

PATRICK TRINKLER

Fondateur et directeur général de CYSEC

Patrick Nicolet, fondateur et partenaire principal de Linebreak SA, ancien directeur des technologies de Capgemini

Patrick, vous êtes un spécialiste de la cybersécurité dans l'espace, le plus à la pointe en Europe. Vous travaillez avec l'Agence spatiale européenne, comme je l'ai déjà mentionné, ainsi qu'avec le Centre national d'études spatiales en France. Quel est l'état de la cybersécurité dans l'espace ?

Patrick Trinkler

Merci de m'avoir invité. Je vais commencer par présenter l'espace comme évolution 3.0 au lieu de 2.0. Pour moi, il s'agit vraiment de la finalisation de la numérisation du monde, de donner accès à Internet à entre deux et trois milliards de personnes, de pouvoir connecter un milliard d'objets connectés dans le monde. Voilà vraiment le rôle que l'espace aura à l'avenir et il ne suivra pas tant les lois de la physique que les lois de la théorie de l'information. L'espace sera la connexion entre le cloud et les appareils intelligents, la connexion entre le cloud et l'Edge. Comme mentionné précédemment, il existe deux principaux cas d'utilisation dans l'espace commercial. Le premier concerne les communications et le second, l'observation de la Terre. La communication représente entre 80 et 90 % d'un marché incroyable qui augmente de 20 % par an et où on trouve différents acteurs. Il y a les acteurs traditionnels qui utilisent l'orbite géostationnaire, et qui subissent la pression des nouveaux acteurs de l'orbite terrestre basse, ou OTB, comme Starlink. Pour être compétitifs, ils doivent intégrer de nouvelles technologies comme la communication par liaisons optiques plutôt que par liaisons électromagnétiques. Le résultat est qu'il n'y a plus de latence ou de problèmes de connexion, et vous n'avez pas besoin de demander la permission à un pays avant d'installer une antenne car vous avez la fréquence du pays, ce qui est une évolution majeure. Cependant, seuls quelques pays auront accès à ce type de technologie et à la fourniture de connexions partout dans le monde. C'est pourquoi on peut voir des analogies entre la mise en œuvre de la 5G, avec un acteur comme Huawei qui possède ce type de technologie, et certains risques de problèmes de souveraineté des données. La même analogie existe au sujet de la 5G et de l'accès à ce type de technologie.

D'autre part, on trouve de nouveaux acteurs autour de l'OTB dont le leader est Starlink, qui a déjà installé 1 million de terminaux et dispose de 3 000 satellites tous connectés entre eux. Nous pouvons voir les avantages de ce type de technologie en Ukraine. On peut couvrir la Terre entière avec ce type de satellite, avec une connexion à faible latence, et qui est très bon marché. Un terminal Starlink coûte 1 000 euros, et la connexion coûte 100 euros par mois, ce qui n'est vraiment pas cher. Dans ce cas, comme mentionné précédemment, le coût pour le développement, le lancement et l'exploitation pendant trois à cinq ans de ce genre de satellite

revient à 300 000 euros. Pour cela, on utilise des start-up prêtes à l'emploi, ce qui pose des problèmes de sécurité car n'importe quel pirate n'importe où dans le monde peut accéder à ce type de technologie. C'est le risque lié au déploiement de l'OTB pour la communication. La question n'est pas tant la souveraineté que la sécurité car on utilise une technologie standard. Il peut y avoir également une question de souveraineté parce qu'il n'existe que quelques lanceurs pour ce genre de technologie, donc vous devez fournir votre satellite avant le lancement à, par exemple SpaceX, et vous ne pouvez pas contrôler votre satellite lorsque vous le lancez.

On trouve de nouveaux acteurs pour ce genre d'utilisation. La communication est l'hyperscaler. Comme mentionné plus tôt, l'espace est le lien entre le cloud et l'Edge et les hyperscalers comme Amazon, Microsoft et Google, qui veulent jouer dans ce domaine. Par exemple, AWS d'Amazon est l'un des principaux nouveaux acteurs de la nouvelle industrie spatiale. Si je le veux, ma start-up peut avoir accès gratuitement aux services d'Amazon pendant deux ans avec des milliers de technologies incluses. C'est un vrai leader dans ce domaine. Nous en avons quelques exemples en ce moment avec le lancement d'un satellite qui comprend probablement une connexion au cloud et une technologie d'intelligence artificielle et d'exploration de données qui peut traiter et manipuler les données directement dans le cloud. L'idée est qu'on n'a pas besoin de communiquer les données mais qu'il suffit de les traiter dans le cloud avec l'avantage qu'il n'y a pas de problème de refroidissement ou d'accès physique aux données. En réalité, ces nouveaux acteurs lanceront des satellites dans le monde entier pour débloquer ce cloud, ce centre de données dans l'espace. Il y a un certain risque autour de la souveraineté des données car cela ne sera fait que par des entreprises qui disposent de ce type de technologie.

L'autre cas d'utilisation que j'ai mentionné précédemment est l'observation de la Terre. L'observation de la Terre représente 10 ou 20 % du marché commercial dans l'espace. Il s'agit ici de quelque chose qui est vraiment connecté à l'Internet traditionnel. Nous avons l'exemple de l'Ukraine, mais nous pouvons aussi avoir des exemples de fermes pour lesquelles on prend des images des troupeaux. On envoie ces informations du satellite vers le cloud, on les traite avec un algorithme et après on peut envoyer un drone ou un robot pour agir sur la ferme. Voilà l'observation de la Terre à l'avenir et il y a beaucoup d'acteurs qui, ainsi, auront accès à vos données et les protégeront, qui auront une certaine souveraineté sur elles et qui utiliseront ces données comme si vous étiez un bien et qui pourraient également partager ce bien avec d'autres entreprises.

Enfin, comme mentionné plus tôt, il existe des questions de sécurité et de souveraineté, et des risques concrets avec des exemples de l'impact des piratages de terminaux dans une région donnée, qui peuvent faire s'effondrer tout un secteur dans une autre partie du monde. L'idée est d'intégrer plus de sécurité et de nouvelles normes. Une nouvelle norme a été développée par le CCSDS pour fournir du matériel de sécurité cryptographique qui fera fonctionner la logique applicative dans l'espace et sur Terre afin de protéger ces nouveaux biens.

Patrick Nicolet

Merci Patrick. La démocratisation de l'espace, avec l'Edge connecté aux opérations, signifie qu'en fait, nous importons les problèmes de cybersécurité dans l'espace. Ainsi, une activité



peut avoir les mêmes problèmes qu'elle soit dans l'espace ou sur Terre. Nous répliquons dans l'espace une partie de l'infrastructure que nous avons sur Terre, mais les problèmes de cybersécurité et de protection des données resteront.