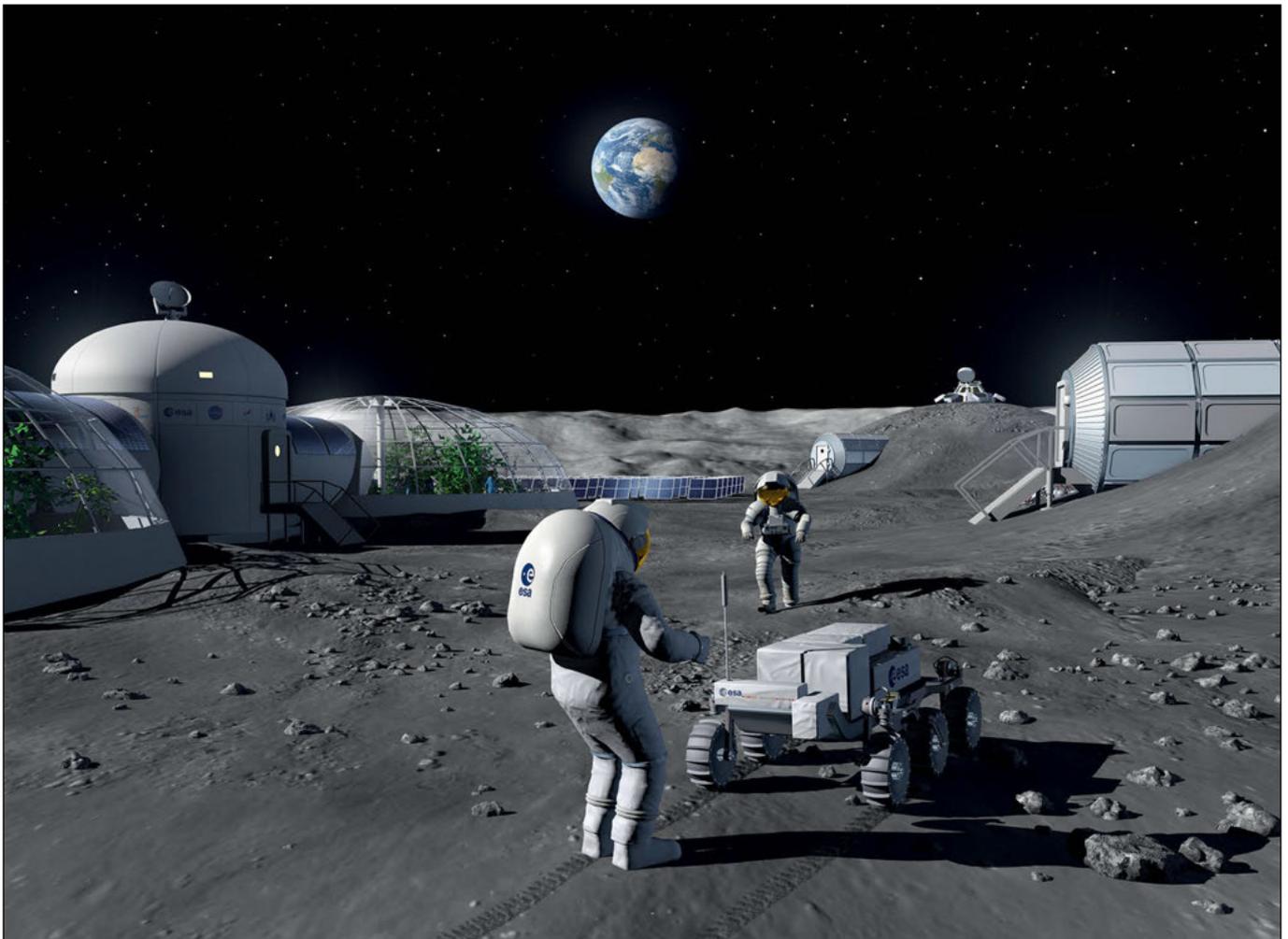


LES TÉLÉCOMMUNICATIONS TERRE-LUNE AVEC LUNANET

LE LUNANET SE DÉFINIT PAR UN RÉSEAU DE TÉLÉCOMMUNICATIONS CAPABLE D'APPUYER LES MISSIONS HUMAINES D'EXPLORATION ET LES OPÉRATIONS SCIENTIFIQUES VERS LA LUNE. VOICI À QUOI POURRAIT RESSEMBLER CE RÉSEAU.

Les premières briques du système de télécommunications LunaNet seront constituées par des *nodes* (nœuds) pour assurer le déploiement lunaire et les premières installations permanentes. Les caractéristiques de ce réseau combinent un ensemble de systèmes interopérables avec des partenaires gouvernementaux et commerciaux. Le but du système est de soutenir les missions Artemis III, Artemis IV, Artemis V et les missions commerciales concernées par la phase IOC et EOC (Initial Operational Capability et Enhanced Operational Capability soit capacité opérationnelle initiale puis améliorée)

À long terme, le retour vers et sur la Lune aboutira peut-être à la multiplication des activités à la surface de notre satellite naturel, entraînant la nécessité d'un réseau de télécommunications entre les différents éléments (base, rovers, station sur orbite, satellites) et la Terre.



© ESA/Pierre Carril



Une première spatiale

La structure du réseau LunaNet constitue une première dans l'exploration spatiale humaine, car il pose les bases des communications interplanétaires en vue d'une présence de notre civilisation hors de la Terre. Le design de LunaNet englobe en effet l'ensemble des systèmes fournissant les services de temps, de navigation et de communications vers des utilisateurs autour de la Lune et vers la Terre.

Autrement dit, les équipements du réseau se trouveront à la fois sur orbite lunaire et à la surface de la Lune. En ce qui concerne le segment lunaire, une chaîne spécifique est envisagée pour laquelle une interface pourrait être mis en oeuvre vers les segments sol de la Terre. Un système de relais entre les deux segments est à l'étude dans lequel la configuration des échanges s'appuierait sur un lien privé.

Pour établir le lien entre les deux segments, le LunaNet sera construit à travers une combinaison de fournisseurs d'accès qui seront eux-mêmes donneurs de services. Les interfaces entre les segments sont divisibles en plusieurs catégories.

La première comprend les interfaces physiques et les protocoles entre un utilisateur et un fournisseur. La seconde concerne les interfaces entre les différents fournisseurs d'accès.

La déclinaison des interfaces se divise ensuite dans une série de connexions faisant intervenir des typologies d'interfaces : liaison entre le système lunaire et terrestre, liaison entre les utilisateurs de surface lunaire, liaison entre

les utilisateurs de surface et ceux sur orbite lunaire et terrestre, liaison entre les fournisseurs de service selon les cas d'usages de liaisons.

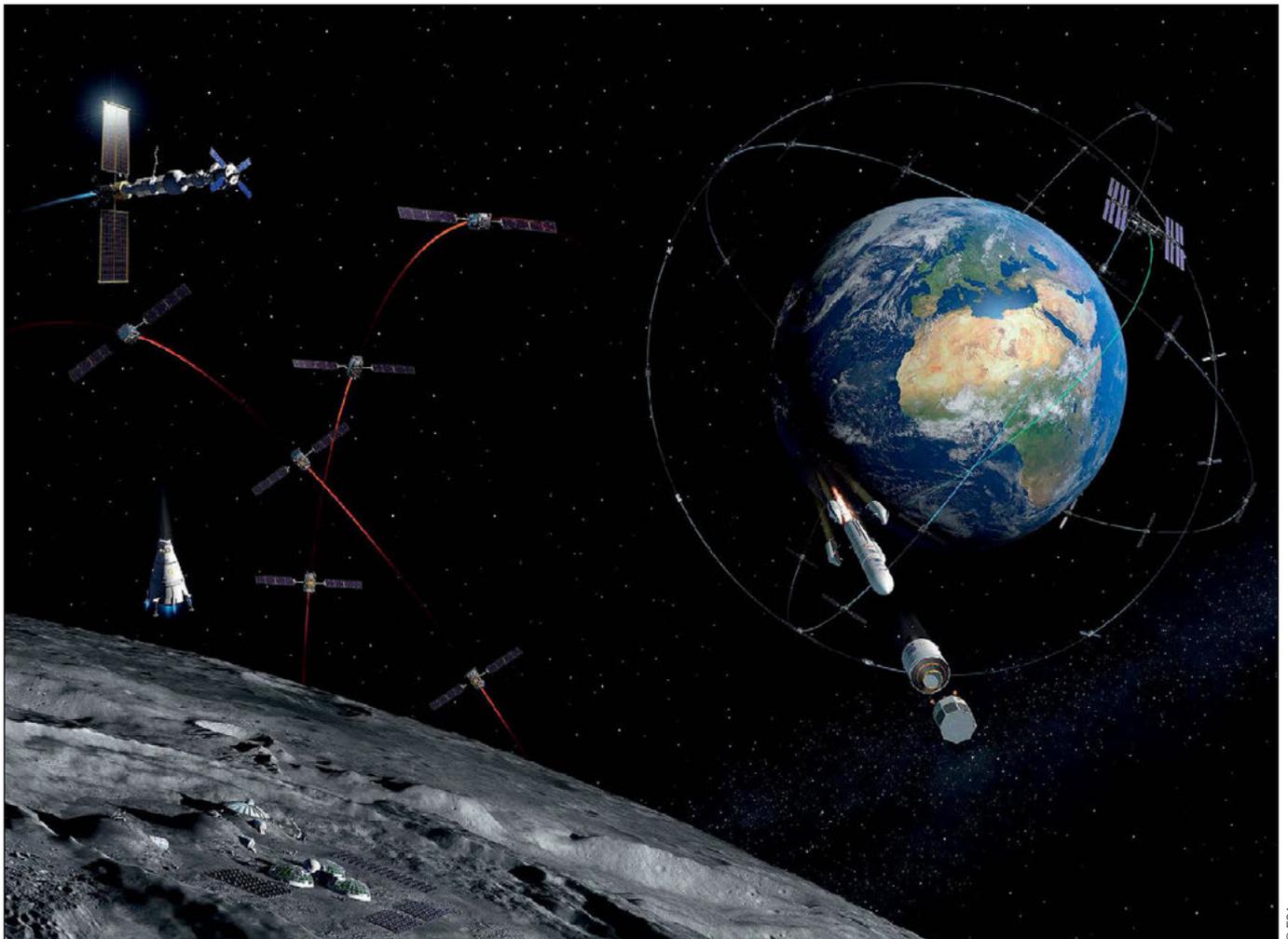
La transmission des données permanentes s'effectue à travers une communication dans l'espace et une liaison à partir du sol lunaire. Les utilisateurs pourront établir des communications par le biais de ces deux canaux selon des standards et des protocoles connus.

Un internet de l'espace

Ainsi, l'Internet Protocol pourrait côtoyer le Bundle Protocol dans le cadre du Consultative Committee on Space Data Standards, de l'Advanced Orbiting Systems et de l'IETF (Internet Engineering Task Force). Cet Internet de l'Espace s'appuie sur trois caractéristiques des télécommunications spatiales : le temps réel, le temps décalé, les messages de services.

Les applications supportant cette chaîne de transmission sont liées aux alertes, à la Position Navigation and Timing (positionnement, navigation et horaire) et à l'acquisition de service. Ainsi, le service LunaSAR correspond au signal dit Search

La connexion entre les différents engins (habités ou non) autour de la Terre ou de la Lune (et à la surface de celles-ci) exigera un réseau où l'aspect cybersécurité sera incontournable.



© ESA

© ESA



© ESA

Ces deux images extraites d'une vidéo de l'Agence Spatiale Européenne (ESA) illustrent une des applications possibles du concept LunaNet, à savoir la possibilité pour les astronautes d'être en liaison avec leurs proches sur Terre.

And Rescue qu'on retrouve dans les constellations de satellites de navigation (Galileo européen, Beidou chinois, Glonass russe et GPS américain) qui se trouvent sur orbite terrestre. Ce service LunaSAR offrira donc la capacité de superviser un signal de détresse à partir de n'importe quels équipements et infrastructures se trouvant sur le sol lunaire.

D'autres services existeront comme le suivi de la météorologie spatiale ou l'usage de liens optiques et radios pour des missions de mesure à partir de la Terre. L'ensemble crée une architecture interplanétaire dans laquelle les télécommunications Terre-Lune utilisent les bandes X, Ka ou optique pour la connexion avec des nodes relais sur orbite lunaire. Ces nodes connectés entre eux avec une bande radio complémentaire (la bande S) communiquent avec des engins sur orbite lunaire et des entités se trouvant à la surface sélène. Les stations terrestres existeront effectueront l'émission et la réception du signal lunaire à partir d'une constellation de satellites de navigation.

Une nécessaire surveillance du réseau

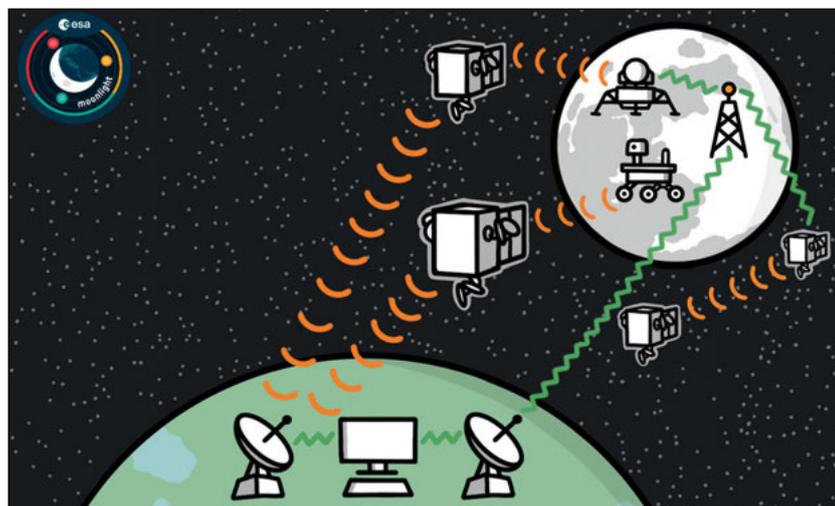
Ce qui signifie que les infrastructures terrestres devront être en mesure de superviser et de suivre l'état du réseau lunaire en prenant en compte des paramètres nouveaux. Ces derniers concernent la capacité à gérer des architectures intégrées avec différents systèmes et protocoles, à comprendre l'effet du milieu spatial sur le traitement du signal, à garantir la disponibilité du signal dans des délais de performance acceptable pour les équipages se trouvant sur orbite autour de la Lune ou à sa surface.

À cet effet, dans ces missions de surveillance du réseau, les caractéristiques du segment sol incluent une réponse à incident inédite et complexe. Pour autant, les principaux points peuvent être vus à partir du fonctionnement actuel des centres de contrôle des systèmes de navigation ou des observa-

toires terrestres. Ainsi, le cas de l'observatoire d'Entoto en Éthiopie démontre comment le LunaNet pourrait s'intégrer dans cette posture de supervision du signal. Le télescope optique de cet observatoire est relié à une unité de commande et de contrôle basée sur un système de navigation, le GPS. Cette même unité est reliée à plusieurs interfaces sur la base d'une relation client-serveur de type Open-TLP (basé sur le TCP/IP d'internet) vers des utilisateurs, des entités externes et un data-center pour le lien de secours. Le dôme, le télescope et la station météo de l'observatoire d'Entoto s'appuient donc sur cette relation client-serveur à travers une interface logicielle. Le réseau doit assurer la continuité d'activité du système pour remplir les fonctions des segments suivants : interface utilisateur pour la surveillance et le suivi, pour le système de management des données, pour le télescope, pour le module de contrôle et de commande. Si ces services séparés sont interdépendants, ils partagent pourtant la même architecture pour les senseurs optiques, les éléments actifs du réseau et pour le processus logiciel.

Dans le cas où ce processus n'est plus disponible, l'agence spatiale d'Éthiopie (fondée en 2016 ou Ethiopian Space Science and Technology Institute) perdrait la capacité de se connecter.

Cet exemple montre que la chaîne des transmissions vers la Lune exige une application originale des concepts opérationnels de cybersécurité. D'autant que cette sécurité est liée à l'introduction généralisée des techniques numériques dans le fonctionnement des engins et des télécommunications.



© SSTL/ESA

Schéma simplifié du principe de multiples liaisons entre des éléments sur la Lune ou autour et la Terre.

Le satellite Lunar Pathfinder de SSTL (Surrey Satellite Technology Ltd au Royaume-Uni) prévu pour un lancement en 2024/25 apportera des services de télécommunications pour plusieurs engins sur orbite lunaire ou à la surface.



Cybersécurité spatiale

Cette cybersécurité spatiale possède deux volets. Un premier volet qui concerne la manière dont celle-ci est applicable par les équipages en orbite ou sur le sol lunaire. Le second volet traite de la sécurisation du signal entre la Lune et la Terre pour assurer les services d'alerte et de télémétrie pour le segment sol.

Le **premier point** tient aux propriétés du cyberspace à considérer. L'émission et la réception du signal traverse plusieurs milieux sur les bandes C et K : l'atmosphère, le champ électromagnétique terrestre, le vide relatif de l'espace. Il y a également les effets de la météorologie spatiale : rayonnement cosmique galactique, effets des ondes gravitationnelles, sursaut radio rapide, sursaut gamma. De plus, d'autres conditions de déploiement Telecom apparaissent dans l'architecture des télécommunications spatiales.

Examinons le service Internet à large bande Starlink. À partir d'environ 2.000 satellites actifs sur orbite basse pour une cible à 42.000 (avec une autorisation de lancement de 12.000 satellites en 2020), Starlink propose un débit descendant de 60,24 Mbit/s et ascendant de 17,64 Mbit/s pour une latence annoncée de 20 ms. Cette constellation constitue un réseau inédit au regard des contraintes de sécurité des transmissions : prise en compte du roaming, du mouvement du satellite au regard du terminal de réception, synchronisation laser entre satellites, routage terrestre avec les stations au sol, routage inter-satellites, doubles bonds en bande K. Quant à l'antenne de 48 cm du terminal, elle peut être sujette au brouillage et aux attaques de type *man-in-the-middle* (interception du signal entre son émetteur et son récepteur).

Le **second point** concerne la vulnérabilité de la couche transport lors de l'émission et la réception du signal entre les objets orbitaux et les stations au sol. Les *command and control* des systèmes s'appuient sur des protocoles, des schémas connus en input et output : interface Internet, shell, UDP, TCP, Wireshark. À cela s'ajoute du matériel *Red Team* et *Green Team* (carte DVB, décodeur, parabole). Une *Red Team* est une équipe chargée de tester la solidité d'un réseau de communications en cherchant à utiliser des techniques d'intrusion. La *Green Team* est celle qui s'occupe de mettre à niveau un réseau de communications à partir de contre-mesures identifiées.

L'analyse des IP datagramme et des UDP datagramme montre des champs multiples pouvant se résumer à des ID (des identifiants), le type de chiffrement, l'orbite du satellite, la fréquence, la polarisation, la synchronisation. Les modèles 3D de visualisation permettent ensuite de travailler sur les cycles temporels du satellite sur orbite pour mieux se connecter. L'utilisation de l'US catalog of space objects (catalogue américain des objets spatiaux) complète l'analyse en fournissant les données orbitales du satellite.

Tout ceci signifie que la science de la cybersécurité spatiale impose d'effectuer des tests de robustesse d'équipements reliés dans une chaîne complexe entre le segment sol et le segment spatial.

Une sécurité embarquée

La généralisation des services essentiels à l'économie via les réseaux spatiaux encourage également une cybersécurité spatiale embarquée. Elle décrit les

systèmes numériques embarqués dans les vaisseaux, les modules, les lanceurs et les satellites qui sont les plus nombreux. Il existe peu de standards de cybersécurité appliqués aux satellites. Ils ont une masse de lancement, un contrôle d'altitude, des panneaux solaires pour l'énergie électrique, une orbite avec des périodes, une inclinaison, un mât d'antenne et des instruments de bord. Et pour maîtriser les processus d'exécution automatique des tâches demandées par la station au sol ou les équipages, chaque commande doit répondre à une action identifiée pour laquelle un ordinateur de bord ou des circuits électroniques effectuent des calculs. Lors du dernier Hack-a-Sat (qu'on peut traduire par *pirater un satellite*) organisé en 2020 par l'Air Force et le Digital Defense Service, la prise de contrôle du mécanisme "tracker" a permis de modifier l'orientation d'un satellite test et de prendre en photo la Lune. Tout comme en 1998 où le satellite ROSAT a vu ses panneaux solaires changés d'orientation en direction du Soleil. D'autres cas similaires se sont déroulés au cours des années 2000. La cybersécurité embarquée traite aussi l'interface homme-machine où la sécurité cognitive permet d'interpréter correctement les données des terminaux pour mener au sol ou dans l'espace des actions de remédiation. Lors de la mission Apollo 11, des codes d'alarme de l'ordinateur de bord sont apparus lors de la descente finale du module lunaire. Le compte-rendu radio des astronautes mentionnaient une alarme que seule la station au sol pouvait interpréter. Les astronautes se trouvaient sous l'effet tunnel de la phase d'atterrissage. Il s'agissait des alarmes 1201 et 1202 que Jack Garman, ingénieur informatique, et Steve Bales, officier de navigation, avaient rencontrées lors des simulations. Les alarmes étaient dues à un problème avec le cycle de calcul du radar d'atterrissage et l'algorithme de commande d'accélérateur. Et les 72 Ko de mémoire de l'ordinateur avait des difficultés pour traiter les quantités de commandes qui lui arrivait. Le sol envoya aux astronautes une instruction sur la marche à suivre (en l'occurrence : ne pas tenir compte de l'alarme). Autrement dit, la science de la cybersécurité spatiale n'est pas uniquement technique. Elle prend en compte la capacité des équipages, à travers les données de leurs écrans, à bien réagir et à comprendre une situation de vol dans le milieu spatial.

Le LunaNet, marquant le premier réseau interplanétaire, intégrera donc des problématiques connues dans un nouveau contexte de déploiement opérationnel qui inclut d'appliquer les principes de cybersécurité dans l'espace.