PATRICK TRINKLER

Founder and CEO of CYSEC

Patrick Nicolet, Founder and Managing Partner of Linebreak Ltd., former Group Chief Technology Officer of Capgemini

It is a very serious topic so, Patrick, you are a specialist in cybersecurity in space, the most advanced in Europe, working with the European Space Agency, as I mentioned before, as well as with the Centre national d'études spatiales in France. What is the state of cybersecurity in space?

Patrick Trinkler

Thank you for the invitation. Maybe I will start by presenting space as a 3.0 evolution not 2.0. From my point of view, it is really the finalization of the digitalization of the world, to give access to the Internet to two to three billion people, to be able to connect a billion IoT devices in the world. That is really the role space will have in the future and will not really follow the law of physics but follow the laws of information theory. Space will be the connection between the Cloud and intelligent devices, the connection between the Cloud and the Edge. As mentioned before, there are two major use cases in the commercial space, the first is communications and the second, Earth observation. Communication is 80% to 90% of an incredible market that is increasing by 20% a year and in this case there are different players. There are the traditional ones that use GEO orbit, and they are under pressure from new players in the LEO orbit, like Starlink. In order to compete, they will integrate new technologies like communicating via optical connections rather than electromagnetic connections. This means there is no longer any latency or connection problems, and you do not need to ask a country before installing an antenna because you have the frequency of the country, which is a big evolution. However, only a few countries will have access to this kind of technology and to providing connections all over the world. That is why there are some analogies with implementation of 5G with a player like Huawei that has this kind of technology and some risk of data sovereignty issues. There will be the same analogy around 5G and the access to this kind of technology.

On the other hand, there are new players who work around the LEO orbit and the leading one is Starlink, which has already installed 1 million terminals and has 3,000 satellites all connected together. We can see the benefit of this kind of technology in Ukraine. They can cover the global Earth with this kind of satellite, with a low-latency connection, and it is very cheap. A Starlink terminal is EUR 1,000, and the connection is EUR 100 per month, which is really very cheap and in this case, as mentioned before, the cost of this kind of satellite for the development, launch and operating for three to five years, is EUR 300,000. In this case, off-the-shelf start-up companies are used, which raises some security issues because this kind of technology is accessible to different hackers around the world. That is the risk around the LEO

deployment for communication. It is not about sovereignty, it is more security because it is standard technology. It may be sovereignty too because there are only some launchers for this kind of technology, so you need to provide your satellite to SpaceX, for example, before launch and you cannot control your satellite when you launch it.

There are some new players for this kind of use case, communication is the hyperscaler. As mentioned before, space is the connection between the Cloud and the Edge and hyperscalers like Amazon, Microsoft and Google, who want to play in this kind of field. For example, Amazon's AWS is one of the leading new players in the new space industry. If I want, my start-up can have access to the services of Amazon for two years free of charge with thousands of technologies inside and it is a real leader in that. There are some examples of that right now with the launch of a satellite with probably connection to the Cloud inside and AI and data mining technology to process and manipulate data directly in the Cloud. That is the idea that you do not need to communicate the data but process it in the Cloud and the advantage of that is that there is no problem with cooling or physical access to the data. Really, these new players will launch some satellites around the world to unblock this Cloud, this data center in space. There is some risk around the sovereignty of data because it will only be done by companies that have this kind of technology.

The other use case I mentioned before is Earth observation. Earth observation is 10% or 20% of the commercial market in space and, in this case, it is something that is really connected to the traditional Internet. We have the example of Ukraine, but we can also have examples from farms where you have images of herds, where you send this information from the satellite to the Cloud, process it with an algorithm and after you can send a drone or robot to carry out some action on your farm. That is the future of Earth observation and there are a lot of players in this case who will have access to your data and protect it, have some sovereignty over it and use this data like you are an asset and also share the asset with other companies.

Finally, as mentioned before, there are issues of security and sovereignty, and concrete risks with examples of the impact of hacks of terminals in some regions, which can collapse an industry in another part of the world. The idea is to integrate security and new standards, and a new standard has been developed by the CCSDS to provide cryptographic security material to operate business logic in space and on the ground to protect these new assets.

Patrick Nicolet

Thank you, Patrick. The democratization of space, with Edge being connected to the operations, means we basically import the cybersecurity problems into space. Therefore, an activity can have the same problems whether it is in space or on Earth. We will replicate part of the infrastructure we have on Earth in space, but the problems of cybersecurity and data protection will remain.