and DoDD require that space mission assurance and resilience be included in space system planning. This taxonomy is an appropriate basis for that planning and should be used to address these policy requirements*". Les élémenents (ex : "*deception*") peuvent être interprétés de plusieurs manières selon leur nature duale (militaire et commerciale ou civile). Le texte est accessible à < https://fas.org/man/eprint/resilience.pdf>. Consulté le 22.04.2017

5. Recommandations pour la mise en œuvre de la clause

5.1. Les tests

Comme mentionné, la prochaine étape est de tester cette clause sur le terrain et d'en recueillir le *feedback* de la part de partenaires comme le CNES, Airbus ou Thalès Alenia Space, en passant par Aérospace Valley et les *start-ups* qui y sont incubées. Ainsi nous échangerons avec des poids lourds tout comme avec des nouveaux entrants ou des facilitateurs, sans oublier des organisations internationales telles UNIDROIT, des agences intergouvernementales telles l'ESA, ou encore les professionnels du droit et, éventuellement mettre sur pied un groupe de travail semblable à celui de La Haye sur les ressources minières dans l'espace extra-atmosphérique[150]). Une approche transversale et holistique est à préconiser pour maximiser les échanges créatifs, ce qui rendra notre projet plus résilient.

5.2. UNIDROIT

Pour les contrats de long terme, UNIDROIT est une source incontournable de légitimité en ce qui concerne l'innovation juridique dans le domaine du droit international privé, qui est notre champ d'action immédiat. Profitant du fait de la prolifération actuelle des législations nationales, nous croyons que c'est le moment opportun d'entamer un tel travail, tant que les lois sont fraiches et ouvertes à amélioration, amendements, etc. Si la résilience vit un succès contractuel, elle sera sujette à une éventuelle place dans les refontes législatives à l'avenir, démontrant ainsi comment les contrats peuvent influer sur le droit privé et public et confirmer que le droit possède bel et bien un rôle proactif.

[150] Plus d'informations sur le site web du groupe : http://law.leiden.edu/organisation/publiclaw/iiasl/working-group/the-hague-space-resources-governance-working-group.html, consulté le 22 août 2017

5.3. Les lignes directrices

Basé sur les résultats de l'enquête sur le terrain à suivre, il serait pertinent de rédiger un manuel de bonnes pratiques en ce qui concerne la résilience des infrastructures spatiales, grâce à un apport véritablement collectif et transversal. Le fonctionnement du groupe de travail pourrait se dérouler à travers quelques retraites d'idéation, d'échanges et de *brainstorming* par année, avec des intervenants légaux et techniques du secteur spatial (académique, public et privé) pour mettre en place des processus internes de résilience souple au niveau organisationnel qui faciliteraient par la suite le test de contrats flexibles de résilience, contenant des clauses plus ou moins spécifiques liées à la résilience lourde (spécificités techniques). Tout au long de cet exercice, nous étudierons le niveau du retour sur investissement à long terme et les avantages concurrentiels qu'engendre la résilience, afin d'inciter avec succès les parties prenantes à l'adopter. Nous pourrons nous inspirer de groupes de travail comme celui de La Haye sur les ressources spatiales ou le groupe de McGill sur les usages militaires du secteur spatial (MILAMOS[151]), ce qui nous conduira à rédiger un manuel collectif sur la résilience spatiale.

Conclusion

À la fin de cet exercice, nous pouvons prendre du recul et voir comment nous sommes partis de zéro pour ensuite déceler un manque et un besoin avant de nous lancer à la rédaction d'une clause qui pourrait potentiellement contribuer à solutionner une partie du problème identifié. Du moins, nous avons réussi à rassembler des concepts relevant de plusieurs disciplines pour en faire une approche transversale se focalisant sur la continuité des services spatiaux tout en signalant la nature critique des infrastructures spatiales.

[151] *Manual on International Law Applicable to Military Uses of Outer Space* (MILAMOS), accessible à : http://www.mcgill.ca/milamos/, consulté le 21 août 2017

Nous avons évoqué ce que sont les infrastructures spatiales et leur besoin de protection contre les risques mentionnés qui étendent la portée de leur vulnérabilité à toutes les autres infrastructures critiques avec lesquelles elles interagissent. La protection que nous proposons relève du concept de résilience, que nous avons scindé en deux parties (souple et lourde) afin de couvrir les aspects légaux, organisationnels et techniques, favorisant ainsi une approche transdisciplinaire où le droit des contrats occupe un rôle proactif. La résilience cultive la capacité endogène de surmonter un événement perturbateur ainsi que de s'adapter, apprendre de l'expérience et anticiper. Nous avons rédigé un prototype de clause contractuelle en ce sens et invitons les acteurs du spatial à prendre part au dialogue et de contribuer à une initiative d'innovation juridique ayant pour objectif l'assurabilité de la continuité des services spatiaux, sur le long terme.

C'est un défi à relever dans un contexte de privatisation du secteur spatial, qui devient graduellement partie intégrante de notre vie quotidienne, puisque nous dépendons de nombreuses applications spatiales (télécoms, GPS, etc.) de manière significative. De plus, comme les systèmes spatiaux sont de plus en plus fractionnés et interdépendants, nous sommes témoins de la cybernétisation accrue de l'architecture spatiale et nous anticipons l''intégration de l'intelligence artificielle, du *machine learning* et de la singularité dans le secteur. Cette évolution requiert une approche inclusive et ouverte, contribuant aux bases de la capacité résiliente afin de facilité l'essor de l'économie spatiale (orbite terrestre, cislunaire et interplanétaire) à travers le temps.

ANNEXES

ANNEXE 1: *DEFINITIONS OF RESILIENCE*[152]

Table 1.1 Literature review about resilience definitions

Author	Definition
Holling (1973)	Ecological systems resilience is a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables
Wildavsky (1991)	Resilience is the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back
Horne and Orr (1998)	Resilience is the ability of a system to withstand stresses of environmental loading…[it is] a fundamental quality found in individuals, groups, organizations, and systems as a whole
Haimes (1998)	Resilience is the ability of system to return to its optimal condition in a short period of time. Considering resilience one of four strategies for hardening a system, together with security, redundancy and robustness
Mileti (1999)	Local resiliency with regard to disasters means that a locale is able to withstand an extreme natural event without suffering devastating losses, damage, diminished productivity, or quality of life and without a large amount of assistance from outside the community
Comfort (1999)	Resilience is the capacity to adapt existing resources and skills to new situations and operating conditions
Adger (2000)	Social resilience is the ability of groups or communities to cope with external stresses and disturbances as a result of social, political, and environmental change
Gunderson et al. (2002)	Engineering resilience is the speed of return to the steady state following a perturbation ecological resilience is measured by the magnitude of disturbance that can be absorbed before the system is restructured
Fiksel (2003)	Resilience is the essence of sustainability the ability to resist disorder
Bruneau et al. (2003)	Resilience is defined in terms of three stages: the ability of a system to reduce the probability of an adverse event, to absorb the shock if the adverse event occurs, and to quickly re-establish normal operating conditions. So resilience thus encompasses the four characteristics of robustness, redundancy, resourcefulness, and rapidity. Are considered four types of resilience: technical; organizational; economic; and social
Allenby and Fink (2005)	Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must
Rose and Liao (2005)	Regional economic resilience is the inherent ability and adaptive response that enables firms and regions to avoid maximum potential losses
Hollnagel (2006)	Resilience is defined as the intrinsic ability of an organization (system) to maintain or regain a dynamically stable state, which allows it to continue operations after a major mishap and/or in the presence of a continuous stress
Manyena (2006)	Evaluating all the possible definitions provided from the 1990s to nowadays, resilience could be viewed as the intrinsic capacity of a system, community or society predisposed to a shock or stress to adapt and survive by changing its non essential attributes and rebuilding itself

(continued)

[152] Compilation à partir de Urban Resilience, supra, note 10.

Table 1.1 (continued)

Author	Definition
Woods (2006)	Resilience is defined as the ability of systems to anticipate and adapt to the potential for surprise and failure
Holmgren (2007)	Resilience is the ability of the system to return to a stable condition after a disruption. Distinguishing robustness and resilience, using robustness to imply that the system will remain (nearly) unchanged even in the face of disruption
Tierney and Bruneau (2007)	Resilience is both the inherent strength and ability to be flexible and adaptable after environmental shocks and disruptive events
DHS-RSC (2008)	Resilience is the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance
Haimes (2009)	Resilience is defined as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risk
Vugrin et al. (2010)	Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels

ANNEXE 2: *ONTOLOGY OF RESILIENCE*

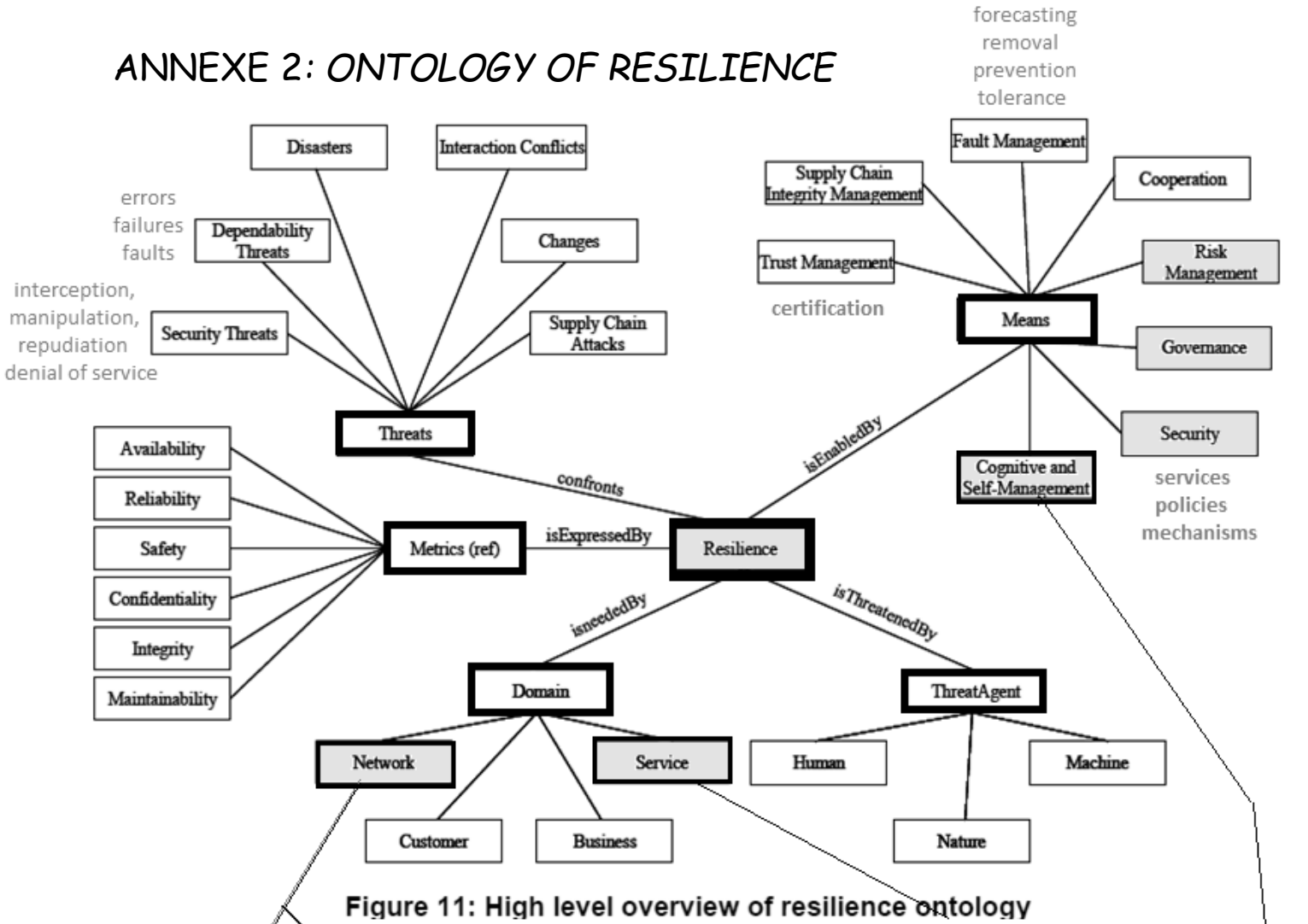


Figure 11: High level overview of resilience ontology

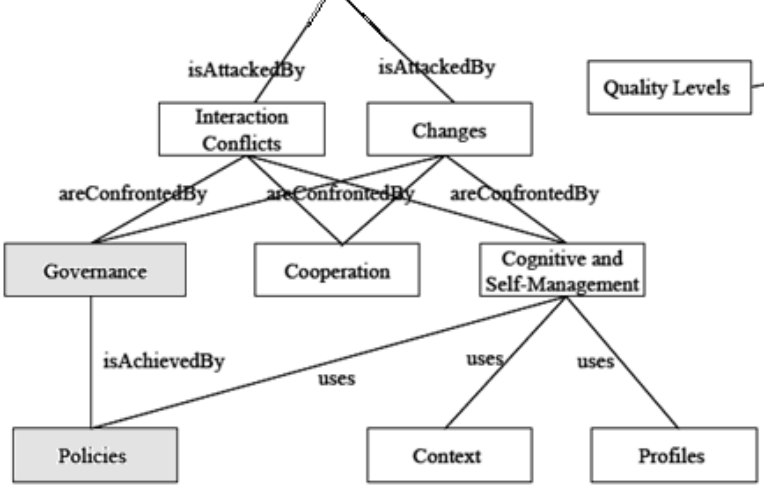


Figure 27: "Network" domain "Threats" and "Means"

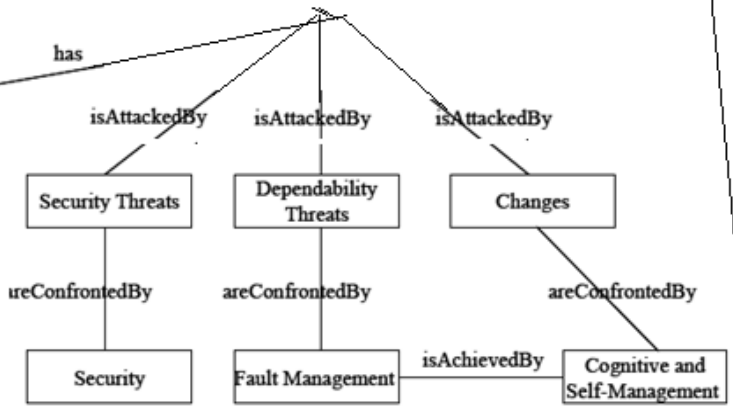
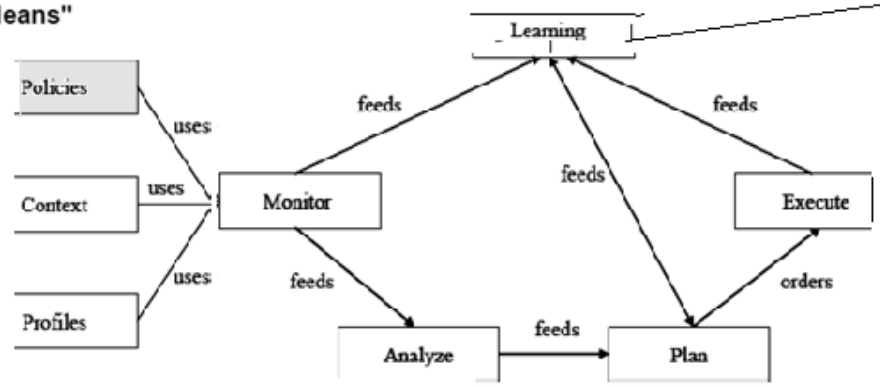


Figure 29: "Service" domain "Threats" and "Means"

Ontology figure (adapted and compiled) ENISA Report on Ontologies and Taxonomies of Resilience, available at: https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjC4LfcssXUAhVMaVAKHYT5BxsQFggoMAA&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fontology_taxonomies%2Fat_download%2FfullReport&usg=AFQjCNE_Z5K4Ikn761TOQy1i_dc-7MkotQ&sig2=TTndDXQm1Ol6DSG8wLz5iQ. (Accessed on 21.11.2016).



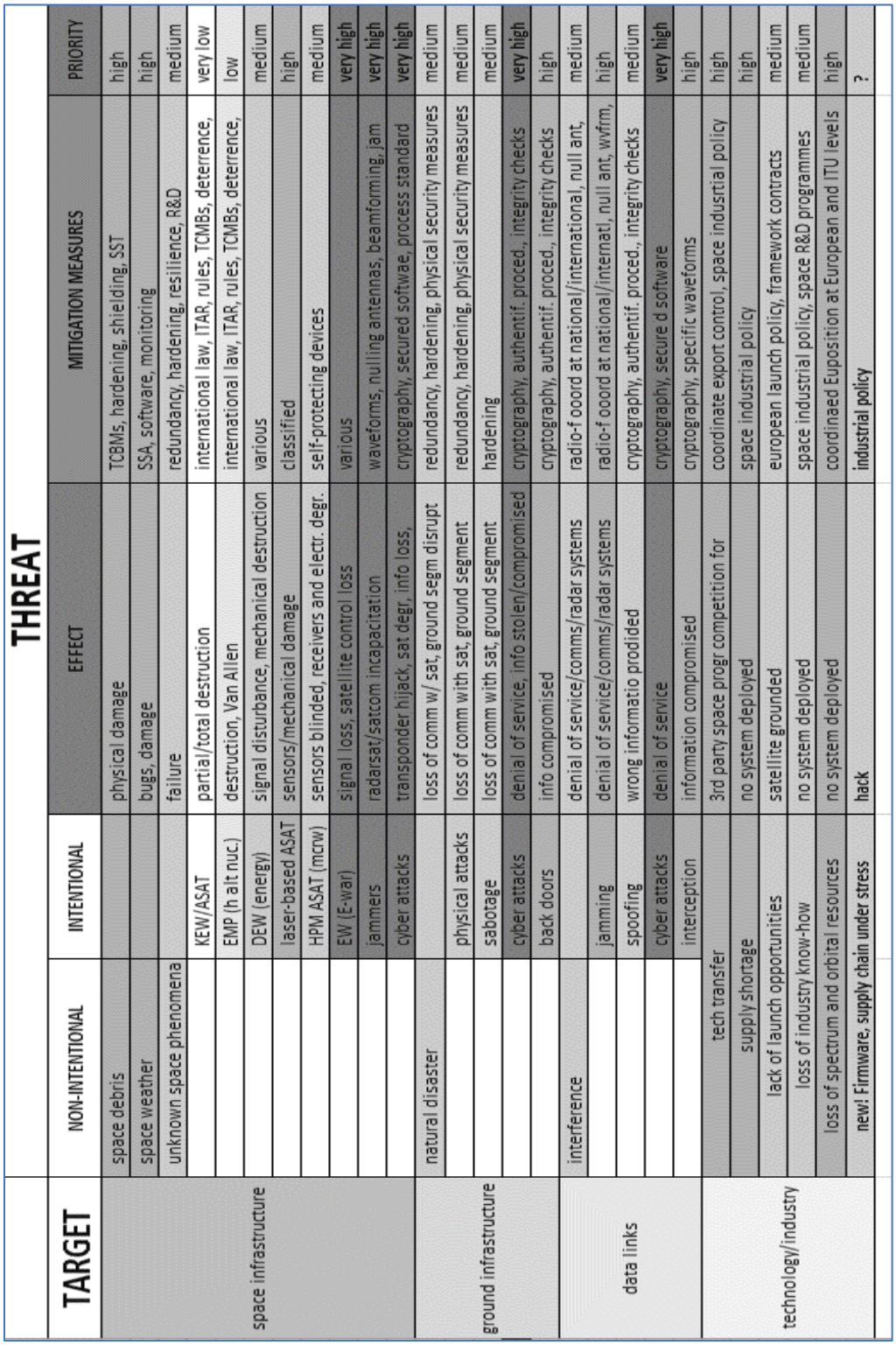
ANNEXE 3: *NATIONAL SPACE STRATEGIES AND PRIORITIES*[153]

TABLE 7: MENTIONS OF HEADLINE GOALS/PRIORITIES IN CURRENT SPACE STRATEGIES

	European Space Strategies (2000, 2007, 2011)	Member State Strategies (FR, DE, IT, UK, ES)	Space Security Strategies (UK, US)
Industrial Policy/Space sector support	3	4	1
Security and Defence (& dual use)	3	3	1
Science and technology	3	3	0
Applications (EO, GNSS, SatCom)	3	2	0
International cooperation	3	4	2
ISS and Exploration	2	3	0
Access to Space/Non-dependence	2	2	0
Vision - Citizen focus	2	2	0
Governance & regulation within EU	2	0	0
Markets for space services	1	2	0
SSA	1	0	0
Shape (contribute to) Europe in space	0	4	0
Space sustainability/stability	0	2	2
Public private partnerships	0	1	0
Establish unified legal framework	0	1	0
Resilience/protection	0	0	1
Space security risks	0	0	1
Deter aggression	0	0	1
Operate in degraded environment	0	0	1

[153] Handbook on Space Security. K-U Schrogl (ed.) : Handbook on Space Security, Springer, 2015.

ANNEXE 4: *RISKS AND THREATS IN SPACE*[154]



TARGET	THREAT				
	NON-INTENTIONAL	INTENTIONAL	EFFECT	MITIGATION MEASURES	PRIORITY
space infrastructure	space debris		physical damage	TCBMs, hardening, shielding, SST	high
	space weather		bugs, damage	SSA, software, monitoring	high
	unknown space phenomena		failure	redundancy, hardening, resilience, R&D	medium
		KEW/ASAT	partial/total destruction	international law, ITAR, rules, TCMBs, deterrence,	very low
		EMP (h alt nuc.)	destruction, Van Allen	international law, ITAR, rules, TCMBs, deterrence,	low
		DEW (energy)	signal disturbance, mechanical destruction	various	medium
		laser-based ASAT	sensors/mechanical damage	classified	high
		HPM ASAT (mcrw)	sensors blinded, receivers and electr. degr.	self-protecting devices	medium
		EW (E-war)	signal loss, satellite control loss	various	very high
		jammers	radarsat/satcom incapacitation	waveforms, nulling antennas, beamforming, jam	very high
		cyber attacks	transponder hijack, sat degr, info loss,	cryptography, secured softwae, process standard	very high
ground infrastructure	natural disaster		loss of comm w/ sat, ground segm disrupt	redundancy, hardening, physical security measures	medium
		physical attacks	loss of comm with sat, ground segment	redundancy, hardening, physical security measures	medium
		sabotage	loss of comm with sat, ground segment	hardening	medium
		cyber attacks	denial of service, info stolen/compromised	cryptography, authentif. proced., integrity checks	very high
		back doors	info compromised	cryptography, authentif. proced., integrity checks	high
data links	interference		denial of service/comms/radar systems	radio-f ooord at national/internationl, null ant,	medium
		jamming	denial of service/comms/radar systems	radio-f ooord at national/internatl, null ant, wvfrm,	high
		spoofing	wrong informatio prodided	cryptography, authentif. proced., integrity checks	medium
		cyber attacks	denial of service	cryptography, secure d software	very high
		interception	information compromised	cryptography, specific waveforms	high
technology/industry	tech transfer		3rd party space progr competition for	coordinate export control, space industrial policy	high
	supply shortage		no system deployed	space industrial policy	high
	lack of launch opportunities		satellite grounded	european launch policy, framework contracts	medium
	loss of industry know-how		no system deployed	space industrial policy, space R&D programmes	medium
	loss of spectrum and orbital resources		no system deployed	coordinaed Euposition at European and ITU levels	high
	new! Firmware, supply chain under stress		hack	industrial policy	?

[154] Information retrieved from Pellegrino, supra, note 11.

ANNEXE 5: *EXAMPLE OF PROCESSES*

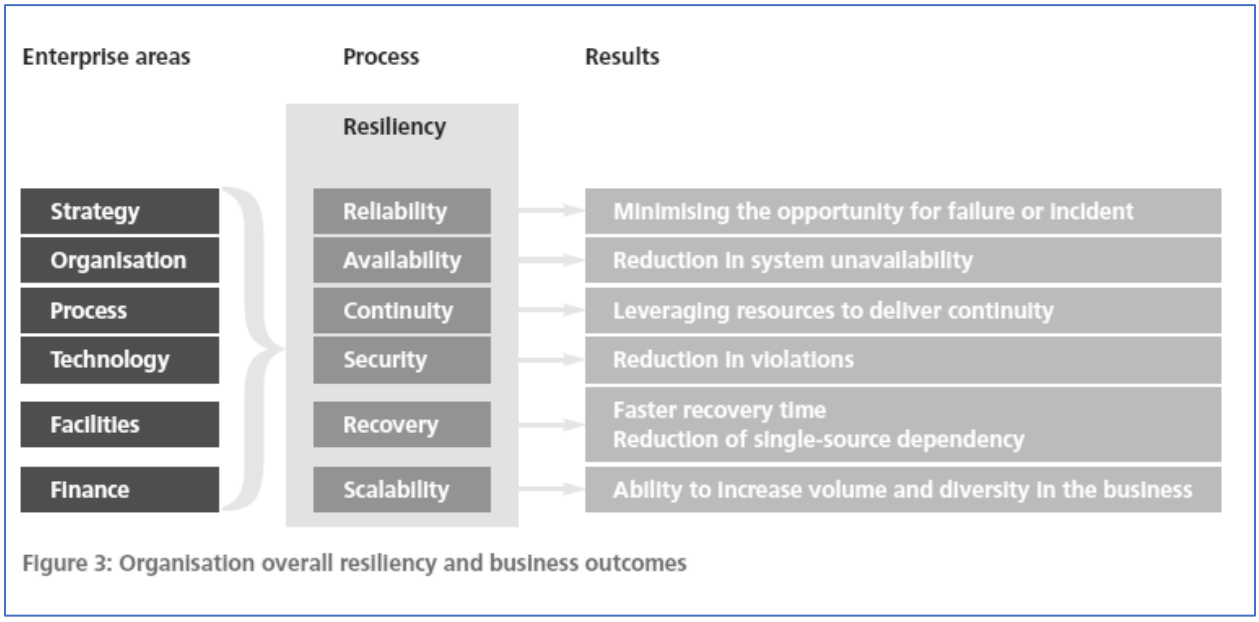


Figure 3: Organisation overall resiliency and business outcomes

End2End Report: Organisation overall resilience and business outcomes describing the resilience process according to enterprise areas.

ANNEXE 5.1: *CONTRACTUAL CLAUSES*

5.1: TRANSFER OF TITLE AND RISK

9. TITLE AND RISK OF LOSS

9.1 TRANSFER OF TITLE.

Transfer of title, free and clear of all liens and encumbrances of any kind, to each Deli verable Item (other than Satellites) shall pass to Customer at Final Acceptance of such Deli verable Item. Transfer of title, free and clear of all liens and encumbrances of any kind, to e ach Satellite shall pass to Customer at the time of Initial Handover of such Satellite, or, in t he event of a Constructive Total Loss or Total Loss of such Satellite, at the time of such Co nstructive Total Loss or Total Loss, or, in the event such Satellite is placed in storage, as pr ovided in Article 14.4 (Storage).

9.2 TRANSFER OF RISK OF LOSS.

Risk of loss or damage to each Deliverable Item shall pass to Customer at Final Accept ance of such Deliverable Item; provided, however, risk of loss or damage to each Satellite an d its Launch Vehicle shall pass at Launch of such Launch Vehicle; provided, however, (x) in t he event of a Terminated Ignition for a Satellite, risk of loss or damage for such Satellite a nd its Launch Vehicle shall revert to Contractor upon such Terminated Ignition and shall agai

n pass to Customer upon the subsequent Launch of such Satellite and its Launch Vehicle, and (y) in the event a Satellite is placed in Storage, risk of loss or damage to such Satellite shall pass in accordance with Article 14.4 (Storage).

ANNEXE 5.2.1: *DUTY TO CORRECT*

13.2 DUTY TO CORRECT.

(a) Without limiting the obligations of Contractor or the rights of Customer under this Contract, prior to Launch of any Satellite or Delivery of any other Deliverable Item, Contractor shall, at its expense, promptly correct any Defect related to any Deliverable Item or component thereof that Contractor or Customer discovers during the course of the Work or from other spacecraft of a class similar to the satellites being built by Contractor, and notwithstanding that a payment may have been made in respect thereof, and regardless of prior reviews, inspections, approvals, or acceptances. This provision is subject to the right of Contractor to have any items containing a Defect returned at Contractor's expense to Contractor's facility for Contractor to verify and correct the Defect.

(b) At Contractor's expense, Contractor shall use reasonable efforts to correct any such Defect in any Launched Satellite delivered in-orbit hereunder, to the greatest extent that such Defect may be corrected by on-ground means, including transmission by Contractor of commands to such Satellite(s), to eliminate or mitigate any adverse impact resulting from any such Defect, to establish work-around solutions, or to otherwise resolve such Defect. Contractor shall coordinate and consult with Customer concerning such on-ground resolution of Defects in Launched Satellites.

(c) Contractor shall fulfill the foregoing obligations at its own cost and expense, including all costs arising from charges for packaging, shipping, insurance, taxes, and other matters associated with the corrective measures, unless it is reasonably determined after investigation that Customer directly caused the Defect in question, in which case Customer shall pay all such costs.

(d) If Contractor fails to correct any Defect with respect to those Satellites that have not been Launched or with respect to any other Deliverable Item within a reasonable time after notification from Customer and after the Parties have followed the provisions of Article 13.1 (Notice of Defects) above, Customer may, by separate contract or otherwise, correct or replace such items or services, and, unless it is reasonably determined after investigation that Customer directly caused the Defect in question, Contractor shall pay to Customer the reasonable cost of such correction or replacement. The amount payable by Contractor shall be verified at Contractor's request by an internationally recognized firm of accountants appointed by Contractor. The costs of such verification shall be paid by Contractor. The verification of such correction cost shall be without prejudice to the right of either Party in any arbitration proceeding and shall not be binding upon the arbitrators.

(e) Contractor acknowledges and agrees that it shall not be entitled to payment for any additional costs incurred as a consequence of any Defect where the Defect arises directly from Contractor's fault. If correction of any Defect causes a delay in the Delivery of any Work, despite the efforts of Contractor to correct the Defect, the provisions of Article 10 (Liquidated Damages for Late Delivery) shall apply as appropriate in addition to the remedies in this Article 13 (Corrective Measures in Unlaunched Satellites and Other Deliverable Items) and Article 31 (Failure to Make Adequate Progress).

(f) After notification of a Defect to Contractor, Customer, in its sole discretion, may elect in writing, pursuant to Article 34.4 (Waiver of Breach of Contract), not to require correction or replacement of such items or services or to waive the Defects noted for the Satellites that have not been Launched, if any. In such event, Contractor shall promptly provide Customer with a written price proposal for the cost of correction of such Defect at the time of waiver.

(g) Subject to the provisions of any applicable Law, Contractor agrees to enforce any manufacturer's warranty given to it in connection with any Work to be provided under this Contract, and upon Customer's written request, Contractor shall assign to Customer such warranty protection to correct any defective Work not otherwise corrected by Contractor.

ANNEXE 5.2.2 DUTY TO CORRECT (DIGITAL GLOBE[155])

11.2. DUTY TO CORRECT.

(a) Without limiting the obligations of Contractor or the rights of Customer under this Agreement, prior to Launch of the Satellite, Contractor shall, at its expense, promptly correct any Defect related to any Contract Deliverable or component thereof that Contractor or Customer discovers during the course of the Work, and notwithstanding that a payment may have been made in respect thereof, and regardless of prior reviews, inspections, approvals, or acceptances (with the exception of waivers and deviations previously agreed-upon). This provision is subject to the right of Contractor to have any items containing a Defect returned at Contractor's expense to Contractor's facility for Contractor to verify and correct the Defect.

(b) Following Launch of the Satellite, Contractor duty to correct any Defect in the Contract Deliverables or components thereof is solely limited to using reasonable efforts to correct any Defect in the Satellite to the extent that such Defect may be corrected by transmitting Satellite commands and/or transmitting modifications in the Satellite Flight Software in order to mitigate or eliminate the operational effects of the Defect. Contractor

[155] ''*SATELLITE PURCHASE AGREEMENT #8862, BY AND BETWEEN DIGITALGLOBE, INC. AND BALL AEROSPACE & TECHNOLOGIES CORP. October 2, 2006*'', accesible à : https://www.lawinsider.com/contracts/2D93BYAjimsHOylZMgU8gu/digitalglobe/purchase-agreement/2008-04-14, consulté le 14.06.2017.

shall coordinate and consult with Customer concerning said resolution of Defects in the Satellite.

(c) Contractor shall fulfill the foregoing obligations at its own cost and expense, including all costs arising from charges for packaging, shipping, insurance, taxes, and other matters associated with the corrective measures, unless it is reasonably determined after investigation that Customer directly caused the Defect in question, in which case Customer shall pay all such costs.

(d) If Contractor fails to correct any material Defect with respect to the unlaunched Satellite or with respect to any other Contract Deliverable within a reasonable time after notification from Customer and after the Parties have followed the provisions of Article 11.1 above, then, with the prior written consent of Contractor (said consent not to be unreasonably withheld), Customer may, by separate contract or otherwise, correct or replace such items or services and Contractor shall pay to Customer the reasonable cost of such correction or replacement., In the event of any dispute regarding the above, Article 22.2 shall apply. The amount payable by Contractor shall be verified at Contractor's request by an internationally recognized firm of accountants appointed by Contractor.

(e) Contractor may at its option, either correct the Defect or seek a waiver. In the event the Defect is waived, Contractor shall promptly provide Customer with a written price proposal for such change.

(f) Notwithstanding anything herein to the contrary, in the event there is a total loss of the Satellite prior to launch such that the Delivery of the Satellite would be delayed by more than one hundred eighty (180) days, then DG shall have the option of either requiring that Contractor replace the Work up to the point of loss at Contractor's sole expense or return to Customer all payments made by Customer as of the date of the loss.

(g) This duty to correct does not apply to CFE.

ANNEXE 5.3.1: *SATELLITE REPLACEMENT*[156]

24.2 Replacement Satellite

24.2.1 Purchaser shall have an option (the "Satellite Replacement Option"), which Purchaser may exercise in writing at any time ("Satellite Replacement Option Exercise") during the period from EDC until the later of (a) EDC plus [***] months and (b) provided that the

[156] ''*CONTRACT Between Hughes Network Systems, LLC And Space Systems/Loral, Inc. for the Hughes Jupiter Satellite Program*'', juin 8, 2009, accessible sur le site de la FCC: https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwirj-i-9cXUAhXPalAKHRUnAx4QFggzMAI&url=http%3A%2F%2Flicensing.fcc.gov%2Fmyibfs%2Fdownload.do%3Fattachment_key%3D829255&usg=AFQjCNHjYgxSMCAoM5krQUspTPskHshvEg&sig2=S7i6ou7deQSD0_Z1fPCs-w, consulté le 18.96.2017.

Satellite has not been placed in Ground Storage for reasons other than attributable to Contractor, [***] after Launch of

78 Use or disclosure of the data contained on this sheet is subject to the restriction on the title page.

the Satellite (or Total Loss of the Satellite in connection with a failed Launch), to order a replacement satellite for the Satellite, including Satellite Unique Ground Products and updates to Deliverable Data, as required (the "Replacement Satellite"). Upon Satellite Replacement Option Exercise, Contractor shall construct and Deliver the Replacement Satellite, and shall perform all Launch Support Services, Mission Support Services and other services (not including training) in accordance with the terms and conditions of this Contract, except as expressly modified by this Article 24. Contractor shall Deliver the Replacement Satellite on or before [***] months from Satellite Replacement Option Exercise.

24.2.2 The price for the Replacement Satellite shall be as set forth in Section 1.2.3 of Exhibit E, Payment Plan. The total Replacement Satellite price includes Launch Support Services, Mission Support Services and other services required to be provided by Contractor under this Contract. The payment plan for the Replacement Satellite shall be the payment plan applicable at the time of the Satellite Replacement Exercise set forth in Section 2.3 of Exhibit E, Price and Payment Plan (with reference to "Replacement Satellite Payment Plan").

24.2.3 The Parties shall promptly incorporate the exercise of this option into the Contract through an Amendment according to Article 34.5.

ANNEXE 5.3.2 *ADDITIONAL SATELLITES*[157]

27.2 Additional Satellites.

Purchaser shall have the option (but shall not be obligated), which Purchaser may exercise in writing at any time, to order Contractor to construct and deliver on the ground to a designated launch site in accordance with and subject to the terms and conditions of this Contract, one or more additional satellites (each an "Additional Satellite") that will be identical to the Jupiter 2 Satellite, [***].

In the event Purchaser exercises an option set forth in this Article 27.2, Contractor shall construct the applicable Additional Satellite in accordance with and subject to the terms and conditions of this Contract (including without limitation any changes to the design of such Additional Satellite in accordance with this Article 27.2) and shall deliver the applicable Additional Satellite to the launch site designated by Purchaser therefor on [***] after the option is exercised, but in no event earlier than [***] after the Delivery of the Satellite that

[157] ''*Contract between Echostar Operating Corporation and Space Systems/Loral, LLC for the Jupiter 2 Satellite Program*'', 2013, accessible à : http://licensing.fcc.gov/myibfs/download.do?attachment_key=1004726 , consulté le 18.06.2017.

is Delivered immediately prior to the applicable Additional Satellite. The firm fixed price for each Additional Satellite shall be [***]

Each Additional Satellite price will include Satellite, Deliverable Data, Support and Training Services, Launch Support Services, Mission Operations Support Services, certain Risk Management Services, a Dynamic Satellite Simulator and other services required to be provided by Contractor under this Contract.

ANNEXE 5.4: *WARRANTIES*

2.1) *Sample of Warranty Clause[158] Parts:*

1. *Rights of the of the Customer in Case of Defects*
   - *1.1 The Customer shall examine the delivery immediately upon receipt in order to identify any defects and in case of any obvious defect, shall inform the Seller accordingly in writing within a period of 2 weeks. The Customer must notify the Seller of any defects that are not apparent within one year or receipt of the delivery at the latest. Where the Customer fails to provide notification within these exhaustive time limits, the delivery shall be deemed approve, with the result that the Customer loses its rights to assert defects in accordance with sections 1.2 and 1.4.*
   - *1.2 Where the delivery is defective, the Seller shall, at its discretion, be entitled to and repair the delivery or to deliver a defect-free item.*
   - *1.3 The Seller shall be entitled to make remedial action dependent on the Customer paying a reasonable proportion of the remuneration, having regard to the defect. The Seller shall be entitled to refuse repair or a new delivery where it can only be carried out at disproportionate cost.*
   - *1.4 Where repair by the Seller fails to remedy the defect on 2 individual occasions, the Seller refuses to effect subsequent performance or where the Seller fails to provide subsequent performance within a reasonable time defined by the Customer, the Customer shall be entitled to reduce the purchase price or withdraw from the contract and demand reimbursement of unnecessary expenditure, or compensation for damages instead of performance are excluded in case of minor defects.*
   - *1.5 The Customer is not entitled to any remedies as a result of defects that are due e.g. to incorrect storage, operation, maintenance or excessive or inappropriate use of the delivery, to the use of unsuitable tooling and resources, construction work and construction sites or improper changes, corrective maintenance work and damage to seals in the delivery or b other breach of contractual specifications and product regulations on the part of the Customer or a third party.*
   - *1.6 The Customer's claims shall be subject to a limitation period of one year subsequent to delivery.*

[158] Ines Scharlach in "Contracting for Space", supra, note 97, p. 263

1) *Sample of WARRANTY by launcher to insurer: FFSA-SP 101 (launch policy) 15.12.2003*[159], *accompanied by a CERTIFICATION:*

A) WARRANTY:

1. *(Launch Policy)*

The insured warrants that at all times the following pre-launch quality control documents have complied with:

- all written procedures of the Insured and/or the Satellite manufacturer and/or the launch service provider, as far as applicable to the subject matter of this Policy, AND

- all contractual documents signer (a) between the Insured and the Satellite manufacturer or (b) between the Insured and the launch service provider or (c) between Insured, the Satellite manufacturer and the launch service provider including but not limited to the statement of work, the technical specifications, the product assurance plan and the test plan, AND

- all NASA recommendations and MIL standards, ESA/ECSS documents, as far as applicable to the subject matter of this Policy.

Prior to Attachment of Risk, the Insured shall provide written confirmation that:

- *all quality control documents used by the Insured or by the Satellite manufacturer or by the launch service provider have been updated, AND*
- *the Satellite operational procedures available to the Insured incorporate all lessons learned from other satellites of a similar design as far as applicable to the Satellite, AND*
- *the launch service provider has incorporated all lessons learned on previous launch(es).*

B) CERTIFICATION:

Prior to Attachment of Risk, the Insured shall certify in writing to Insurers that:

(a) The Spacecraft, Launch Vehicle and all associated equipment used have passed qualification and acceptance tests including flight readiness review, and fully meet the requirements of the Contract or a written waiver has been issued and a summary of such waiver has been provided to Insurers;
(b) It has no knowledge if any deficiencies if the Spacecraft or any subsystem equipment, and/or component therein;
(c) No anomaly(is)/failure(s) or deviation(s) in performance have been identified by the Insured and/or reported to the Insured on any spacecraft manufactured by the Insured and/or same Launch Vehicle and/or Insured provided equipment of the ground or in-orbit of the same type; and
(d) Any anomaly(ies)/failure(s) or deviation(s) in performance identified or reported have been fully investigated by the Insured and/or Launch Vehicle Sub-Contractor I qddOrdance with the applicable quality procedure(s) and the Insured and/or Launch Vehicle Sub-Contractor

[159] "Les Spécificités des Contrats d'Assurance d'Objets Spatiaux", by Cédric Wells, dans Ravillon, supra, note 63, pp.63-65

has taken all steps to eliminate the risk of a similar anomaly on the Spacecraft and/or Launch Vehicle in accordance with the applicable quality procedure(s), and informed the Insurers of such anomaly(ies)/failure(s) or deviation(s) in performance and associated corrective steps if relevant to the Spacecraft.

2.2) *WARRANTIES, CONTINUED: IRIDIUM Article 7*

3. *Article 7*

4. ***REPRESENTATIONS AND WARRANTIES***

5. *The Contractor makes the representations and warranties contained in this Article 7. Each such representation and warranty shall be deemed made as of the execution date of this Contract, and if necessary, Contractor shall supplement such representations and warranties as of EDC.*

6. *7.1 Contractor's Performance. In connection with Contractor's performance of its obligations under this Contract, Contractor shall maintain its ISO 9001 certification and obtain and maintain AS9100 certification, perform work in a skillful and workmanlike manner and otherwise abide by common standards, practices, methods and procedures in the commercial aerospace industry (and not solely in the commercial launch services industry). For the avoidance of doubt and with the exception of any acts of Contractor Gross Negligence, Contractor's undertaking in this Section 7.1 does not apply to the performance of or liability with respect to any Launch Services following the moment of Intentional Ignition with respect to any Launch Service. With the exception of ISO 9001 and AS9100, Customer represents and warrants that its Satellite manufacturer Associate Contractor is subject to substantially similar contractual obligations as those set forth in this Section 7.1.*

ANNEXE 5.5: *CODE WARRANTY (AFTER ACCEPTANCE)*

6.1) *(i) CODE*[160].

Contractor represents and warrants that (i) it shall use commercially reasonable efforts to ensure that no viruses or similar items are coded or introduced into the Work; (ii) it shall not introduce into the Work any code that would have the effect of disabling or otherwise shutting down all or any portion of the Work; (iii) it shall not develop, or seek to gain access to the Work through, any special programming devices or methods, including trapdoors or backdoors, to bypass any Customer security measures protecting the Work; and (iv) the operation of the Work shall not be affected by the change of date on or after January 1, 2000. This warranty shall begin upon Final Acceptance of the Work embodying the code at

[160] XM Sat, supra, note 65.

issue and continue for the operating life of the Satellites and Ground Spare Satellite, and any optional Satellites which may be provided hereunder.

(j) REMEDIES.

(1) Notwithstanding anything to the contrary herein, Customer shall have the right at any time during the period of the warranties set forth in this Article 18.3 (Warranties for Deliverable Items) to require that any Work not conforming in any material respect to this Contract be promptly corrected or replaced (at Contractor's option and expense) with conforming Work, subject to paragraph (g) of Article 8.2 (Shipment Readiness Review) and paragraph (e) of Article 8.3 (Flight Readiness Review). If Contractor fails or is unable to correct or replace such defective Work within a reasonable period after notification from Customer, Customer may then require Contractor to repay such portion of the Contract Price as is equitable under the circumstances in lieu of repairing or replacing such defective Work.

*(2) **During the operational lifetime of the Satellites**, Contractor shall provide the following for software delivered under this Contract: with respect to software for ground equipment delivered hereunder, Contractor shall correct errors, including modifying code and making operational modifications, in such software as required for the Satellites to operate in accordance with Exhibit A (Spacecraft Performance Specifications) for the operating life of the Satellites; and with respect to flight firmware and software, Contractor shall, to the extent feasible, correct such firmware and software as required for the Satellites to operate in accordance with Exhibit A (Spacecraft Performance Specifications) for the operational lifetime of the Satellites. During the operational lifetime of the Satellites, Contractor shall, in a timely manner, provide access to engineering, software and operations support personnel, including and/or involving Contractor's Subcontractors and vendors, where feasible, for the purpose of resolving errors, problems, or issues relating to the ground equipment, software, data, and operations products to be Delivered pursuant to this Contract.*

(3) In the event Contractor, for whatever reason, fails to perform its obligations under paragraph (2) above, with respect to any flight or ground software delivered under this Contract, which software Contractor either owns or has rights in, Contractor agrees to provide Customer access to the source code and related documentation for such software so as to enable Customer to perform tasks contemplated by paragraph (2) above. With respect to other software (that is, software that Contractor does not own or have rights in), Contractor shall use its reasonable best efforts to provide Customer with similar access to source code and related documentation for such software. Contractor shall ensure that all of Contractor's source code for the flight firmware and software and ground software is appropriately maintained, stored, catalogued, and archived as necessary to maintain such source code to object code integrity.

ANNEXE 5.6: FORCE MAJEURE (*IRIDIUM*)

Article 22
FORCE MAJEURE

22.1 Neither Party shall be liable for any delay in the performance of its obligations under this Contract, or a delay or failure of performance of its first-tier contractor(s), if such delay or failure to perform is due to a Force Majeure event and provided that the affected Party seeking to invoke this Article 22 notifies the other Party in writing within five (5) Business Days after the occurrence of a Force Majeure event (or the date the affected Party reasonably became or should have become aware of the Force Majeure event), including a detailed description of the causes thereof and such Parties' Reasonable Efforts to avoid the Force Majeure event or mitigate the impact thereof, such as establishment of work-around plans, alternate sources, extended operations or other means, including use of alternate viable subcontractors. For the avoidance of doubt, failure by either Party timely to obtain any required governmental license, permit or authorization shall not be deemed a Force Majeure event.

22.2 If a delay or failure in the performance of a Party's obligations under this Contract is due to either Party or their subcontractor performing work under a DO/DX rated contract other than that to be performed under this Contract, such delay will be evaluated pursuant to the terms of this Article 22. For the avoidance of doubt, any delay due to a DO/DX rated order issued before or after EDC, where the specific impact is known or should have reasonably been known by the relevant Party and taken into account in connection with its performance obligations under this Contract, will not be considered a Force Majeure event.

22.3 If a Force Majeure event impacts a Launch Slot for any Launch Service to be performed under this Agreement, the affected Party seeking to invoke this Article 22 shall notify the other Party immediately, and as soon as possible thereafter, provide the information detailed in Section 22.1.

22.4 Any unavailability of a Launch Site or Launch Range for reasons due to the actions or omissions of the competent Launch Site or Launch Range authority and not primarily attributable to Contractor shall be deemed to be a Force Majeure event. For the avoidance of doubt, termination of a Launch Service by the competent Launch Site or Launch Range authority (or by the Launch Vehicle's flight termination system) due to the Launch Vehicle's failure to meet the applicable Contractor and Launch Site or Launch Range safety requirements and parameters that results in the unavailability of a Launch Site or Launch Range shall not be deemed to be a Force Majeure event. Furthermore, lack of compliance with the non-recurring Launch Vehicle qualification criteria provided for in Section 11.1.1(A)(ii) shall not be excused as a Force Majeure event. If requested by the non-affected Party, the affected Party shall provide reasonable evidence or justification supporting a Force Majeure event claimed under this Section 22.4.

*22.5 With respect to any Force Majeure event lasting up to [***…***] months (as applied to independent Force Majeure events in the aggregate or a specific Force Majeure event that temporarily ceases and subsequently re-occurs due to the original circumstances causing such Force Majeure event), the period of performance under this Contract with respect to the affected Launch Service(s) shall be extended without penalty by the duration of the Force Majeure event and Customer's obligation to make payments hereunder with respect to Launch Services due during the*

period of a Force Majeure event shall be extended for a period equal to the duration of the Force Majeure event without penalty.

*22.6 With respect to any Force Majeure event lasting more than [***…***] months (as applied to independent Force Majeure events in the aggregate or a specific Force Majeure event that temporarily ceases and subsequently re-occurs due to the original circumstances causing such Force Majeure event), Customer, upon written notice to Contractor, may terminate any affected Launch Service(s) not yet performed under this Contract. In the event of such termination, Contractor shall [***…***] associated with [***…***] by Contractor [***…***]. Any [***…***] shall be [***…***] to Customer [***…***] Days of [***…***].*

ANNEXE 5.7: *IRIDIUM ® Systems Re-orbit plan SOW*

Plan Execution Flexibility

Boeing's ability to modify the Re-Orbit schedule and satellite Re-Orbit groupings is necessary to accommodate system re-configuration changes, satellite system failures and any unplanned events which happen during Re-Orbit execution. Boeing will have maximum flexibility in these areas to insure the overall success of Re-Orbiting the Iridium Constellation.

*Agreements between Motorola and U.S.A.F. Space Command/NORAD associated with satellite tracking and close approach notification have been extended to Boeing. NORAD's support for simultaneous maneuvering of a least [***…***] satellites is essential to the Boeing Plan because limitations on the number of simultaneous maneuvering satellites could adversely impact Boeing's ability to complete the Boeing Plan in the scheduled time frame necessary to allow satellite re-entry and impact during the period that is covered by the Re-Orbit insurance policy.*
http://investor.iridium.com/secfiling.cfm?filingid=1193125-11-81407&cik

ANNEXE 6: *SPACE ACT AGREEMENTS GUIDE*

https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=1050&s=1I

Sample of Space Act Agreements (NASA) cross-waivers

2.2.9.1.1. Liability and Risk of Loss (Cross-Waiver with Flow Down Sample Clause)

A. Each Party hereby waives any claim against the other Party, employees of the other Party, the other Party's Related Entities (including but not limited to contractors and subcontractors at any tier, grantees, investigators, customers, users, and their contractors or subcontractor at any tier),

or employees of the other Party's Related Entities for any injury to, or death of, the waiving Party's employees or the employees of its Related Entities, or for damage to, or loss of, the waiving Party's property or the property of its Related Entities arising from or related to activities conducted under this Agreement, whether such injury, death, damage, or loss arises through negligence or otherwise, except in the case of willful misconduct.

B. Each Party further agrees to extend this cross-waiver to its Related Entities by requiring them, by contract or otherwise, to waive all claims against the other Party, Related Entities of the other Party, and employees of the other Party or of its Related Entities for injury, death, damage, or loss arising from or related to activities conducted under this Agreement. Additionally, each Party shall require that their Related Entities extend this cross-waiver to their Related Entities by requiring them, by contract or otherwise, to waive all claims against the other Party, Related Entities of the other Party, and employees of the other Party or of its Related Entities for injury, death, damage, or loss arising from or related to activities conducted under this Agreement.

2.2.9.1.2. Liability and Risk of Loss (Cross-Waiver of Liability for Agreements Involving Activities Related to the ISS Sample Clause) (Based on 14 C.F.R. 1266.102)

A. The objective of this Article is to establish a cross-waiver of liability in the interest of encouraging participation in the exploration, exploitation, and use of outer space through the International Space Station (ISS). The Parties intend that the cross-waiver of liability be broadly construed to achieve this objective.

C. Cross-waiver of liability:

1. Each Party agrees to a cross-waiver of liability pursuant to which each Party waives all claims against any of the entities or persons listed in paragraphs C.1.a. through C.1.d. of this Article based on Damage arising out of Protected Space Operations. This cross-waiver shall apply only if the person, entity, or property causing the Damage is involved in Protected Space Operations and the person, entity, or property damaged is damaged by virtue of its involvement in Protected Space Operations. The cross-waiver shall apply to any claims for Damage, whatever the legal basis for such claims, against:

- *a. Another Party;*
- *b. A Partner State other than the United States of America;*
- *c. A Related Entity of any entity identified in paragraph C.1.a. or C.1.b. of this Article; or*
- *d. The employees of any of the entities identified in paragraphs C.1.a. through C.1.c. of this Article.*

2. In addition, each Party shall, by contract or otherwise, extend the cross-waiver of liability, as set forth in paragraph C.1. of this Article, to its Related Entities by requiring them, by contract or otherwise, to:

- *a. Waive all claims against the entities or persons identified in paragraphs C.1.a. through C.1.d. of this Article; and*

b. *Require that their Related Entities waive all claims against the entities or persons identified in paragraphs C.1.a. through C.1.d. of this Article.*

3. For avoidance of doubt, this cross-waiver of liability includes a cross-waiver of claims arising from the Convention on International Liability for Damage Caused by Space Objects, which entered into force on September 1, 1972, where the person, entity, or property causing the Damage is involved in Protected Space Operations and the person, entity, or property damaged is damaged by virtue of its involvement in Protected Space Operations.

4. Notwithstanding the other provisions of this Article, this cross-waiver of liability shall not be applicable to:

a. *Claims between a Party and its own Related Entity or between its own Related Entities;*
b. *Claims made by a natural person, his/her estate, survivors or subrogees (except when a subrogee is a Party to this Agreement or is otherwise bound by the terms of this cross-waiver) for bodily injury to, or other impairment of health of, or death of, such person;*
c. *Claims for Damage caused by willful misconduct;*
d. *Intellectual property claims;*
e. *Claims for Damage resulting from a failure of a Party to extend the cross-waiver of liability to its Related Entities, pursuant to paragraph C.2. of this Article; or*
f. *Claims by a Party arising out of or relating to another Party's failure to perform its obligations under this Agreement.*

ANNEXE 7: *DISPUTE RESOLUTION ESA GCC CLAUSE 35*

CLAUSE 35: DISPUTE RESOLUTION

35.1 Conciliation

The Parties shall use their best efforts to settle any dispute arising out of the Contract amicably. Upon failure of reaching an amicable settlement the dispute may be submitted to arbitration as per the procedure described in sub-clause 35.2. Referral of a dispute to the Dispute Adjudication Board (DAB) shall not suspend the performance of the Contract or any part of it. If a dispute (of any kind whatsoever) arises out of the Contract between the Parties, either Party may refer the dispute to the DAB appointed by the Parties to that aim comprising of the following five (5) members; two senior representatives from each Party – one from the technical area and the other representing the area of procurement and the Agency's Industrial Ombudsman. The dispute shall be referred to the DAB In Writing, with the supporting Documentation attached and copy to the other Party. The DAB may, depending on the nature of the dispute, involve appropriate technical expertise or appoint a technical panel composed of technical expertise from both sides to advise on the matter at hand. Both Parties

shall promptly make available to the DAB, all information, Documentation, access to the facilities and the Parties' sites as the DAB may require for the purposes of making a decision on such dispute, subject to national or international security restrictions. The DAB shall issue its decision within two (2) Months from the submission of the written notification of the dispute to the DAB. In case the DAB fails to issue its decision within the above deadline, or in case either Party is dissatisfied with the DAB's decision, such Party may give written notice to the other Party of its dissatisfaction. In either event, this notice of dissatisfaction shall state that it is submitted under the present sub-clause and shall set out the matter in dispute and the reason(s) for dissatisfaction. If the DAB has given its decision within the abovementioned deadline and no notice of dissatisfaction has been submitted by either Party within ten (10) Working Days after receiving the DAB's decision, the Parties shall proceed in compliance with the decision of the DAB. Neither Party shall be entitled to submit a dispute to arbitration as per the provisions of the present sub-clause below, unless a notice of dissatisfaction has been given in accordance with the present sub-clause.

35.2 Arbitration

The Contract shall specify the country and location within that country where the Arbitration Tribunal shall sit; normally the Arbitration Tribunal shall have its seat in the country where the Contractor has its legal seat or where the Contract is to be executed. Arbitration proceedings shall be conducted in English unless otherwise agreed between the Parties. If no other arbitration is foreseen in the Contract, any dispute arising out of the Contract shall be finally settled in accordance with the Rules of Arbitration of the International Chamber of Commerce (ICC) by one or more arbitrators appointed in conformity with those rules. Conduct of such proceedings shall be in accordance with the ICC rules in force at the time arbitration is requested by either of the Parties. The award shall be final, conclusive and binding on the Parties; no appeal shall lie against it. The enforcement of the award shall be governed by the rules of procedure in force in the state/country in which it is to be executed.

BIBLIOGRAPHIE

LÉGISLATION

An Act to establish the Department of Homeland Security, and for other purposes (Homeland Security Act of 2002), 6 U.S.C.: Domestic Security.

Commercial Space Launch Competitiveness Act, H.R.2262 - U.S, accessible à : < https://www.congress.gov/bill/114th-congress/house-bill/2262/text>. (consulté le 18.02.2017).

Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection (https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure) [COM(2006) 786 final – Official Journal C 126 of 7.6.2007]. accessible à : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33260. (consulté le 23.03.2017).

COUNCIL DIRECTIVE 2008/114/ of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, accessible à : http://eur-lex.europa.eu/legal-ontent/EN/TXT/?uri=CELEX:32008L0114. (consulté le 12.04.2017).

European Parliament resolution of 12 June 2012 on ''Critical Information Infrastructure Protection – Achievements and Next steps: towards Global Cyber-security'', accessible à : http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF, (consulté le 18.02.2017).

French Space Operation Act (SOA) of June 3rd, 2008. Accessible à: http://download.esa.int/docs/ECSL/France.pdf. (consulté le 22.11.2016).

"National Security Space Strategy", Unclassified Summary, 2010. accessible à : < https://www.hsdl.org/?view&did=10828>. (consulté le 08.01.2017).

National Space Security Policy of the UK, accessible à : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307648/National_Space_Security_Policy.pdf (consulté le 14.04.2017).

National Strategy For Homeland Security, October 2007, accessible à : <https://www.dhs.gov/nationalstrategy-homeland-security-october-2007> (consulté le 30 mars, 2017)

UK Cabinet Office Summary of the 2016 Sector Security and Resilience Plans", produced by the Cabinet, accessible à : www.gov.uk/government/organisations/cabinet-office (consulté le 11.02.2017).

US National Space Security, Unclassified). Summary, January 2011, accessible à : http://archive.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf (consulté le 30 mars, 2017).

TFEU (Treaty Functioning EU), Internal Mkt Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004, establishing ENISA (OJ L 077, 13/03/2004.

JURISPRUDENCE

British Columbia Supreme Court, Atmospheric Diving Systems Inc. v. International Hard Suits Inc. (1994), 89 B.C.L.R. (2d) 356 (S.C), in Understanding, "Best Efforts" And Its Variants (Including Drafting Recommendations), by Kenneth A. Adams. Accessible à : http://www.adamsdrafting.com/downloads/Best-Efforts-Practical-Lawyer.pdf. (consulté le 03.03.2017).

Martin Marietta Corp. v. Intelsat, 763 F. Supp. 1327 (D. Md. 1991) U.S. District Court for the District of Maryland - 763 F. Supp. 1327 (D. Md. 1991) May 13, 1991, accessible à : http://law.justia.com/cases/federal/district-courts/FSupp/763/1327/1586244/. (consulté le 12.03.2017).

Telesat Canada v. Boeing Satellite Systems International, Inc., 2010 ONSC 4023

CONTRATS

BOEING: Fixed Price Contract for the P904 Telesat Canada v. Boeing Satellite Systems International, Inc., 2010 ONSC 4023

CALIFA ENTERTAINMENT: Transponder Service Agreement between Califa Entertainment Group Inc. and Loral SpaceCom Corp concerning Skynet transponder Servic, 1999, accessible à : http://contracts.onecle.com/playboy/loral.transponder.1999.02.08.shtml. (consulté le 23.03.2017).

DIGITAL GLOBE : SATELLITE PURCHASE AGREEMENT #8862, BY AND BETWEEN DIGITALGLOBE, INC. AND BALL AEROSPACE & TECHNOLOGIES CORP. October 2, 2006, accessible à : https://www.lawinsider.com/contracts/2D93BYAjimsHOylZMgU8gu/digitalglobe/purchase-agreement/2008-04-14, consulté le 14.06.2017.

ECHOSTAR : Contract between Echostar Operating Corporation and Space Systems/Loral, LLC for the Jupiter 2 Satellite Program, 2013, accessible à : http://licensing.fcc.gov/myibfs/download.do?attachment_key=1004726 , consulté le 18.06.2017.

ESA GCC : la version 2015 des GCC, accessible à : http://esamultimedia.esa.int/docs/LEX-L/Contracts/ESA_REG_002_rev2_new_Annex1_revised.pdf. (consulté le 17.04.2017).

HUGHES NETWORK : CONTRACT Between Hughes Network Systems, LLC And Space Systems/Loral, Inc. for the Hughes Jupiter Satellite Program, June 8, 2009, accessible à :

https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwirj-i-9cXUAhXPalAKHRUnAx4QFggzMAI&url=http%3A%2F%2Flicensing.fcc.gov%2Fmyibfs%2Fdownload.do%3Fattachment_key%3D829255&usg=AFQjCNHjYgxSMCAoM5krQUspTPskHshvEg&sig2=S7i6ou7deQSD0_Z1fPCs-w, consulté le 18.96.2017.

IRIDIUM : CONTRACT FOR LAUNCH SERVICES No. IS-10-008 Between Iridium Satellite LLC and Space Exploration Technologies Corp (Iridium 2010): 2.5 Primary and Backup Launch Site accessible à : http://investor.iridium.com/secfiling.cfm?filingid=1193125-11-81407&cik. (consulté le 02.02.2017).

XM SATELLITE : The clauses come from the Satellite Purchase Contract for In-Orbit Delivery - XM Satellite Radio Inc. and Boeing Satellite Systems International Inc., accessible à : http://contracts.onecle.com/xm/boeing.sat.2001.05.15.shtml. (consulté le 28.01.2017).

DOCTRINE

“Security Engineering: A Guide to Building Dependable Distributed Systems”, by Ross J. Anderson, 2nd Edition, April 2008 and “Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance”, by Stuart Jacobs, 2nd Edition, February 2016.

Bruneau Michel and Reinhorn Andrei: Overview of the Resilience Concept, Proceedings of the 8th U.S. National Conference on Earthquake Engineering, April 18-22, 2006, San Francisco, California, USA, accessible à : <https://www.eng.buffalo.edu/~bruneau/8NCEEBruneau%20Reinhorn%20Resilience.pdf> (consulté le 21 mars, 2017)

Cimellaro, Gian Paolo, ‘’Urban Resilience for Emergency Response and Recovery: Fundamental Concepts and Applications”, Springer 2016.

Gheroghe, Adrian V, (ed), “Infranomics, Sustainability, Engineering Design and Governance’, Springer, 2015

Gopalakrishnan, K and Peeta, S.,“Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent, Springer, 2010

Hollnagel E, Nemeth CP, and Dekker S.: Resilience Engineering Perspectives, vol 1: Remaining Sensitive to the Possibility of Failure, Ashgate Publishing Ltd., 2008.

Huth, Oliver and Roelandt, Rafael: Specific Aspects and Characteristics of Satellite Capacity Agreements in the Satellite Communication Business, in Contracting for Space, ed by LJ Smith and I. Baumann, Routledge, 2011, p. 161 p. 32.

Kaufmann, Mareile, ‘’Resilience, Emergencies and the Internet: Security In-Formation”, Routledge, Jun 14, 2017.

Kurzweil, Ray, ''The Singularity is Near'', New York: Penguin Group, 2005.

Loquin, E. 2008, Le partage des risques dans les contrats de location des transpondeurs, in Gestion et partage des risques dans les projets spatiaux, edited by L. Ravillon, Paris, Pedone, 11.

Monteiro de Lima Demange, Lia Helena : The Principle of Resilience, LAW: PELR: Vol. 30: Iss. 2 (2013), <http://digitalcommons.pace.edu/pelr/vol30/iss2/11/> consulté le 21 mars, 2017).

Muresan, Liviu, and Georgescu, Alexandru: The Road to Resilience in 2050, Critical Space Infrastructure and Space Security, Pages 58-66 | publié en ligne, 23 déc 2015. (consulté le 29.01.2017).

Ravillon, Laurence: Typology of Contracts in the Space Sector, in Contracting for Space, by LJ Smith and I. Baumann, Routledge, 2011

K-U Schrogl (ed.): Handbook on Space Security, Springer, 2015.

Senge, Peter M., ''The Fifth Discipline: The Art & Practice of the Learning Organization'', Doubleday and Currency, 1990.

Vincent-Jones, Peter,``Contractual Governance: Institutional and Organizational Analysis``, Oxf J Leg Stud (2000) 20 (3): 317-351.

Walker, Brian and Salt, David, "Resilience Thinking: Sustaining Ecosystems and People in a Changing World'', Island Press, 2012.

Weber, Rolf H., "Realizing a New Global Cyberspace Framework Normative Foundations and Guiding Principles: Global Cyberspace Framework", Springer, 2014.

White, Stewart et al., ''Satellite Communications in Europe: Law and Regulartion'', Longman, 1994.

CHAPITRES

Andersson and Malm, ''Public-Private Partnerships and the Challenge of Critical Infrastructure Protection'', in ``International CIIP Handbook 2006``, by Abele-Wigert, Isabelle, Myriam Dunn, Office for Official Publication of the European Communities, 2006, p.140.

Bank, Christan, ''The Complexities of International Space Industry Contracts, Ch 12, in, ''Contracting for Space: Contract Practice in the European Space Sector'', edited by Smith, L. J. and Baumann, I., Routledge, 2011.

Baumann, Ingo, ''The Use of Service Level Agreements in Space Projects", in, ''Contracting for Space: Contract Practice in the European Space Sector'', edited by Smith, L. J. and Baumann, I., Routledge, 2011, p. 25.

Bologna, Sandro, Fasani, Alessandro, and Martellini, Maurizio, “Fortress to Resilience”, in “Cyber Security Deterrence and IT Protection for Critical Infrastructures”, ed. by Maurizio Martellini, Springer, 2013.

Brunner, E. M., & Suter, M. (2008). International CIIP handbook 2008/2009. Center for Security Studies, (CSS), EHT Zurich, in Space as a Critical Infrastructure, by Markus Hesse and Marcus Hornung, Chapter 10, in Handbook on Space Security, ed. by Kai-Uwe Schrogl, Springer 2015, p.152

Creydt, Matthias et Horl, Kai-Uwe : ‘’Export Control Issues in Space Contracts”, Ch 24, in ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011

Couston, Mireille, ‘’Space Contracts: The Legal and Financial Liability Regime in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011.

Du Parquet, Alain, “Specific Clauses of LSAs”, in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011.

Elriz, M. and Newman, P.,“Contract Management”, by M. Elriz and P. Newman, Ch 20 in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011.

Gaycken, Krueger, Nickolay (eds.), “The Governance of Network and Information Security In the European Union: The European Public-Private Partnership for Resilience (EP3R)” in ‘’The Secure Information Society’’. Berlin: Springer Publ., 2012

Hesse, Markus and Hornung, Marcus: Critical Infrastructure, Chapter 10, in Handbook on Space Security, p.152, citing Commission of the Hesse, Markus, and Hornung, Marcus: Space as a Critical Infrastructure, citing the International CIIP in Handbook on Space Security, Ed. by Schrogl, K-U, Springer, 2015, p.152,

Huth, Oliver, and Roelandt, Rafael, “Specific Aspects and Characteristics of Satellite Capacity Agreements in the Satellite Communication Business”, in ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011, p. 32.

Ravillon, Laurence, “Typology of Contracts in the Space Sector”, in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011, p. 161.

Reinhorn, Andrei M. and Cimellaro, G. P., ‘’Consideration of Resilience of Communities in Structural Design”, in Performance-Based Seismic ‘’Engineering: Vision for an Earthquake Resilient Society’’, Fischinger, Chapter: 27, Publisher: Springer Netherlands, Editors: Fischinger M., pp.401-421, 2012.

Scharlach, Ines, “Performance and Warranty Articles in Space Industry Contracts”, in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011., p. 263.

Smith, L. J. and Baumann, I., “Conclusions and Outlook’’, Ch. 34, in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011.

Stjernevi, Gunilla and Katsampani, Eleni, “Space Contracting within the Framework of the European Space Agency”, in, ‘’Contracting for Space: Contract Practice in the European Space Sector’’, edited by Smith, L. J. and Baumann, I., Routledge, 2011, p. 181.

PÉRIODIQUES

Alexander, Jandria S, “Achieving Mission Resilience for Space Systems”, in Aerospace Corporation’s publication “CROSSLINK®”, V13, No 1 (Spring 2012), accessible à: http://www.aerospace.org/crosslinkmag/spring2012/achieving-mission-resilience-for-space-systems/. (consulté le 13.02.2017).

Folke, et al., ‘’ADAPTIVE GOVERNANCE OF SOCIAL-ECOLOGICAL SYSTEMS’’, Annual Review of Environment and Resources, Vol. 30:441-473 (21 Nov. 2005).

Georgescu, Alexandru; Botezatu, Ulpia-Elena; Popa, Alina-Daniela; Popa, Stefan; Arseni, Stefan Ciprian: ‘’CRITICAL INFRASTRUCTURE DEPENDENCY ON SPACE SYSTEMS’’, Scientific Bulletin "Mircea cel Batran" Naval Academy; Constanta19.1 (2016): 527.

Karpouzoglou, Timothy, et al., “Advancing adaptive governance of social-ecological systems through theoretical multiplicity’’, Environmental Science & Policy 57 (2016) 1–9.

Kaufmann, Mareile, “Resilience governance and ecosystemic space: a critical perspective on the EU approach to Internet security, Environment and Planning: Society and Space 2015, volume 33, pages 512 – 527.

Kitano, H.: ‘’Systems Biology: A Brief Overview’’. Science, 295, 1662–1664 (2002).

Hodgson, Dave, et al., ‘’Some Thoughts on Resilience What do you mean, ‘resilient’?’’, Feature Issue, in ‘’Trends in Ecology & Evolution’’, Volume 30, Issue 9, 503 – 506.

Holling, C.S., “Resilience and Stability of Ecological Systems’’, Annual Review of Ecology and Systematics, Vol. 4:1-23 (Nov 1973).

Humby Tracy-Lynn: ‘’Law and Resilience: Mapping the Literature’’, Seattle Journal of Environmental Law, V4 Issue 1, 2014. Accessible à : http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1032&context=sjel. (consulté le 20.02.2017).

Muresan, Liviu and Georgescu, Alexandru, "The Road to Resilience in 2050, Critical Space Infrastructure and Space Security", Pages 58-66 | Publié en ligne: 23 Déc 2015.

Pradham, Subhav et al. ''Towards a Resilient Deployment and Configuration Infrastructure for Fractionated Spacecraft'', Institute for Software-Integrated Systems, Vanderbilt University, Nashville, accessible à : http://www.dre.vanderbilt.edu/~gokhale/WWW/papers/APRES13_DnC.pdf (consulté le 20 Aug. 2017)

Reidenberg, Joel, "Lex Informatica: The Formulation of Information Policy Rules through Technology'', 76 Tex. L. Rev. 553 (1997-1998), accessible à : http://ir.lawnet.fordham.edu/faculty_scholarship/42 (consulté le 23.02.2017).

Wagner, A.: ''Robustness and Evolvability: A Paradox Resolved''. ProcBiolSci, 275, 91–100 (2008).

RAPPORTS

Brundtland Commission, formally known as the World Commission on Environment and Development (WCED), In Resilient Citiies. United Nation's 1972 Stockholm Conference. "Sustainable development" was presented by Ward and Dubos (1972).

Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007]ENISA: Enabling and managing end-to-end resilience — January 2011, accessible à : <https://www.enisa.europa.eu/publications/end-to-end-resilienc> (consulté le 12.02.2017)

COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection, accessible à : <http://eurlex.europa.eu/legal-ontent/EN/TXT/?uri=CELEX:32008L0114> (consulté le 18.02.2017)

Department of Defense (DoD) White Paper : "Space Domain Mission Assurance: A Resilience (Disaggregation, Distribution, Diversification, Protection, Proliferation) accessible à : < https://fas.org/man/eprint/resilience.pdf>. (consulté le 22.04.2017).

ENISA Report: "Enabling and managing end-to-end resilience", p. 31, accessible à : https://www.enisa.europa.eu/publications/end-to-end-resilience/at_download/fullReport. (consulté le 03.01.2017). [End2End]

ENISA Report : "Methodologies for the Identification of Critical Information Infrastructure Assets and Services: Guidelines for Charting Electronic Data Communication Network", accessible à : https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis. (consulté le 10.02.2017)

ENISA Report : ''National and International Cyber Security Exercises'', Final Report | 0.99 | DECEMBER 2015 2114 Cyber Europe:, p. 22. accessible à : https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises. (consulté le 04.04.2017).

ENISA Report: ''National Cyber Security Strategies (NCSSs)'', 2013. accessible à : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map. (consulté le 12.02.2017).

ENISA REPORT : ''Ontology and Taxonomies of Resilience Report'', accessible à : https://www.enisa.europa.eu/publications/ontology_taxonomies. (consulté le 12.01.2017).

ENISA Report: "Resilience of the Internet Interconnection Ecosystem" (Inter-X: Resilience of the Internet Interconnection Ecosystem Full Report), April 2011, accessible à : https://www.enisa.europa.eu/publications/interx-report, consulté le 01.03.2017.

ENISA Report: "Security Guide for ICT Procurement: Security Guide for Electronic Communications Service Providers", December 2014, accessible à : https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement. (consulté le 12.02.2017).

Hamerli, Berhard, and Renda, Andrea, "Protecting critical infrastructure in the EU. CEPS Task Force Report", 16 December 2010.

Pellegrino, Massimo, Stang, Gerald : "Space security for Europe Report", European Union for Security Studies by Massimo Pellegrino and Gerald Stang - No29 - 07 July 2016. Available at: http://www.iss.europa.eu/publications/detail/article/space-security-for-europe/. (consulté le 11.03.2017).

RAMSES: Climate change vulnerability and adaptation indicators. The European Topic Centre on Air and Climate Change (ETC/ACC), under contract of the European Environmental Agency (EEA,) Harley, M., Horrocks, L.,
Hodgson, N., van Minnen, J., 2008., Bilthoven,, N, in WP 2: Taxonomy of architecture and infrastructure indicators, D2.1:Synthesis review on resilient architecture and infrastructure indicators, Reference code: RAMSES – D2.1RAMSES PROJECT Grant Agreement n° 308497, Main authors: James Kallaos, Annemie Wyckmans (NTNU) and Gaëll Mainguy (IVE), Contributing authors: Ludivine Houssin, Georges Valentis (IVE), Floriana F. Ferrara (T6-ECO), Bernd Hezel, Ephraim Broschkowski (CMF), Astrid Westerlind-Wigström (ICLEI), Rolf André Bohne, Fernanda Pacheco (NTNU), Partners owning: NTNU and IVE, Contributions: T6 ECO, CMF, ICLEI, accessible à : http://www.ramsescities.eu/fileadmin/uploads/Deliverables_Uploaded/28022014_deliverable_ramses_d2_1.pdf >, consulté le 21.01.2017).

''Space Security Index 2016'', November 2nd, 2016. Section 3.4, accessible à : https://www.congress.gov/bill/114th-congress/house-bill/1678. (consulté le 06.12.2017).

UN Agenda 21, UNCED, 1992, accessible à : https://sustainabledevelopment.un.org/outcomedocuments/agenda21. (consulté le 23.03.2017).

UNIDROIT : art 1.11 of the UNIDROIT Working Group on Long-Term Contracts Principles, 2016, accessible à :

http://www.unidroit.org.cloud.seeweb.it/english/governments/councildocuments/2016session/cd-95-03-e.pdf; http://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016. (consulté le 20.03.2017).

Union of Concerned Scientists, "UCS Satellite Database", accessible à : <http://www.ucsusa.org/nuclearweapons/space-weapons/satellite-database.html#.VmXWlnYrLIV> (consulté le 20.04.2016).

ACTES DE COLLOQUES

Del Monte, Luca and Zatti, Stefano: "Preliminary Reflections About the Establishment of a Cyber-Security Policy for a Sustainable, Secure and Safe Space Environment", IAC, Jerusalem, 2015.

DeNardis, Laura and Raymond, Mark, ''Thinking Clearly About Multistakeholder Internet Governance'', GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013, accessible à : https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2354377_code895291.pdf?abstractid=2354377&mirid=1. (consulté le 14.03.2017).

Giobbe, Francesco and Vechiatto, Jean-Claude: ''La Gestion des Risques dans le Cadre d'un PFI: L'Exemple de Paradigm au Royaume-Uni, in Gestion et partage des risques dans les projets spatiaux'', Journée d'études de la commission spatiale Société Française de Droit Aérien et Spartial, Ed by Laurence Ravillon, Dijon 2007

Heinich, Julia : ''La Prévention Contractuelle du Contentieux", in "Le Réglement des Différends dans l'Industrie Spatiale", Colloquium Proceedings, CREDIMI 2015, ed. by Laurence Ravillon, Lexis Nexis, 2016.

Rapp, Lucien : "Space industrial war: Towards a risk of creeping takeovers in the global space industry?'', Manfred Lachs Conference, Montreal, 2016, accessible à : https://www.mcgill.ca/iasl/events/mlc2016, consulté le 19.06.2017.

Wells, Cedric., "Les Spécificités des Contrats d'Assurance d'Objets Spatiaux", by Cédric Wells, in Ravillon, « Gestion et partage des risques dans les projets spatiaux », ed. by L. Ravillon, Paris, Pedone, 2007, pp.63-65.

VIDÉO

''A World Without Satellites?'', World Economic Forum, 2012, accessible à : https://www.weforum.org/open-forum/event_sessions/a-day-without-satellites-a8646c27-68ae-499e-98b9-1166041b14db/, consulté le 20.06.2017.