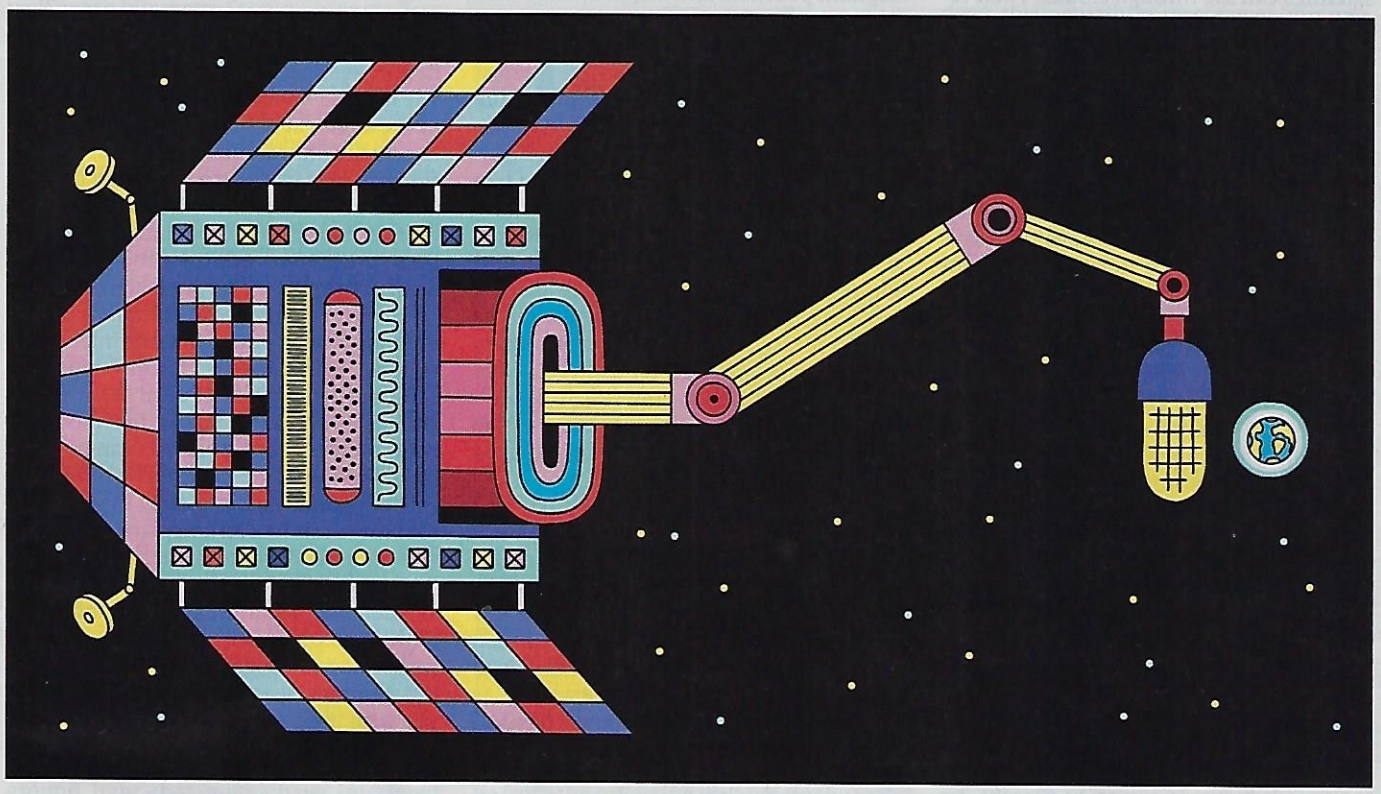


Espionage (1)

Ears in the sky

By listening for radio and radar signals, a new generation of satellites can track human activity, both licit and illicit

In the middle of last year, Ecuadorians watched with concern as 340 foreign boats, most of them Chinese, fished just outside the Exclusive Economic Zone (EEZ) around their country's westernmost province, the Galapagos Islands. The law of the sea requires such vessels to carry GPS-based automatic identification systems (AIS) that broadcast where they are, and to keep those systems switched on. Some boats, however, failed to comply. There were more than 550 instances of vessels not transmitting their locations for over a day. This regular radio silence stoked fears that the boats concerned were sneaking into Ecuador's waters to plunder its fish.

Both local officials and China's ambassador to Ecuador denied this, and said all the boats were sticking to the rules. In October, however, HawkEye 360, a satellite operator based in Virginia, announced it had detected vessels inside Ecuador's EEZ on 14 occasions when the boats in question were not transmitting AIS (see map on next page). HawkEye's satellites could pinpoint these renegades by listening for faint signals emanating from their navigation radars and radio communications.

HawkEye's satellites are cubesats, a standard design the size of a shoebox that can be furnished with whatever kit the owner chooses. Being small, cubesats are cheap to build and launch. HawkEye deployed its first cluster, of three of them, in 2018. They are now in an orbit that takes them over both of Earth's poles. This means that, as the planet revolves beneath them, every point on its surface can be monitored at regular intervals.

Initially, the data the satellites collected were downloaded to a tracking station on Svalbard, a Norwegian island in the Arctic Ocean. But business has since boomed. HawkEye now counts a dozen governments among its customers, as well as private clients. The firm has therefore recruited the services of a second ground station, in Antarctica, and it put a second cluster into orbit on January 24th. It plans three more such launches this year, and also intends to widen its network of ground stations yet further.

Given this success, it is hardly surprising that at least six other companies are operating or developing similar systems. Quilty Analytics, a research firm in Florida, expects the number of radio-frequency (RF) intelligence satellites of this sort in orbit to multiply from a dozen at the beginning of January to more than 60 by the end of next year.

→ Also in this section

72 How to look around corners

73 Self-vaccination by honeybees

74 An evolutionary surprise

Unmixed signals

RF-intelligence satellites detect where a transmission is coming from in two ways. One, trilateration, relies on measuring minute differences in a signal's arrival time at each member of a cluster. The other uses the Doppler effect—the shift in a signal's frequency if the transmitter is moving relative to the receiver. Together, according to HawkEye, these can pinpoint a signal's source to within 500 metres of its true origin. Kleos Space, a Luxembourgeois company that launched its first cluster in November and hopes to put two more up later this year, says its accuracy ranges between 3,000 and 200 metres.

A cluster sweeps a band of territory 2,000km wide so, circling the planet every 90 minutes or so, it can revisit many areas several times a day. Moreover, unlike spy satellites fitted with optical cameras, RF ▸▸

satellites can see through clouds. Their receivers are not sensitive enough to detect standard mobile phones. But they can pick up satellite phones, walkie-talkies and all manner of radar. And, while vessels can and do illicitly disable their AIS, switching off their communications gear and the radar they use for navigation and collision-avoidance is another matter entirely. "Even pirates don't turn those things off," says John Beckner, boss of Horizon Technologies, a British firm that plans its first launch in August.

RF data are also cheap to collect. Satellites fitted with robotic high-resolution cameras are costly. Flying shoeboxes that capture and timestamp radio signals are not. Horizon says that building, insuring and launching its August mission should cost no more than about $1.4m.

America's National Geospatial-Intelligence Agency (NGA), one of that country's numerous spying operations, is a big user of RF intelligence. It employs HawkEye's data to find guerrilla camps and mobile missile-launchers, and to track both conventional warships and unconventional ones, like the weaponised speedboats sometimes deployed by Iran. Robert Cardillo, a former director of the agency who now advises HawkEye, says dozens of navies, Russia's included, spoof AIS signals to make warships appear to be in places which they are not. RF intelligence is not fooled by this. Mr Cardillo says, too, that the tininess of RF satellites makes them hard for an enemy to destroy.

Beside matters military, the NGA also uses RF data to unearth illicit economic activity—of which unauthorised fishing is merely one instance. Outright piracy is another. And the technique also works on land. In 2019, for example, it led to the discovery of an illegal gold mine being run by a Chinese company in a jungle in Gabon. And in 2020 the managers of Garamba National Park in the Democratic Republic of Congo began using HawkEye data to spot elephant poachers and dispatch rangers to deal with them.

There are commercial uses, too. Andy Bowyer, Kleos's boss, reports interest among telecoms firms keen to locate rogue transmitters, such as unlicensed ham radios, that are operating within their domains. Regulators, meanwhile, would like the firm to create "heat maps" of shifting patterns of legitimate transmissions. These would help them select sites for mobile-phone towers and also give them a better idea of the value in particular places of licences to use parts of the radio spectrum that are going up for auction. Some charities, too, have an interest in Kleos's data. RF information can, for example, flag up routes taken by migrants likely to need food and other aid.

Declustering

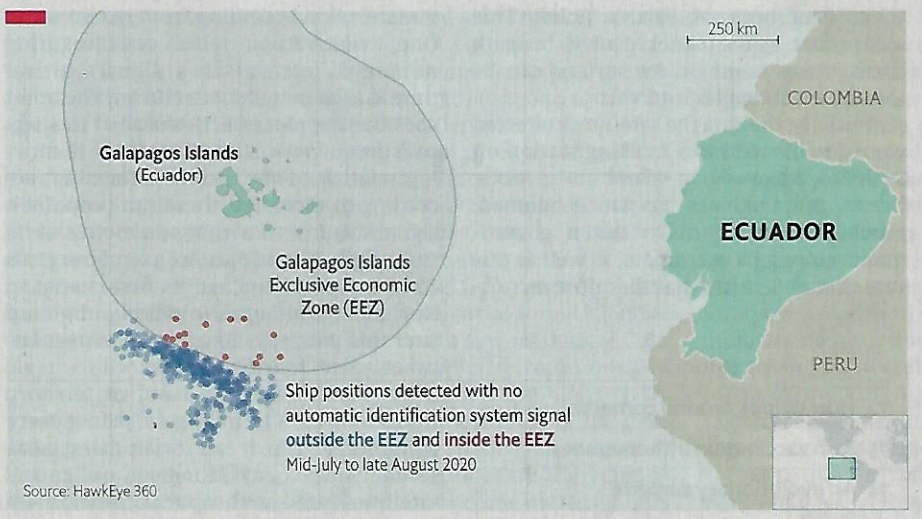
Using satellite clusters to gather RF intelligence is clever. But engineers at Unseenlabs, a firm in Rennes, France, reckon it is already outdated. At the moment, Unseen has three satellites in orbit and sells data to about ten navies, including France's, as well as to maritime insurers and a handful of big defence contractors. But its satellites operate independently, rather than as a cluster, for Unseenlabs' engineers have devised a detection system, which they claim is accurate to within 5,000 metres, that requires but a single satellite.

How this system works remains a secret—and one that, according to Clément Galic, Unseenlabs' boss, is protected by the French state. After several attempts were made to steal it, he says, the defence ministry's Directorate General of Armaments offered its assistance in defending the details from cybertheft.

Secret or not, though, Unseenlabs may soon have competitors in the single-satellite-RF-intelligence market, for Horizon, too, says that it has worked out how to perform the trick—a claim backed up by the fact that its launch in August will loft but a single device. Shortly after it filed an application for a patent in America on the wizardry involved, the government there classified it. Even so, Mr Beckner drops a hint. The method involves assessing differences in the angles at which a target's signals arrive during the satellite's arc across the sky. Horizon says its system will be accurate to within 3,000 metres. By the middle of next year, it, too, plans to operate three satellites in different orbits—enough to scan most of the planet every two hours or so.

Horizon also plans to compile a library of unique radar-pulse "fingerprints" of the world's vessels, for the tiny differences in componentry that exist even between examples of the same make and model of equipment mean that signals can often be linked to a specific device. It will thus be able to determine not merely that a vessel of some sort is in a certain place, but which vessel it is, and where else it has been.

Unseenlabs, for its part, has already catalogued the radar fingerprints of many thousands of vessels, several hundred of which have, subsequent to the events of last summer, spent time in the Galapagos EEZ with their AIS beacons switched off. It remains to be seen what Ecuador's authorities will do with that information. But no one can say they weren't told. ■



Espionage (2)

Round the bend

How to see what is hidden from view

IN A LOCKED room in a busy city, some terrorists are holding a hostage. The curtains are mostly drawn, cutting off any direct line of sight for those outside. In a building across the street, a team of engineers are set a task: they can have whatever equipment they need, but they must paint as clear a picture as possible of what is happening inside the room.

This was the challenge given in 2015 to Daniele Faccio, then at Heriot-Watt University, in Edinburgh, by Dstl, a British government defence laboratory. He and his team eventually found a way to see around corners from a distance of 50 metres—which was reckoned impressive at the time, even though the system they devised could detect only the motion and position of hidden objects, rather than taking pictures of them. Now, however, Xu Feihu and Pan Jianwei of the University of Science and Technology of China, in Hefei, have blown that record out of the water. As they describe in the *Proceedings of the National Academy of Sciences*, they have managed to ▸▸