Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Berne, le 25 octobre 2023

« Cyberrisques dans l'espace »

Rapport du Conseil fédéral en réponse au postulat 21.4176 Bellaiche « Cyberrisques dans l'espace » du 17 décembre 2021

Table des matières

Condensé

L'importance et l'utilisation de l'espace ne cessent de croître, et avec elles les liens de dépendance vis-à-vis des applications associées. En conséquence, les vulnérabilités directes et indirectes liées à d'éventuelles défaillances des services spatiaux ou des manipulations ciblées se sont elles aussi accrues. Ces évolutions vont de pair avec la numérisation croissante des processus de l'État et de la société. Les satellites, pilotés par logiciels, sont également concernés par cette vague de numérisation, ce qui élargit l'exposition aux attaques de ces applications à l'ensemble de leur système. L'interconnexion numérique accrue et la diversification des acteurs et des chaînes d'approvisionnement se traduisent, comme pour les applications terrestres, par une augmentation des cyberrisques. La cybermenace émanant d'acteurs étatiques malveillants et de criminels pèse sur les applications aussi bien terrestres que spatiales. Dans ce contexte, l'interface critique entre espace et cybersécurité prend toujours plus d'importance.

Au regard de ces évolutions et de la situation internationale actuelle en matière de politique de sécurité, le présent rapport fournit un état des lieux concernant les liens de dépendance critiques de la Suisse pour assurer sa stabilité en matière de sécurité et d'approvisionnement vis-à-vis des services et capacités des infrastructures spatiales. Par ailleurs, il identifie des mesures qui permettraient d'élargir la marge de manœuvre de la Suisse. Face à des dépendances et des vulnérabilités croissantes, la Suisse pourra mieux se protéger en mettant en place un système redondant, en développant de manière ciblée ses propres capacités ou encore en soutenant des infrastructures nationales.

La diversification des acteurs et services spatiaux ainsi que les tendances technologiques entraînent une augmentation des cyberrisques pour notre pays. Le présent rapport détaille ces cyberrisques pour les trois segments des infrastructures spatiales (segment sol, liaison de données et segment spatial). Le rapport parvient à la conclusion que la Suisse, avec un portefeuille d'infrastructures spatiales relativement limité et peu critique en termes d'approvisionnement et de sécurité, dispose de possibilités restreintes pour renforcer la cybersécurité de l'exploitation à un niveau purement national. En tant que place de recherche et de développement de technologies employées dans des infrastructures spatiales, la Suisse peut toutefois engager des mesures de renforcement de la cybersécurité dès la phase de développement, ou créer des incitations ou normes sectorielles pour le développement et la production.

Le rapport présente également l'engagement de la Suisse dans des instances multilatérales, des organisations internationales et des programmes de développement consacrés à des thématiques spatiales, et à l'interface entre espace et cybersécurité. La Suisse participe activement à différents organes de l'ONU, que ce soit dans les domaines des utilisations pacifiques, sûres et durables de l'espace, de la gouvernance de l'espace (UNCOPUOS et UNGA), de la coordination de l'utilisation de la radiocommunication et des positions orbitales de tous les satellites (UIT) ou de la météorologie (OMM) et la météorologie spatiale (OMM et UNCOPUOS). La Suisse est membre fondateur d'organisations intergouvernementales telles que l'ESA ou EUMETSAT. Du fait de sa participation à différentes composantes du programme spatial européen, elle peut prendre part à la conception des systèmes internationaux d'infrastructures spatiales et a, de fait, accès aux infrastructures importantes pour elle, tout comme aux données et services en résultant. Pour défendre ses intérêts, préserver son accès à l'espace et accroître sa résilience ainsi que sa compétitivité et sa pertinence dans ce domaine, la Suisse a besoin d'une coopération internationale. Le rapport identifie des mesures à même d'élargir sa marge de manœuvre. Concrètement, il s'agit de poursuivre l'engagement de notre pays au sein de forums internationaux en faveur d'une utilisation pacifique, sûre et durable de l'espace, ainsi que d'intensifier la coopération internationale dans la recherche et les projets spatiaux. Il convient en particulier de développer la collaboration avec l'ESA, EUMETSAT et l'UE dans le domaine spatial, de créer des synergies avec des organisations nationales et de garantir l'accès aux procédures internationales de passation de marchés.

Le rapport présente enfin la situation juridique qui s'applique lors de la transmission de données dans l'espace. Compte tenu de l'essor des prestations spatiales commerciales, les acteurs de l'espace sont de plus en plus diversifiés. La situation juridique lors de la transmission de données dans l'espace devient donc plus complexe, à l'instar des évolutions juridiques rencontrées pour l'internet ou l'intelligence artificielle. Le cadre juridique suisse applicable à la transmission des données dans l'espace est fixé par la loi sur les télécommunications. Le 16 février 2022, le Conseil fédéral a décidé de l'élaboration d'un projet de consultation concernant une loi relative à l'espace. La Confédération a également des options dans ce domaine. Compte tenu de la dimension mondiale de la thématique, la Suisse suivra de près les débats juridiques menés au sein des forums internationaux consacrés au statut légal des données transmises et enregistrées dans l'espace

1 Introduction

Les applications spatiales s'invitent de multiples façons dans les activités quotidiennes des milieux économiques, de la société et de l'État. Les coordonnées GPS et les relais spatiaux sont devenus des composantes essentielles non seulement des réseaux de communication mondiaux et des prévisions météorologiques, mais aussi des exploitations agricoles, des réseaux électriques, des réseaux de transport, des distributeurs de billets et des montres numériques. En parallèle, l'utilisation militaire de l'espace s'est également accrue et elle évoluera rapidement dans les années à venir. L'importance croissante et l'utilisation grandissante de l'espace font également croître les dépendances vis-à-vis des applications spatiales associées. En conséquence, les vulnérabilités directes et indirectes liées à d'éventuelles défaillances des services spatiaux ou des manipulations ciblées se sont elles aussi accrues. Une panne de services satellitaires, même partielle, peut être suivie d'effets dès lors que ces services sont utilisés sans redondances sûres et suffisantes.
L'utilité, les dépendances et les vulnérabilités croissantes des applications spatiales vont de pair avec une numérisation progressive des activités de l'État et de la société. Les satellites, pilotés par logiciels, sont eux aussi touchés par cette vague de numérisation, ce qui élargit l'exposition aux attaques de ces applications à l'ensemble de leur système. Par ailleurs, le nombre d'acteurs publics et privés dans le secteur spatial ne cesse d'augmenter, avec pour but de développer, fabriquer et exploiter des infrastructures de services satellitaires. L'interconnexion numérique accrue et la diversification des acteurs et des chaînes d'approvisionnement se traduisent, comme pour les applications terrestres, par une augmentation des cyberrisques.[1] La cybermenace émanant d'acteurs étatiques malveillants et de criminels pèse sur les applications aussi bien terrestres que spatiales. Dans ce contexte, l'interface critique entre espace et cybersécurité prend toujours plus d'importance.

La guerre en Ukraine a mis en évidence la criticité de cette interface, tant en ce qui concerne le nouvel emploi d'infrastructures spatiales pour mener la guerre que la vulnérabilité des systèmes spatiaux et l'exposition accrue aux attaques du fait de la mise en réseau numérique.[2] L'exemple suivant porte sur des satellites utilisés en tant que système fiable et redondant en cas de conflit. Souhaitant affaiblir les capacités de commandement de l'armée ukrainienne, la Russie a gravement endommagé la structure d'information et de communication terrestre ukrainienne. Toutefois, la constellation de satellites d'une entreprise américaine a non seulement permis à la téléphonie mobile de fonctionner à nouveau, mais aussi de mettre à disposition des canaux particulièrement performants pour une utilisation militaire. La résistance de cette constellation de satellites a contré les tentatives russes de perturbation de ce système.[3] De plus, les moyens d'exploration et d'observation aériennes, absents ou inutilisables, ont pu être compensés par des images satellitaires fournies à l'Ukraine par différents partenaires commerciaux soutenant le pays.[4] Un deuxième exemple, encore tiré du conflit en Ukraine, montre en revanche dans quelle mesure un système spatial en réseau peut élargir la surface d'attaque et exposer des non-belligérants à des dommages collatéraux. Au début de la guerre en Ukraine, une cyberattaque visant une station terrestre d'un exploitant commercial de satellites a altéré le système de contrôle d'une infrastructure critique en Allemagne. Or, un client de l'opérateur de satellites, qui exploite des éoliennes sur les côtes allemandes de la mer du Nord, pilote ses turbines éoliennes par satellite. La cyberattaque russe contre cet opérateur de satellites a alors endommagé temporairement la commande à distance des turbines éoliennes.[5] Compte tenu de l'extension de la surface d'attaque à des acteurs commerciaux fournissant des services spatiaux, des dommages collatéraux peuvent être plus fréquents en cas de conflit.[6]
Les incidents de ce type sont inquiétants sur le plan de la politique nationale et de la politique de sécurité. Ils ont mis sur le devant de la scène mondiale des questions relatives à la sécurité de ces systèmes en réseau. La Suisse est également concernée par des cyberrisques dans l'espace du fait de sa dépen-

[1] Voir The Aerospace Corporation, Protecting Space Systems from Cyber Attack, <https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368> (consulté le 19 février 2023).

[2] Conseil fédéral suisse, Rapport complémentaire au rapport sur la politique de sécurité 2021, sur les conséquences de la guerre en Ukraine, 2022, <file:///C:/Users/frenc/Downloads/Politique-securite-Suisse-Rapport-complementaire-Conseil-federal-2021.pdf>.

[3] Cet exemple montre également comment un État peut, du fait de l'utilisation d'un système privé, se retrouver dans une relation de dépendance avec une entreprise privée dont les intérêts ne correspondent pas forcément en totalité à la stratégie de l'État. <https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk>. (consulté le 10 janvier 2023)

[4] P. ex. Palantirs MetaConstellation, qui alimente directement les images de centaines de satellites dans la plateforme ukrainienne Delta. <https://www.palantir.com/offerings/metaconstellation/> (consulté le 15 février 2023).

[5] «Les États-Unis, la Grande-Bretagne et l'UE ont attribué ces cyberattaques à la Russie. (…) Les attaques visaient très probablement à perturber les canaux de communication utilisés par l'armée ukrainienne. Elles ont toutefois eu des répercussions sur plusieurs pays et sur des équipements de communication sans lien avec les opérations de guerre. Plusieurs éoliennes en Europe ont notamment été touchées. Elles ont continué à produire de l'électricité en mode autonome, mais ne pouvaient plus être surveillées et commandées à distance par les entreprises exploitantes.» pp. 73-74; Le Conseil fédéral suisse, La sécurité de la Suisse 2022, 2022, <https://www.newsd.admin.ch/newsd/message/attachments/72369.pdf> (consulté le 12 janvier 2023).

[6] En septembre 2022, le responsable de la délégation russe dans un groupe de travail des Nations Unies (ONU) a déclaré au sujet des menaces spatiales que des satellites commerciaux utilisés en soutien de forces militaires adverses pouvaient également constituer une « cible légitime de mesures de représailles ». KATRINA MANSON, The Satellite Hack Everyone is Finally Talking About, Bloomberg, 2023, <https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/#xj4y7vzkg> (consulté le 2 mars 2023).

dance vis-à-vis de tiers. L'engagement accru de moyens cyber pour la préparation et l'appui des actions militaires dans des conflits internationaux est un facteur influençant l'évaluation des risques.[7] Outre les cyberattaques ciblées et intentionnelles, dans un contexte militaire ou non, les cyberrisques pour les infrastructures spatiales résultent également de phénomènes naturels et d'erreurs techniques.
Du fait de la diversification des acteurs, de petits pays dotés de solides secteurs de la recherche et du développement peuvent aussi être actifs et influents dans les forums et consortiums internationaux. La place industrielle et scientifique suisse, forte d'un nombre croissant d'acteurs menant des activités spatiales importantes, est représentée dans des communautés scientifiques internationales, des instances et des consortiums.[8]
Au regard de ces évolutions et de la situation internationale actuelle en matière de politique de sécurité, le présent rapport fournit un état des lieux des cyberrisques pesant sur la Suisse du fait de ses liens de dépendance vis-à-vis des infrastructures spatiales. Il importe de souligner que les cyberrisques dans l'espace découlent des mêmes menaces que celles pesant sur les cyberinfrastructures terrestres, c'est-à-dire qu'ils ne sont pas exclusivement liés à des conflits. Les infrastructures spatiales peuvent être attaquées par des acteurs étatiques et criminels, en temps de guerre et de paix, au cours de la mise en place ou de l'exploitation.
Le rapport met en lumière les liens de dépendance critiques de la Suisse vis-à-vis des infrastructures spatiales, les cyberrisques résultant de ces dépendances, la marge de manœuvre internationale de notre pays et la situation juridique en matière de transmission de données.

1.1 Contexte stratégique de la Suisse

Les cyberrisques dans l'espace sont une thématique à laquelle s'attèlent plusieurs départements et services de l'administration fédérale. En 2023, la politique spatiale et celle relative à la cybersécurité sont traitées séparément. La politique spatiale suisse est du ressort du Conseil fédéral.[9] Le Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI) promeut et coordonne les activités suisses d'exploration et d'utilisation de l'espace. Différents départements et offices fédéraux sont impliqués dans l'élaboration et la mise en œuvre de la politique spatiale suisse. Sur mandat du Conseil fédéral, une coopération et une coordination efficaces sont assurées par le Comité de coordination interdépartemental des questions spatiales (IKAR), dont la présidence et le secrétariat incombent au SEFRI.[10]
Considérant l'extension de l'utilisation des applications spatiales ainsi que la diversification et l'augmentation du nombre d'acteurs opérant dans le domaine spatial, le Conseil fédéral a décidé d'actualiser la politique spatiale suisse de 2008 et adopté une nouvelle politique spatiale le 19 avril 2023.[11] En tenant compte de divers documents stratégiques de la Confédération, cette politique forme le cadre général de la gestion des affaires spatiales par la Confédération.[12] La Politique spatiale 2023 se concentre sur trois axes stratégiques : (1) accès et résilience par des participations ciblées à des programmes, des contributions visant à renforcer la capacité d'agir de la Suisse, et un engagement en faveur d'une utilisation durable et responsable de l'espace, (2) compétitivité et pertinence grâce à l'excellence scientifique et à des entreprises compétitives et (3) partenariat et fiabilité dans la coopération internationale et envers les milieux économiques suisses, les milieux scientifiques et les groupes d'utilisateurs.
Concernant les cyberrisques dans l'espace, la Politique spatiale 2023 insiste sur la vulnérabilité des infrastructures spatiales et le besoin de sécurité et de défense dans le secteur au regard de la militarisation croissante de l'espace : « Les capacités militaires créées rendent possibles des actions hostiles sur des cibles spatiales ou terrestres comme p. ex. la destruction de satellites ou des cyberattaques. »[13]
La politique spatiale attire également l'attention sur les dépendances croissantes vis-à-vis des infrastructures spatiales : « L'utilisation très diverse et quotidienne de données et de services provenant de l'es-

[7] Le Rapport sur la politique de sécurité 2022 du Conseil fédéral et son Rapport complémentaire sur les conséquences de la guerre en Ukraine (2022) soulignent l'importance croissante des entreprises technologiques et de leur collaboration avec des États. En font notamment partie les fabricants et exploitants d'infrastructures spatiales mentionnés. Le Conseil fédéral suisse, La sécurité de la Suisse 2022, 2022, <https://www.newsd.admin.ch/newsd/message/attachments/72368.pdf> (consulté le 12 janvier 2023); Conseil fédéral, Rapport sur la politique de sécurité 2021 du Conseil fédéral et son Rapport complémentaire sur les conséquences de la guerre en Ukraine, <file:///C:/Users/frenc/Downloads/Politique-securite-Suisse-Rapport-complementaire-Conseil-federal-2021-1.pdf>.

[8] En novembre 2021 par exemple, le ministère estonien de l'économie a organisé la Cyber and Space Security Conference et depuis 2021, l'ESA organise avec le CYSEC (EPFL Innovation Park, Lausanne) la Conférence CYSAT PARIS avec le seul «European satellite hacking challenge» existant à l'heure actuelle <https://estonia.ee/cssc/>. <https://www.cysec.com/hack-cysat-europes-first-satellite-hack/>.

[9] Le Conseil fédéral s'appuie par ailleurs sur les recommandations de la Commission fédérale pour les affaires spatiales (CFAS), <https://www.sbfi.admin.ch/sbfi/fr/home/recherche-et-innovation/affaires-spatiales/cfas.html> (consulté le 6 juillet 2023). Le centre de compétence de la Confédération pour les questions nationales et internationales relevant du domaine spatial est la division Affaires spatiales du Secrétariat d'État à la formation, à la recherche et à l'innovation SEFRI, <https://www.sbfi.admin.ch/sbfi/fr/home/recherche-et-innovation/affaires-spatiales/politique-spatiale-de-la-suisse.html> (consulté le 6 juillet 2023).

[10] Ibid.

[11] Conseil fédéral, Politique spatiale 2023, 19 avril 2023, <file:///C:/Users/frenc/Downloads/publikation_weltraum_politik_2023_f-1.pdf>.

[12] P. ex. les Rapports sur la politique de sécurité 2016 et 2021, la Stratégie de politique extérieure 2020-2023, la Stratégie de maîtrise des armements et de désarmement 2022-2025 et la Stratégie pour le développement durable 2030. Politique spatiale 2023, 2023, p. 2.

[13] Politique spatiale 2023, 2023, p. 12.

pace accroît la dépendance vis-à-vis des infrastructures spatiales, augmentant ainsi leur vulnérabilité aux pannes ou aux détériorations. De telles dépendances sont particulièrement critiques si elles concernent la sécurité nationale proprement dite. »[14] Le rapport détaille ces dépendances au chapitre 2 « Liens de dépendance de la Suisse vis-à-vis des infrastructures spatiales ».
Le présent rapport s'appuie sur la Politique spatiale 2023 pour en tirer des mesures permettant de réduire les risques auxquels la Suisse est exposée du fait de ses dépendances vis-à vis des infrastructures spatiales. Le premier grand axe « Accès et résilience » déduit des mesures pour notre pays visant à accroître la sécurité des infrastructures spatiales. Les mesures des champs d'action « Compétitivité et pertinence » et « Partenariat et fiabilité » s'appliquent aussi majoritairement à l'interface entre espace et cybersécurité et sont appliquées en conséquence à cette interface dans le présent rapport.
D'autres documents stratégiques du Conseil fédéral abordent les aspects de la sécurité et de l'approvisionnement des infrastructures spatiales, notamment le Rapport sur la politique de sécurité 2021[15], la Stratégie de politique extérieure 2020-2023[16], la Stratégie de politique extérieure numérique 2021-2024[17] et la Stratégie de maîtrise des armements et de désarmement 2022-2025[18]. Ils servent de bases supplémentaires au présent rapport pour tirer des mesures de réduction des cyberrisques. La politique de cybersécurité de la Suisse est pilotée par le Centre national pour la cybersécurité (NCSC). En transformant le NCSC en office fédéral, le Conseil fédéral témoigne de l'importance qu'il accorde à la cybersécurité. Il a ainsi décidé que le NCSC serait rattaché au Département fédéral de la défense, de la protection de la population et des sports (DDPS), devenant ainsi un office fédéral à part entière dès janvier 2024. Le NCSC est chargé de l'élaboration et de la mise en œuvre coordonnée de la cyberstratégie nationale (CSN)[19], qui préconise des mesures pour réduire les cyberrisques au sein de la Confédération, des cantons, des milieux économiques et des hautes écoles. La CSN définit des mesures pour standardiser et promouvoir la résilience des infrastructures critiques face aux cyberrisques, sans toutefois aborder de manière spécifique les cyberrisques liés aux infrastructures spatiales. Le présent rapport s'appuie sur les objectifs stratégiques et les principes de la CSN pour déduire des mesures permettant de protéger la Suisse contre ces cyberrisques en particulier.
D'autres stratégies de la Confédération renvoient ponctuellement à l'interface espace-cybersécurité. La ligne de conduite politique du domaine Cyberdéfense, la Stratégie cyber du DDPS, renvoie au potentiel existant en matière de coordination entre les sphères d'opérations Cyber et Espace, en particulier pour les missions de l'armée. La Stratégie cyber du DDPS n'a toutefois pas de vocation interdépartementale.[20] Les cyberrisques dans l'espace sont également traités dans l'interface entre protection de la population et domaine cyber : la Stratégie nationale de protection des infrastructures critiques 2018 – 2022 (PIC) souligne les vulnérabilités d'infrastructures critiques si des services spatiaux fournis par des tiers (p. ex. Global Positioning System, GPS ou Galileo) venaient à tomber en panne.[21]

Dans ce contexte, le Conseil national a, en adoptant le postulat 21.4176 « Cyberrisques dans l'espace » en date du 17 décembre 2021, prié le Conseil fédéral « d'établir une vue d'ensemble qui présentera la situation de la Suisse face à la numérisation croissante de l'espace et aux cyberrisques qui y sont inhérents, et de formuler les mesures qui s'imposent dans ce contexte. » Les stratégies concernant l'interface entre espace et cybersécurité ont été renouvelées en 2023 et intégrées dans le présent rapport. Le 5 avril 2023, la nouvelle CSN globale a été adoptée par le Conseil fédéral[22], puis la Politique spatiale 2023 le 19 avril 2023 et la stratégie PIC actualisée le 16 juin 2023.[23]

[14] Ibid.

[15] Ainsi, le Rapport sur la politique de sécurité 2021 du Conseil fédéral renvoie par exemple, dans le développement du modèle de conflit, à des opérations relevant du domaine spatial et à l'importance de services spatiaux tels que la navigation ou la communication par satellite pour des États, les milieux économiques et la société. En guise de mesures de renforcement de la résilience et de la sécurité d'approvisionnement en cas de crises internationales, sont cités la consolidation de l'accès à des services utilisant l'espace pour la communication, la navigation et l'observation de la Terre, ainsi que l'engagement international en faveur de l'utilisation durable et pacifique de l'espace extra-atmosphérique. La politique de sécurité de la Suisse. Rapport du Conseil fédéral (2021) FF 2021 2895, pp. 10, 45.

[16] Stratégie de politique extérieure 2020-2023, 2020, <https://www.eda.admin.ch/content/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/Aussenpolitische-Strategie-2020-23_FR.pdf>.

[17] Stratégie de politique extérieure numérique 2021–2024, 2020, <https://www.eda.admin.ch/content/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf>.

[18] Stratégie de maîtrise des armements et de désarmement 2022–2025, 2022, <https://www.eda.admin.ch/content/dam/eda/fr/documents/aussenpolitik/strategien/strategie-ruestungskontrolle-und-abruestung-2022-2025-FR.pdf>.

[19] Le Conseil fédéral, Centre national pour la cybersécurité (NCSC), Cyberstratégie nationale (CSN), 2023, <file:///C:/Users/frenc/Downloads/Nationale-Cyberstrategie-NCS-2023-04-13-FR.pdf>.

[20] L'administration fédérale répartit les responsabilités en matière de cyberrisques dans trois domaines: cybersécurité, cyberdéfense et poursuite pénale de la cybercriminalité. Stratégie cyber du DDPS, 2021, p. 21, <https://www.newsd.admin.ch/newsd/message/attachments/66200.pdf>.

[21] Stratégie nationale de protection des infrastructures critiques 2018-2022, FF 2018, 503 ss, p. 513.

[22] Cyberstratégie nationale CSN, 2023.

[23] La nouvelle politique spatiale accorde davantage d'importance à l'interface critique entre domaine cyber et espace. Politique spatiale 2023, 2023, pp. 12, 14; Stratégie nationale de protection des infrastructures critiques, 2023, FF 2023, 1659.

1.2 Mandat

Le présent rapport répond au postulat 21.4176 intitulé « Cyberrisques dans l'espace » du 30 septembre 2021, déposé par la Conseillère nationale Judith Bellaiche et transmis le 17 décembre 2021. Le postulat est formulé comme suit.

> *Le Conseil fédéral est prié d'établir une vue d'ensemble qui présentera la situation de la Suisse face à la numérisation croissante de l'espace et aux cyberrisques qui y sont inhérents, et de formuler les mesures qui s'imposent dans ce contexte.*

Il est motivé comme suit.

> *En janvier 2021, un rapport du CSS de l'EPF de Zurich a relevé une tendance à l'utilisation croissante de l'espace pour la transmission de données à des fins étatiques et commerciales. Ces prochaines années, des dizaines de milliers de petits satellites commerciaux seront mis en orbite, ce qui nous mettra devant le fait accompli sur des questions telles que la souveraineté en matière d'utilisation de l'espace et créera des situations de dépendance. La Suisse ne dispose pas de son propre parc de satellites et elle est particulièrement dépendante d'autres Etats et d'entreprises étrangères. Cela soulève des questions sur le maintien de la sécurité des données étatiques (militaires) et privées.*
> *Dans un rapport, le Conseil fédéral présentera sa stratégie concernant ces évolutions et les cyberrisques qui y sont inhérents pour l'Etat, pour les entreprises et pour les particuliers. Le rapport exposera notamment les points suivants:*
>
> - *les liens de dépendance de la Suisse vis-à-vis des infrastructures spatiales,*
> - *les probables cyberrisques qui en découlent,*
> - *la marge de manœuvre et l'influence de la Suisse dans certaines agences et certains consortiums,*
> - *la possibilité de participer à un système européen de communication par satellite,*
> - *l'examen de la situation juridique lors de la transmission de données dans l'espace et la formulation des mesures requises.*

Dans sa prise de position du 24 novembre 2021 relative au postulat, le Conseil fédéral a constaté que dans le contexte de la numérisation croissante de l'espace, les cyberrisques qui en découlent requièrent de l'attention et que du point de vue de la cybersécurité et de la cyberdéfense, l'espace et les satellites ne sont pas les seuls en point de mire. Les infrastructures terrestres et les flux de données servant à l'utilisation des satellites doivent aussi être considérés dans leur globalité. Il est donc indiqué de s'occuper globalement de la numérisation de l'espace et des cyberrisques qui y sont inhérents.

Le présent rapport en réponse au postulat définit tout d'abord des termes clés et des concepts afin d'introduire la thématique. Aux chapitres 2 à 6, les cinq questions clés du postulat sont ensuite traitées selon l'état actuel des connaissances. Dans les différents récapitulatifs, des conclusions et des mesures sont déduites des réponses apportées. La question clé de la marge de manœuvre et de l'influence de la Suisse dans certaines agences et certains consortiums est traitée sommairement. La Confédération, dans son rôle d'instance étatique, n'est pas représentée dans des consortiums privés, ces derniers ne sont donc pas l'objet du présent rapport.
Le rapport s'intéresse également aux cyberrisques pertinents pour la Suisse en matière de sécurité et d'approvisionnement des infrastructures spatiales dans leur ensemble. Il insiste sur les cyberrisques pesant sur les prestations et les compétences civiles de l'administration fédérale et des infrastructures critiques. Les cyberrisques pour les services et les infrastructures d'autres niveaux administratifs n'en sont pas moins importants, mais ils ne sont pas traités de façon explicite dans ce cadre. Tous les chiffres et faits figurant dans le présent rapport reposent sur des informations accessibles au grand public.

1.3 Définition des notions et concepts

Les notions et concepts essentiels pour la compréhension de ce rapport sont expliqués ci-après.[24] Le rapport propose également une introduction aux structures globales des infrastructures spatiales, sans s'attarder sur les détails techniques.

[24] D'autres termes techniques sont expliqués au chap. 9 « Glossaire ».

1.3.1 Cyberinfrastructures, cyberrisques et cybersécurité

Le présent rapport utilise les termes se rapportant aux cyberrisques conformément à la terminologie de la CSN. Les termes déterminants qui y figurent sont les suivants.

- **Cyberinfrastructures :** infrastructures d'information et de communication (matériel et logiciel), qui échangent, créent, enregistrent et traitent des données ou les transforment en actions (physiques).[25]
- **Cyberrisque :** risque d'un événement (mesuré au moyen du produit de la probabilité de survenance et de l'ampleur des dommages), nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements.[26]
- **Cybersécurité :** ensemble des mesures visant à prévenir et gérer les incidents, à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet.[27]

1.3.2 Cybermenace

La CSN définit la cybermenace comme toute circonstance susceptible de causer un cyberincident. La cybermenace a une influence directe sur la probabilité de survenance d'un cyberincident et donc sur la dangerosité des cyberrisques.
La CSN établit une distinction entre les cyberincidents causés par des cyberattaques et ceux causés par des erreurs humaines, des défaillances techniques ou des développements techniques.
Elle distingue cinq types de cyberattaques en fonction de l'objectif des attaques, des acteurs impliqués et des cibles visées.[28]

- **Cybercriminalité :** sont considérées comme cybercriminelles des infractions commises contre des infrastructures TIC (technologies de l'information et de la communication) ou rendues possibles par les TIC. Dans la cybercriminalité, le mobile de l'enrichissement (monétaire) est au premier plan. Comme le but des auteurs de ces attaques n'est pas de compromettre le fonctionnement de la société, de l'économie ou de l'État, les effets immédiats se limitent en général aux victimes concernées. La cybercriminalité est la menace présentant la probabilité de survenance la plus élevée.
- **Cyberespionnage :** les attaques de cyberespionnage visent à s'emparer d'informations confidentielles à des fins politiques, militaires ou économiques, ou à observer les activités des victimes. Le cyberespionnage est pratiqué par des acteurs aussi bien étatiques que non étatiques. En général, les conséquences ne sont pas immédiatement visibles, car les préjudices politiques et économiques n'apparaissent qu'au moment où les auteurs des attaques mettent à profit les connaissances qu'ils ont acquises. En outre, de telles opérations entraînent souvent d'énormes dépenses et dommages collatéraux, car les cybercriminels exploitent les failles à plusieurs reprises.[29]
- **Cybersabotage :** le cybersabotage perturbe ou détruit le bon fonctionnement des TIC au moyen de cyberattaques, ce qui peut également avoir des conséquences physiques en fonction de la nature du sabotage et de la cible attaquée.[30] Les attaques de cybersabotage peuvent avoir des motifs très divers et les auteurs vont des « loups solitaires » en proie par exemple à des frustrations personnelles aux acteurs étatiques poursuivant des objectifs politiques. Dans tous les cas, l'objectif de ce genre d'attaques est lié à la démonstration de force et à l'intimidation, associées à l'intention de déstabiliser une organisation, voire la société entière.
- **Cybersubversion :** on parle de cybersubversion quand des acteurs étatiques ou paraétatiques se livrent à des cyberattaques ciblées pour saper le système politique d'un autre État. De telles attaques visent par exemple des processus démocratiques (élections et votations) et sont souvent combinées à des campagnes de désinformation.
- **Cyberopérations dans des conflits militaires :** l'utilisation de moyens économiques et criminels dans les conflits militaires est aujourd'hui une pratique courante (guerre hybride). Les cyberattaques sont un instrument particulièrement adéquat, car il est souvent difficile d'en déterminer l'auteur ; elles sont relativement peu coûteuses, peuvent être utilisées à n'importe quelle

[25] Cyberstratégie nationale CSN, 2023.

[26] Ibid. ; les cyberrisques prennent la forme, sans s'y limiter, de pertes financières, d'interruptions de service ou de dommages liés à une panne des cyberinfrastructures utilisées pour les fonctions d'information et d'exploitation.

[27] Cyberstratégie nationale CSN, 2023.

[28] Il convient de noter que ces cinq types de cyberattaques apparaissent souvent sous forme combinée et qu'ils se recoupent. Cyberstratégie nationale CSN, 2023, p. 4.

[29] Alors que les tensions géopolitiques s'exacerbent, la pratique du cyberespionnage s'intensifie elle aussi. La menace est d'autant plus grande que les gouvernements ont un pouvoir de pression sur les fabricants de produits informatiques, de sorte que ceux-ci laissent délibérément des failles de sécurité dans leurs produits. Étant donné que les chaînes d'approvisionnement des produits TIC sont d'une grande complexité et que la Suisse est largement tributaire des fabricants étrangers, le cyberespionnage reste une menace centrale pour la Suisse.

[30] Le cybersabotage d'infrastructures critiques peut aller des pannes ou des dérangements, p. ex. dans l'approvisionnement énergétique ou l'alimentation en eau, à des conséquences physiques sous la forme de coupures de courant ou de contamination des eaux.

distance et permettent d'avoir un impact politico-militaire dans la zone grise située au niveau infraguerrier.

Outre les cyberattaques ciblées et délibérées, des actes involontaires ou des événements liés aux conditions naturelles et à la technique sont parfois à l'origine de cyberincidents. Jusqu'ici, l'expérience a montré que de nombreux cyberincidents de grande ampleur ne sont pas provoqués par des attaques ciblées, mais reposent sur des enchaînements de circonstances, telles que des erreurs humaines ou des pannes techniques, liées à une préparation insuffisante.
Les évolutions technologiques sont considérées comme un autre facteur influençant la cybermenace. Ils peuvent réduire les menaces existantes en améliorant la sécurité d'un point de vue technique. Cependant, elles accroissent aussi la complexité des cyberinfrastructures du fait de la mise en réseau supplémentaire, ou induisent directement de nouvelles menaces en étant utilisées par les auteurs dans des cyberattaques. Associées à d'autres évolutions, les trois technologies de base que sont l'informatique en nuage (cloud computing), l'internet des objets (IdO) et l'intelligence artificielle (IA) auront une influence significative sur la cybermenace.[31]

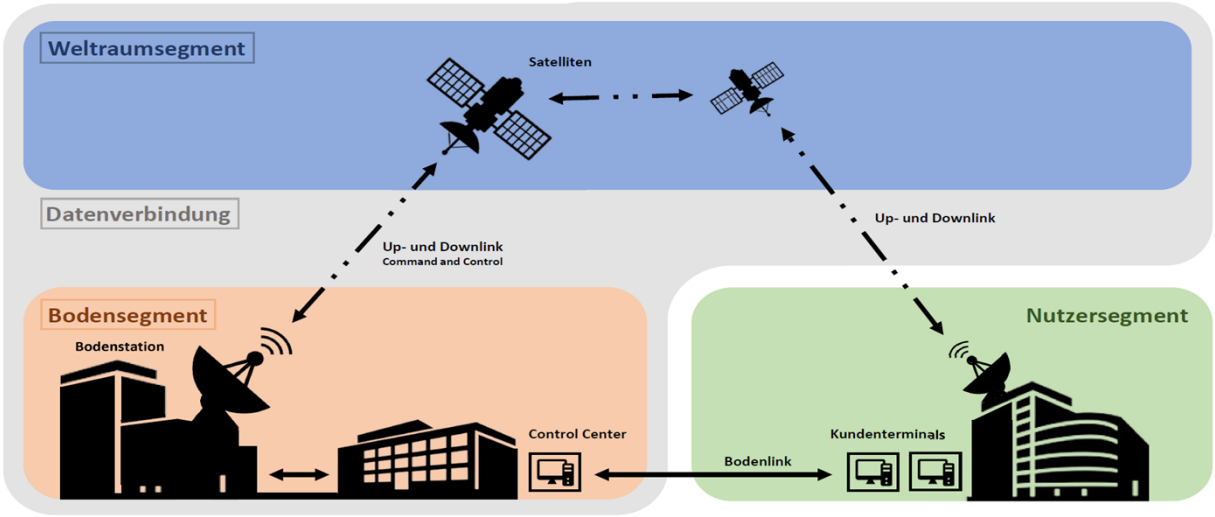
Au chapitre 3 « Cyberrisques découlant des liens de dépendance », le présent rapport considère les phénomènes de cybermenace comme des facteurs influençant fondamentalement les formes que prennent les cyberrisques. Le rapport esquisse la thématique de l'apprentissage automatique (machine learning) dans l'espace. Des évolutions des technologies de base (informatique en nuage, IdO et autres applications d'IA) mais aussi d'autres technologies de base (p. ex. informatique quantique ou cryptographie) sont considérées en lien avec les risques qui en découlent. N'étant pas spécifiques à la thématique de l'espace, elles ne sont pas traitées plus avant dans le présent rapport.

1.3.3 Espace et infrastructures spatiales

Le postulat et le présent rapport utilisent le terme « espace ». Il n'existe pas de définition internationale de la frontière entre espace (extra-atmosphérique) et espace aérien, ni, de ce fait, de la frontière entre l'aéronautique et l'aérospatiale. La Fédération Aéronautique Internationale fixe la frontière délimitant la Terre et l'espace à une altitude de 100 km (ligne de Kármán) en tant *qu'espace au-dessus de l'espace aérien, qui commence environ 100 km au-dessus de la surface terrestre*. L'US Air Force fixe la limite à une altitude de 50 miles.

Les infrastructures spatiales se composent de trois segments principaux : le segment sol, le segment spatial et la liaison de données entre les deux. Le segment utilisateur doit être considéré comme un segment contigu. Il relie les infrastructures spatiales et l'utilisateur final (ill. 1).[32]

Ill. 1 : Infrastructures spatiales[33]



[31] Définition de l'informatique en nuage (cloud computing), de l'internet des objets, de l'intelligence artificielle : voir glossaire. Cyberstratégie nationale CSN, 2023, p. 7.

[32] Les systèmes spatiaux englobent différentes composantes en fonction de la catégorie d'utilisation. Pour le renseignement spatial, elles englobent par exemple, en plus des infrastructures représentées (ill. 1), des fusées porteuses (segment spatial) et des spatioports (segment sol). Le système représenté montre les infrastructures spatiales pertinentes pour les catégories d'utilisation dans lesquelles la Suisse a des liens de dépendance directs (en particulier les systèmes spatiaux basés sur des satellites).

[33] <https://en.wikipedia.org/wiki/Ground_segment#/media/File:Ground_segment.png>.

Segment spatial (ou secteur spatial) : le segment spatial englobe tous les objets spatiaux d'un système spatial. Il se compose par exemple d'un ou de plusieurs satellites, dans le cas d'une constellation.

Liaison de données : la liaison de données se rapporte aux liaisons entre le segment spatial et le segment sol (ce que l'on appelle les liaisons montantes et descendantes [uplink et downlink]), ainsi qu'aux liaisons de données au sein d'un segment spatial (de satellite à satellite).

Segment sol (ou secteur terrestre) : le segment sol renvoie à la partie terrestre d'un système spatial, qui englobe tous les équipements et éléments nécessaires à l'exploitation d'un objet spatial et à la mise à disposition de services pour l'utilisation. Les composantes du segment sol peuvent par exemple prendre la forme d'antennes paraboliques et de stations réceptrices, de centres d'opérations pour la commande, de capacités pour l'analyse des données et d'antennes pour la transmission de données.[34]

Segment utilisateur : le segment utilisateur est la liaison entre le segment spatial et l'utilisateur final. Dans le cas d'un service d'imagerie, il traite ainsi les données brutes de la caméra d'un objet spatial, reçues via le segment sol, afin de les préparer pour l'utilisateur et les lui envoyer.[35] La liaison avec l'utilisateur final est assurée par une liaison de données directe avec le segment spatial (liaison montante et descendante) ou via un lien terrestre avec le segment sol.

Les infrastructures spatiales sont utilisées à des fins diverses. Les catégories d'utilisation des satellites peuvent être représentées dans les statuts politiques et juridiques suivants.[36]

Type	Description	Exemples de services
COM ***Commercial***	Utilisation à but lucratif par un acteur privé	▪ Téléphonie ▪ Prises de vue ▪ Liaisons à large bande
CIV ***Civil***	Utilisation non commerciale ou étatique civile	▪ Projets académiques ▪ Service radioamateur ▪ Initiatives communautaires
GOV ***Gouvernemental***	Utilisation non militaire, étatique	▪ Renseignement spatial ▪ Surveillance environnementale ▪ Météorologie
PPP ***Partenariat public-privé***	Utilisation étatique et commerciale	▪ Télécommunication ▪ Navigation ▪ Prises de vue
MIL ***Défense***	Utilisation purement militaire / renseignement	▪ Télécommunication militaire ▪ Détection précoce ▪ Prises de vue classifiées
DUAL ***Dual***	Utilisation militaire et civile	▪ Détermination de la position par satellite ▪ Prises de vue ▪ Renseignement électronique

2 Liens de dépendance de la Suisse vis-à-vis des infrastructures spatiales

La Suisse dépend des infrastructures spatiales à deux égards : d'une part, du fait de l'utilisation directe de services et d'applications tels que la navigation, la communication par satellite, l'observation météorologique et de la Terre, tout comme l'observation de la météorologie spatiale. Lorsque des autorités et des organisations de sécurité publique ont recours à ces services et applications, ces dépendances directes peuvent avoir un impact sur la sécurité et l'approvisionnement. D'autre part, il existe des dépendances indirectes lorsque ces services et applications sont mis en œuvre dans des aspects importants de la vie quotidienne, tels que l'approvisionnement énergétique, la logistique, les transports et les TIC. En fonction de leur criticité pour le fonctionnement de l'économie et le bien-être de la population, ces infrastructures sont subdivisées en sous-secteurs. Concernant ces dépendances indirectes, le rapport en réponse au postulat se concentre sur les sous-secteurs d'infrastructures critiques en Suisse qui présentent une très forte criticité et une dépendance directe vis-à-vis des systèmes spatiaux. Cela vaut en

[34] UN General Assembly, Threats to the security of space activities and systems, 2022, A/AC.294/2022/WP.16, <https://documents.unoda.org/wp-content/uploads/2022/08/20220817_A_AC294_2022_WP16_E_UNIDIR.pdf>.

[35] Département fédéral de la défense, de la protection de la population et des sports (DDPS), Règlement 50.041 f, Terminologie des règlements de conduite de l'armée, définition17 (BFA 17), 2018; DDPS, EM cdmt Op, Valeurs de référence et catégories pour le domaine spatial, 2021.

[36] Département fédéral de la défense, de la protection de la population et des sports (DDPS), Règlement 50.041 f, Terminologie des règlements de conduite de l'armée 17 (BFA 17), 2018.

particulier pour les sous-secteurs critiques du transport routier et ferroviaire, de l'approvisionnement en électricité et des télécommunications.[37]
Dans l'analyse des dépendances indirectes des infrastructures critiques, il est primordial d'examiner les effets en cascade, c'est-à-dire de regarder dans quelle mesure la panne d'une infrastructure est susceptible de mener à des pannes d'autres services.[38] L'ampleur des effets en cascade et leur enchaînement sont influencés par la durée du dérangement ou de la panne touchant les services spatiaux et de la mise en place de mesures de résilience. Capables d'enrayer les effets en cascade, ces dernières peuvent jouer un rôle essentiel. Dans le domaine des systèmes techniques, il peut par exemple s'agir d'interruptions ciblées du fonctionnement ou de découplage de secteurs en réseau visant à circonscrire l'étendue des effets en cascade. Le présent rapport ne traite pas de ces dépendances indirectes de manière exhaustive, pour se concentrer plutôt sur les infrastructures hautement critiques dont la défaillance compromet directement la situation de la Suisse en matière de sécurité et d'approvisionnement.[39]
Dans le domaine de l'acquisition ou de la mise à disposition des services et capacités critiques au niveau de la sécurité ou de l'approvisionnement décrits dans ce chapitre, la Suisse fait état d'une dépendance fondamentale vis-à-vis des infrastructures spatiales. La Confédération et le secteur privé ont besoin de tiers pour la fabrication et l'exploitation d'infrastructures spatiales, pour la cyberinfrastructure sous-jacente, et pour la fourniture des services de ces capacités critiques. En Suisse, un petit nombre de satellites et de stations au sol sont exploités, la plupart du temps par des entreprises privées.[40] L'inventaire des infrastructures spatiales (stations au sol) de l'Armée suisse est peu critique pour l'exécution de la mission de l'armée.

2.1 Dépendances directes

Positioning, Navigation, Timing (PNT)
Les signaux PNT (Positioning, Navigation, Timing) des systèmes de géolocalisation et de navigation par satellite (Global Navigation Satellite System, GNSS) représentent le service d'infrastructures spatiales auquel les utilisateurs publics et privés ont le plus souvent recours. Le positionnement et la navigation par satellite reposent notamment sur la transmission d'indications temporelles extrêmement précises. Pour cette raison, ces satellites, outre la déduction d'informations de localisation, permettent simultanément des synchronisations temporelles à grande échelle, par exemple pour les réseaux d'énergie et de transmission de données, et pour les systèmes de traitement des données. À cette fin, on emploie surtout le système GPS américain et, dans une moindre mesure jusqu'ici, le système européen Galileo, le système russe GLONASS et le système chinois BeiDou.
Les services PNT sont utilisés avant tout parce qu'ils sont disponibles en tout lieu, à tout moment et surtout gratuitement.[41] Par ailleurs, ils permettent d'obtenir un maximum de précision avec assez peu d'exigences techniques. Toutefois, il n'existait jusqu'ici aucune garantie quant à la disponibilité et l'intégrité des signaux. Le signal PNT à service public réglementé (Public Regulated Service, PRS) mis en place par l'Union européenne (UE) dans le cadre de son programme Galileo fait figure d'exception à cet égard. Il s'agit d'un signal PNT fiable et à haute disponibilité auquel pourront uniquement accéder des utilisateurs étatiques autorisés. L'accord de coopération passé entre la Suisse et l'UE pour la participation à Galileo et à l'European Geostationary Navigation Overlay Service (EGNOS) prévoit que la Suisse, en passant un accord spécial additionnel, puisse accéder au signal PRS. Jusqu'à présent, l'UE ne s'est toutefois pas montrée disposée à engager des négociations avec la Suisse pour la conclusion de cet accord.
À l'exception de l'utilisation du signal PRS en cours de mise en place, et dont la fiabilité et la qualité seront garanties par l'UE, il incombe aux utilisateurs de s'assurer de la disponibilité et surtout de l'inté-

[37] Office fédéral de la protection de la population OFPP, Les infrastructures critiques, <https://www.babs.admin.ch/fr/aufgabenbabs/ski/kritisch.html> (consulté le 20 janvier 2023).

[38] Les effets en cascade se caractérisent par une dynamique complexe et multidimensionnelle qui se développe en une multitude de nouveaux effets différents après un évènement déclencheur, sur une période plus ou moins longue. Le premier évènement peut avoir des causes naturelles, techniques ou humaines mineures et les évènements consécutifs peuvent engendrer des disruptions plus ou moins fortes d'ordre physique, sociétal, économique ou politique. PESCAROLI/ALEXANDER, A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor, GRF Davos Planet@Risk, 2015, <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e056c0990d341ce554b98d25d2bca935623ad76>.

[39] Ce rapport s'intéresse aux dépendances indirectes d'infrastructures critiques en Suisse qui présentent une très forte criticité. Office fédéral de la protection de la population OFPP, Les infrastructures critiques, <https://www.babs.admin.ch/fr/aufgabenbabs/ski/kritisch.html> (consulté le 20 janvier 2023).

[40] Conformément à l'UCS Satellite Database, quinze satellites en orbite sont entre les mains d'acteurs suisses selon la situation de mai 2022 (acteurs privés et hautes écoles). UCS Satellite Database, <https://www.ucsusa.org/resources/satellite-database> (consulté le 12 janvier 2023). Avant la mise en service de constellations de satellites, l'utilisation des fréquences et la position orbitale doivent tout d'abord être coordonnées au plan international avec les 193 administrations de l'ONU. Ce processus de coordination peut prendre jusqu'à sept ans. En mai 2023, la base de données de l'UIT-R recense env. 100 satellites détenus par des exploitants suisses et qui se trouvent dans cette phase de coordination. On peut donc s'attendre à ce que le nombre de satellites d'exploitants suisses augmente considérablement dans les années à venir. BR IFIC (Space services) – Database description, UIT-R, <https://www.itu.int/en/ITU-R/space/Pages/bificDatabase.aspx>.

[41] La Suisse verse à l'UE une somme annuelle pour la mise en place et l'exploitation de Galileo/EGNOS. Galileo/EGNOS ne sont pas gratuits à proprement parler.

grité des signaux PNT. Les organisations de la Confédération pour lesquelles les services PNT sont importants dans l'accomplissement des tâches ont conscience de cette vulnérabilité. La qualité des signaux est vérifiée en continu.

Observation de la météorologie spatiale
L'observation de la météorologie spatiale porte notamment sur les tempêtes solaires, le vent solaire et le rayonnement cosmique, tout comme sur la surveillance des objets proches de la Terre et potentiellement dangereux, comme des astéroïdes, des météorites, des satellites ou des déchets spatiaux s'écrasant sur la Terre. Dans ces différents domaines, on utilise aujourd'hui principalement des données satellites, la dépendance vis-à-vis des défaillances ou des pannes est donc élevée.

Observation météorologique et de la Terre
L'observation des phénomènes météorologiques et de la Terre présente aujourd'hui de fortes dépendances vis-à-vis des données obtenues par satellite et envoyées sur la Terre. L'accès aux données des satellites météorologiques est réglementé contractuellement dans le cadre de l'adhésion de la Suisse à l'Organisation européenne pour l'exploitation des satellites météorologiques (EUMETSAT). En outre, le Conseil fédéral a décidé le 16 février 2022 et réaffirmé le 21 juin 2023 son intention d'obtenir une participation de la Suisse au programme européen d'observation de la Terre, Copernicus. Ce dernier propose un vaste éventail de géoinformations dans des domaines tels que la surveillance de l'environnement.[42] Du fait de la mise en réseau internationale, l'utilisation des données des satellites d'observation météorologique et de la Terre mène également à une utilisation indirecte de la communication par satellite. Les informations des satellites météorologiques s'appliquent aussi indirectement dès lors que des services météo sont utilisés. Il en va de même pour les services de localisation et de navigation, qui jouent un rôle important dans la création de géodonnées utilisées par un grand nombre d'acteurs publics et privés. L'observation de la Terre par satellite joue un rôle croissant dans la création de rapports de situation pour les autorités de politique étrangère et de sécurité, telles que la diplomatie, les services de renseignement, l'armée, l'aide en cas de catastrophe et l'aide au développement. Une défaillance ou une manipulation des données peut limiter le suivi de la situation, la planification et la conduite des interventions.

Communication et médias
Les téléphones satellitaires sont utilisés dans différentes organisations de crise, principalement au titre de technologie de repli. Au niveau fédéral, c'est notamment le cas au Département fédéral des affaires étrangères (DFAE), au Département fédéral de justice et police (DFJP) et au DDPS. Dans ce cas, l'accès aux services de communication est réglementé par contrat avec des opérateurs en Suisse ou à l'étranger, qui s'appuient à leur tour sur les services d'opérateurs de satellites étrangers. Si la communication n'est plus totalement disponible via les réseaux réguliers, comme le réseau mobile en Suisse, il est possible de recourir à la téléphonie satellitaire. Une défaillance simultanée de ces deux technologies porterait atteinte à la capacité d'intervention des organisations de crise et conduirait à une situation problématique du point de vue de la sécurité. Hors des autorités et des organisations dont la sécurité est critique, une panne de la communication par satellite n'engendre pas en soi une pénurie d'approvisionnement. Au sens de la loi sur l'approvisionnement du pays, la communication par téléphones satellitaires ne relève pas des services importants pour l'approvisionnement.
Les personnes recevant exclusivement les signaux de radio et de télévision par l'intermédiaire d'un réflecteur parabolique peuvent être gênées par une panne des signaux PNT. En Suisse toutefois, ce service n'est pas considéré comme important pour l'approvisionnement.

2.2 Dépendances indirectes

Approvisionnement énergétique
Les réseaux d'approvisionnement en électricité, en particulier, utilisent les signaux PNT de manière diverse et variée. L'alimentation électrique doit conserver une tension équilibrée dans le réseau. Plus les réseaux de transmission et d'approvisionnement, tout comme leurs systèmes de contrôle, sont nombreux et étendus d'un point de vue géographique, plus il est important de pouvoir contrôler rapidement et précisément la tension du secteur afin d'éviter des pannes. L'utilisation de signaux PNT pour la surveillance du réseau fonctionne à merveille, et ceux-ci sont donc largement employés. L'approvisionnement en électricité n'est pas uniquement une infrastructure critique, il est aussi déterminant dans le déclenchement et l'amplification d'effets en cascade. Le transport de grandes quantités d'électricité sur un vaste réseau constitue l'un des liens de dépendance les plus critiques vis-à-vis des infrastructures

[42] Le Conseil fédéral, Le Conseil fédéral vise une participation à Copernicus, 16 février 2022, <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87213.html>.

spatiales. Dans le cas du dérangement des turbines d'éoliennes en mer du Nord cité en introduction, ce n'est pas l'utilisation du signal PNT qui a été perturbée, mais la communication par satellite pour le pilotage des turbines.

Logistique et transport
Les systèmes de navigation par satellite sont utilisés afin d'accroître l'efficacité dans la logistique. Des systèmes de planification des tournées peuvent surveiller les données de position de navires ou de camions en temps réel et optimiser ainsi les chargements et la gestion du trafic. En cas de dérangement ou de panne des systèmes de navigation par satellite, la navigation, le trafic routier et l'aviation peuvent continuer à fournir leurs prestations d'approvisionnement. On note dans ce cas une perte d'efficacité, mais pas de perturbation significative de l'approvisionnement. Selon la durée du dérangement ou de la panne et l'étendue du périmètre concerné, d'importantes répercussions négatives risquent d'apparaître. Comme c'est le cas de l'approvisionnement en électricité, les effets en cascade peuvent jouer un rôle important dans la logistique et le transport.

Télécommunication et radiodiffusion
Utilisés directement dans la communication par satellite pour la téléphonie, la radio et la télévision, les signaux PNT font aussi l'objet d'une utilisation indirecte dans la communication. On y a recours pour la synchronisation des réseaux de téléphonie mobile. Une perturbation ou une panne des signaux PNT signifierait que dans toute la Suisse, les téléphones portables ne pourraient être utilisés que de façon limitée voire plus du tout en cas d'impossibilité des opérateurs d'engager des mesures appropriées à même d'assurer la synchronisation du réseau même sans signaux GNSS.
Dans le domaine de la radiodiffusion, des restrictions ou des pannes des signaux PNT seraient critiques pour la diffusion terrestre de programmes radio numériques (T-DAB). En effet, l'infrastructure T-DAB repose sur des réseaux d'émetteurs à isofréquences, qui doivent être synchronisés par la technologie GNSS. Si cette synchronisation est impossible faute de signal GNSS, cette situation peut entraîner, dans certaines zones ou dans tout le pays, une interruption de la réception de la radio. Dans des situations d'urgence, la population ne pourrait donc plus être informée par la radio.

2.3 Évaluation des dépendances

Les services satellitaires sont importants dans le secteur public, de façon ponctuelle dans des domaines se rapportant à la sécurité, notamment pour l'armée. Les instances publiques auxquelles n'incombe aucune tâche de sécurité immédiate n'ont guère à craindre de conséquences critiques directes dans ce domaine.
Dans l'ensemble, c'est au niveau de l'approvisionnement en électricité à grande échelle que la dépendance indirecte vis-à-vis de l'utilisation des signaux PNT est la plus forte. Dans la téléphonie mobile, la diffusion de programmes radio numériques, le trafic routier (surveillance et pilotage de réseaux et de signalisations, conduite en réseau, services de protection et de sauvetage), la navigation (détermination de la position, recherche et sauvetage), le trafic ferroviaire (commande et contrôle des trains) et l'aviation (processus de vol et d'atterrissage, surveillance, recherche et sauvetage), des pannes de signaux PNT d'une durée limitée entraîneraient surtout une restriction des performances. Toutefois, si les perturbations venaient à durer et gagnaient un vaste territoire, les pannes pourraient avoir des impacts croissants.
Le préjudice économique lié à une panne de services météo par satellite pourrait être sérieux, car différents secteurs sont tributaires de prévisions météorologiques de grande qualité (p. ex. dans le secteur de l'énergie et des transports). Il en va de même pour les services de géolocalisation. À plus ou moins long terme, une panne aurait des conséquences qualitatives sur les bases de planification spatiale et de conduite, y compris celles des autorités chargées de la sécurité.
Une défaillance prolongée de satellites d'observation et de télédétection, qui observent la Terre sur différentes plages de fréquences, pourrait nuire durablement à la recherche, en particulier dans le domaine des sciences du climat et de la Terre. Cela vaut également pour d'autres domaines qui dépendent de telles données.[43]
Des explications exposées ci-dessus, on peut conclure que des perturbations ou une panne totale des signaux PNT pourraient déclencher des effets en cascade. Ce sont alors les réseaux d'approvisionnement en électricité et de transport routier qui seraient principalement touchés, ce qui se répercuterait sur d'autres secteurs. Toutefois, il convient d'indiquer également que dans certains domaines, les services spatiaux contribuent à accroître la résilience des infrastructures terrestres.
Une grande partie des services satellitaires peut être remplacée à moyen terme par des systèmes terrestres ou aériens. Cette solution peut néanmoins limiter fortement la disponibilité et l'efficacité des services concernés.

[43] Voir p. ex. University of Zurich Department of Geography, Remote Sensing, <https://www.geo.uzh.ch/en/units/rs>.

2.4 Conclusion et mesures possibles

Divers secteurs dépendent des infrastructures spatiales et cette dépendance de la Suisse devrait encore s'accentuer, en particulier dans le domaine des services PNT. Cette évolution survient parallèlement à la dépendance croissante vis-à-vis des services liés à internet dans presque tous les domaines de notre vie. Cette tendance s'explique d'une part par l'utilisation de la navigation par satellite et son efficacité, et d'autre part, par les exigences de précision accrues pour la synchronisation temporelle de réseaux terrestres, par exemple pour les réseaux de communication modernes tels qu'on en trouve dans la téléphonie mobile et la radiodiffusion. Dans certains cas, des systèmes basés sur internet (NTP ou signaux horaires radio pour les données temporelles, API de géolocalisation pour des données de position)[44] peuvent offrir une alternative, pour autant que ces alternatives ne tirent pas elles-mêmes leurs signaux horaires des systèmes satellitaires en tant que deuxième source ou source principale.[45]
Par ailleurs, il faut s'attendre à une forte augmentation de la dépendance vis-à-vis des satellites météo et d'observation de la Terre. Cette évolution est encouragée par la commercialisation croissante de services satellitaires qui, jusqu'ici, étaient exploités par des acteurs étatiques, généralement avec un accès libre aux données.
L'évolution dans le domaine des systèmes de transport autonomes semble plus difficile à prévoir : au vu de leur utilisation croissante, l'importance des systèmes de navigation par satellite devrait croître et l'appréciation actuelle devra alors être revue. Dans les systèmes de transport autonomes, le passage à une utilisation sans conducteur n'est pas envisageable dans un avenir proche. Du point de vue actuel, une détermination de la position alternative, sans satellite, ne semble pas être praticable, ou seulement de façon limitée, notamment parce qu'une navigation s'effectuant uniquement sur la base de méthodes alternatives n'est pas prévue techniquement et que, selon la technologie utilisée, elle ne fonctionnera pas partout ou ne sera pas assez précise.

Des mesures de renforcement de la sécurité sont abordées dans la Politique spatiale 2023. D'une part, des solutions alternatives (spatiales ou terrestres) et la diversification des applications spatiales permettront de limiter au maximum les conséquences d'une panne ou d'une perturbation. D'autre part, le développement ciblé de capacités propres ou d'infrastructures nationales peut accroître l'autonomie et la résilience. Les capacités propres sont développées en particulier dans les domaines de la surveillance de l'espace (Space Situational Awareness [SSA]) et de l'évaluation des signaux GNSS.[46] Des partenariats stratégiques bilatéraux et multilatéraux sont examinés et, en cas de besoin, développés en complément à la participation à des programmes internationaux et aux activités nationales.[47]

3 Cyberrisques résultant des liens de dépendance

La Suisse dépend aujourd'hui des infrastructures spatiales de multiples manières. Tous les cyberrisques se rapportant aux infrastructures spatiales sont donc importants pour la Suisse. Ces cyberrisques se manifestent tant lors de la fabrication du matériel et des logiciels informatiques utilisés dans les infrastructures spatiales que de l'exploitation de ces derniers. Ils concernent fondamentalement tous les domaines partiels des infrastructures spatiales – le segment spatial, le segment sol et la liaison de données entre les deux. Tandis que la fabrication et le segment sol des infrastructures spatiales présentent des cyberrisques similaires à ceux des infrastructures purement terrestres, le segment spatial en particulier, mais aussi la liaison de données, font état de quelques facteurs de risques supplémentaires ou devant être évalués différemment.
La conception des infrastructures spatiales et leur but ont une influence sur la cybermenace, les agresseurs possibles et donc la forme des cyberrisques. L'utilisation publique et commerciale de satellites pour l'observation de la Terre (p. ex. images haute résolution sur lesquelles on peut distinguer des infrastructures critiques) et la situation dans l'espace sont considérées comme des services critiques. De par leur but, les infrastructures spatiales qui fournissent des prestations critiques ont une surface d'attaque permettant d'obtenir des effets critiques en matière d'approvisionnement ou de sécurité. Outre les cyberattaques ciblées, les cyberincidents causés par des défaillances humaines, des pannes techniques et l'évolution technologique font également partie des cyberrisques pesant sur les infrastructures spatiales.

[44] Définition Network Time Protocol (NTP), Application Programming Interfaces (API), voir glossaire.

[45] Voir p. ex. infrastructure NTP strate 1 basée sur le GNSS de la Time Stamping Authority (TSA). Office fédéral de l'informatique OFIT, service TSA, <https://www.bit.admin.ch/bit/fr/home/subsites/generalites-concernant-la-swiss-government-pki/service-tsa.html> (consulté le 12 janvier 2023).

[46] Définition Space Situational Awareness (SSA), voir glossaire.

[47] Politique spatiale 2023, 2023, p. 17.

Quelques-uns des risques apparaissant pour la fabrication et l'exploitation des infrastructures spatiales et pour le segment spatial, le segment sol et la liaison de données sont esquissés ci-après. Pour un examen plus détaillé des cyberrisques, il convient de se reporter notamment au Rapport relatif aux menaces de sécurité pour les missions spatiales du Comité consultatif pour les systèmes de données spatiales (CCSDS) ou à la matrice de Space Attack Research and Tactic Analysis (SPARTA) d'Aerospace Corporation.[48]
Les mauvaises performances de satellites, volontaires ou non, peuvent avoir un impact sur les affaires ou la politique de sécurité. Il existe donc peu d'informations publiques sur l'ampleur et la fréquence effectives des différents incidents. Par conséquent, les recherches dans ce domaine ne peuvent être que limitées, ce qui complique la présentation exhaustive des risques dans ce chapitre.

3.1 Fabrication

Lors de la fabrication de matériel et de logiciels informatiques destinés aux infrastructures spatiales, des vulnérabilités peuvent être intégrées délibérément ou non et conduire ainsi à des cyberrisques lors du fonctionnement. Ces risques ne sont pas fondamentalement différents de ceux qui existent pour la production de composants d'autres cyberinfrastructures. Ils englobent notamment la mise en place de portes dérobées permettant une intrusion privilégiée dans un système. Si les composants de matériel informatique et les éléments logiciels ne sont pas standard mais montés spécifiquement pour des infrastructures spatiales, la production est alors concentrée au sein d'un petit nombre de fabricants, ce qui augmente la dépendance vis-à-vis de ceux-ci et réduit les possibilités d'influencer la conception des composants à un niveau de sécurité maximal. Par ailleurs, l'utilisation de composants électroniques d'occasion ou non originaux par souci d'économie peut poser problème. Dans le segment spatial, la défaillance ou la panne d'un composant électronique est généralement synonyme de perte du système correspondant. Il n'est guère possible de réparer ou de remplacer les composants défectueux. Avec les satellites à orbite terrestre basse (Low Earth Orbit LEO), ce risque est légèrement plus faible car ceux-ci ont généralement une longévité réduite.

3.2 Exploitation

L'exploitation du système englobe le segment sol, la liaison de données et le segment spatial. Comme pour la fabrication, les cyberrisques liés à l'exploitation des systèmes sont fondamentalement les mêmes que ceux d'une infrastructure purement terrestre. Les différences ou les risques supplémentaires principaux sont mentionnés ci-après pour le segment sol, le segment spatial et la liaison de données.

3.2.1 Segment sol

Le segment sol est, de fait, exposé aux mêmes cyberrisques que les autres infrastructures terrestres critiques. Les infrastructures, le matériel, les logiciels et le flux de données peuvent être influencés afin de perturber, manipuler ou entraver le service.[49] L'accès au segment spatial via la liaison de données offre toutefois des possibilités supplémentaires d'infliger des dommages critiques.
Lors de la gestion des cyberrisques, on peut faire appel à des Cybersecurity Frameworks, tels que celui du National Institute of Standards and Technology (NIST), qui définit notamment un ensemble de mesures permettant de limiter les cyberrisques. Parmi ces mesures figurent l'application rapide de correctifs, de mises à jour et de mises à niveau proposés par les fabricants ou encore des tests de pénétration dans lesquels des spécialistes sont chargés d'attaquer l'infrastructure afin d'en identifier les failles.[50]
Pensé à l'origine pour des infrastructures critiques, le Framework NIST est aujourd'hui largement utilisé dans le secteur privé. Il répond à la multiplicité des risques et des mesures selon le secteur, le but et le type des infrastructures en proposant des lignes directrices d'application. C'est notamment le cas pour le segment sol des infrastructures spatiales.[51]

[48] Le CCDS est un forum multinational pour le développement de normes à destination des systèmes de communication et de données pour des missions spatiales. The Consultative Committee for Space Data Systems, Security Threats Against Space Missions Informational Report, 2022, <https://public.ccsds.org/Pubs/350x1g3.pdf>; Space Attack Research & Tactic Analysis (SPARTA), The Aerospace Corporation, <https://sparta.aerospace.org/>.

[49] «Infrastructure» signifie ici l'environnement extérieur, tel que les immeubles. Le «matériel» renvoie aux composants matériels des outils informatiques devant être utilisés.

[50] Définition des correctifs, mises à jour, mises à niveau et tests de pénétration, voir glossaire.

[51] NIST Computer Security Resource Center, NISTIR 8401, Satellite Ground Segment: Applying the Cybersecurity Framework, 2022, <https://csrc.nist.gov/publications/detail/nistir/8401/final>.

3.2.2 Segment spatial

Le segment spatial est exposé aux effets des phénomènes naturels (p. ex. événements météorologiques dans l'espace tels que tempêtes solaires, rayonnement général) ou de nature technique (p. ex. collisions de satellites avec d'autres objets dans l'espace, tels que des débris spatiaux).[52] Les événements naturels, et en particulier les tempêtes solaires, recèlent des cyberrisques importants pour les infrastructures spatiales. Parce qu'elles émettent un rayonnement électromagnétique, les tempêtes solaires peuvent endommager physiquement les infrastructures spatiales et conduire ainsi à des cyberincidents prenant la forme de pannes des cyberinfrastructures de services critiques, telles que la radiocommunication à haute fréquence ou le GPS.[53]
Parmi les effets de nature technique, on peut citer les cyberattaques ciblées contre des satellites. Les attaques de satellites équipés de cyberinfrastructures peuvent avoir temporairement un impact important, mais elles sont souvent réversibles. Toutefois, lorsqu'une attaque porte sur le système de commande et de contrôle d'un satellite, ce dernier peut alors être rendu inutilisable, et ceci de manière irréversible. Une prise de contrôle du satellite en lui-même par des tiers peut s'effectuer par voie physique ou numérique. Les auteurs de l'attaque peuvent par exemple désactiver durablement les fonctions du satellite, gérer la consommation de carburant ou endommager des capteurs. Par ailleurs, comme le transport des satellites vers l'espace est souvent confié à des tiers, ce qui peut ouvrir la voie à une ingérence physique ou numérique par autrui. Tous ces modes d'action peuvent fondamentalement toucher les cybercomposants du satellite et perturber ou empêcher son fonctionnement. Ce risque est accru lorsque des satellites exécutent plusieurs services simultanément pour différents fournisseurs. Le partage d'un satellite avec des entités potentiellement non dignes de confiance accroît notamment le risque que des acteurs malveillants fassent fuiter des données en détournant des informations via des canaux secondaires.

Les vulnérabilités des composants logiciels et matériels posent problème dans tous les domaines, et pas seulement dans le segment spatial. Toutefois, comme les composants logiciels et matériels défectueux ou manipulés dans le segment spatial ne peuvent être que très rarement remplacés (et à très grands frais), il convient d'accorder une attention particulière à ces vulnérabilités. Les progrès accomplis dans le domaine de l'In-Orbit Servicing (opérations de maintenance en orbite) pourraient venir améliorer la correction des vulnérabilités dans le segment spatial. Néanmoins, cet In-Orbit Servicing recèle à son tour de nouveaux risques, car les technologies correspondantes pourraient aussi être détournées pour des attaques.
L'usage prévu du satellite influe sur le matériel et le logiciel utilisés, l'orbite sur laquelle le satellite est placé et la conception du satellite. Les satellites à orbite terrestre basse sont généralement de plus petite taille et majoritairement utilisés à des fins commerciales. Leur durée de vie est plus courte et les coûts de lancement et d'exploitation sont inférieurs. Lors de la construction de ces satellites, on utilise souvent des composants commerciaux standards (Commercial off-the-shelf, COTS) et des puces de semi-conducteurs tels qu'on les rencontre dans l'industrie de l'automobile et de la téléphonie mobile. Lors du développement de ces composants et de ces puces, les exigences et les différentes menaces auxquelles est exposé le segment spatial ne sont pas prises en compte. La prévention des risques liés à l'utilisation de composants COTS nécessite d'engager des mesures adéquates lors du choix et de l'utilisation de ceux-ci.[54]
La vulnérabilité inhérente à l'utilisation de composants COTS est prise en compte par les grands fabricants. Les satellites commerciaux LEO sont produits en grandes quantités dans le cadre de cycles itératifs. De ce fait, ils sont plus récents que les satellites étatiques et mieux protégés vis-à-vis des cybermenaces.[55] L'utilisation de la constellation de satellites commerciaux, qui a offert une structure d'information et de communication fiable et redondante lors de la guerre en Ukraine, a prouvé la cybersécurité élevée des satellites commerciaux LEO : en dépit de nombreuses cyberattaques et tentatives de perturbations de la liaison de données, cette constellation de satellites a résisté grâce aux mises à niveau régulières des logiciels.[56]

---

[52] Office fédéral de la protection de la population (OFPP), Dossiers sur les dangers et scénarios, <https://www.babs.admin.ch/fr/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html> (consulté le 20 février 2023).

[53] Les tempêtes solaires peuvent causer des dommages aux infrastructures spatiales et terrestres, p. ex. aux réseaux d'alimentation en électricité. Outre les dommages classiques subis par de telles infrastructures terrestres critiques, les tempêtes solaires pourraient aussi endommager des cyberinfrastructures terrestres spécifiques, telles que des câbles sous-marins. Ces dégâts pourraient entraîner des pannes prolongées de l'internet. SANGEETHA ABDU JYOTHI, Solar Superstorms: Planning for an Internet Apocalypse, SIGCOMM, 2021, <https://www.ics.uci.edu/~sabdujyo/papers/sigcomm21-cme.pdf>; DAISY DOBBRIJEVIC. Coronal mass ejections: What are they and how do they form?, Space.com, 2022, <https://www.space.com/coronal-mass-ejections-cme> (consulté le 10 février 2023).

[54] PETER MATTHEWS, The Great Debate: Should COTS Components Be Used in Space?, Microwave Journal, 2022, <https://www.microwavejournal.com/articles/38974-the-great-debate-should-cots-components-be-used-in-space>; CHEN/HODSON, NESC Assessment – Recommendations on Use of Commercial-Off-The-Shelf (COTS) Parts for NASA Missions, NTRS – NASA Technical Reports Server, 2022, <https://ntrs.nasa.gov/search?q=20205011579>.

[55] P. ex. avec des satellites des constructeurs SpaceX (Starlink), Spire (LEMUR) ou Planet (Flock).

[56] TARIQ MALIK, Elon Musk Says SpaceX Focusing on Cyber Defense After Starlink Signals Jammed Near Ukraine Conflict Areas, Space.com, 2022, <https://www.space.com/elon-musk-spacex-starlink-cyber-defense-ukraine-invasion>.

Au contraire, des satellites plus onéreux et plus imposants sont nécessaires pour des missions de longue durée sur des orbites plus éloignées.[57] De fabrication et de lancement complexes, ceux-ci incitent à considérer davantage les cyberrisques par rapport à chaque mission. Compte tenu de la longévité des installations, les failles éventuelles ne pouvant être supprimées depuis le sol sont exposées plus longtemps, ce qui accroît la probabilité de leur détection par des intrus. Le risque posé par des vulnérabilités dans les cyberinfrastructures est donc particulièrement important pour ces satellites complexes et coûteux.
Outre les risques et facteurs de risques déjà évoqués, diverses tendances s'accompagnent d'un besoin accru de cybersécurité pour les satellites. Parmi ces tendances, on trouve les satellites définis par logiciels, les constellations de satellites, les capacités accrues des capteurs pour les petits et les grands satellites et l'apprentissage machine directement dans l'infrastructure de bord. Les satellites définis par logiciels peuvent être configurés à distance. Toutefois, cette configuration n'est pas réservée à l'utilisateur légitime, elle peut aussi être effectuée par un potentiel agresseur. Les constellations de satellites, composées d'un réseau de satellites identiques ou de même type et dotés d'une commande commune, peuvent permettre à un agresseur de prendre le contrôle de l'ensemble de la constellation de satellites en une seule opération. Les capacités accrues des capteurs, en particulier pour les petits satellites (LEO notamment), augmentent l'efficacité des satellites dans la collecte de données. Mais ces capacités accrues font que les satellites deviennent des cibles de plus en plus intéressantes. De même, l'apprentissage machine directement à bord du satellite peut participer à l'attrait d'une attaque, du fait des possibilités d'attaque plus nombreuses, par exemple via les données d'apprentissage utilisées. Dans cet apprentissage machine à bord, d'autres risques émanent aussi du positionnement dans le segment spatial, tels que la possibilité limitée de surveiller et d'influencer le processus d'apprentissage, à la différence de l'apprentissage machine au sol.

3.2.3 Liaison de données

Les liaisons de données entre le segment sol et le segment spatial peuvent, tout comme les liaisons de données au sein du segment spatial (de satellite à satellite), être écoutées, détournées, perturbées, interrompues ou manipulées. La faible intensité du signal adressé au récepteur expose tout particulièrement l'utilisation du GNSS, et surtout les signaux GPS, aux dérangements (brouillage ou jamming) et aux manipulations (leurrage ou spoofing). Le brouillage peut s'effectuer de façon délibérée (par malveillance), par exemple au moyen de brouilleurs GNSS, ou involontaire sous l'effet de la forte puissance d'émission de systèmes de radar ou de communication. Du fait de l'utilisation de protocoles de communication de plus en plus complexes, les agresseurs peuvent utiliser un brouillage « intelligent » qui requiert moins de puissance qu'un brouillage conventionnel. Il maximise son efficacité à l'aide de signaux perturbateurs ciblés. Le leurrage GNSS consiste à transmettre intentionnellement de faux signaux GNSS, pour masquer par exemple la véritable position. Plus difficile à détecter que le brouillage, le leurrage imite précisément les signaux et nécessite des appareils plus complexes.[58] S'agissant des perturbations et interruptions des liaisons de données, la météorologie spatiale doit également être considérée comme un facteur de risques.[59]
Contrairement à ce qui se faisait par le passé, les liaisons de données sont de plus en plus cryptées afin d'éviter les écoutes et les manipulations. Cette protection est particulièrement importante pour la commande et la maintenance d'objets d'un système spatial (p. ex. satellites) via une liaison de données. Ainsi, si des agresseurs parvenaient à installer un logiciel manipulé lors de la mise à jour informatique d'un satellite (maintenance) s'effectuant par une liaison de données, leurs possibilités d'ingérence seraient alors multiples.
Ces dernières années, le support laser s'est de plus en plus imposé pour la transmission de données entre le segment sol et les satellites, ou entre satellites. En termes de sécurité, il présente en effet des avantages par rapport aux ondes radio coniques traditionnelles : un agresseur a alors moins de marge en ce qui concerne sa position lorsqu'il souhaite écouter, détourner, perturber ou interrompre une liaison de données. Il est aussi très difficile de déterminer l'origine et la destination des rayons laser.
Outre l'utilisation d'algorithmes cryptographiques éprouvés et certifiés visant à sécuriser le contenu des liaisons de données, la mise en place d'un concept de sécurité global du segment sol jusqu'au satellite et inversement est également judicieuse. Les principes de « Security by Design », dans lesquels la sécurité est intégrée d'emblée dans la cyberinfrastructure, viennent supporter cette démarche. Pour contrôler la mise en œuvre, il convient par ailleurs d'effectuer régulièrement des tests de pénétration et d'éliminer rapidement les vulnérabilités éventuellement détectées. Les correctifs, mises à jour et mises à

[57] À l'exception des satellites géostationnaires, qui sont stationnés sur une orbite éloignée (35 786 km), mais également considérés comme faisant partie des satellites à mission commerciale. Ils sont principalement utilisés pour des services de communication. Pour plus d'explications sur les orbites satellitaires, voir le glossaire.

[58] Brouillage et leurrage de signaux GNSS – un risque sous-estimé?, Bodet Time, 2020, < https://www.bodet-time.com/fr/produits/serveurs-de-temps/articles-et-ressources/1572-brouillage-et-leurrage-de-signaux-gnss-un-risque-sous-estime.html>.

[59] Voir le chap. 3.2.2 « Segment sol ». Ce risque vaut pour tous les segments de l'infrastructure spatiale.

niveau doivent également être installés dans un délai convenable, tout du moins ceux qui sont importants pour la sécurité et mis à disposition par les constructeurs.[60]

3.3 Conclusion et mesures possibles

Dans les trois segments, l'infrastructure spatiale « segment sol – liaison de données – segment spatial » présentent de nombreux cyberrisques différents. L'accroissement de la sécurité des différents éléments, par exemple par la mise en œuvre du Cybersecurity Framework recommandé dans le NISTIR 8401 pour les stations au sol[61], tout comme le renforcement du système global, notamment par la prise en compte des risques et recommandations du CCSDS pour les missions spatiales[62], contribuent à réduire le nombre et l'effet des cyberrisques. Il s'agit ici d'identifier tous les maillons de la chaîne – allant d'une protection sûre à l'élimination des éléments, en passant par l'exploitation et l'utilisation – et de s'assurer d'une sécurité maximale pour ceux-ci. Eu égard à l'exemple fourni par la guerre en Ukraine concernant les cyberrisques en cas de conflits, il appartient notamment de sécuriser les technologies commerciales déployées pour des services sur des infrastructures critiques lors d'interventions civiles et militaires. Des technologies à double usage (dual-use) utilisées dans des infrastructures spatiales devraient faire l'objet de mesures de sécurité appropriées pour des cibles militaires.[63]

Dotée d'un portefeuille national d'infrastructures spatiales relativement réduit et peu critique en matière d'approvisionnement et de sécurité, la Suisse dispose de possibilités limitées de renforcement de la cybersécurité. En tant que pôle de recherche et de développement, plusieurs champs d'action s'ouvrent néanmoins à elle. Les mesures concrètes envisageables pour la Suisse sont (1) le renforcement de la cybersécurité de toutes les composantes matérielles et logicielles par la mise en place de principes « Security by Design » dès la phase de développement, (2) des incitations ou des obligations nationales pour les fabricants et exploitants privés d'infrastructures spatiales pour la sécurité des chaînes de livraison et du réseau.[64]
Ces mesures doivent être rattachées à l'objectif stratégique « Fiabilité et disponibilité de l'infrastructure et des services numériques » de la CSN. Elles précisent une priorité de la mesure 6 « Résilience, normalisation et régulation » – soit la détermination de la nécessité d'adopter des réglementations par secteur et, au besoin, l'élaboration des modèles correspondants – pour le pôle de recherche et développement suisse œuvrant dans les infrastructures spatiales.[65] Ces mesures soulignent un principe de la CSN : la protection de la Suisse contre les cyberrisques est une tâche commune de la société, des milieux économiques et de l'État.[66]

4 Marge de manœuvre et influence de la Suisse dans des organisations et instances internationales

La dépendance de la Suisse vis-à-vis des services spatiaux s'accroît (voir chap. 2). Notre pays répond à cette vulnérabilité croissante, inhérente aux cyberrisques, d'une part en augmentant sa résilience et la sécurité de ses infrastructures, et d'autre part grâce à des partenariats internationaux et à sa participation dans des organisations et programmes mondiaux.
La Suisse s'engage au sein d'organisations et d'instances internationales dans les domaines de l'espace et de la cybersécurité. À différents échelons administratifs et pour divers aspects des thèmes transversaux, le Conseil fédéral a défini des priorités stratégiques, dont font notamment partie la CSN générale, la Stratégie cyber du DDPS, la Stratégie de politique extérieure 2020-2023, la Stratégie de politique

[60] Définition des correctifs, mises à jour et mises à niveau, voir glossaire.

[61] National Institute of Standards and Technology Interagency Report 8401. L'Institut national des normes et de la technologie (National Institute of Standards and Technology - NIST) est un laboratoire des États-Unis, qui, pour les autorités fédérales et d'autres organisations, développe, teste et recommande des procédures éprouvées dans des domaines tels que la cybersécurité. Des rapports internes au NIST et inter-administrations (NISTIR) décrivent des travaux de recherche techniques. La série comprend des rapports intermédiaires ou finaux sur des travaux exécutés par le NIST à destination de sponsors externes (étatiques ou non).

[62] Voir également p. ex. les recommandations du US White House Memorandum on Space Policy Directive 5 «Cybersecurity Principles for Space Systems». Security Threats Against Space Missions Informational Report, 2022; The White House, Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, 2020, <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>.

[63] Définition de Dual-Use, voir glossaire. BOSCHETTI/GORDON/FALCO, Space Cybersecurity Lessons Learned from the ViaSat Cyberattack, ASCEND, 2022, <https://arc.aiaa.org/doi/pdf/10.2514/6.2022-4380>.

[64] NAYEF AL-RHODAN, Cyber security and space security, 2020, <https://www.thespacereview.com/article/3950/1> (consulté le 12 décembre 2022).

[65] Cyberstratégie nationale CSN, 2023, pp. 20-21.

[66] Cyberstratégie nationale CSN, 2023, p. 12.

extérieure numérique 2021-2024, la Stratégie de maîtrise des armements et de désarmement 2022-2025, la Stratégie nationale de protection des infrastructures critiques et la Politique spatiale de la Suisse 2023.
Jusqu'à présent, les thématiques de l'espace et du domaine cyber ont été traitées séparément au sein des instances internationales. Il n'existe pas d'instance multilatérale chargée principalement et spécifiquement de l'interface entre espace et cybersécurité. Au lieu de cela, un grand nombre d'organisations internationales ou d'initiatives du domaine spatial se consacrent à la cybersécurité au sein de sous-comités. Le présent rapport se limite à évoquer au chap. 4.1 ces organisations et initiatives qui s'intéressent aux thématiques spatiales ou à l'interface espace-cybersécurité.
La cybersécurité est traitée comme un sujet majeur dans un petit nombre d'organisations et d'instances multilatérales, internationales et régionales. La Suisse participe activement à ces processus et a largement contribué à leur succès ces dernières années.[67] Ces instances s'intéressent toutefois en majorité à de vastes mesures de cybergouvernance et de cybersécurité et se penchent rarement sur des problématiques sectorielles spécifiques.

4.1 Représentation de la Suisse au sein d'organisations et d'instances consacrées aux thématiques spatiales

La partie ci-après présente des organisations et des instances se consacrant à des thématiques spatiales ou à l'interface espace-cybersécurité et dans lesquelles la Suisse est représentée.[68]

Organisation	Mandat de l'organisation et de l'instance dans l'espace et rôle de la Suisse
Agence spatiale européenne (European Space Agency – ESA)	L'Agence spatiale européenne (ESA) coordonne la coopération européenne dans le domaine de la recherche spatiale et de l'utilisation commerciale de l'espace. Membre fondateur de l'ESA, la Suisse verse une contribution annuelle de quelque 195 millions de francs suisses pour les programmes et activités de l'agence. De par son adhésion à l'ESA et sa participation aux programmes de l'UE (voir ci-dessous), elle apporte une contribution importante au secteur spatial européen et au développement d'une gouvernance spatiale européenne. Elle veille ainsi à faire accéder les secteurs économiques et scientifiques suisses à des procédures internationales d'appels d'offres. Dans le cadre de l'ESA, la Suisse prend également part au développement de programmes phares européens tels que Copernicus ou Secure « IRIS^2 » (voir chap. 5).
	Interface espace-cybersécurité L'ESA mène des activités groupées dans le domaine espace-cybersécurité, d'une part pour protéger ses propres systèmes, et d'autre part, pour promouvoir les capacités correspondantes des États membres.[69] L'Agence dispose d'une stratégie de cybersécurité qui devrait être publiée d'ici fin 2023.

[67] L'ONU traite la cybersécurité dans des processus isolés, au succès desquels la Suisse a largement contribué ces dernières années, notamment dans le cadre de la conduite du «UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security» de 2019 à 2020 et d'une participation au «UN-Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace» de 2019 à 2021. Au sein de ces forums, la Suisse œuvre pour un cyberespace libre, ouvert et sûr. Elle se mobilise concrètement en faveur de la mise en œuvre du cadre normatif afin d'initier un comportement responsable des États dans le cyberespace. Elle s'engage notamment pour l'application et la concrétisation des règles existantes dans le domaine du droit international dans le cyberespace, y c. le droit humanitaire international et les droits humains. Au niveau européen, la Suisse est active au sein de l'OSCE et participe à la mise en œuvre de mesures de confiance dans le cyberespace. Elle a également des activités dans le domaine du développement des cybercapacités, notamment en tant que membre du Forum mondial sur la Cyber Expertise (Global Forum on Cyber Expertise - GFCE).

[68] Cette liste n'est pas exhaustive.

[69] Cf. Agence spatiale européenne, Cybersecurité, <https://technology.esa.int/program/cybersecurity> (consulté le 21 juin 2022).

Agence de l'Union européenne pour le programme spatial (*EU Agency for the Space Programme – EUSPA*)	L'Agence de l'Union européenne pour le programme spatial (EUSPA) œuvre dans les domaines de l'observation de la Terre, de la navigation par satellite, de la connectivité, de la recherche spatiale et de l'innovation, et soutient les investissements dans les infrastructures et technologies critiques. L'EUSPA encadre également des tâches dans le domaine des composantes du programme de télécommunications gouvernementales par satellite de l'Union européenne (European Union Governmental Satellite Communications, GOVSATCOM ; Copernicus) et fait office d'interlocutrice pour le service d'exploitation « Space Surveillance and Tracking » de l'UE (EU SST). La Suisse n'est pas représentée au sein de l'EUSPA, mais elle est directement impliquée dans les composantes EUSPA du programme spatial européen pour la navigation par satellite (Galileo et EGNOS). L'UE délègue à l'ESA (voir ci-dessus) des activités de recherche et de développement dans le domaine de son programme spatial et confie l'exploitation des systèmes à l'EUSPA. L'accord GNSS, passé entre l'UE et la Suisse prévoit que cette dernière puisse participer à l'EUSPA.[70] Les modalités précises de cette participation doivent encore être définies dans un accord complémentaire. Un projet d'accord a été rédigé, mais sa signature est bloquée par l'UE qui invoque des questions institutionnelles en suspens. Le positionnement rapide et le développement d'éléments clés des systèmes sont essentiels pour que la Suisse puisse exercer son influence, en particulier par l'intermédiaire de programmes de l'ESA.[71] Le Conseil fédéral a décidé le 16 février 2022 et réaffirmé le 21 juin 2023 que la Suisse entendait participer au programme européen d'observation de la Terre Copernicus.[72] **Interface espace-cybersécurité** Pour la protection des composantes spatiales européennes, l'EUSPA exécute des activités de sécurité opérationnelle, de technique de sécurité et de cybersécurité.
Organisation européenne pour l'exploitation de satellites météorologiques (*European Organisation for the Exploitation of Meteorological Satellites – EUMETSAT*)	L'Organisation européenne pour l'exploitation de satellites météorologiques (EUMETSAT) exploite des satellites météorologiques et met les données d'observation à la disposition de ses États membres. La Suisse est membre de cette organisation et représentée par MétéoSuisse.
Organisation internationale de télécommunications par satellites (*International Telecommunications Satellite Organization – ITSO*), Organisation internationale de télécommunications mobiles par satellites (*International Mobile Satellite Organization – IMSO*) et Organisation européenne de télécommunications par satellites (*European Telecommunications Satellite Organization – EUTELSAT IGO*)	Les organisations satellitaires intergouvernementales ITSO, IMSO et EUTELSAT IGO supervisent les services des prestataires privés de services de télécommunications par satellites Intelsat Ltd, Inmarsat plc et Eutelsat SA dans le domaine du service public.[73] ▪ **ITSO :** l'ITSO fournit des services publics de télécommunications internationales d'une grande fiabilité et de haute qualité, et les promeut afin de répondre aux besoins de la société de l'information et de la communication. L'ITSO supervise Intelsat Ltd. Elle compte 149 États membres. ▪ **IMSO :** l'IMSO contrôle la conformité des services de communications mobiles par satellites fournis par Inmarsat plc dans le système mondial de détresse et de sécurité en mer (SMDSM) vis-à-vis du cadre réglementaire établi par l'Organisation maritime internationale (OMI). L'IMSO coordonne également le système d'identification et de suivi des navires à grande distance tel qu'il a été établi par l'OMI (Long-Range Identification and Tracking). Elle compte 104 États membres. ▪ **EUTELSAT IGO :** l'Organisation européenne de télécommunications par satellites a pour mission de veiller à ce qu'Eutelsat SA observe, dans le cadre de ses activités, les principes de service public et de service universel, de couverture paneuropéenne du système de satellites, de non-discrimination et de concurrence loyale. Elle compte 49 États membres. La Suisse est membre de l'ITSO, de l'IMSO et d'EUTELSAT IGO.

[70] L'accord GNSS est un accord de coopération passé entre l'UE et la Suisse, qui permet à cette dernière de participer aux programmes européens de navigation par satellite Galileo et EGNOS.

[71] L'EUSPA participe notamment à l'initiative de développement d'un programme européen de connectivité sécurisée dans l'espace (EU Secure Connectivity Programme) et à divers autres programmes et instances de l'UE qui sont ainsi codéveloppés (notamment Horizon Europe, programmes CEF ou DEP). EUR-Lex, Règlement (UE) 2023/588 du Parlement européen et du Conseil du 15 mars 2023 établissant le programme de l'Union pour une connectivité sécurisée pour la période 2023-2027, 2022, <https://eur-lex.europa.eu/eli/reg/2023/588/oj>.

[72] Communiqué de presse du Conseil fédéral du 16 février 2022, Le Conseil fédéral vise une participation à Copernicus, consultable à l'adresse : <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87213.html>.

[73] Définition de service public, voir glossaire.

Conférence européenne des administrations des postes et des télécommunications (CEPT)	La CEPT œuvre à créer des marchés dynamiques dans le domaine des postes et des télécommunications européennes.[74] Membre fondateur de la CEPT, la Suisse participe activement à la conception de la réglementation européenne harmonisée des fréquences de radiocommunications dans le secteur satellitaire. Elle exerce ainsi une influence directe sur les services satellitaires utilisables en Europe et en Suisse.
Agence européenne de défense (AED)	L'Agence européenne de défense pour les domaines du développement des capacités de défense, de la recherche, des acquisitions et de l'armement est une agence intergouvernementale européenne créée en 2004 pour la planification, l'acquisition et la recherche en lien avec l'armement. La Suisse a passé un accord de coopération (Framework for Cooperation) avec l'Agence européenne de défense et à ce titre, elle siège au sein du Ad Hoc Working Group on Space.[75]
Comité des utilisations pacifiques de l'espace extra-atmosphérique de l'ONU (*UN Committee on the Peaceful Uses of Outer Space – UNCOPUOS*)	L'UNCOPUOS encourage la coopération internationale dans l'utilisation pacifique de l'espace extra-atmosphérique et clarifie les questions juridiques résultant de l'utilisation de ce dernier. Sur recommandation de l'UNCOPUOS, le Comité international sur les GNSS (ICG) et l'Initiative internationale sur la météorologie spatiale ont ainsi été créés. La Suisse a ratifié dans les années 1960 et 1970 quatre des cinq traités sur l'espace extra-atmosphérique élaborés par l'UNCOPUOS. Ces traités définissent les grands principes de la recherche spatiale et de l'utilisation de l'espace, tout comme des aspects spécifiques tels que la responsabilité des États et l'immatriculation dans le registre des objets spatiaux de l'ONU. La Suisse est devenue membre de l'UNCOPUOS en 2008 afin de participer à la gouvernance mondiale des activités spatiales. Elle encourage des règles communes d'utilisation pacifique, sûre et durable de l'espace, mais aussi la mise en œuvre de technologies spatiales pour le développement durable, dans le domaine sanitaire notamment. Elle siège au sein des groupes de travail et d'experts correspondants. La Suisse a ainsi participé au développement des lignes directrices de l'ONU aux fins de la viabilité à long terme des activités spatiales.[76] **Interface espace-cybersécurité** La réalisation pacifique et sans entrave d'activités spatiales (sans cyberinterférences), tout comme la mitigation d'effets de météorologie spatiale, font partie intégrante du domaine de tâches de l'UNCOPUOS.
Assemblée générale des Nations Unies (*UN General Assembly – UNGA*) et Conférence du désarmement de l'ONU	Outre son engagement auprès de l'UNGA concernant l'utilisation pacifique, sûre (dans le sens de *safety*) et durable de l'espace (quatrième commission), la Suisse s'engage pour la sécurité de l'espace (dans le sens de *security* ; première commission). Pour ce faire, elle s'engage notamment dans le cadre du groupe de travail de l'Assemblée générale des Nations Unies « Groupe de travail à composition non limitée sur la réduction des menaces spatiales au moyen de normes, de règles et de principes de comportement responsable » (OEWG Space Threats) pour l'élaboration de principes de comportement responsable dans l'espace.[77] Dans le cadre de la Conférence de Genève sur le désarmement, la Suisse promeut l'ouverture de négociations visant à prévenir une course aux armements dans l'espace (Prevention of an Arms Race in Outer Space, PAROS). Elle considère que le projet de traité relatif à la prévention du déploiement d'armes dans l'espace et de la menace ou de l'emploi de la force contre des objets spatiaux (Draft Treaty on the Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects ; PPWT), présenté par la Russie et la Chine en 2008 et révisé en 2014, constitue une excellente base pour l'ouverture de négociations. Les blocages permanents qui paralysent cet organe depuis 20 ans empêchent néanmoins tout progrès dans ce domaine. **Interface espace-cybersécurité** La dépendance croissante vis-à-vis des services spatiaux et la vulnérabilité accrue en résultant du fait des cyberrisques font partie intégrante des discussions dans le cadre des « OEWG Space Threats », où est notamment traitée la protection des infrastructures et cyberinfrastructures terrestres.

[74] Office fédéral de la communication, CEPT – Conférence européenne des administrations des postes et des télécommunications, <https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/activites-internationales/activites-de-l-ofcom-dans-les-organismes-internationaux/cept.html> (consulté le 10 janvier 2023).

[75] Agence européenne de défense, Ad Hoc Working Group Space, <https://eda.europa.eu/what-we-do/all-activities/activities-search/ad-hoc-working-group-space> (consulté le 2 février 2023).

[76] Les lignes directrices aux fins de la viabilité à long terme des activités spatiales développées par l'UNCOPUOS (A/74/20, annexe II) ont été approuvées par l'Assemblée générale de l'ONU (A/RES/74/82).

[77] A/RES/76/231.

Organisation météorologique mondiale (OMM)	L'OMM vise notamment à mettre en place, à travers son « WMO Space Programme », un système mondial d'observation météorologique et a créé un groupe d'experts sur la météorologie spatiale. Ce programme soutient par ailleurs la mise en œuvre de conventions internationales dans le domaine environnemental.[78] La Suisse est membre de l'OMM.
Union internationale des télécommunications (UIT)	L'UIT est une sous-organisation de l'ONU. À l'aide de mesures réglementaires et techniques, le secteur des radiocommunications de l'UIT (UIT-R) veille à ce que le trafic international des radiocommunications (y c. la communication satellitaire) puisse se faire sans entrave par-delà les frontières. L'UIT est chargée de la coordination internationale de l'ensemble des satellites. Celle-ci comprend l'utilisation de la radiocommunication et les positions orbitales de tous les satellites. La Suisse est membre de l'UIT.
	Interface espace-cybersécurité Le Règlement des radiocommunications de l'UIT contient plusieurs dispositions de protection contre les perturbations de la radiocommunication et de la communication qui doivent être observées par les États membres. Les commissions d'études (*study groups*) dans les départements de la radiocommunication, de la normalisation et du développement publient des études techniques ou des normes relatives à la cybersécurité des infrastructures spatiales.[79]

4.2 Conclusion et mesures possibles

La Suisse participe à la conception de l'espace et de la navigation spatiale au sein d'instances et d'organisations internationales depuis les années 1960. Pour défendre ses intérêts, elle a besoin de la coopération internationale. La Suisse est reconnue au plan international comme un acteur fiable. Elle s'engage activement au sein de différentes instances de l'ONU, qu'il s'agisse des utilisations pacifiques, sûres et durables de l'espace, de la gouvernance spatiale (UNCOPUOS et UNGA), de la coordination de l'utilisation la radiocommunication et des positions orbitales de tous les satellites (UIT) ou encore de la météorologie (OMM) et de la météorologie spatiale (OMM et UNCOPUOS). Notre pays est représenté dans de nombreuses organisations et instances qui se consacrent à des thématiques spatiales, à l'interface espace-cybersécurité ou au renforcement de la cybergouvernance et de la cybersécurité. [80]
En tant que membre fondateur des organisations intergouvernementales précitées, telles que l'ESA ou EUMETSAT, et grâce à sa participation à certaines composantes du programme spatial européen, la Suisse peut contribuer aux systèmes d'infrastructures astronautiques internationaux et accéder aux infrastructures importantes pour elle, tout comme aux données et services en résultant. Grâce à une coopération internationale dans le cadre du développement et de l'exploitation d'infrastructures spatiales, des pays « isolés » comme la Suisse peuvent tirer profit de la pleine capacité des systèmes d'infrastructures astronautiques, tout en n'en finançant qu'une partie.
Les potentielles mesures d'élargissement de la marge de manœuvre de la Suisse au sein des organisations et instances internationales sont indiquées dans divers documents stratégiques du Conseil fédéral. La Suisse doit conforter son statut d'acteur fiable dans les organisations internationales et continuer à se mobiliser, dans des forums internationaux, pour le respect du droit international public et l'évolution de ce dernier au sein de la communauté internationale. La Suisse s'engage en faveur d'une utilisation pacifique et sûre de l'espace, ainsi que d'une viabilité à long terme des activités spatiales aux fins de la réduction des menaces dans et depuis l'espace, et encore d'un comportement transparent et responsable dans toutes les activités liées à l'espace.[81] À cette fin, elle promeut l'établissement de règles, de normes et de directives applicables à l'échelle mondiale. Par sa participation à ces instances et forums internationaux, notre pays doit aussi analyser et évaluer davantage les développements liés à l'utilisation militaire de l'espace. Dans le domaine de l'utilisation du spectre des fréquences radioélectriques et des positions orbitales, la Suisse préserve ses intérêts en participant activement à l'élaboration de la réglementation mondiale.[82]
La Suisse doit en outre intensifier sa coopération internationale dans le domaine spatial, en particulier avec l'ESA, EUMETSAT et l'UE. L'accès aux appels d'offres internationaux doit être assuré pour les milieux économiques et scientifiques.[83] Au moyen d'une participation encore plus forte, notamment à

[78] Organisation météorologique mondiale, programme spatial mondial de l'OMM (WSP), <https://community.wmo.int/en/activity-areas/wmo-space-programme-wsp> (consulté le 20 juillet 2023).

[79] P. ex. UIT, recommandation SA.2142, 2021, <https://www.itu.int/rec/R-REC-SA.2142/en>; UIT, Harmful Interference and Infringements of the Radio Regulations, 2013, <https://www.itu.int/en/ITU-R/terrestrial/workshops/RRS-13-Africa/Documents/Harmful%20Interference.pdf>; ITU BR-SSD e-Learning Center, Harmful Interference to Space Services, <https://www.itu.int/en/ITU-R/space/elearning/presentations/UIT_SSD_028.pdf>.

[80] Stratégie de politique extérieure numérique 2021-2024, p. 17.

[81] Politique spatiale 2023, 2023, p. 17.

[82] Politique spatiale 2023, 2023, p. 20.

[83] Politique spatiale 2023, 2023, p. 16.

des programmes internationaux de développement technologique et de recherche, la Suisse peut concourir au succès commun dans le développement et l'exploitation d'infrastructures spatiales, et s'assurer ainsi durablement d'un accès à ces dernières, préserver ses intérêts et accroître sa résilience.[84] Le Conseil fédéral a par ailleurs inscrit dans la Politique spatiale 2023 que la Suisse entendait participer pleinement aux programmes d'infrastructures importants pour elle.
Grâce au développement d'éléments et de technologies-clés des infrastructures spatiales, la Suisse contribue à ce que les infrastructures spatiales européennes soient compétitives et autonomes sur le plan mondial,[85] ce qui peut contribuer non seulement à l'importance de la Suisse, mais aussi à son rayonnement national et international.[86] Cette mesure vient soutenir l'objectif fondamental d'intensification de la présence et de la visibilité de notre pays dans les manifestations et les forums internationaux. À cette fin, le réseau externe de la Confédération doit être davantage utilisé pour la promotion d'activités économiques et scientifiques.[87] Il s'agit également de faciliter et de renforcer les réseaux et les alliances, dans un cadre national, bilatéral ou international.
Ces mesures possibles doivent être attribuées à différents axes stratégiques, objectifs, champs d'action et mesures de documents stratégiques du Conseil fédéral.[88] Il convient de mettre en exergue, d'une part, un objectif du champ d'action « Cyberespace et espace extra-atmosphérique » de la Stratégie de maîtrise des armements et de désarmement 2022-2025 et, d'autre part, une mesure de mise en œuvre du Rapport sur la politique de sécurité 2021. Les libellés sont les suivants : « La Suisse s'engage pour le renforcement et le développement des instruments de gouvernance concernant l'espace extra-atmosphérique »[89] et, en renforcement de la résilience et la sécurité d'approvisionnement dans les conflits internationaux, on envisage la « consolidation de l'accès à des services utilisant l'espace pour la communication, la navigation et l'observation de la Terre, et de l'engagement international en faveur du renforcement de l'utilisation durable et pacifique de l'espace extra-atmosphérique ».[90] Les mesures possibles se recoupent fondamentalement avec les axes stratégiques « Accès et résilience », « Compétitivité et pertinence » et « Partenariat et fiabilité » de la Politique spatiale 2023.

5 Possibilité de participation à des systèmes européens de communication satellitaire

En Suisse, la communication par satellite n'est utilisée par l'État qu'à titre ponctuel.[91] L'administration fédérale n'exploite pas de satellites qui lui sont propres. La communication satellitaire bénéficie toutefois d'une importance croissante, tout particulièrement dans le domaine de la sécurité.[92]
Dans les systèmes de communication satellitaire, la transmission des données, des images et des sons entre émetteurs et récepteurs est assurée par des satellites de télécommunication. Le système de communication à proprement parler se compose de satellites, d'un segment sol pour la commande, le contrôle, l'interconnexion et la sécurisation du système global, et d'un segment utilisateur, qui permet la communication des utilisateurs (finaux) proprement dite, via les liaisons satellitaires. Le segment sol et le segment utilisateur, et indirectement les satellites, font alors souvent partie de systèmes de communication de plus grande envergure, également reliés par voie terrestre.
Il convient d'établir ici une distinction entre les systèmes de communication par satellite à caractère commercial et public (étatique). Les premiers sont construits, exploités et commercialisés par des prestataires privés, les seconds sont sous le contrôle et la souveraineté d'acteurs étatiques. Tous permettent à différents segments de clientèle d'utiliser les services de communication correspondants, une utilisation militaro-étatique des systèmes de communication satellitaire commerciaux étant tout aussi envisageable qu'une utilisation privée d'un système de communication satellitaire mis en place et géré par l'État. La plupart des systèmes actuels de communication par satellite sont de nature commerciale et des acteurs étatiques font aussi appel à leurs capacités. Récemment, l'utilisation de systèmes privés par les forces de défense ukrainiennes a été largement commentée.
Compte tenu de la conception de plus en plus stratégique des systèmes de communication par satellite, on s'efforce de développer, en particulier en Europe, des systèmes ou des réseaux de systèmes de communication satellitaire gérés par l'État, afin de les mettre à la disposition d'utilisateurs étatiques.

[84] Politique spatiale 2023, 2023, p. 17.

[85] P. ex. avec les coiffes des lanceurs Ariane et Vega ou les horloges atomiques pour le système de navigation par satellite Galileo.

[86] Politique spatiale 2023, 2023, p. 19.

[87] Ibid.

[88] Voir chapitre 1.1 «Situation de départ stratégique de la Suisse». En particulier Stratégie de politique extérieure 2020-2023, 2020, pp. 15-20; Rapport sur la politique de sécurité 2021, 2021, pp. 10, 45 ; Stratégie de politique extérieure numérique 2021-2024, 2020, pp. 9, 13; Stratégie de maîtrise des armements et de désarmement 2022-2025, 2022, p. 30; Politique spatiale 2023, 2023.

[89] Stratégie de maîtrise des armements et de désarmement 2022-2025, 2022, p. 30.

[90] La politique de sécurité de la Suisse Rapport du Conseil fédéral (2021) FF 2021 2895, p. 45.

[91] La politique de sécurité de la Suisse Rapport du Conseil fédéral (2016) FF 2016 7763.

[92] La politique de sécurité de la Suisse Rapport du Conseil fédéral (2021) FF 2021 2895.

La participation aux systèmes européens de communication par satellite, c'est-à-dire aux différents programmes de développement de l'ESA, permet à la Suisse de se positionner assez tôt à l'aide de ses compétences clés, pour ensuite s'imposer comme une partenaire fiable et une utilisatrice de systèmes opérationnels grâce à ses contributions spécifiques. Dans le cadre de l'AED, la Suisse a montré de l'intérêt pour le programme GOVSATCOM. Toutefois, cette initiative ne s'est pas concrétisée jusqu'à présent. Le Conseil fédéral vise une participation de la Suisse au programme européen d'observation de la Terre Copernicus durant l'actuelle période du programme allant de 2021 à 2027.[93] Une extension de la participation suisse au programme spatial européen nécessite l'ouverture de négociations correspondantes et d'accords spécifiques pour la participation aux composantes supplémentaires du programme de communication satellitaire.[94] L'UE considère la coopération avec la Suisse dans le cadre des programmes européens (y c. Copernicus) à la lumière de ses relations globales avec la Suisse.
Au niveau bilatéral, les accords de coopération principalement liés à la politique de sécurité et passés avec des États occidentaux et leurs partenaires industriels sont au premier plan. Toutes les coopérations doivent être vérifiées individuellement quant à leur conformité au cadre juridique en vigueur, mais aussi à l'indépendance et à la neutralité de la Suisse.

5.1 Programmes avec participation de la Suisse

La Suisse participe aujourd'hui aux programmes européens ou nationaux suivants aux fins du développement de systèmes et de services de communication satellitaire :

- programme ESA pour la recherche et le développement de systèmes de télécommunication (Advanced Research in Telecommunications Systems, ARTES), y compris leur application, et les initiatives spécifiques pour la transmission sûre de données dans le domaine spatial ou pour la distribution quantique de clés (QKD),[95]
- programme ESA en lien avec l'« Infrastructure for Resilience, Interconnectivity and Security by Satellite » de l'UE (« IRIS^2 » ; précédemment « Secure Connectivity Initiative »),[96]
- ESA Centre européen pour la sécurité spatiale et formation avec son centre de compétences en cybersécurité (Security Cyber Centre of Excellence), point de contact central pour les cyber-tests, les formations et les expériences concernant des développements classifiés ou non dans un environnement sûr et contrôlé,[97]
- programmes nationaux et partenariats public-privé (PPP) dans le cadre de l'ESA, notamment le développement de la plateforme HummingSat (lancé par la Suisse) pour des petits satellites de télécommunication géostationnaires basés sur des technologies d'impression 3D.

5.2 Conclusion et mesures possibles

Les mesures de participation à des communications satellitaires européennes sont régies par les objectifs stratégiques de la Politique spatiale 2023, visant à promouvoir l'excellence scientifique, renforcer la compétitivité et intensifier la coopération.[98] Pour tirer pleinement profit de ses compétences clés dans des programmes de développement européens pour la communication satellitaire, la Suisse doit se positionner assez tôt. Cette démarche implique d'une part la participation aux programmes de développement de l'ESA dans le domaine de la communication satellitaire (sûre) pour le renforcement et le développement des compétences clés. D'autre part, elle nécessite aussi de prendre part aux composantes pertinentes du programme spatial européen pour l'accès aux services et aux acquisitions récurrentes, importantes pour l'industrie aérospatiale suisse d'un point de vue commercial. La Suisse doit s'imposer comme une partenaire et une utilisatrice fiable des systèmes opérationnels.

---

[93] Communiqué du Conseil fédéral du 16 février 2022, Le Conseil fédéral vise une participation à Copernicus, consultable sous: <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87213.html>.

[94] Par le biais de l'accord de coopération EGNSS, la Suisse participe intégralement et sans limitation temporelle à la partie de programme «Galileo et EGNOS» du programme spatial de l'Union européenne. Voir également à ce sujet le chapitre 2.4.1. «Représentation de la Suisse dans des agences sur des thématiques spatiales».

[95] ESA TIA, <https://artes.esa.int/>; ESA TIA, Space Systems for Safety and Security (4S), <https://artes.esa.int/space-systems-safety-and-security-4s>; ESA TIA, Quantum encryption to boost European autonomy, <https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Quantum_encryption_to_boost_European_autonomy>.

[96] Le Conseil fédéral, La Suisse participe à de nouveaux programmes de l'ESA et s'engage pour les ambitions renforcées de l'Europe spatiale, 2022, <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-91890.html>; ESA, Ministers back ESA's bold ambitions for space with record 17% rise, 2022, <https://www.esa.int/About_Us/Corporate_news/Ministers_back_ESA_s_bold_ambitions_for_space_with_record_17_rise>; Conseil de l'UE, Le Conseil et le Parlement européen s'accordent pour stimuler les communications sécurisées grâce à un nouveau système satellitaire, 2022, https://www.consilium.europa.eu/fr/press/press-releases/2022/11/17/council-and-european-parliament-agree-on-boosting-secure-communications-with-a-new-satellite-system/>; European Commission, IRIS²: the new EU Secure Satellite Constellation, <https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en>.

[97] Le Security Cyber Centre of Excellence permet notamment de reproduire, dans un environnement de synthèse, des applications et des infrastructures opérationnelles critiques, afin de les tester et les valider à l'aide de scénarios de cybermenaces sur mesure. Les capacités du centre de compétences sont élargies en continu et peuvent être utilisées par l'ESA et ses partenaires (États membres).

[98] Politique spatiale 2023, 2023, pp. 18-19.

6 Aspects juridiques de la transmission de données dans l'espace

6.1 Cadre juridique international en matière de transmission de données dans l'espace

La transmission de données dans l'espace n'est réglementée par aucun traité spécifique de droit international public. S'appliquent ici les principes généraux du droit international public, du droit spatial international et d'autres ouvrages normatifs particuliers, concernant notamment les télécommunications internationales.

La Suisse a ratifié quatre des cinq traités sur l'espace de l'ONU,[99] dont le Traité sur l'espace de 1967, qui a été ratifié par 113 États.[100] Parmi les grands principes de ce traité, on trouve l'exploration et l'utilisation libres de l'espace par tous les États (art. I), tout comme les principes de « due prise en compte » et la « gêne nuisible » aux activités d'autres États parties (art. IX). Le Traité sur l'espace de 1967 stipule que les États parties doivent mener l'exploration de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, conformément au droit international, notamment la Charte des Nations Unies, en vue de maintenir la paix et la sécurité internationales et favoriser la coopération et la compréhension internationales (art. III). Les États parties sont responsables, du point de vue du droit international, des activités nationales dans l'espace extra-atmosphérique, qu'elles soient entreprises par des organismes gouvernementaux ou par des entités non gouvernementales (art. VI). Le droit international public ne détermine pas clairement dans quelle mesure ces principes de base s'étendent aussi à la transmission de données dans l'espace et cette question n'est réglée par aucune jurisprudence ni pratique constante des États.
Au-delà des principes de base, un arsenal législatif international s'applique à la Suisse. La Constitution de l'UIT ratifiée par la Suisse et la convention de l'UIT décrivent les principes de cette organisation, dont son rôle dans les domaines de la normalisation (UIT-T), du développement des télécommunications (secteur du développement des télécommunications, UIT-D) et des radiocommunications (UIT-R). L'UIT-R est chargée de l'assignation du spectre de fréquences pour les services de radiocommunication mondiale, qui sont codifiés dans le Règlement des radiocommunications.[101] En matière de services spatiaux, l'UIT-R applique les procédures internationales de coordination et d'immatriculation des systèmes spatiaux et stations au sol, qui sont reconnues internationalement après l'adoption des fréquences radio correspondantes dans le Fichier de référence international des fréquences (MIFR). Elle gère les procédures correspondantes des plans d'attribution ou d'allocation de l'UIT.[102]
Le Règlement des radiocommunications de l'UIT, ratifié et mis en place par la Suisse (traité de droit international public entre États membres de l'ONU)[103], constitue la base de la coordination et de la notification efficaces de satellites. Il porte notamment sur l'utilisation de la radiocommunication et les positions orbitales des satellites. Les procédures du Règlement des radiocommunications assurent la reconnaissance internationale et la protection réglementaire des satellites.
La Suisse a par ailleurs conclu différents accords avec des organisations internationales : la Convention portant création d'une Agence spatiale européenne (ESA), dont les programmes sont consacrés à des activités de recherche et de développement, et des accords sur l'exploitation de systèmes spatiaux, comme la Convention portant création de l'Organisation internationale de télécommunications mobiles par satellites (IMSO) et de l'Organisation internationale de télécommunications par satellites (ITSO), de l'Organisation européenne de télécommunications par satellites (EUTELSAT IGO) et de l'Organisation européenne pour l´exploitation de satellites météorologiques (EUMETSAT).

[99] La Suisse a ratifié quatre des cinq traités sur l'espace : le Traité du 27 janvier 1967 sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes (RS 0.790), l'Accord sur le sauvetage des astronautes, le retour des astronautes et la restitution des objets lancés dans l'espace extra-atmosphérique (RS 0.790.1), la Convention sur la responsabilité internationale pour les dommages causés par des objets spatiaux (RS 0.790.2) et la Convention sur l'immatriculation des objets lancés dans l'espace extra-atmosphérique (RS 0.790.3).

[100] En juin 2023, 113 États ont ratifié le Traité sur les principes réglant les activités des États en matière d'exploitation et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes (RS 0.790). United Nations Office for Disarmament Affairs, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, <https://treaties.unoda.org/t/outer_space> (consulté le 24 juillet 2023).

[101] Art. 1.8 RR (2020) Radiocommunication spatiale: toute radiocommunication assurée au moyen d'une ou plusieurs stations spatiales, ou au moyen d'un ou plusieurs satellites réflecteurs ou autres objets spatiaux».

[102] Secteur des radiocommunications (UIT-R) (itu.int) www.itu-int>Radiocommunications.

[103] Règlement des radiocommunications du 17 novembre 1995 (RS 0.784.403.1).

Concernant la transmission de données dans l'espace, il n'existe par ailleurs aucune obligation concrète de la Suisse au plan international. Celle-ci surveillera les débats organisés dans les forums internationaux concernant le statut juridique des données transmises et enregistrées dans l'espace.[104] Elle est représentée au sein de diverses instances internationales et divers forums traitant de cybergouvernance et de cybersécurité (voir chap. 4) et participe activement à ces processus. Quand bien même ces organes traitent principalement de mesures globales de cybergouvernance et de cybersécurité, les résultats de ces discussions devraient aussi être pertinentes pour la transmission de données dans le domaine spatial. Dans ce contexte, une approche est de considérer que la législation sur la cybersécurité dans l'espace ne diffère pas fondamentalement de celle de la cybersécurité sur Terre. Ainsi, les dispositions du droit civil ou pénal national peuvent aussi s'appliquer à des activités qui se déroulent dans l'espace.

6.2 Cadre juridique suisse en matière de transmission de données dans l'espace

Le cadre juridique suisse pour la transmission de données dans l'espace est fixé par la loi sur les télécommunications (LTC).[105] Celle-ci prévoit essentiellement deux articles qui sont également importants dans le cadre de la transmission de données par des satellites :

- Art. 43 Confidentialité des données : *Il est interdit à toute personne qui a été ou qui est chargée d'assurer un service de télécommunication de donner à des tiers des renseignements sur les communications des usagers; de même, il lui est interdit de donner à quiconque la possibilité de communiquer de tels renseignements à des tiers.*
- Art. 48*a* Sécurité : la LTC révisée oblige désormais les fournisseurs de services de télécommunication enregistrés en Suisse à lutter contre les cyber-attaques. À cette fin ou pour la protection des installations, les fournisseurs de services de télécommunication sont autorisés à dévier ou empêcher des communications ou à supprimer des informations. Le Conseil fédéral peut également édicter d'autres réglementations sur la protection de la sécurité des informations et des infrastructures et services de télécommunication, en particulier concernant la disponibilité et l'exploitation d'installations ou la garantie d'infrastructures redondantes et l'annonce de perturbations. Il convient de noter ici que les exploitants des satellites qui fournissent les services de télécommunication à la Suisse doivent être enregistrés en tant fournisseurs de services de télécommunication. Ils sont donc responsables de l'intégrité des données transmises par leur biais.

Conformément à l'art. 25 LTC, l'Office fédéral de la communication (OFCOM) est responsable de la gestion du spectre des fréquences. En s'appuyant sur les conventions internationales et les publications pertinentes du Comité des communications électroniques (ECC) de la CEPT, l'OFCOM élabore le plan national d'attribution des fréquences (PNAF),[106] où figurent des conditions cadres techniques et réglementaires obligatoires pour l'ensemble des utilisateurs du spectre de fréquences (y c. les satellites). Le PNAF est approuvé chaque année par le Conseil fédéral. Les droits individuels d'utilisation des fréquences sont accordés aux utilisateurs sous la forme de concessions de radiocommunication. Les attributions de l'OFCOM englobent également la coordination internationale et la notification de satellites pour des organisations suisses, des entreprises ou des autorités et stations au sol sur le territoire suisse. La coordination et la notification de satellites sont régies par le Règlement des radiocommunications ratifié mis en place par la Suisse.[107]
Du fait de la grande distance, les signaux de radiocommunication émis par les satellites sont extrêmement faibles sur Terre. Pour les réceptionner dans une qualité suffisante, il faut des antennes à faisceaux hertziens, telles que des antennes paraboliques utilisées pour la réception de la télévision par satellite. Si, pour l'utilisation de l'internet, des signaux doivent être renvoyés vers l'espace, il faut ici aussi des antennes à faisceaux hertziens, dont le rayonnement est limité par la loi sur la protection de l'environnement (art. 11, al. 1, LPE ; RS 814.01) et l'ordonnance correspondante sur la protection contre le rayonnement non ionisant (annexe 1, ch. 61 ss, ORNI ; RS 814.710).[108]

---

[104] Stefan Soesanto, Terra Calling: Defending and Securing the Space Economy, EPF de Zurich, 2021, <https://doi.org/10.3929/ethz-b-000460220>.

[105] Loi du 30 avril 1997 sur les télécommunications (RS 784.10).

[106] Frequency Allocation Plan, <https://www.ofcomnet.ch/#/fatTable>.

[107] Règlement des radiocommunications du 17 novembre 1995, entré en vigueur le 1er juin 1998 (RS 0.784.403.1). Le Règlement des radiocommunications est régulièrement actualisé à l'occasion des Conférences mondiales des radiocommunications puis ratifié par le Conseil fédéral. < https://www.fedlex.admin.ch/eli/cc/2005/778/fr >.

[108] Les antennes émettrices doivent être installées de sorte que personne ne puisse entrer dans leur faisceau d'émission. En dehors de ce dernier, l'exposition est faible. Ce sont les cantons ou les communes qui sont responsables de l'octroi des autorisations de construction et du contrôle des installations.

Les aspects juridiques de la transmission de données, en particulier ceux concernant les cyberrisques dans l'espace, peuvent aussi se rapporter à d'autres domaines du droit public, tels que la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[109] ou la nouvelle loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI)[110]. Selon le cas de figure et dans le cadre des cyberrisques, on ne peut exclure, même si le lieu du délit ou de l'infraction est situé dans l'espace, que des dispositions du droit civil et pénal déterminant en Suisse soient applicables, par exemple si les actes en question ont des répercussions sur le territoire suisse ou sur des personnes ou objets qui s'y trouvent.

6.3 Conclusion et mesures possibles

Au vu de la diversification des acteurs présents dans l'espace en raison du développement des services spatiaux à caractère commercial, la situation juridique pour la transmission de données devient plus complexe et connaît une évolution comparable à celle de l'internet ou de l'intelligence artificielle.[111] Compte tenu de la dimension mondiale de cette thématique, la Suisse suivra de près les débats menés au sein des forums internationaux consacrés au statut juridique des données transmises et enregistrées dans l'espace.[112] Dans notre pays, le cadre juridique de la transmission de données dans l'espace est avant tout fixé par la loi sur les télécommunications (LTC) et d'autres actes législatifs fédéraux.

Compte tenu des évolutions observées dans le secteur spatial aux niveaux national et international, le Conseil fédéral a décidé le 16 février 2022, en plus de l'actualisation de la politique spatiale, d'élaborer un avant-projet de loi spatiale nationale en vue d'une consultation. La Suisse crée ainsi un cadre juridique national pour les traités sur l'espace de l'ONU qu'elle a ratifiés. Ce cadre se rapporte à l'autorisation et à la surveillance des activités spatiales, à des questions de responsabilité et à l'immatriculation des objets spatiaux dans un registre national.[113] Une loi spatiale nationale permettrait non seulement à la Suisse d'encadrer en droit interne ses obligations internationales, mais aussi de renforcer la sécurité juridique dans ce domaine pour tous les acteurs concernés.[114] Les questions de transmission des données ne sont pas l'objet principal de cette nouvelle loi fédérale.

7 Conclusion

Le rapport présente les dépendances critiques des services et capacités d'infrastructures spatiales pour la stabilité de la Suisse en matière de sécurité et d'approvisionnement. Ces dépendances devraient encore s'accroître à l'avenir. Allant de pair avec une diversification des acteurs du secteur spatial et des services spatiaux, mais aussi des tendances technologiques, on constate une multiplication des cyberrisques qui résultent de ces dépendances pour la Suisse. Pour mieux se protéger face à cette vulnérabilité croissante, notre pays doit prendre les mesures possibles suivantes :

1. mettre en place des systèmes redondants (spatiaux ou terrestres) et diversifier les applications spatiales afin de limiter autant que possible les effets d'une défaillance ou d'une perturbation ;
2. encourager le développement ciblé de capacités propres ou d'infrastructures nationales afin d'accroître l'autonomie et la résilience.[115]

Le rapport met en lumière les cyberrisques résultant des dépendances d'infrastructures spatiales pour la Suisse. Les infrastructures spatiales « Segment sol – Liaison de données – Segment spatial » font état, dans les trois segments, de nombreux cyberrisques différents. Dotée d'un portefeuille relativement réduit d'infrastructures spatiales, également peu critique en termes d'approvisionnement et de sécurité, la Suisse dispose de possibilités restreintes pour renforcer la cybersécurité dans le cadre de l'exploitation des infrastructures spatiales. En tant que pôle de recherche et de développement de technologies utili-

[109] RS 235.1.

[110] RS 128.

[111] P. ex. Cloud Computing (définition, voir glossaire). JAMES DALY, Why cloud and edge are launching the next space race, IBM, 2020, <https://www.ibm.com/blog/ibm-space-tech-cloud-edge-communication-breakthrough/>.

[112] STEFAN SOESANTO, Terra Calling: Defending and Securing the Space Economy, ETH Zürich, 2021, <https://doi.org/10.3929/ethz-b-000460220>.

[113] Politique spatiale 2023, 2023, p. 21. Lors de l'élaboration de la loi spatiale nationale, il importe de prendre en compte les processus de coordination internationale des fréquences de radiocommunication et des positions orbitales des satellites.

[114] Le projet est élaboré par le Département fédéral de l'économie, de la formation et de la recherche (DEFR) en collaboration avec les autres départements concernés. Le Conseil fédéral, Mise à jour de la politique spatiale suisse et élaboration d'un cadre juridique national pour le domaine spatial, <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87205.html).

[115] Politique spatiale 2023, 2023, p. 17.

sées dans des infrastructures spatiales, elle peut toutefois prendre les mesures suivantes dans le domaine du développement et de la fabrication :

3. renforcer la cybersécurité de tous les éléments logiciels et matériels par l'application de principes de « Security by Design » durant la phase de développement ;
4. créer des incitations ou des conditions nationales pour des fabricants et exploitants privés d'infrastructures spatiales, dans le but d'assurer la sécurité des chaînes d'approvisionnement et des réseaux.[116]

La Suisse s'engage au sein d'instances multilatérales, d'organisations internationales et de programmes de développement consacrés à des thématiques spatiales et à l'interface espace-cybersécurité. Elle est reconnue comme étant un acteur fiable. Pour préserver ses intérêts et accroître sa compétitivité et sa pertinence, la Suisse a besoin de la coopération internationale. Afin d'élargir sa marge de manœuvre au plan international, elle peut prendre les mesures suivantes :

5. préserver son statut d'acteur fiable dans les organisations internationales et se mobiliser encore en faveur d'une utilisation pacifique, sûre et durable de l'espace au sein des forums internationaux ;[117]
6. intensifier la coopération internationale dans la recherche et les projets spatiaux en intensifiant sa participation aux programmes internationaux de développement technologique et de recherche, afin d'assurer durablement l'accès à des infrastructures spatiales, de défendre ses intérêts et de renforcer sa résilience ;[118]
7. se positionner assez tôt pour le renforcement et le développement de ses compétences clés au sein de programmes de développement européens de communication satellitaire, et de s'imposer comme une partenaire et une utilisatrice fiable des systèmes opérationnels.[119]

Pour finir, la Suisse entend prendre la mesure suivante quant à la situation juridique de la transmission des données dans l'espace :

8. suivre de près les débats consacrés au statut juridique des données transmises et enregistrées dans l'espace, de plus en plus fréquents au sein de forums internationaux.[120]

Ce rapport a déduit huit mesures possibles à partir des questions centrales du postulat. Les mesures 1 et 2 et de 5 à 8 doivent être attribuées à différents axes stratégiques, objectifs, champs d'action et mesures des documents stratégiques du Conseil fédéral, et concrétisent certains champs d'action de la Politique spatiale 2023.[121] La mise en œuvre concrète est assurée par les départements dans leurs domaines de compétences respectifs, dans le cadre des crédits autorisés. La mise en œuvre sera évaluée par les départements responsables. Le DEFR, en collaboration avec le DFAE, le Département fédéral de l'intérieur (DFI), le Département fédéral des finances (DFF), le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) et le DDPS feront rapport au Conseil fédéral concernant la mise en œuvre de la Politique spatiale 2023.[122]
Les mesures 3 et 4 entrent dans le cadre de la CSN. La mise en application de la stratégie est menée par le comité de pilotage de la CSN, qui élabore un plan de mise en œuvre et fait rapport au Conseil fédéral et aux cantons par l'intermédiaire de son secrétariat assuré par le CSNC. Les acteurs centraux financent en principe eux-mêmes les travaux de mise en œuvre. Au sein de la Confédération, ils emploient les ressources leur ayant été allouées pour la mise en œuvre des deux précédentes cyberstratégies.[123]

Le compte rendu sur les cyberrisques de sécurité et d'approvisionnement dans le système global des infrastructures spatiales est à imputer aux mesures concernant l'objectif « Responsabilisation » de la CSN. La mesure 3 « État de la menace » mène à une évaluation qui doit fournir aux milieux économiques, à la société et à l'administration une base solide pour identifier et mettre en œuvre leurs mesures

[116] Cyberstratégie nationale CSN, 2023, pp. 20-21.

[117] Notamment Stratégie de politique extérieure 2020-2023, 2020, pp. 15-20; Rapport sur la politique de sécurité 2021, 2021, pp. 10, 45 ; Stratégie de politique extérieure numérique 2021-2024, 2020, pp. 9, 13 ; Stratégie de maîtrise des armements et de désarmement 2022-2025, 2022, p. 30 ; Politique spatiale 2023, 2023.

[118] Politique spatiale 2023, 2023, pp. 16-20.

[119] La politique de sécurité de la Suisse. Rapport du Conseil fédéral (2021) FF 2021 2895, p. 45 ; Politique spatiale 2023, 2023.

[120] STEFAN SOESANTO, Terra Calling: Defending and Securing the Space Economy, ETH Zürich, 2021, <https://doi.org/10.3929/ethz-b-000460220>.

[121] Notamment Stratégie de politique extérieure 2020-2023, 2020, p. 15-20; Rapport sur la politique de sécurité 2021, 2021, pp. 10, 45; Stratégie de politique extérieure numérique 2021-2024, 2020, p. 9, 13; Stratégie de maîtrise des armements et de désarmement 2022-2025, 2022, p. 30; Politique spatiale 2023, 2023.

[122] Politique spatiale 2023, 2023, p. 2.

[123] Cyberstratégie nationale CSN, 2023, p. 35.

de réduction des risques de manière ciblée et à moindre coût.[124] Les cyberrisques sont évalués en continu dans l'administration fédérale, en étroite collaboration avec les cantons, l'économie et la société. L'évaluation de la menace doit alors mettre en lumière les menaces globales et déployant des effets à large échelle, mais aussi les menaces spécifiques à certains processus ou domaines d'activité.
À un niveau d'abstraction supérieur, le présent rapport est également conforme aux priorités de la mesure 4 « Analyse des tendances, des risques et des dépendances », par exemple la veille technologique ou l'analyse des risques de dépendances par rapport aux produits ou à des fournisseurs en Suisse.[125]

[124] Cyberstratégie nationale CSN, 2023, p. 16.

[125] Cyberstratégie nationale CSN, 2023, p. 18.

8 Liste des abréviations

API	Application Programming Interface
ARTES	Advanced Research in Telecommunications Systems
CCSDS	Consultative Committee for Space Data Systems Comité Consultatif pour les Systèmes de Données Spatiales
CEPT	Conférence Européenne des Administrations des Postes et des Télécommunications European Conference of Postal and Telecommunications Administrations
COTS	Commercial off-the-shelf
CSN	Cyberstratégie nationale
CSS	Centre for Security Studies
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DG DEFIS	Direction générale de l'industrie de la défense et de l'espace de l'UE
DoSA	Defense of Space Assets
ECC	Electronic Communications Committee
EGNOS	European Geostationary Navigation Overlay Service Système européen de navigation par recouvrement géostationnaire
EPF	École polytechnique fédérale
ESA	European Space Agency Agence spatiale européenne
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites Organisation européenne pour l´exploitation de satellites météorologiques
EUSPA	Agence de l'Union européenne pour le programme spatial EU Agency for the Space Programme
EUTELSAT	European Telecommunications Satellite Organization Organisation européenne de télécommunications par satellites
FAI	Fédération Aéronautique Internationale
FST	Fournisseur de services de télécommunication
Galileo	Système global de navigation par satellite de l'UE
GLONASS	Global Navigation Satellite System
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GOVSATCOM	European Union Governmental Satellite Communications
GPS	Global Positioning System Système global de navigation par satellite
IA	Intelligence artificielle
ICG	International Committee on GNSS Comité international pour le GNSS
IdO	Internet des objets
IKAR	Comité de coordination interdépartemental des questions spatiales
IMSO	International Mobile Satellite Organization Organisation internationale de télécommunications mobiles par satellites
ITSO	International Telecommunications Satellite Organization Organisation internationale de télécommunications par satellites

LEO	Low-Earth Orbit Orbite terrestre basse
LPD	Loi sur la protection des données (RS 235.1)
LPE	Loi sur la protection de l'environnement (RS 814.01)
LSI	Loi sur la sécurité de l'information (RS 128)
LTC	Loi sur les télécommunications (RS 784.10)
MIFR	Master International Frequency Register Fichier de référence international des fréquences
NCSC	Centre national pour la cybersécurité
NEO	Near-Earth Objects Objets géocroiseurs
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OEWG	Open-Ended Working Group Groupe de travail à composition non limitée
OFCOM	Office fédéral de la communication
OFEV	Office fédéral de l'environnement
OFPP	Office fédéral de la protection de la population
OMI	Organisation maritime internationale
OMM	Organisation météorologique mondiale
ONU	Organisation des Nations Unies
ORNI	Ordonnance sur la protection contre le rayonnement non ionisant (RS 814.710)
PAROS	Prevention of an Arms Race in Outer Space Prévention de la course aux armements dans l'espace
PESCO	Permanent Structured Cooperation Coopération structurée permanente
PIC	Protection des infrastructures critiques
PNAF	Plan national d'attribution des fréquences
PNT	Positioning, Navigation, Timing
PPP	Public-Private Partnerships Partenariats public-privé
PPWT	Draft Treaty on the Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects Projet de traité relatif à la prévention du déploiement d'armes dans l'espace et de la menace ou de l'emploi de la force contre des objets spatiaux
PRS	Public Regulated Service Service public réglementé
QKD	Quantum Key Distribution Distribution quantique de clés
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation
SPARTA	Space Attack Research & Tactic Analysis
SSA	Space Situational Awareness
SST	Space Surveillance and Tracking Surveillance et suivi d'objets dans l'espace
SW	Space Weather Météorologie de l'espace
T-DAB	Terrestrial Digital Audio Broadcasting
TIC	Technologies de l'information et de la communication
UE	Union européenne
UIT	Union internationale des télécommunications
UIT-D	Secteur du développement des télécommunications de l'UIT
UIT-R	Secteur des radiocommunications de l'UIT

UIT-T	Secteur de la normalisation des télécommunications de l'UIT
UNCOPUOS	UN Committee on the Peaceful Uses of Outer Space Comité des utilisations pacifiques de l'espace extra-atmosphérique de l'ONU
UNGA	United Nations General Assembly Assemblée générale des Nations unies

9 Glossaire

Application Programming Interface (API)	Une API établit la communication entre deux programmes ou systèmes, en temps réel. Des informations sont alors échangées sous forme standardisée entre une application et différentes parties de programmes. La transmission des données et des ordres s'effectue de manière structurée, selon une syntaxe définie. Une API est la couche réseau qui traite les transmissions de données entre systèmes.[126]
Apprentissage machine	L'apprentissage machine (*machine learning*) est un sous-domaine de l'intelligence artificielle. Cette technologie vise à apprendre aux machines à tirer des enseignements des données et à s'améliorer avec l'expérience, au lieu d'être explicitement programmées pour le faire. Dans ce domaine, les algorithmes sont entraînés à trouver des motifs (*patterns*) et des corrélations dans de grands ensembles de données, ainsi qu'à prendre les meilleures décisions et à émettre les meilleures prévisions en s'appuyant sur leur analyse. Avec la pratique, les applications de *machine learning* s'améliorent. Plus le volume de données auxquelles elles ont accès est important, plus elles deviennent précises [127]
Biens dual-use-	Les biens *dual-use*, ou biens à double usage, sont des marchandises, des technologies et logiciels qui sont utilisables à des fins aussi bien civiles que militaires.[128]
Brouillage (jamming)	On entend par brouillage, ou perturbation de signal, l'interruption d'une liaison entre un appareil et son point de départ dans une liaison sans fil. Les appareils situés dans un réseau sans fil envoient et reçoivent des informations au moyen de paquets de données, sur une fréquence déterminée. Lors d'un brouillage des signaux, un brouilleur est utilisé pour envoyer un « bruit de fond », qui perturbe la bande de fréquences sur laquelle des appareils sans fil échangent des paquets de données.[129]
Cloud Computing	Le *cloud computing* (informatique en nuage) est un modèle permettant d'établir en tout lieu et à la demande un accès à un réseau partagé et à un ensemble commun de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services). Ces ressources peuvent être fournies rapidement avec un effort de gestion et une interaction minimes avec le fournisseur de services.[130]
Correctifs, mises à jour et mises à niveau	Les correctifs (*patches*) sont de petites mises à jour logicielles qui suppriment un ou plusieurs problèmes d'une application. Ils sont habituellement mis à disposition par des fabricants ou des programmeurs afin d'éliminer des imperfections ou des erreurs au sein d'une application. Les correctifs sont créés rapidement après l'apparition d'un problème. L'installation ou l'activation d'un correctif s'effectue généralement en cours de fonctionnement, sans que les utilisateurs ne s'en rendent compte. Si un correctif inclut de nouvelles fonctions ou par exemple une adaptation d'une présentation, on parle de mises à jour. Celles-ci requièrent généralement une interruption pour leur installation. À la différence des mises à jour, les mises à nouveau englobent des extensions fonctionnelles essentielles, et éventuellement de nouveaux domaines de fonctionnalités.[131]

[126] Was ist eine Application-Programming-Interface (API)?, Datacenter Insider, <https://www.datacenter-insider.de/was-ist-ein-application-programming-interface-api-a-735797/>; What is an API?, IBM, <https://www.ibm.com/topics/api>.

[127] Was ist maschinelles Lernen?, SAP, <https://www.sap.com/swiss/insights/what-is-machine-learning.html#:~:text=Maschinelles%20Lernen%20ist%20die%20Verschmelzung,f%C3%BCr%20die%20Analyse%20zu%20erstellen.>.

[128] Loi sur le contrôle des biens (LCB, RS 946.202), <https://www.fedlex.admin.ch/eli/cc/1997/1697_1697_1697/fr>.

[129] What is Signal Jamming and What Can You Do About It?, Make Use Of, 2022, <https://www.makeuseof.com/what-is-signal-jamming/>.

[130] MELL/GRANCE, NIST Special Publication 800-145 The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, NIST, 2011, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

[131] Patch, Update, Upgrade. Aspectra. <https://www.aspectra.ch/blog/patch-update-upgrade--b512>; <https://odion.com/?faqs=was-ist-der-unterschied-zwischen-update-upgrade-release-und-change-request#:~:text=Updates%20sind%20technische%20Modifikationen%2C%20Verbesserungen,neue%20Funktionsbereiche.>.

Cybercriminalité	La cybercriminalité englobe l'ensemble des infractions et omissions commises dans le cyberespace. Une distinction est faite entre cybercriminalité et criminalité numérique. Relèvent de la cybercriminalité les infractions qui sont dirigées contre l'internet, des systèmes informatiques ou leurs données, et qui exigent un travail d'investigation technique de la part des autorités de poursuite pénale. La criminalité numérique désigne les infractions qui étaient jusqu'ici principalement commises dans le monde analogique. En raison des progrès de la transformation numérique, ces délits classiques sont de plus en plus souvent commis à l'aide de moyens informatiques.[132]
Cyberincident	Tout événement nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements, qu'il soit accidentel ou provoqué intentionnellement par un tiers non autorisé.[133]
Cybermenace	Toute circonstance ou tout événement susceptible d'engendrer un cyberincident.[134]
Cybersécurité	La situation dans laquelle le traitement des données, notamment l'échange de données entre les personnes et les organisations par l'intermédiaire d'infrastructures d'information et de communication, fonctionne comme prévu.[135]
Effets en cascade	Lorsque des systèmes ou éléments techniques sont branchés en série (en électronique, on parle de mise en cascade) ou d'une façon difficile à appréhender, des effets en cascade apparaissent. Certains peuvent être indésirables, voire catastrophiques, et être, du point de vue de leurs conséquences, disproportionnés par rapport à un déclencheur (*trigger*) souvent banal.
Flux de données	Le flux de données est le mouvement de données dans un système composé de logiciels, de matériel ou d'une combinaison des deux. Le flux de données est souvent défini à l'aide d'un modèle ou d'un diagramme dans lequel l'ensemble du processus de déplacement de données est représenté lors de son passage d'un composant à l'autre ou sein d'un programme ou d'un système, en tenant compte de la façon dont il change de forme au cours du processus.[136]
Infrastructures critiques	On entend par infrastructures critiques les processus, les systèmes et les installations essentiels au bon fonctionnement de l'économie et le maintien des moyens de subsistance de la population.[137]
Intelligence artificielle (IA)	L'intelligence artificielle est un terme générique employé pour désigner les applications dans lesquelles les machines fournissent des performances intellectuelles imitant les capacités humaines. On y trouve l'apprentissage machine (*machine learning*), le traitement du langage naturel (NLP, *natural language processing*) et le *deep learning*, domaine particulier de l'apprentissage machine qui se concentre sur les réseaux de neurones artificiels et les grandes quantités de données.[138]
Internet des objets (IdO) ou Internet of Things (IoT)	Réseau d'objets physiques équipés de capteurs, logiciels et autres technologies visant à connecter ceux-ci avec d'autres appareils et systèmes via l'internet, de sorte que des données puissent être échangées entre les objets.[139]
Leurrage (spoofing)	Le terme de leurrage (tromperie, dissimulation, manipulation, *spoofing* en anglais) désigne une technique d'attaque par laquelle des cybercriminels pé-

[132] Ibid.

[133] Ibid.

[134] Cyberstratégie nationale CSN, 2023.

[135] Ibid.

[136] What Does Dataflow Mean?, Techopedia, <https://www.techopedia.com/definition/6743/dataflow>.

[137] Stratégie nationale de protection des infrastructures critiques, 2023, FF 2023, 1659 ss, p. 3.

[138] Was ist künstliche Intelligenz?, SAP, <https://news.sap.com/germany/2018/03/was-ist-kuenstliche-intelligenz/>. (consulté le 10 avril 2023); Was ist Deep Learning?, datasolut, <https://datasolut.com/was-ist-deep-learning/#:~:text=Deep%20Learning%20(tiefes%20Lernen)%20ist,und%20Entscheidungen%20genauer%20zu%20t%C3%A4tigen.>.

[139] Was ist das IoT?, Oracle, <https://www.oracle.com/ch-de/internet-of-things/what-is-iot/>. (consulté le 20 avril 2023)

	nètrent dans des ordinateurs ou des réseaux en usurpant une identité digne de confiance.[140]
Liaison montante/descendante (*uplink / downlink*)	Dans la télécommunication satellitaire, une liaison descendante est la liaison d'un satellite vers une ou plusieurs stations terrestres ou un ou plusieurs récepteurs. Une liaison montante est la liaison d'une station terrestre à un satellite.[141]
Network Time Protocol	Network Time Protocol (NTP) est un protocole de synchronisation des horloges de systèmes informatiques.[142]
Orbites de satellites	Les satellites sont généralement classifiés sur la base de leur orbite (distance par rapport à la surface de la Terre), qui a un effet direct sur leur puissance de réception et la vitesse à laquelle ils se déplacent autour de la planète. On distingue fondamentalement les orbites suivantes, associées à l'utilisation respective des satellites. - Les satellites à orbite terrestre basse (Low Earth Orbit – LEO) évoluent à une altitude d'environ 160-1500 km au-dessus de la surface terrestre. Ils ont une période de révolution courte, de 90 à 120 minutes. Ils conviennent particulièrement pour la télédétection, l'observation haute résolution de la Terre et la recherche, car les données peuvent être relevées et transmises assez rapidement. - L'orbite terrestre moyenne (Medium Earth Orbit – MEO) se trouve entre l'orbite basse et l'orbite géostationnaire, et se situe généralement à une altitude comprise entre 5000 et 20 000 km. Des services de positionnement et de navigation tels que le GPS utilisent généralement les satellites MEO. - Les satellites en orbite géostationnaire (geostationary orbit – GEO) se trouvent à 35 786 km au-dessus de la surface de la Terre, juste au-dessus de l'équateur. Les objets GEO semblent immobiles vus de la Terre, car leur vitesse de rotation est identique à celle de notre planète. Une antenne terrestre peut toujours être orientée vers le même appareil dans l'espace, raison pour laquelle ce type de satellites est employé pour des services de communication disponibles en continu tels que la télévision, la téléphonie ou la météorologie. L'un des inconvénients des satellites GEO résident dans le long temps de latence de la communication en temps réel, dû à la grande distance par rapport à la Terre.[143]
Positioning, Navigation, Timing (PNT)	Le positionnement, ou données de position, est la détermination d'une position et, le cas échéant, de l'orientation dans le référentiel spatial avec une précision connue. La navigation est la détermination de la position actuelle et souhaitée et l'orientation, l'application de corrections de cap et de vitesse pour atteindre la destination. Le timing, également appelé signal temporel, est la synchronisation d'horloges par rapport à un temps standard (p. ex. UTC) avec une précision connue.[144]
Quantum Key Distribution Distribution quantique de clés	La distribution quantique de clés est une méthode connue et déjà pratiquée dans la cryptographie quantique. Par la mise en œuvre d'effets de la mécanique quantique, deux partenaires de communication peuvent échanger une clé hors d'écoute à destination du cryptage symétrique. La sécurité de l'échange de clés ne repose plus sur des algorithmes mathématiques ni des hypothèses concernant la puissance de calcul, mais sur des lois physiques de

[140] Spoofing – Definition, IT-Security.Network, <https://it-service.network/it-lexikon/spoofing>.

[141] What is downlink and uplink?, TechTarget, <https://www.techtarget.com/searchmobilecomputing/definition/downlink-and-uplink#:~:text=In%20satellite%20telecommunication%2C%20a%20downlink,station%20up%20to%20a%20satellite.>.

[142] Network Time Protocol (NTP): Definition und Funktionsweise, IONOS, <https://www.ionos.de/digitalguide/server/knowhow/network-time-protocol-ntp/>.

[143] Types of Satellites: Different Orbits & Real-World Uses, EOS Data Analytics, <https://eos.com/blog/types-of-satellites/>.

[144] Office fédéral de topographie Colloque Swisstopo Positioning, Navigation, Timing (PNT). <https://www.swisstopo.admin.ch/content/events/de/swisstopo-internet/events2022/colloquium-21-22/20220114/_jcr_content/contentPar/downloadlist/downloadItems/272_1642173963101.download/220114_Kolloquium_PNT_alle.pdf>.

	la mécanique quantique. L'échange quantique de clés a déjà été utilisé dans la pratique. Les distances pouvant être parcourues sont toutefois limitées.[145]
Résilience	L'aptitude d'un système, d'une organisation ou d'une société à faire face à des perturbations internes ou externes et à maintenir son bon fonctionnement ou à le rétablir aussi rapidement et complètement que possible.[146]
Satellites définis par logiciels	D'une manière générale, la définition par logiciel signifie que des composants matériels traditionnels sont remplacés par des logiciels. Le *software defined networking* est un concept de réseau qui procède d'un découplage du matériel et du logiciel. Autrement dit, le pilotage du réseau est séparé du matériel qui exécute la transmission des données à proprement parler. La possibilité de reconfigurer des satellites signifie que la mission peut varier tout au long de la durée de vie et être adaptée aux nouvelles exigences.[147]
Security by Design	*Security by Design* est une approche de conception appliquée dans le développement de matériel informatique et de logiciels. La sécurité du matériel ou du logiciel est prise en compte dès la phase de développement et intégrée dans le cycle de vie global d'un produit. Les critères de conception englobent notamment la minimisation de la surface d'attaque (exposition), l'utilisation du cryptage et de l'authentification et l'isolation de domaines importants pour la sécurité. La sécurité est testée en continu.[148]
Semi-conducteur (puces)	Un semi-conducteur est une substance dotée de propriétés électriques spécifiques qui convient comme base d'ordinateurs et d'autres appareils électroniques. Il s'agit en général d'un élément chimique solide ou d'une liaison qui peut conduire l'électricité dans certaines conditions, mais pas dans d'autres. Un semi-conducteur contrôle et pilote le flux de courant dans des appareils et installations électroniques. C'est donc un composant apprécié pour fabriquer des puces électroniques pour des composants informatiques et un grand nombre d'appareils électroniques, dont les disques statiques (SSD).[149]
Service public	Par service public, on entend une desserte de base de qualité, comprenant des biens et des prestations d'infrastructure, accessibles à toutes les catégories de la population et offerts dans toutes les régions du pays à des prix abordables et aux mêmes conditions.[150]
Space Situational Awareness	La *space situational awareness* (SSA) se rapporte à la connaissance de l'environnement spatial, y compris l'emplacement et la fonction d'objets spatiaux et de phénomènes de météorologie spatiale.[151]
Test de pénétration	Un test de pénétration, ou *pentest*, ou encore test d'intrusion, décrit une méthode permettant de déterminer la sécurité actuelle d'un paysage informatique ou d'une application (web). C'est un contrôle de la sécurité des systèmes IT de toute taille et il est particulièrement important pour les entreprises. Pour mener à bien ce contrôle de sécurité, la personne procédant au test emploie des moyens et des méthodes qu'emploierait un pirate pour pénétrer dans le système. Les tests de pénétration permettent de constater quelle est la vulnérabilité d'un système face à de telles attaques.[152]
Vulnérabilité	Une vulnérabilité dans la technologie de l'information (IT) est une erreur de code ou de conception qui constitue une faille de sécurité potentielle pour un

[145] Was ist Quantenschlüsselaustausch?, Security Insider, <https://www.security-insider.de/was-ist-quantenschluesselaustausch-a-5fd80c11f9b676caa394bcac7c73feb4/>.

[146] Cyberstratégie nationale CSN, 2023.

[147] Was ist Software-Defined Networking (SND)?, IP Insider, <https://www.ip-insider.de/was-ist-software-defined-networking-sdn-a-657442/>; Software Defined Satellites, Businesscom, <https://www.bcsatellite.net/blog/software-designed-satellites/#:~:text=The%20term%20Software%20Defined%20Satellite,adjusted%20based%20on%20changing%20demands.>.

[148] Was ist Security by Design?, Security Insider, <https://www.security-insider.de/was-ist-security-by-design-a-1071181/>.

[149] ANDREW ZOLA, Halbleiter, ComputerWeekly.de, <https://www.computerweekly.com/de/definition/Halbleiter>. (consulté le 20 avril 2023)

[150] Un service public de qualité - image de marque de la Suisse, Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC, <https://www.uvek.admin.ch/uvek/fr/home/detec/entreprises-liees-a-la-confederation/service-public-de-qualite.html>.

[151] Space Situational Awarenes (SSA), SatCen, <https://www.satcen.europa.eu/page/ssa>.

[152] Penetrationstest – Definition. IT-Service.Network. <https://it-service.network/it-lexikon/penetrationstest>.

point d'extrémité ou un réseau. Les vulnérabilités créent de possibles vecteurs d'attaques par le biais desquels les agresseurs peuvent exécuter des codes ou accéder à la mémoire d'un système cible.[153]

[153] Vulnerability (information technology), Whatls.com, <https://www.techtarget.com/whatis/definition/vulnerability>.