N°4 - JANVIER/MARS 2025

CYBER-IT

LA CYBER EST UN MARATHON PAS UN SPRINT !

OBJECTIF LUNE
Pouvons-nous vivre dès à présent sur la lune ?

RENCONTRE
Qui de mieux qu'un astronaute pour nous parler de l'espace

DATA CENTER
Nos données dans l'espace

STARLINK
Une cible de choix ?

DOSSIER SPECIAL

CYBERSÉCURITÉ DANS LE DOMAINE SPATIAL

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

Pourquoi ce thème de la cybersécurité dans l'espace ?

Tout simplement, à la suite d'une discussion avec des amis et d'un rapide tour d'horizon de mes contacts sur LinkedIn, l'idée s'est imposée à moi naturellement. Avoir une idée, c'est très bien, pouvoir mettre en œuvre cette idée, c'est encore une autre affaire ! J'ai dû me démener afin de trouver des informations concrètes, des interlocuteurs qui pouvaient et surtout voulaient m'ouvrir les portes de leurs métiers. Ce ne fut pas simple… loin de là ! Le domaine spatial est complexe et très souvent impénétrable.

Les informations doivent être un maximum gardées pour des questions de sécurité. Il est évident que je ne vais pas entrer dans les détails très techniques ou secrets de la fabrication de satellites, mais j'ai essayé de toucher du bout du doigt cet univers que bon nombre trouvent extraordinaire ou encore fantastique.

J'ai eu la chance d'avoir dans mes contacts plusieurs personnes dont le domaine est directement lié au sujet de ce magazine, je me suis donc appuyé sur leurs expertises et leurs connaissances afin d'être au plus près de la réalité dans les différents sujets évoqués.

Également, c'est avec un peu de persévérance et de persuasion que la chance m'a été offerte d'interviewer l'un des pionniers de la conquête spatiale française, un homme dont le rêve a été exhaussé : voyager dans l'espace !

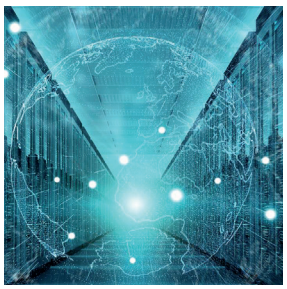
Merci à tous les contributeurs de ce nouveau numéro, et j'espère que vous prendrez autant de plaisir à la lire que moi à l'écrire !

ARNAUD LEROY

Une campagne de Sponsoring Solidaire est en cours !

Le principe ? Vous voulez votre logo dans le magazine, vous souhaitez mettre en avant un projet via une publication ? Alors faisons-le ensemble ! Vous donnez à une des associations choisies par le comité éthique de Cyber-IT et le tour est joué.
Tout le monde est gagnant, une action solidaire pour aider ceux qui en ont vraiment besoin ! (Plus d'infos sur la page de Cyber-IT) ou par mail)

SOMMAIRE



DOSSIER SPECIAL

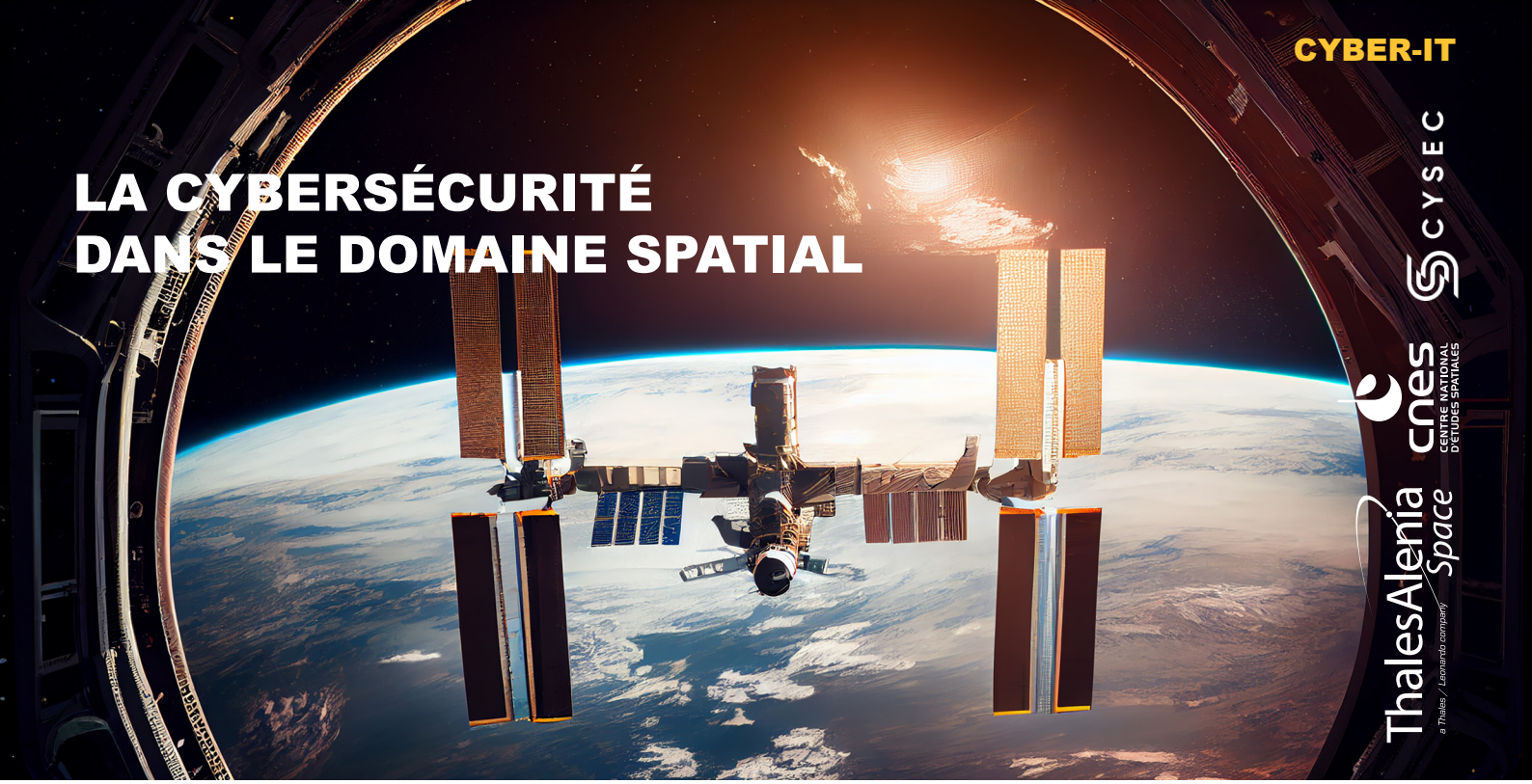
DOSSIER SPECIAL

L'ESPACE

Avec la participation de THALES ALENIA SPACE - CNES - CYSEC - ETH ZURICH

Crédit photo : CNES

La cyber est un marathon pas un sprint !



LA CYBERSÉCURITÉ DANS LE DOMAINE SPATIAL

Merci aux différents experts ainsi qu'aux équipes de CYSEC avec qui j'ai pu collaborer sur ce dossier spécial pour leur aide et leur disponibilité :

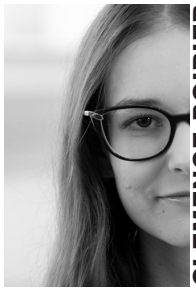
STEPHANE DESCOUS

THALES

ThalesAlenia Space

JULIEN AIRAUD

cnes CENTRE NATIONAL D'ÉTUDES SPATIALES



CLEMENCE POIRIER

ETH zürich

Stéphane Descous est depuis le 1er janvier 2025, Directeur de la Cybersécurité des Produits du Groupe Thales, basé à Toulouse.

Auparavant, il a exercé pendant près de sept ans au sein de Thales Alenia Space (TAS), où il a occupé divers postes clés en cybersécurité.

Il a notamment été Auditeur interne Cyber pour le programme GALILEO, Responsable de la Cybersécurité pour le domaine Navigation France, puis Chief Product Security Officer de TAS, avec un rôle transversal au sein de l'entreprise.

Titulaire d'un Master 2 en Expertise économique et juridique des systèmes d'information.

Julien Airaud est Expert Sénior Cybersécurité spatiale auprès du CNES (Centre National d'Études Spatiales). Depuis presque quinze ans, il a mené des projets en cybersécurité des systèmes orbitaux et des systèmes de lancement. Il a désormais la charge des activités de préparation du Futur dans le domaine.

Titulaire d'un Master 2 en Sécurité de l'Information de l'Université de Limoges, il intervient dans de nombreux établissements de l'enseignement Supérieur. Il modère, contribue ou participe régulièrement à différents organismes des domaines spatiaux ou de cybersécurité.

Clémence Poirier est chercheuse senior en cyberdéfense au sein du Center for Security Studies (CSS) de l'ETH Zurich.

Ses domaines de recherche comprennent la cybersécurité spatiale, les conflits électroniques et cybernétiques dans l'espace, ainsi que les questions plus larges de sécurité et de défense spatiales.

Titulaire d'un Master en Relations Internationales, Sécurité Internationale et Défense ainsi que d'une Licence en Langues Étrangères Appliquées (Anglais, Russe, Espagnol) de l'Université Jean Moulin Lyon III, France.

DOSSIER SPECIAL

Enjeux stratégiques céleste

Depuis les premiers balbutiements de la conquête spatiale, l'espace est devenu un terrain d'exploration et de compétition sans précédent.

Les satellites qui sillonnent aujourd'hui le ciel ont connu une évolution fulgurante. Ils jouent désormais un rôle crucial dans notre vie quotidienne.

Ils nous fournissent des services indispensables tels que les communications, la navigation par satellite (GPS), la météorologie, l'observation de la Terre et bien d'autres encore.

Cette omniprésence des satellites dans notre société en fait une cible de choix pour les acteurs malveillants.

L'espace, autrefois considéré comme un sanctuaire, est devenu un nouveau champ de bataille, où les enjeux économiques, politiques et stratégiques sont considérables.

L'investissement massif de Nations et d'entreprises dans le développement de leurs capacités spatiales et le contexte géopolitique entraînent une intensification de la compétition et une augmentation des risques de conflits.

Parallèlement à cette évolution, les satellites sont devenus de plus en plus complexes et numériques.

La miniaturisation des composants électroniques, l'intégration de logiciels sophistiqués et l'utilisation de systèmes d'exploitation ont considérablement augmenté leurs capacités.

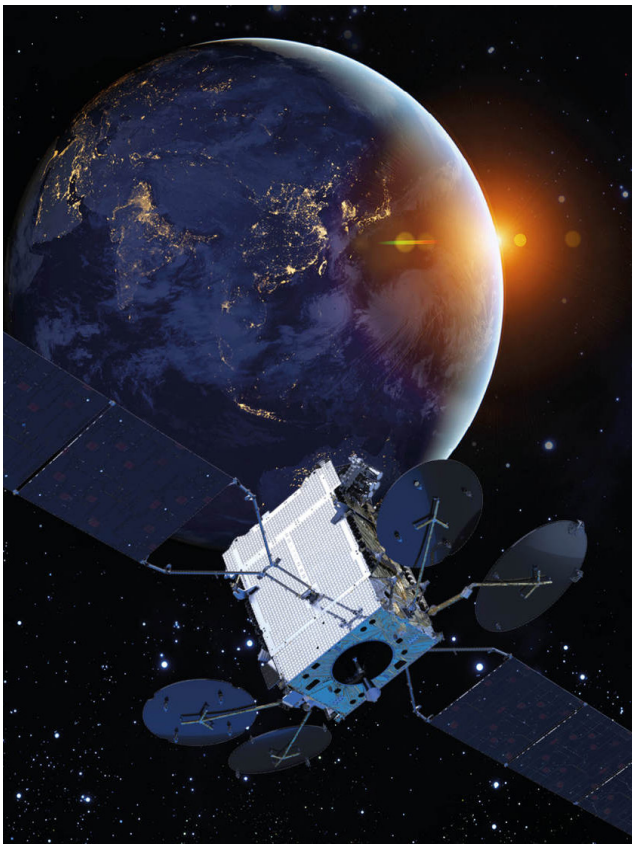
Cependant, cette digitalisation accrue les rend également plus vulnérables aux cyberattaques.

Les satellites sont en effet de véritables ordinateurs volants de plus en plus exposés aux mêmes types de menaces que les systèmes informatiques terrestres, tels que les virus, les logiciels malveillants et les piratages.

De plus, l'interconnexion croissante entre les satellites et les infrastructures terrestres crée de nouvelles vulnérabilités.

Les données collectées par les satellites sont transmises vers des stations au sol, puis distribuées à travers des réseaux terrestres ou d'autres satellites, infrastructures.

Cette interdépendance offre toujours plus d'opportunités pour les attaquants de pénétrer dans les systèmes spatiaux et de perturber leurs opérations.



Selon l'ancien responsable de la sécurité de Thales Alenia Space, ***Stephane Descous***, le plus important est notre capacité à nous challenger sur la détection des événements dans l'espace.

Aujourd'hui, ne plus avoir de liaison avec le spatial serait catastrophique, car nous sommes dépendants de ces liaisons.

De plus, il faut être très attentif aux diverses manipulations de l'information que l'on reçoit; il faut être autonome quant aux décisions que nous sommes amenés à prendre.

Dans les années 1990, l'Union Européenne est dans une situation de forte dépendance vis-à-vis des États-Unis en matière de technologies spatiales de navigation par satellite.

Bien que les performances du GPS soient perçues comme suffisantes pour les usages courants, une amélioration de ces performances est nécessaire pour le développement d'applications plus exigeantes dans le domaine du génie civil, de l'agriculture ou du transport et pour rendre possibles les usages avec de fortes exigences de sécurité. C'est ainsi que le projet EGNOS est lancé.

Dès 1999, dans un rapport d'information de l'Assemblée Nationale sur la guerre du Kosovo, les députés s'inquiètent de la part grandissante des équipements militaires (missiles, aéronefs) dépendant du GPS, et donc « entièrement sous contrôle américain ». L'Union Européenne, en 2001, lance donc son projet GALILEO qui offre une possibilité de localisation d'une très grande précision.

Plusieurs autres programmes, des projets ambitieux visant à développer ses propres capacités spatiales sont en cours. Il est prévu de fournir des services de connectivité sécurisés à l'UE et à ses États membres ainsi qu'une connectivité aux autorités gouvernementales, aux entreprises privées et aux citoyens.

Clémence Poirier nous en dit plus en prenant comme exemple l'attaque du réseau KA-SAT :

"Quelques heures avant l'invasion de l'Ukraine, la Russie a lancé une cyberattaque contre le réseau satellitaire KA-SAT de l'opérateur américain Viasat.

Il s'agissait d'abord d'un déni de service sur les modems utilisateurs et ensuite d'une exploitation de vulnérabilité sur le réseau VPN de l'opérateur du segment sol de KA-SAT qui a permis le déploiement d'un « wiper malware » qui a effacé le disque dur de tous les modems utilisateurs, utilisés par l'armée ukrainienne.

Après cela, j'ai identifié 124 opérations cyber contre le secteur spatial dans le cadre de la guerre en Ukraine. Il y en a probablement beaucoup plus, car de nombreuses opérations ne sont pas rendues publiques.

57 entités différentes ont été ciblées, parmi lesquelles Starlink, la NASA, Lockheed Martin, Boeing, l'Agence spatiale européenne (ESA), l'Agence spatiale suédoise, etc. Dans l'ensemble, 61% des opérations ont ciblé des entreprises spatiales, 32% d'agences spatiales et 3% d'instituts de recherche.

Cela n'est pas surprenant compte tenu de l'utilisation généralisée de services spatiaux commerciaux dans le conflit."

Les principaux risques identifiés évoluent avec le temps. Durant les quarante dernières années, les attaques se focalisaient sur le segment sol, sur l'espionnage émanant de divers acteurs, qu'ils soient étatiques ou non. Également, des opérations de brouillage étaient observables, mais elles ne sont jamais dans le champ visible, sauf si c'est du laser, ce qui peut arriver contre des optiques de satellites.

Aujourd'hui, il est possible de détruire un satellite depuis la terre, mais il ne faut pas oublier que cela produit des débris qui peuvent heurter les satellites d'autres pays et donc avoir des répercussions très fortes. Néanmoins, l'impact ne peut pas être contrôlé et prédit avec précision dans ce genre d'attaque. Un satellite peut être rendu inopérant sans le détruire et donc le rendre tout aussi incontrôlable et dangereux.

La prise en main sur un satellite peut se voir classer en deux catégories :

Celle de la plateforme est une possibilité, en quelque sorte, prendre le contrôle sur le matériel pour le dévier de son utilisation première, dévier sa trajectoire et le faire sortir de son orbite, par exemple.

Mais aussi la prise en main sur la charge utile, c'est-à-dire les fonctionnalités premières telles que l'observation. Détourner l'observation d'une zone à un moment précis peut être très utile pour certaines organisations ou États.

DOSSIER SPECIAL

Dans le cas du conflit russo-ukrainien, les attaques par déni de service distribué (DDoS) représentent 65 % des attaques, tandis que 11 % sont des intrusions et 9 % sont des fuites de données.

Les wiper malware ne constituent donc pas un type d'attaque courant, et aucune autre opération de ce type n'a été identifiée pour le moment. La plupart des opérations contre le secteur spatial étaient des attaques assez simples avec des conséquences temporaires.

Les opérations identifiées sont presque toutes menées indépendamment des opérations sur le champ de bataille. Sur la base de données publiques, aucune cyberattaque contre un système spatial n'a été menée dans le cadre d'une opération conjointe.

Néanmoins, de nombreuses opérations sont liées à des événements du conflit. Par exemple, l'entreprise finlandaise d'imagerie satellitaire ICEYE a été prise pour cible après avoir annoncé la fourniture d'images satellites à l'Ukraine.

De la même manière, les entreprises de la défense sont souvent ciblées parce qu'elles fabriquent des équipements de défense utilisés en Ukraine, mais les hackers sont parfois surpris de trouver des informations sur le spatial. Ce fut le cas lors de l'attaque du groupe prorusse Killnet contre Lockheed Martin, qui est un des grands maîtres d'œuvres de nombreux systèmes de la NASA et de l'USAF.

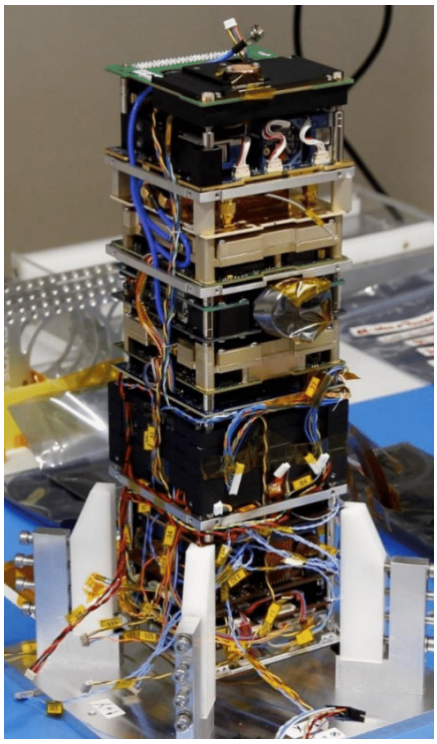
L'information au grand public n'est pas forcément aisée sur des sujets aussi techniques et spéciaux que le domaine spatial et les systèmes satellitaires; néanmoins, certaines entités comme CYSEC ont pu mettre en avant des événements comme CYSAT qui regroupent des acteurs du domaine et qui démontrent les capacités et les évolutions.

Mathieu Bailly, le chargé des activités spatiales de CYSEC, nous explique que, dans le cadre de la troisième édition du CYSAT, l'événement européen dédié à la cybersécurité dans l'industrie spatiale, l'Agence Spatiale Européenne (ESA) a organisé une simulation de prise de contrôle à distance du satellite OPS-SAT, un nanosatellite de l'ESA à visée de démonstration.

L'équipe de cybersécurité offensive de Thales a relevé le défi en identifiant des vulnérabilités permettant de perturber le fonctionnement du satellite.

Les participants ont mis en œuvre différentes techniques de hacking éthique pour prendre le contrôle du système de gestion des senseurs : système de géolocalisation, système de gestion d'attitude et caméra.

Ces actions peuvent conduire à un endommagement important, voire à une perte de contrôle du satellite. Cet exercice unique, qui a mobilisé au sein de Thales l'équipe de sécurité offensive, avec le support du CESTI (le Centre d'évaluation de la sécurité des technologies de l'information du



Le nano satellite OPS-SAT

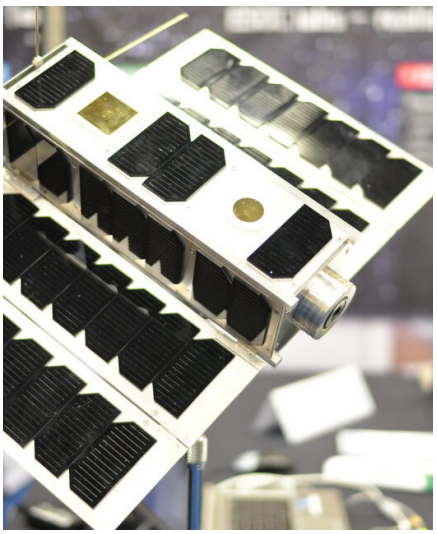
Groupe), démontre la nécessité d'une cyberrésilience avancée, appliquée à l'environnement très spécifique des satellites.

L'équipe Thales, composée de quatre chercheurs en cybersécurité, est parvenue à s'introduire dans le système à bord du satellite.

Après avoir pris la main sur l'environnement applicatif au travers de droits d'accès standards, ils ont réussi à introduire un code malveillant en exploitant plusieurs vulnérabilités. Cela leur a notamment permis de compromettre les données retransmises vers la Terre, notamment en modifiant les images captées par le satellite.

Ils ont également réussi à atteindre d'autres objectifs, comme le masquage de certaines zones géographiques sur les prises de vue satellitaires, tout en dissimulant leurs activités à l'ESA.

> "
>
> **Le maintien en condition de sécurité est un enjeu clé dans notre activité**
>
> "
>
> **Julien Airaud**
> Space Cybersecurity Senior Expert - CNES



Maquette du du satellite OPS-SAT

Les principaux piliers pour mieux sécuriser les infrastructures spatiales

Le premier pilier est tout d'abord d'être conscient du risque cyber et de modéliser la menace qui pèse contre l'entreprise/l'agence en la réactualisant aussi souvent que nécessaire.

Le deuxième pilier est d'intégrer la cybersécurité dès le début de la conception de la mission spatiale mais également dans l'élaboration des designs. C'est ce qu'on appelle couramment le cyber by design.

Le troisième pilier est le maintien en condition de sécurité, car, une fois mis en service, il faut être capable de procéder aux diverses mises à jour et maintenances par exemple.

Le quatrième pilier est de se préparer à une attaque, d'avoir un plan de réponse à incident qui définit les rôles de chacun en cas d'attaque, les points de contact dans les administrations et les obligations de déclarations aux autorités, les options envisageables dans différents cas de figures. Faire divers exercices de mise en situation pour sans cesse améliorer ce plan et s'assurer d'un rétablissement rapide des systèmes.

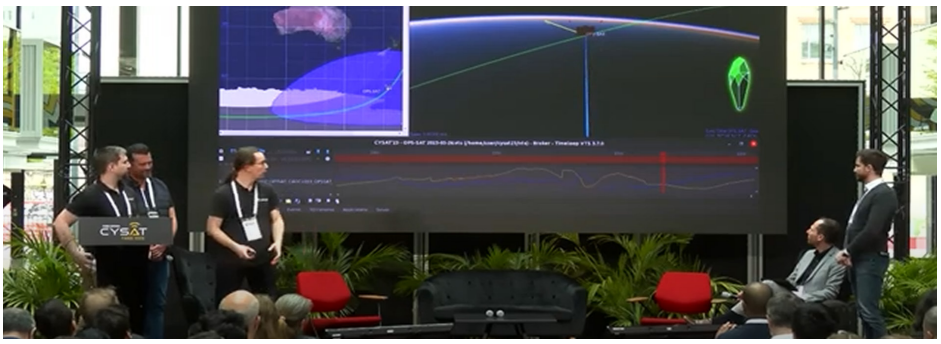


Photo de la prise en main à distance du satellite lors du Hack CySat

DOSSIER SPECIAL

L'espace, le nouveau Far west ?

La possibilité de voir des attaques sur des constellations entières est possible. Des attaques peuvent se dérouler à plusieurs moments du cycle de vie d'un satellite.

En effet, un satellite peut être visé avant même le lancement. La menace est réelle, car plus le temps passe et plus les lanceurs et objets, logiciels liés sont numérisés.

Les lancements sont protégés par les Forces Armées de Guyane, par le dispositif TITAN, mais leur mise en œuvre est civile.

Dans les cas de lancements plus sensibles, le secteur est balisé par des légionnaires. La marine est également engagée dans les mers aux alentours. Ce fut le cas lors du lancement d'Ariane 6.

170 légionnaires et artilleurs sol-air du 3ème Régiment étranger d'infanterie ont veillé à empêcher toute intrusion dans la zone protégée, tandis que dans les airs, la protection était assurée par un hélicoptère Puma et deux hélicoptères Fennec.

En mer, 30 marins du Patrouilleur Antilles-Guyane (PAG) La Confiance et une partie des équipages des vedettes côtières de surveillance maritime Charente et Organabo ont quant à eux effectué une patrouille dans la zone maritime interdite autour du centre spatial.

À la moindre alerte, au moindre doute, il y a une réaction des équipes et dans certains cas, un arrêt complet du processus.

Les constellations de satellites se veulent résilientes, c'est-à-dire qu'il y a plusieurs satellites pour un seul et même service. Si un satellite tombe, un autre prendra le relais et ainsi de suite. Néanmoins, afin d'assurer un service minimum, plusieurs satellites sont nécessaires ; un service ne peut se reposer que sur un seul satellite uniquement.

Les systèmes (orbitaux ou lanceurs) sont exposés pendant le transport, tout comme leur fabrication, recette, assemblage final, intégration et autres ils nécessitent donc une protection permanante tout le long du cycle de vie.

Une attaque avant lancement a un coût et prend énormément de temps. Le résultat serait-il aussi gratifiant pour engager une telle logistique ?

"

Clémence Poirier nous indique qu'en 2021, deux ordinateurs d'employés d'Ariane Espace qui n'étaient pas protégés et contenaient des données confidentielles sur le lanceur Ariane 6 ont été volés par un dealer et retrouvés dans une cave d'une cité de Seine-Saint-Denis.

Heureusement, le voleur ne savait probablement pas ce qu'il avait dans les mains et la police a pu retrouver les ordinateurs. Toutefois, cela aurait pu fournir des informations critiques en vue d'une cyberattaque s'ils étaient tombés entre de mauvaises mains. Ce risque est très commun puisqu'entre 2017 et 2020, la NASA a comptabilisé entre 274 et 430 pertes et vols d'équipement informatique par an. Ces chiffres sont répertoriés par la NASA

comme des cyberattaques.

Les satellites d'une constellation étant tous identiques, si une vulnérabilité est découverte et exploitée sur un satellite, elle peut aussi l'être sur tous les satellites de la constellation. Pour le moment, il n'y a pas d'exemple de prise de contrôle d'une constellation. Toutefois, cela reste une opération complexe à réaliser sans être détecté.

Au début de la guerre en Ukraine, SpaceX a annoncé avoir dû allouer des ressources supplémentaires à la cyberdéfense et à l'antibrouillage du fait de la recrudescence de la menace.

Je tiens toutefois à préciser que, dans le cadre de mes recherches, je n'ai trouvé aucun exemple d'opération dont le point d'entrée était le segment spatial (le satellite en orbite). Toutes les opérations identifiées ont visé le segment utilisateur, le segment sol ou l'environnement informatique de l'entreprise.

Viser les systèmes spatiaux au sol suffit pour affecter le fonctionnement des réseaux satellitaires.

"

Julien Airaud, Expert senior en cybersécurité spatiale au CNES, nous apporte plus de précisions sur la sécurité à proprement parler :

"Notre champ d'évolution, l'espace, n'est pas accessible à tout le monde : l'environnement est très contraignant et les technologies que nous pouvons embarquer, notamment en cybersécurité, sont limitées par le ratio taille/poids/puissance du véhicule.

L'accès à l'espace a tendance à se démocratiser et le nombre d'objets en orbite (utiles ou débris) et leur trafic progressent exponentiellement, comme le droit international renvoie la responsabilité des potentiels dégâts causés au pays opérateur et que l'espace doit rester un milieu utilisable, les États soumettent les opérations spatiales à licences, dont l'obtention peut parfois être soumise à la conformité de l'opérateur à des exigences de cybersécurité.

Parmi ces exigences, on retrouve l'application de mesures de protection triviales dans le domaine de l'IT, mais beaucoup plus complexes pour un véhicule spatial.

C'est pourquoi de nombreux protocoles ont été développés et standardisés pour le spatial après de nombreux tests entre agences pour répondre aux contraintes d'interopérabilité des missions et de l'environnement (puissance disponible, temps de propagation, etc.).

Ainsi, plusieurs groupes internationaux œuvrent à la standardisation de technologies pour le spatial : le CCSDS, l'ECSS, l'ISO ou l'IEEE ont des activités plus ou moins avancées dans le domaine de la cybersécurité spatiale.

La préoccupation historique est la protection des liaisons bord-sol et inter-véhicules, avec des mécanismes pour authentifier et/ou chiffrer les communications.

Nous restons cependant proches de standards terriens, par exemple, nous employons AES. Les clés maîtresses sont souvent chargées au sol. Une fois que le satellite a ses clés, il est vulnérable si les clefs sont divulguées. La gestion des clés est donc un sujet important pour nous.

On pousse aussi vers la crypto asymétrique qui fait défaut au domaine spatial. Les charges utiles communiquent entre elles et les plateformes également, donc c'est compliqué à mettre en place, car on parle de milliers de communicants. Nous travaillons donc désormais à la cryptographie post-quantique, mais aussi à la détection des intrusions bord.

Notre principale menace est l'absence de mesures de protection, souvent liée au fait que les opérateurs considèrent le satellite comme isolé, donc intouchable, en oubliant le sol.

C'est pourquoi le CNES a choisi de publier prochainement des guides d'hygiène de cybersécurité des systèmes spatiaux."

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

MICHEL TOGNINI

Rencontre avec l'un des 10 Français à être allés dans l'espace

Nous sommes allés à la rencontre de ce pionnier et avons eu la chance de parler de sa carrière et de sa vision de l'avenir avec les nouvelles avancées dans le domaine spatial.

Voici l'interview de l'homme derrière le casque d'astronaute, un homme qui garde toujours son regard tourné vers l'avenir et la transmission de son savoir.

" Crois en tes rêves et n'abandonne pas trop tôt ! "

Bonjour Monsieur Tognini, merci de nous honorer de votre présence sur ce numéro spécial espace, pouvez-vous vous présenter ?

Bonjour.
pour ce qui est de mon parcours, j'ai effectué mes études dans la région parisienne et j'ai suivi une spécialisation de la Troisième à la Terminale pour me préparer aux arts & métiers afin de devenir ingénieur. Par la suite, j'ai suivi deux ans de classes préparatoires en maths sup et maths spé à Grenoble, à l'école des pupilles de l'air. Il s'agit d'une école à vocation militaire qui prépare à l'école de l'air. J'ai opté pour cette école car je voulais devenir ingénieur et me rapprocher des métiers dans l'aéronautique. Mon amour pour l'aviation m'a conduit à intégrer une école militaire où j'ai pu assouvir ma passion en pilotant des avions et en pratiquant des sports extrêmes. Après l'École de l'air, j'ai enchaîné les expériences en tant que pilote de chasse, d'abord sur SMB2 puis sur Mirage F1.

Mon expertise m'a ouvert les portes de l'école des pilotes d'essai en Angleterre. Avec trois ans d'expérience en tant que chef pilote d'essai, j'ai saisi l'opportunité de postuler pour devenir astronaute. Sélectionné en 1985, j'ai dû adapter mes projets en raison de l'accident de la navette Challenger.

J'ai alors effectué un entraînement et un vol en Russie avant de participer à une mission spatiale américaine en 1999. Suite à l'accident de Columbia, j'ai consacré ma carrière à la formation des futurs astronautes européens en tant que directeur du centre des astronautes européens.

Pouvez-vous m'expliquer en quelques mots vos deux missions effectuées dans l'espace ?

C'est vrai que j'ai eu le plaisir de participer à deux missions spatiales : Soyouz TM-15 en 1992 et STS-93 en 1999.

C'était une mission spatiale russo-française qui a été réalisée en juillet 1992. Elle a marqué une étape importante dans l'histoire spatiale française, car elle a permis de belles avancées dans plusieurs domaines, notamment grâce aux expériences menées durant la mission, comme celles sur la croissance des plantes en microgravité, sur leurs cellules ainsi que sur l'impact de cette microgravité sur les différents éléments physiques. En tant que scientifique, j'ai été au cœur de ce dispositif.

J'ai eu un certain rôle d'ambassadeur de la France, car j'étais le premier Français à rejoindre la station MIR. L'histoire retiendra la conversation que j'ai eue avec le président Mitterrand comme un symbole.

En ce qui concerne mon second vol, il a eu lieu exactement 7 ans après le premier, en juillet 1999. La mission a été marquante à plusieurs niveaux.

Nous devions décoller avec le télescope Chandra afin de le déployer et le mettre en orbite. C'était aussi une première, car Eileen était la première femme à commander une navette.

Une grande réussite !

15 jours dans l'espace n'est-ce pas court quand on s'est entraîné pendant plusieurs années ?

Je dirais que c'est plutôt que c'est progressif avec le temps. À l'époque, c'était la moyenne des missions. Aujourd'hui, on voit des missions qui sont plutôt de six mois et à l'avenir, elles seront encore plus longues.

D'ailleurs, des études sont déjà en cours pour connaitre la façon dont le corps va se comporter durant les prochains vols habités, on peut citer Mars 500. Il s'agissait d'une simulation ambitieuse d'une mission habitée vers Mars, réalisée sur Terre entre 2010 et 2011. Ce projet avait pour objectif de tester la résistance psychologique et physiologique d'un équipage confiné dans un environnement simulant les conditions d'un voyage spatial de longue durée vers Mars.

Pour revenir à mes vols, je dirais que nous avons eu de la chance d'être sélectionnés et voir des choses que peu de monde ont vu.

En tournant autour de la Terre 16 fois par jour, il m'a été donné de voir des zones que je n'aurais jamais eu l'occasion de voir de mes yeux par la suite.

Alors oui, c'est beaucoup d'années d'entrainement, mais ça vaut le coup d'être vécu.

Michel Tognini

Il y a eu beaucoup d'imprévus lors de votre deuxième mission pour déployer le télescope Chandra. La peur est-elle présente à ce moment-là dans votre tête ?

Nous partons avec confiance au moment du décollage. Nous sommes accompagnés par du monde : les ingénieurs, nos amis, nos collègues astronautes, nos familles et bien d'autres.

C'est vrai qu'il y a eu pas mal d'imprévus avant le décollage, qui a été à plusieurs reprises reporté. Mais nous sommes tellement préparés que cela est devenu moins stressant.

Nous envisageons beaucoup d'éventualités quand nous sommes en simulateur au sol. Il faut savoir que les simulations sont extrêmement proches des conditions réelles. Les instruments sont les mêmes, les dispositions des commandes sont les mêmes aussi. Par exemple, ce qui fait que je n'ai pas découvert tout cela en arrivant dans la navette, c'est aussi moins de stress.

Lors de l'allumage des moteurs, un morceau de métal s'est détaché du moteur trois (à droite) et a heurté la surface interne de la buse du réacteur en arrachant trois tubes de refroidissement contenant de l'hydrogène.

Un court-circuit a coupé en partie le moteur droit et cela a été compensé par le système de secours qui a augmenté l'arrivée d'hydrogène, ce qui a entraîné une augmentation de la chaleur, ce qui, au final, a entraîné un arrêt prématuré des trois moteurs de la navette.

On a frôlé la catastrophe !

Un ingénieur au sol a été décoré pour son travail sur cette mission d'ailleurs !

Quel œil portez-vous sur les nouveaux acteurs du spatial comme Space X ou encore Blue Origins, par exemple ?

La navette columbia

Elon Musk a réussi là où les agences spatiales se sont arrêtées. Personnellement, je pense que c'est un pari gagnant, tant sur le plan financier que sur le plan technique.

C'est un deal gagnant/gagnant, car chaque vol est analysé et scruté minutieusement pour en tirer les leçons de ce qui a pu être dysfonctionnel et pouvoir améliorer cela au prochain vol.

La grande force de SpaceX et de facto de son fondateur Elon Musk, c'est sa capacité à fédérer autour de lui et à inculquer un rythme de travail qui est exceptionnel. On peut dire que les USA ont retrouvé leur indépendance spatiale.

Il est beaucoup question de voyage touristique dans l'espace, par exemple, mais cela reste encore très cher, de l'ordre de 50 millions d'euros le billet lors de la dernière mission Polaris.

Néanmoins, je suis persuadé que nous irons sur Mars, mais pas avec le calendrier qu'Elon Musk a mis en place, mais nous irons, c'est une certitude.

Vous êtes à l'origine du recrutement de Thomas Pesquet, est-ce une fierté de voir sa réussite aujourd'hui ?

Le recrutement d'un astronaute est un processus long et rigoureux, qui nécessite des compétences exceptionnelles et une préparation intensive.

Thomas Pesquet, est sans doute l'astronaute français le plus connu de sa génération. Il communique énormément et a démocratisé la communication sur les métiers du spatial.

Bien sûr, c'est une grande fierté d'avoir pu être à l'origine de son recrutement. Il faut savoir qu'au départ, les candidats de la première vague de recrutement étaient plus de 8 400 dans la première phase, puis à la fin, ils n'ont été que 6 à être sélectionnés. La seconde vague, plus récente, a vu pas moins de 20 000 candidatures.

C'est une fierté, car je vois en lui un homme qui donne l'exemple à la plus jeune génération.

Je suis sûr que les futures campagnes de sélection devraient connaître un succès similaire.

Il y a aussi de la fierté à avoir pu recruter Sophie Adenot qui va faire son premier vol dans l'espace en 2026.

Thomas Pesquet

Avoir écrit des livres est-ce un devoir de mémoire pour les jeunes générations ou un besoin ?

Les deux !

Je pense qu'il est de mon devoir de laisser une trace pour les prochaines générations. Ils pourront y découvrir de manière étonnante ce qu'on a pu accomplir.

Ces livres sont une façon de marquer l'histoire tant sur le plan technique que descriptif. Il faut garder des écrits pour les prochains siècles à venir.

Rester dans l'histoire en quelque sorte.

Pour l'anectode le titre "Un café dans l'espace" est lié au fait que la première chose que l'on est proposé dans l'espace

Vous savez, quand on est astronaute, il y a une partie opérationnelle où l'on fait les choses et une partie transmission où l'on explique les choses.

Je suis arrivé dans cette deuxième phase.

Couverture du livre

Avec le recul, que diriez-vous à l'enfant que vous étiez si vous le pouviez le rencontrer aujourd'hui ?


Jean-Loup Chretien et Michel Tognini

Si je pouvais revenir revoir qui j'étais étant jeune, je dirais à cet enfant de croire en ses rêves et de ne surtout pas abandonner trop tôt ! Tu es capable.

A l'école, petit, je n'étais pas bon, je dois le reconnaître… En sixième, j'ai rencontré un prof de maths qui m'a fait passer de dernier à premier. Cette matière qui était très compliquée est devenue un jeu facile. Ce sont ce genre de rencontre qui change des vies !

Si un jeune veut devenir professeur, mathématicien ou encore boulanger, peut importe le métier que l'on souhaite exercer, il faut se donner à fond pour réussir et s'accrocher!

Tous les métiers méritent que l'on se donne à 100 % pour réussir pleinement.

Ce professeur m'a donné envie d'étudier. Je travaille d'ailleurs avec des professeurs et je constate que nous avons un corps enseignant extraordinaire.

Il y a des enfants qui sont perdus mais qui réussissent à survivre grâce à l'éducation.

Tout le monde devrait avoir cette rencontre magique avec un prof qui le tire vers le haut !

Merci d'avoir pris le temps de nous répondre. Auriez-vous un dernier mot pour conclure cet interview ?

Je terminerai cette interview en vous donnant deux citations que j'aime vraiment :

« La terre est le berceau de l'humanité, mais ne peut pas rester dans le berceau éternellement » de Konstantin Tsiolkovski.

« Pour ce qui est de l'avenir, il ne s'agit pas de le prévoir, mais de le rendre possible » d'Antoine de Saint-Exupéry.

Interviews

de ceux qui font la cyber et l'IT d'aujourd'hui et de demain

Une nouvelle fois, notre section interviews est au rendez-vous.
Six nouveaux visages, pour six nouvelles rencontres !

SOUFIANE TAHIRI

Responsable sécurité offensive - Peaksys

Hello Soufiane, peux-tu nous en dire un peu plus sur toi ?

"Hello Arnaud,

Je suis Soufiane, passionné de bidouillage informatique, mais j'ai toujours été aussi passionné par la nature, les animaux, le dessin, le bois et les questions philosophiques... qui n'ont rien à voir avec l'informatique"

Quel a été ton parcours ?

"Je ne sais pas si c'est un parcours type, mais disons que mes études n'ont pas spécialement contribué à mon "insertion professionnelle", j'ai eu la chance de fréquenter "virtuellement" des gens qui s'intéressaient à la sécurité informatique bien avant que ça devienne la mode (vers les années 2003).

J'ai appris à leur côté plein de choses, de la rétro-ingénierie aux tests d'intrusion (terme qui n'existait pas à l'époque) en passant par du développement, ce qui m'a permis de décrocher un job le jour où payer les factures était devenu plus important que d'apprendre à reverser un malware...

Sinon j'ai eu un parcours scolaire assez chaotique mais pour ce que ça vaut j'ai fait un peu d'économie à la fac"

Quelles sont tes missions au quotidien ?

"Aujourd'hui je suis responsable d'une petite équipe de pentesters. Le quotidien consiste principalement à se dispatcher les missions, et à conduire des tests d'intrusion

Il m'arrive aussi de faire de la veille plus ou moins active, un peu de renseignement sur la menace, un peu de recherche et développement toujours orienté offensif"

À quoi ressemble une journée type pour toi ?

"Une journée type est comme pour tout le monde j'imagine, répondre à des mails, assister à des réunions et essayer de trouver le maximum de façon d'abuser d'un système d'information ou d'une application quelconque avant "les méchants"

Qu'est-ce qui te plaît et te déplaît dans ton métier ?

Ce qui me plaît dans mon métier c'est le challenge permanent, t'as beau te considérer bon en ce que tu fais, tu finis souvent par ne pas comprendre ce qui se passe sur ton écran.
Ce qui le déplaît dans mon métier, c'est que c'est devenu justement un métier :) le métier tue souvent la passion"

Un mot pour la fin ?

"Aussi bons qu'on se croit être, il y a et il y aura toujours meilleur que nous. Ce domaine est fait avant tout de partage et d'humilité, ne jamais perdre de vue ça : partage, humilité."

HUSSEIN AISSAOUI

Architecte Cybersécurité - SFR Business

Salut Hussein, beaucoup te connaissent, mais dis-nous qui es tu ?

"Salut Arnaud !

Alors je suis un architecte en CYBER SECURITE qui fait du 360 au niveau de la Cyber , je ne me fixe aucunes limites de sujets ou de périmètres"

Quel a été ton parcours ?

"Je suis à l'origine un expert sur les technologies Microsoft Active Directory et messagerie Exchange et un passionné de basket qui m'a fait aiméer les challenges et la gestion.

Et au fur et à mesure des missions de plus en plus complexes et intéressantes, j'ai ajouté la casquette Sécurité qui s'est tout naturellement transformée en CYBERSECURITE qui englobe tout désormais"

Quelles sont principalement tes missions ?

"Au quotidien ? Ma mission est de partager mon expertise cyber sur tous les périmètres classiques ou plus confidentiels .

Et construire la meilleure défense cyber face aux menaces qui évoluent jour après jour .

Que ce soit au niveau des technologies ou des conflits dans le monde qui génèrent toujours des nouvelles menaces "

A quoi ressemble une journée type pour toi ?

"C'est simple , une journée type n'existe pas, car je bois beaucoup de littérature cyber (énormément) je découvre et travaille en continu et prends en compte toutes les nouvelles menaces sous toutes leurs formes .

Donc ma journée type, c'est beaucoup de LIVE CYBER"

Qu'est-ce qui te plaît et te déplaît dans ton travail ?

"Absolument tout me plait... vraiment !
Et plus précisément tout ce qui est innovant et qui permet d'apporter un regard nouveau et des méthodes nouvelles de sécurisation. Et l'IA est une formidable opportunité de monter d'un cran au niveau cyber (attaque et défense)

Et ce qui me déplait... le fait qu'il n'y a que 24H dans une journée"

Un mot pour la fin ?

"Nous ne sommes qu'au début de la cyber et de l'IA associées... Et cela nous promet des évolutions fantastiques.

Le tout est de savoir est-ce que nous en profiterons où bien nous subirons... A nous de faire en sorte que la cyber nous fasse du bien à nous et à nos entreprises."

MARC-ANTOINE LEDIEU

Avocat, RSSI legal et conférencier

Bonjour Marc-Antoine, raconte-nous qui tu es en quelques mots ?

"Bonjour Arnaud, je suis Marc-Antoine LEDIEU, avocat au barreau de Paris depuis bientôt trente ans. Depuis 1997, je rédige des contrats IT techniques pour encadrer le business des professionnels du numérique, depuis 2014, j'explique les lois et la technique en mode "vulgarisation", notamment avec des bandes dessinées accessibles sur mon site web.

C'est en 2013 que je me suis orienté dans le domaine cyber. En 2017, les malwares WannaCry et NotPetia ont eu pour conséquence l'apparition d'annexes contractuelles spéciales "cybersécurité" dans les contrats IT BtoB. Les réglementations DORA et NIS2 (décembre 2022) et LPM2023 sont les textes relatifs aux règles obligatoires de cybersécurité, qui nous occupent beaucoup en ce moment..."

Quel a été ton parcours ?

"Mon parcours débute avec des études en droit des affaires et en droit des contrats.
Pour mieux comprendre les aspects techniques, je me suis autoformé sur les domaines du numérique, de la blockchain et de la cybersécurité.

En 2021, j'ai obtenu la certification ISO 27001 Lead Auditory et messagerie Exchange et un passionné de basket qui m'a fait aimer les challenges et la gestion.

Et au fur et à mesure des missions de plus en plus complexes et intéressantes, j'ai ajouté la casquette Sécurité qui s'est tout naturellement transformée en CYBERSECURITE qui englobe tout désormais"

Quelles sont tes missions principalement ?

"Je ne plaide que très rarement. Je m'occupe essentiellement de projets de déploiement DORA et NIS2.

Ma communication en BD (sur mon site web et mon profil LinkedIn) me prend du temps, ainsi que le suivi de l'actualité technique et juridique. Je donne des cours sur le droit de la cyber et participe à des conférences de "hackers".

Comme je suis également RSSI Legal, j'accompagne les RSSI sur la partie juridique (réglementation, normes techniques, jurisprudence, etc.) de leur métier"

A quoi ressemble une journée type pour toi ?

"Mes journées commencent par 1h minimum de documentation (journal officiel, presse en ligne, etc.) dans l'univers du numérique.
Puis, je fais les prestations pour mes clients (conseil, négociation, etc ...)"

Qu'est-ce qui te plaît/déplaît dans ton métier ?

"Ce qui me plaît dans mon métier, c'est d'accompagner les entreprises vers une mise en œuvre effective vers la sécurisation de leurs données !

Le coté déplaisant : les entreprises qui négocient systématiquement les prix de mes prestations (car la cyber, c'est facile, ça ne rapporte rien, mais c'est toujours trop cher...)"

Merci as-tu un mot pour la fin ?

"La législation sur la cybersécurité n'est pas un mal mais elle est nécessaire ! Nos entreprises et nos sociétés civiles, sont totalement tributaires du numérique.

Mais aucun de nos systèmes d'information/logiciels n'ont été conçus en intégrant les concepts de la cyber"

DAMIEN BANCAL

Journaliste pour ZATAZ et chercheur en cyber

Bonjour Damien, qui es-tu ?

"Je me nomme Damien Bancal, 52 ans, journaliste, chercheur dans les questions de lutte contre le cybercrime. Fondateur du blog ZATAZ.COM et entrepreneur avec la société VeilleZATAZ.com

Passionné de découverte et de partage. Impatient de ce que je vais apprendre demain"

Peux-tu nous en dire plus sur le parcours qui est le tien ?

"J'ai toujours voulu devenir journaliste, dés mon plus jeune âge, trouver des réponses à des questions, ou rajouter des questions à des questions. À 14 ans je rencontre mon premier pirate, un "phreaker", un spécialiste du piratage télécom. J'écris sur ce sujet. J'avais déjà un blog sur Amstrad CPC [A l'époque les disquettes faisaient 128k].

Des études dans la comm', je bosse déjà en même temps pour des journaux dédiés aux high-tech, jeux vidéo, Etc. ou la presse généraliste. Je rencontre à Lille, Eric, à l'époque webmaster, aujourd'hui Master de la cyber. Il m'invite à lancer mon projet ZATAZ sur le web, le vrai, pas via Skyblog, ZATAZ.COM est lancé.

Nous sommes alors aux portes des années 2000. Le projet ZATAZ a déjà 10 ans.Communiquant passionné j'intègre deux communes dans le Nord de la France, je deviendrai pour l'une d'elles le responsable communication.

2019, une entreprise québécoise vient me chercher en France. Je deviendrai leur responsable de la division Cyber Intelligence à Montreal. La COVID va tuer le projet. Je suis resté 9 mois sans ma femme et mes enfants"

Quelles sont tes missions au quotidien ?

"Compliqué à expliquer sans révéler des secrets professionnels. Nous vivons dans un environnement où le contrôle du social engineering est indispensable.
Donc, je dirai : recherches et enquêtes pour le service veille et le blog. [Les deux entités ne se partagent aucune information].

Avec le SVZ, nous avons une vingtaine d'outils 100% internes, j'en ai créé 14. Production média. Par exemple pour France Info : trouver l'info qui fait mouche concernant l'IA, écrire la chronique radio, passer à l'antenne.
Communication et relationnel : partenaires, lecteurs, futurs clients, pirates, Etc."

Qu'est-ce que te plaît et déplaît dans ton métier ?

J'ai une énorme chance, travailler dans un métier que j'ai toujours voulu. J'ai pu, en plus, y rajouter les options de mon choix.

Mais la chance ne vient pas sans travail, sans rencontres, sans motivation.Le seul petit bémol, les journées ne font que 24h"

À quoi ressemble une journée type pour toi ?

"Variées, c'est le moins que l'on puisse dire. Je n'ai pas de journée type.
Prenons, par exemple, le jeudi, 5h debout, émission TV/Radio de 9h à 12h. Le trajet 'avant/après' me permet de collecter les infos de la nuit pour ZATAZ.COM.
Retour au bureau. Jusqu'à 14h, relationnel SVZ, presse, Etc. 14h, téléphone et outils connectés finissent dans le sas "no connect". On ne peut plus me joindre. Divers travaux de 14h à 20h.

20h, vie de famille.
Minuit, reprise des travaux en cours. Mais ça, dans la condition de "pas d'imprévus". Et une vie sans imprévus, c'est pas fun ! :)"

Merci as-tu un mot pour la fin ?

"J'ai toujours entendu dire que ma curiosité était un vilain défaut, mais croyez-moi, mon défaut est une sympathique curiosité"

JULIEN METAYER

Pentester - Redteamer - Osinter - Mentor

Hello Julien, dis-nous qui es-tu ?

"Salut Arnaud, avec plaisir !

J'ai 47 printemps à mon actif, je suis issu de l'univers du dev à l'origine. Également, j'ai eu l'occasion de faire de la gérance d'infrastructure web, mais il y a environs 6ans je suis revenu au hacking, pentest et redteam.

Au delà de ça, j'organise des enquêtes au sein des entreprises et participe à des missions d'assistance en lien avec le Commandement du MInistère de l'Intérieur dans le CYBERespace (COMCYBER-MI).

De plus, je suis aussi mentor pour l'école Guardia Cybersecurity School. Le reste de mon temps libre? je participe à des conférences sur divers sujets.

J'ai également le plaisir d'être à l'origine du site ozint.eu devenu osintopia"

Peux-tu nous expliquer ton parcours ?

" Il y a déjà 25ans j'ai passé un master de méthodes informatiques appliquées à la gestion des entreprises (MIAGE).

Un peu comme chacun dans notre domaine, je suis autodidacte, j'aime à apprendre. Je suis passé par M2i Formation Diplômante pour faire valider certaines de mes connaissances acquises, d'ailleurs, je tiens a remercier un de mes formateurs, qui est un gars en or, Jordan DOULIEZ :)"

Y a-t-il des choses qui te plaisent/déplaisent dans ton métier ?

"Je te dirais que ce qui me plaît réellement dans mon métier, c'est la variété de ce que je peux voir, je ne m'ennuie pas et je ne me lasse pas.

Le côté humain est également un facteur de satisfaction dans ce métier, mais bien sûr aussi le fait de pouvoir le faire en télétravail. En somme, ce qui me plaît, c'est la gestion flexible de mon temps de travail.

Ce qui me déplait, c'est le fait qu'il est rarement une fidélisation de la clientèle, il faut donc réseauter pas mal. Je dirais aussi que le fait d'être indépendant n'est pas forcément une aide, car il y a beaucoup de mise en concurrence avec des grosses sociétés (ce qui n'est absolument pas un gage de qualité)"

Quelles sont tes missions quotidiennes ?

"Généralement, mes missions tournent autour des pentests web.

J'organise aussi des sessions de veilles et de réseautage, mais cela dépend des périodes. Par exemple, aux alentours des mois d'octobre et de novembre je suis le plus souvent en conférences (pour y participer ou juste y assister)

J'ai la chance d'être indépendant et donc d'être très libre de mon agenda"

As-tu une journée type ?

Je commence toujours mes journées par 2h de veille le matin, le télétravail me laisse libre de commencer mes journées sans horaires fixes. Puis j'enchaîne sur mes diverses missions mentionnées plus haut.

Cela me permet aussi de voyager beaucoup, je profite de cette liberté au maximum. Au final, je fais ce que j'aime.

Je préfère faire ce qui me fait réellement vibrer aujourd'hui, quitte à gagner moins"

Julien, as-tu un mot pour la fin ?

"Dans l'OSINT la guerre d'ego est trop présente, c'est dommage ...

Il est nécessaire d'avoir conscience de ce qu'il se passe sur les réseaux. Également, il est important de faire de la sensibilisation auprès des plus jeunes (éthique, les photos, etc...)"

FRANCK CECILE

Responsable de la conformité en cybersécurité

Bonjour Franck, peux-tu m'en dire plus sur toi ?

"Comme nombre d'entre nous, un passionné, pas tant par la cybersécurité, mais par les nouvelles technologies, les changements que cela apporte à notre quotidien, les risques, les usages détournés que l'on peut en faire ….

Tant sur les aspects purement techniques (même si, disons-le clairement j'ai passé l'âge de trifouiller une Kali) que sur les aspects nécessitant un peu de prise de recul … Enjeux organisationnels, risques géopolitiques, organisation d'un département digital / cybersécurité pour faire face aux challenges métiers …"

Tu peux m'en dire un peu plus sur ton parcours ?

" Technicien IT, Ingénieur et architecte réseau et sécurité, consultant réseau, datacenter, puis cybersécurité.
Et maintenant Cybersecurity GRC Officer.

Je suis passé par pas mal de postes et de missions, tant en client final que dans le service, la régie ou le conseil pur, pas mal d'industries différentes aussi, IT & OT mais au final, en exerçant toujours de près ou de loin dans la sécurité. Plutôt milieu opérationnel au début, et maintenant clairement axé organisationnel."

Quelles sont tes missions au quotidien ?

"De la gouvernance et de la conformité.

Je n'en dis pas plus, mais bien que cet univers soit systématiquement perçu comme "chiant", il y a réellement de quoi s'éclater sur des missions GRC :-) "

À quoi correspond une journée type dans ton travail ?

"Excel et PowerPoint sont mes meilleurs amis, ahah !

Plus sérieusement, je ne suis plus "mains-sur-le-clavier" depuis un moment déjà.

J'ai quitté la technique pour évoluer sur du pilotage, du cadrage, de l'organisation … beaucoup de gros mots que nos amis opérationnels apprécient peu, et c'est compréhensible ; les travaux en GRC sont très peu "palpables".

Mais ils sont complémentaires.

Dans les faits, cela se traduit par énormément de communication, parfois du lobbying, mais surtout, de la prise de recul sur des sujets complexes"

Qu'est-ce qui te plaît et déplaît dans ton métier ?

"Je tourne beaucoup autour du distinguo entre les mondes opérationnel et organisationnel, car ils constituent réellement, selon moi une source de problème pour n'importe qui évoluant en cybersécurité. Indéniablement, les 2 mondes sont complémentaires, et pourtant ils ne se comprennent pas, voire parfois se détestent carrément.

Ajoutons à cela que, quand on exerce côté organisationnel, on ne voit que très difficilement le résultat de notre labeur, tant il est diffus.

En revanche, si le résultat est beaucoup plus concret côté opérationnel, je sais aussi que ne pas réussir à comprendre une démarche ou une stratégie qui ne va pas dans le sens que l'on désire est très frustrant. Malheureusement, il faut faire avec ces problématiques"

Merci Franck, as-tu un mot de fin ?

"L'IA nous sauvera (ou pas)."

LAURENT MINNE

Ingénieur cybersécurité sénior

Salut Laurent, j'ai la chance d'avoir pu m'entretenir avec toi, peux-tu nous dire qui es-tu en quelques mots ?

"Salut Arnaud, alors je suis Laurent Minne, Ingénieur en Cybersécurité Senior, passionné par la sécurité informatique depuis pas mal d'années.

Je travaille pour Acensi en tant que CISO.

Le point le plus important est que je suis un autodidacte depuis une trentaine d'années et je continue à apprendre tous les jours, même avec 48 heures de vols au compteur"

Peux-tu me décrire en quelques mots ton parcours ?

"Pour remonter un peu dans le courant du temps, je suis un profil atypique; j'ai débuté ma carrière profesionnelle en tant qu'installateur d'équipement électrique, parallèlement second de cuisine dans un restaurant en bord de mer dans le sud de la France. Dès mon retour dans le plat pays belge, j'ai entamé une longue carrière au sein d'une entreprise de facility management comme homme à tout faire avec une petite activité autour de la sécurité informatique.

En 2013, ce fut le grand bon pour devenir freelance à titre complémentaire dans le domaine de la sécurité informatique principalement, avec des accents d'administrateur systèmes et réseau. Mes missions furent aussi diverses que nombreuses dont j'ai eu la chance de cotoyer de belles enseignes. Parallèlement, j'ai continué à apprendre de nouvelles techniques, disciplines et surtout, la chance de travailler avec des personnes passionnées pour ne pas dire exaltées.

Le partage, l'entraide, limite intensif n'a fait qu'animer davantage la passion pour la sécurité informatique (Cybersécurité par la suite) et c'est en 2023, que j'ai décidé de créer une communauté, un collectif francophone (toutes et tous bénévoles) autour de la CyberSec qui se nomme "Be•Cyber Community" sous forme d'un canal Discord"

Excellent ! Et quelles sont tes missions quotidiennes ?

"Elles sont diverses; comme je suis un lève tôt, je prends le temps d'effectuer le warm-up en cherchant des outils, ressources intéressantes pour le partage à travers un billet sur Linkedin. Mes principales tâches actuellement sont d'effectuer des analyses de risque sur diverses technologies, recherche d'informations sur la Security Discipline, trouver de nouvelles sources d'inspirations pour en découler des projets intéressants. Les soirs, principalement, je m'occupe de l'entraide pour d'autres communautés telles que Edu.Cyber, Cyber V, Kaisen Linux et quelques associations. Etudier sur des projets open source et libres liés à la Cyber Threat Intelligence et recherches et j'en passe beaucoup d'autres"

À quoi ressemble une journée type pour toi ?

"La journée type idéale est quand j'ai appris quelque chose, sans cela, elle deviendrait ennuyeuse à souhait"

Qu'est-ce qu'il te plaît dans ton métier ?

"Cotoyer des personnes extraordinaires, compétentes, intelligentes et passionnées. Je réitère légèrement mes propos mais le partage d'informations est primordial pour atteindre la journée idéale"

Parfait ! As tu un mot pour la fin ?

"Merci de m'avoir accordé cet entretien. Plusieurs mots de fin; quand les entreprises, quelles que soient leurs tailles, auront comprises que la sécurité informatique est un voyage et non une destination, elles iront loin.

Pour les jeunes désirant arpenter le monde de la CyberSec; ne restez pas passifs, étudier, pratiquer quotidiennement, cravacher, n'ayez pas peur d'échouer, ne pensez pas directement au salaire, pensez à ce qu'il vous passionne et puis le salaire viendra"

SIVANESAN SIVATHASAN

Formateur cybersécurité et consultant

Salut Siva, peux-tu nous en dire plus sur qui tu es ?

"Salut Arnaud ! Alors pour ma part, je suis formateur chez M2i Formation Diplômante et aussi consultant en cybersécurité.

Je suis un passionné par les nouvelles technologies et comme beaucoup autodidacte"

Tu peux m'en dire un peu plus sur ton parcours ?

"Mon parcours est atypique. Bien que mon niveau d'études se limite à un Bac+2, j'ai acquis des certifications équivalentes à un Bac+5.

La connaissance que j'ai pu acquérir jusqu'à présent dans ce domaine provient surtout de l'auto-apprentissage et de mes recherches sur internet"

Quelles sont tes missions au quotidien ?

"Au quotidien, mes missions consistent à former des professionnels et des étudiants sur les différentes facettes de la cybersécurité, ainsi qu'à effectuer une veille sur tous les aspects de ce domaine en constante évolution"

À quoi correspond une journée type dans ton travail ?

"Ma journée type est généralement remplie de préparation de cours, de présentations et d'interactions avec mes apprenants.

Egalement, mes journées sont ponctuées d'échanges avec des clients pour améliorer la sécurité de leur services informatiques"

Qu'est-ce qui te plaît et déplaît dans ton métier ?

"Ce que j'apprécie dans mon métier, c'est la possibilité d'aider les autres à se protéger dans un monde de plus en plus connecté.

Bien que mes journées puissent sembler se répéter, je continue d'apprendre chaque jour sans exception.

Cependant, parfois, les défis techniques et humains peuvent être source de frustration"

Merci à toi, c'était un vrai plaisir ! As-tu tu un mot pour la fin ?

"Merci ! En conclusion, je suis un passionné par ce que je fais et je trouve une franche satisfaction dans le partage de mes connaissances.

Comme le dit Socrate : Le savoir est la seule matière qui s'accroît quand on la partage"

Starlink, une cible de choix ?

Le conflit entre l'Ukraine et la Russie est une guerre en ligne qui dépasse les limites de ce que nous avons jamais observé auparavant.

Nicole Petrucci
chef de la Space Delta 3 de la Force spatiale américaine

Deux jours après l'invasion, les services Starlink ont été activés en Ukraine pour fournir un accès Internet haut débit à la population ukrainienne, au gouvernement et à l'armée ukrainienne.

Le 5 mars 2022, Elon Musk a annoncé que les ressources de SpaceX étaient « réaffectées en priorité à la cyberdéfense et à la lutte contre le brouillage des signaux », suggérant un nombre potentiellement élevé de cyberattaques. En raison de l'intensité des attaques électroniques russes contre Starlink, SpaceX a également dû mettre à jour à distance le logiciel de ses terminaux utilisateurs.

Le groupe de hackers pro-ukrainiens Cybersec a annoncé qu'il riposterait à ces attaques.

En mai 2024, Starlink comptait plus de 3 millions de clients, dont une part importante est enUkraine.

L'analyse des comptes des acteurs de la menace sur les réseaux sociaux a révélé que Starlink est régulièrement mentionné par les hacktivistes. Les groupes prorusses partagent souvent des informations liées à Starlink, mettant en avant la capacité de l'armée


Modem Starlink

russe à acheter des terminaux d'occasion pour son propre usage ou à localiser les

terminaux utilisés par les forces armées ukrainiennes.

Compte tenu de l'importance de Starlink pour les opérations militaires de l'Ukraine et de la capacité de sa population civile à se connecter à Internet, on pourrait supposer que le nombre d'opérations cybernétiques contre Starlink serait très élevé. Étonnamment, l'ensemble des données recueillies ne montre qu'un nombre limité d'opérations ayant ciblé Starlink.

Killnet a mené deux attaques DDoS contre le site officiel et le portail d'authentification de Starlink. Sandworm a infiltré des tablettes Android ukrainiennes, qui étaient utilisées par les soldats ukrainiens et connectées à Starlink afin de récupérer des informations sur la constellation de satellites.

Ce qui ressort, c'est que ces trois cas ont été très médiatisés par rapport à de nombreuses autres attaques contre le secteur spatial, illustrant ainsi la grande valeur de Starlink en tant que cible pour les acteurs de menace prorusses.

Les groupes hacktivistes des deux côtés s'intéressent à cibler Starlink avec des opérations cybernétiques en raison de son potentiel d'effets significatifs sur le front. Par exemple, un porte-parole de l'armée d'Ukraine a déclaré que la Russie utilisait Starlink sur le champ de bataille et que si le groupe était « capable de perturber les communications près des points administratifs russes, ils ne pourront pas voir les données de leurs drones depuis le front ».

Pourtant, l'armée ukrainienne n'a jamais revendiqué d'attaque électronique ou cybernétique contre Starlink dans ses communications publiques.

On peut supposer que l'Armée verrait finalement une attaque contre Starlink comme une arme à double tranchant où à la fois l'Ukraine et la Russie risqueraient d'être affectées.

Constellation Starlink

Starlink avec ou contre l'Ukraine ?

Une question pas si simple...

En avril 2024, Dmitry Kuzyakin, directeur général du Centre russe pour les solutions intégrées sans pilote, qui produit et forme les opérateurs de drones militaires à vue de première personne (FPV), a accusé les forces armées ukrainiennes de pirater les terminaux Starlink pour contourner les restrictions territoriales.

SpaceX a bloqué l'accès des forces armées ukrainiennes à Starlink dans des zones telles que la Crimée ou pour des opérations spécifiques telles que des frappes de drones. Ces accusations proviennent de l'affirmation selon laquelle la Russie a réussi à capturer et à disséquer un drone militaire ukrainien "Baba Yaga", qui était équipé d'une antenne Starlink.

Cela les a amenés à découvrir que des modifications importantes ont été apportées au terminal et au logiciel pour supprimer les restrictions territoriales ainsi que les paywalls, permettant ainsi d'utiliser Starlink en tant que passagers clandestins. Kuzyakin a déclaré qu'un Raspberry Pi (c'est-à-dire un petit ordinateur monocarte) avait probablement été utilisé pour mettre en œuvre ces changements. Kuzyakin a affirmé que de tels changements étaient impossibles à réaliser sans informations internes, soit directement fournies par SpaceX pour soutenir tacitement les Forces armées ukrainiennes, soit provenant d'une fuite de données fournissant des informations sensibles sur Starlink.

Cependant, il reste impossible de vérifier les affirmations de Kuzyakin.

Data center spatiaux c'est pour quand ?

L'explosion des données et la montée en puissance de l'intelligence artificielle poussent les acteurs du numérique à repenser leurs infrastructures.

Face aux limites des datacenters terrestres en termes d'énergie et d'impact environnemental, une solution radicale émerge : les datacenters spatiaux.Si les défis sont nombreux, les perspectives sont prometteuses.

Les datacenters spatiaux pourraient révolutionner le domaine du calcul haute performance en offrant des capacités de calcul et de stockage inégalées. Ils pourraient également jouer un rôle clé dans le développement de nouvelles applications, telles que l'intelligence artificielle, et la recherche scientifique.

Plusieurs sociétés se penchent déjà sur le sujet, en particulier HPE, Thales Alenia Space ainsi qu'Axiom Space, avec des projets ayant chacun des avantages et des inconvénients.

Thales a réalisé une étude de faisabilité baptisée ASCEND. L'étude avait pour objectif de comparer les impacts environnementaux des data centers orbitaux avec les centres de données terrestres. Elle visait également à valider la faisabilité technologique de leur développement, de leur déploiement et de leur opérabilité en orbite.

Afin de réduire significativement la production de CO2 du stockage et du traitement des données numériques, les résultats de l'étude estiment que de telles infrastructures spatiales nécessiteraient le développement d'un lanceur dix fois moins émissif sur l'ensemble du cycle de vie.

De plus, la consommation d'eau nécessaire à leur refroidissement serait éliminée du processus, ce qui serait un atout majeur.

Les infrastructures spatiales modulaires seraient assemblées en orbite grâce aux technologies robotisées qui feront l'objet du démonstrateur EROSS IOD de la Commission européenne, mené par Thales Alenia Space, dont la première démonstration est prévue d'ici 2026.

De leur côté, HPE et Axiom repensent le data center classique et y voient un avenir à moyen terme.

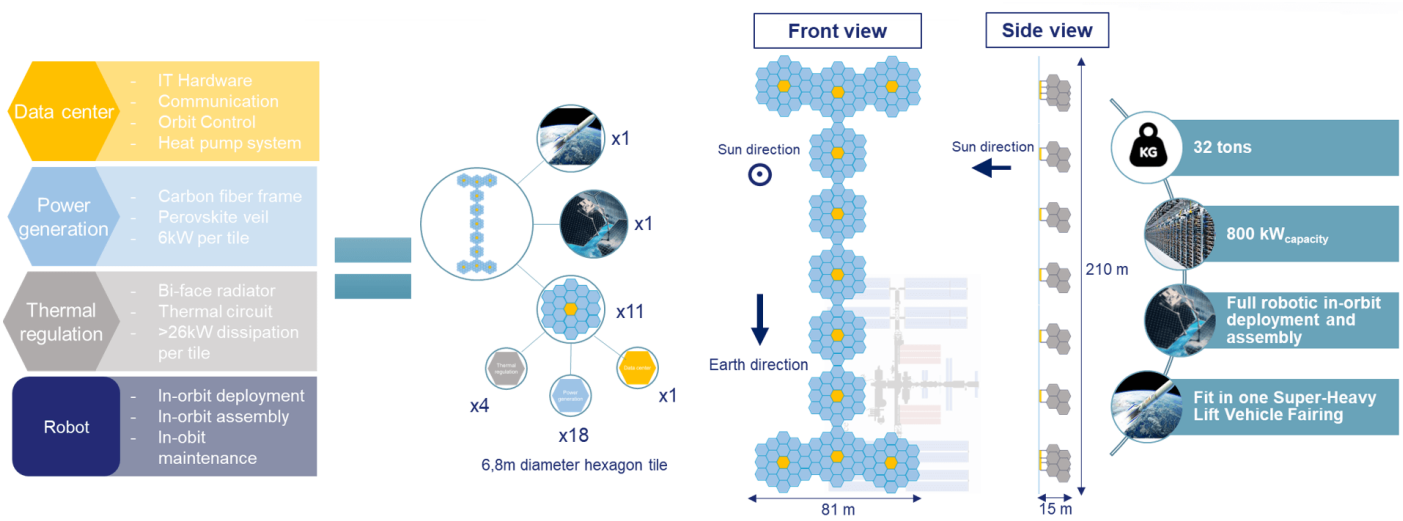
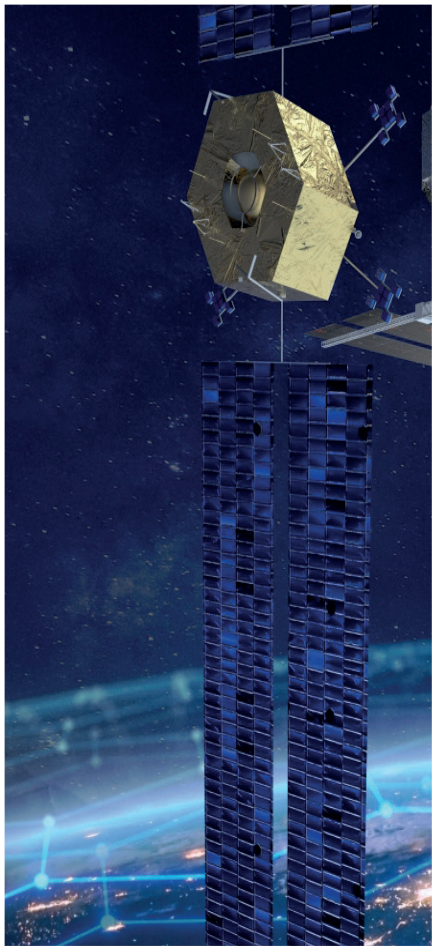
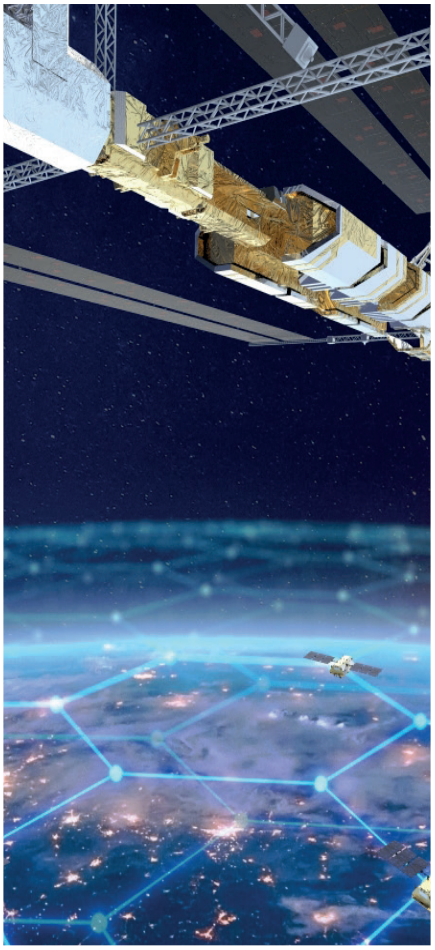
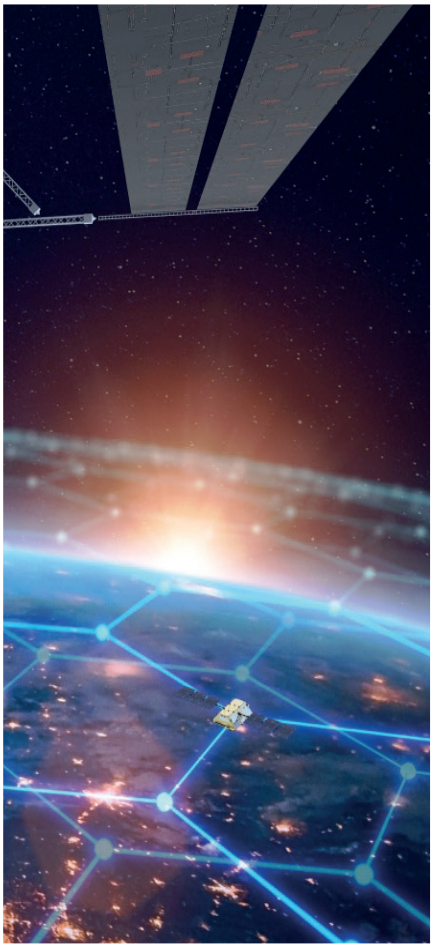


Schéma du fonctionnement prévu avec ASCEND Cloud In Space







Les datacenters en orbite basse terrestre (LEO) pourraient permettre d'économiser les terrains sur Terre, de réduire les coûts de l'électricité grâce à la technologie de l'énergie solaire et même de réduire la latence des données.

Dans l'espace, l'énergie solaire et les batteries fourniraient toute l'énergie, réduisant ainsi les coûts de fonctionnement. Un centre de données en orbite basse, effectuant un tour complet de la Terre toutes les 90 minutes, serait soumis à la lumière du soleil pendant environ 45 minutes à chaque rotation.

Durant le reste du temps, le centre de données fonctionnerait grâce aux batteries connectées à ses panneaux solaires.

La question du refroidissement se pose également. Dans l'espace, il peut exister une différence de plusieurs centaines de degrés entre la lumière solaire et l'obscurité causée par la Terre. Dans l'espace, les systèmes de refroidissement traditionnels perdent de leur efficacité, car la convection ne se produit pas en état de microgravité. Les radiateurs chargés d'ammoniac sont utilisés pour le refroidissement des ordinateurs spatiaux, à l'instar de ceux présents à bord de la Station spatiale internationale (ISS).

Plusieurs points restent cependant encore en suspens. Les modèles de lanceurs en orbite, par exemple, devront être adaptés. La maintenance et la gestion de fin de vie restent également à clarifier. Tout comme l'impact des radiations solaires sur les installations déployées. La gestion de fin de vie des centres de données spatiaux est encore également à clarifier.

ASCEND
Cloud in space

POUVONS-NOUS VIVRE SUR LA LUNE ?

avec l'aide de Jamy Gourmaud via Youtube

En 2026, la Nasa et Space X, la société d'Elon Musk, nous promettent de retourner sur la Lune. Mais avant cela, le satellite de la Terre vit le vaisseau de la mission Artemis 1 être lancé dans sa direction, en 2022.

Cette mission avait pour objectif de faire le tour de la Lune puis de revenir sur Terre. Aucun humain n'était présent à bord du vaisseau, seuls des mannequins ont eu la chance de voir la Lune de près. La prochaine grande étape sera Artemis 2, où les mannequins seront remplacés cette fois par quatre humains, envoyés dans la capsule Orion. Son vol est programmé pour avril 2026.

Mais l'étape la plus impressionnante sera la troisième mission Artemis. Celle-ci devra déposer des astronautes sur le pôle sud de la Lune pour une durée de six jours.

L'objectif de ces missions est de réfléchir à la mise en place d'une future base de lancement lunaire en direction de la planète rouge : Mars ! Mais tout cela ne sera pas possible avant 2040, voire 2050. La NASA souhaite, en quelque sorte, y établir un camp de base, un palier intermédiaire avant de lancer des astronautes sur Mars.

Diifférents problèmes sont liés à la vie sur la Lune :

L'AIR

La Terre possède une atmosphère, cette pellicule d'air qui nous permet de respirer. Sur la Lune, il n'y a pas d'atmosphère. Pour y envoyer de l'air, il faudrait qu'un vaisseau parcoure, dans le pire des cas, lorsque la Lune est la plus éloignée de la Terre, pas moins de 384 400km. Pour comparaison, la station internationale n'est qu'à 400km de la Terre.

Les scientifiques de la Nasa ont peut-être trouvé LA solution grâce à la poussière de Lune qui contient de l'oxygène. Ils ont mis au point un laser atteignant les 1600°C afin de faire fondre cette poussière, composée principalement de régolithe, et d'en extraire l'oxygène qu'elle contient. Les tests ont été réalisés dans un environnement sous vide, donc sans air comme sur la Lune. Les résultats sont déjà concluants pour l'envoi lors d'une future mission Artemis.

La Lune est composée aussi de silice et d'aluminium qui contiennent aussi de l'oxygène en grande quantité. Selon une hypothèse de quelques scientifiques, la Lune pourrait contenir assez d'oxygène pour faire vivre 8 milliards de personnes pendant environ 100 000 ans. Il resterait donc simplement à faire venir de l'azote pour avoir tous les éléments pour reconstituer de l'air sur la Lune. Pour rappel, l'air est constitué de 21% d'oxygène et de 78% d'azote et de 1% de gaz rares.

L'EAU

Sur la Lune, il n'y a pas d'eau, enfin pas d'eau à l'état liquide ou à l'état de vapeur, à cause de la température très élevée durant la journée, environ 150°C. Or, au pôle sud, les scientifiques ont découvert de nombreuses zones de glace dans des cratères à l'abri de la lumière du soleil, protégées sous une épaisse couche de régolite. Les Américains ont mis au point un module d'extraction innovant : le Rocket M.

Ce module est capable de pulvériser la roche et d'extraire la glace, puis de

la transformer en vapeur d'eau en seulement 5 à 10 minutes. Selon ses créateurs, ce robot pourrait exploiter pas moins d'une douzaine de cratères à la journée pour un total de

426 tonnes d'eau récoltées de manière annuelle.

Une partie de cette eau serait utilisée comme carburant pour le moteur des fusées de SpaceX et le reste pourra servir aux astronautes.

Cette quantité d'eau présente sur la Lune ne serait qu'une infime partie de ce que celle-ci pourrait contenir selon des chercheurs chinois qui affirment que la Lune abrite un gigantesque réservoir. Mais attention, il s'agirait non de lacs souterrains, mais de minuscules perles de verre qui se seraient formées après une pluie d'astéroïdes. Les perles contiendraient l'équivalent de 270 milliards de m^3 d'eau. Néanmoins, il faut encore mettre la main dessus et savoir les extraire. Pour le moment, ça n'a pas encore été fait.

LA NOURRITURE

Les Américains ont réussi une grande première : créer un sol similaire à la régolite, la poussière de Lune. Ils ont fait l'expérience d'y planter des graines de pois chiche ; au bout de quelques jours, certaines ont commencé à germer et une partie d'entre elles sont même arrivées à maturité. Il est donc théoriquement possible de faire pousser quelque chose sur la Lune. Des chercheurs australiens vont tenter l'expérience d'envoyer des graines de tomates et de carottes dans un module vers la Lune courant de l'année 2025.

À l'intérieur de ce module, une fois aluni, un petit robot va semer ces graines dans le sol et les cultiver sous serres pour les protéger des températures extrêmes de l'environnement lunaire.

L'ENERGIE

Le soleil va permettre aux astronautes de produire de l'énergie grâce à des panneaux solaires. Ils devront être nombreux cependant pour fournir assez d'électricité pour faire tourner les ordinateurs, les ateliers, les machines, l'éclairage ou encore le chauffage et même faire rouler les véhicules. Le projet américain Blue Alchemist tente de fabriquer des panneaux à partir de la régolite lunaire, ce qui aurait comme avantage d'être produit sur place.

LA REGOLITE

Elle recouvre la totalité de la surface de la Lune sur une épaisseur de trois à vingt mètres. Cette poussière est composée de grains microscopiques dont la taille moyenne est de 19 microns, ce qui correspond à la moitié de la taille d'un cheveu. Ils sont si fins qu'ils collent à la combinaison des astronautes et s'infiltrent dans les moindres rouages des machines, et surtout, ils pénètrent dans l'organisme par les voies respiratoires. En 1969, les premiers hommes qui ont posé le pied sur la Lune ont signalé le problème. Ces poussières dégageaient une odeur de poudre à canon qui leur provoquait des éternuements et de violentes quintes de toux. En 2018, une équipe de chercheurs britanniques a démontré que la poussière lunaire, qui est abrasive, est potentiellement dangereuse pour la santé. Respirer des particules de poussière lunaire serait aussi néfaste pour les bronches que de travailler dans une mine de charbon sans protection. La NASA, avec des entreprises privées, travaille donc sur de nouvelles combinaisons spatiales qui empêcheraient les particules de s'infiltrer. Pour le moment, aucun prototype n'est prêt à ce sujet.

CREDITS

Rédacteur : Arnaud LEROY
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume Poupard

Nous remercions toutes les personnes ayant pris part à ce numéro

Janvier/Mars 2025