'No European country is sufficiently protected against drone attacks today'

Drones are increasingly proving to be a danger to our critical infrastructure. That's why we're rapidly developing technology to detect and take them out of the air. However, many uncertainties remain: 'Shooting down a drone is technically illegal'.

A small drone takes off from a trailer of a truck parked at the edge of the road. A little later we see videos of giant bombers on fire and exploding. This is *Operation Spider Web*. On June 1, Ukraine launched a drone attack deep into Russian territory. They transported large numbers of small, cheap drones in trucks and then launched them near military airports, as far away as Siberia. Eventually, those small drones destroyed dozens of long-range bombers worth billions of dollars.

This operation also gives Europe pause for thought. If a similar attack is launched tomorrow against Belgian military airports, we will have little to stop the drones. That is why the Belgian Defence wants to issue a contract later this year to purchase anti-drone systems for its airports. This is part of a broader trend. Europe is rapidly trying to better protect its critical infrastructure against drones, which are controlled by everyone – from confused amateur pilots to criminals, terrorists and foreign powers.

That is why scientists and companies are working hard to build such anti-drone systems. These are supposed to detect and intercept drones. This requires a combination of different layers of technology.

To stop a drone, we first have to detect it. That's what the Belgian company Senhive does. They already secured the Olympic Games in Paris with their drone detection systems, but the port of Antwerp-Bruges also uses their services. At the heart of their technology are so-called RF, or radio frequency sensors. That is the most popular way to detect drones. "A drone usually flies on an agreed frequency," explains Steven Krekels, CEO of Senhive. 'On that frequency, the pilot and the drone communicate with each other, via radio signals. We developed a sensor in which the antennas pick up the RF signals. We look at who communicates in a certain environment at what frequency, with which protocols, in order to detect where drones are flying. This allows us to determine the location of the drone, and sometimes even that of the pilot.'

These frequencies and protocols are constantly changing. 'Every drone model has a different footprint,' says Krekels. 'We regularly purchase new devices and place them in a sealed room where no other RF signals can penetrate. This is how we learn to detect that drone. We work like a virus scanner. We have a huge library of drone signals, which we are constantly expanding."

Senhive's RF detection is flanked by other detection systems. They also have cameras to visually detect drones and audio sensors to recognise the specific buzzing sound of drones. In addition, they use radar.

BATS, another Belgian anti-drone company, specialises in the latter field. Their drone detection systems rely on radar rather than RF. These systems are more expensive and are mainly sold to governments and armies.

‘Radar is our speciality,’ says Frank Arnold, managing director of BATS. "We have been doing this since our foundation in 1984. Most other drone companies focus on RF. We do that too, but the core of our system is radar.“ They combine that radar with other layers of technology. 'Sensors, sensors, sensors, that's our focus,” says Arnold. “We also work with RF, electro-optical systems, cameras and audio sensors. The trick is to combine all of that effectively.”

Soft and hard kill

Once the drones have been detected, they need to be taken out of the air. This can be done using all kinds of technologies, from jamming to anti-aircraft missiles. BATS also integrates such interception into its systems.

‘If you want to do something about the threat, you start with jamming,’ explains Arnold. "This involves disrupting the drone's RF signal. Ideally, you know the exact position of the drone. Then you send electromagnetic energy to that location and disrupt the connection between the pilot, the drone and the drone's location tracking. In the event of an attack by a large group of drones, you can also jam 360 degrees around you. However, this is not ideal, because you also disrupt non-hostile signals in those frequencies.‘ You can also hack a drone. ’That way, you can take control," says Arnold. “Usually, you would then crash or land the drone. However, this is limited to commercial drones where you know which protocol they use.”

In addition to these softer options, the so-called “hard kill” is sometimes necessary. Some drones, such as those that fly autonomously or are connected to the pilot via a cable, do not emit signals that can be disrupted or hacked. These technologies are very popular in conflicts such as the one in Ukraine. That is why they have to be shot down.

“There are a range of options for this, ranging from drones that intercept other drones to missiles, cannons and guns,” says Arnold. “The cost-benefit analysis is crucial here. Do you want to fire a half-million-pound missile at a two-thousand-pound drone?”

In the workshop of the Belgian company Senhive, employees are working on anti-drone systems. Credit: Debby Termonia

For both hard and soft kills, knowing the exact position of the drone is crucial. This requires combining data from different sensors. ‘Each sensor determines the position of the drone with a certain degree of certainty,’ says Arnold. “By combining data from different sensors, you increase that degree. If the radar is 95 per cent certain that the drone is in a certain position, then RF and cameras can increase that percentage to 99.9 per cent.”

An anti-drone system therefore consists of different layers of technology that are deployed on top of each other. ‘There is no silver bullet,’ says Geert De Cubber, team leader of the Robotics & Autonomous Systems team at the Royal Military Academy (KMS). ‘There is no single technology that is a panacea. Counter-drone solutions must consist of different layers and sensors, which are linked to a response system.’

This, in turn, makes it difficult for organisations such as the Ministry of Defence to determine which system works best. The KMS therefore conducted a research project to better compare such systems.

“We are creating a standard against which counter-drone systems can be tested,” says De Cubber. “You can compare it to the energy label that shows how energy-efficient an electrical appliance is. Nothing like this exists yet for counter-drone systems.”

They are conducting practical tests in which different systems are compared. One such test has already taken place in Nieuwpoort on the coast. “We often see drug smuggling problems there,” says De Cubber. ‘Counter-drone systems will also appear there in the future.’

Low tech

Nevertheless, there are still uncertainties surrounding anti-drone systems. The biggest of these is the regulatory framework. For example, it is illegal in Belgium to shoot down a drone, unless it is done by the police or the Ministry of Defence in very specific circumstances.

‘It is very unclear who is allowed to shoot down drones,’ sighs De Cubber. ‘There is a royal decree on jamming, which allows the Ministry of Defence to jam under certain circumstances. But first you have to apply to the BIPT, the Belgian telecom regulator. That is not ideal in a crisis situation.’

You don't always need high-tech systems to ward off drones. In Ukraine, a number of low-tech solutions are emerging, from installing nets to equipping soldiers with hunting rifles.

“Shooting them down can sometimes be very expensive compared to the cost of a drone,” says De Cubber. “Nets are a good solution in that respect. Rifles, on the other hand, are less successful. We have researched this at the KMS, and unless you shoot with special ammunition, it is very difficult to shoot down a drone. So I am sceptical about that.”

Laser

At the same time, technology is not standing still. In Ukraine, new drone models and technologies are emerging every few weeks. Today, for example, some drones fly by rolling out a fibre optic cable behind them. These drones are not controlled by radio signals, and you cannot detect or jam them via RF. Other technologies are therefore needed.

“RF-controlled drones will become less popular,” says Krekels. “The average hobbyist's drone will continue to fly using RF. But technology will also spread from Ukraine. I certainly see it popping up in criminal circles. Nevertheless, I think that in the coming years, at least 95 per cent of drone flights will be detectable via RF.”

Drones are detected with the help of radio frequency sensors. Senhive secured the Paris Olympics with their drone detection systems. Credit: Senhive

New interception systems are also seeing the light. 'Systems are emerging that allow you to shoot a drone out of the sky with the help of a laser,' says Arnold. 'That has a big advantage: cost. You don't use expensive ammunition or missiles to shoot down a cheap drone.' Companies such as the Australian Electro Optic Systems are developing laser systems that can shoot down twenty drones per minute by overheating them with concentrated energy beams. While lasers are accurate and cause little collateral damage, they have drawbacks such as the need for clear vision and sensitivity to weather conditions and debris.

In the meantime, Europe seems to be waking up, and is rapidly securing its infrastructure. However, whether we can switch quickly enough remains unclear. 'I don't think any European country is sufficiently protected against drone attacks today,' says Arnold. 'We have underinvested in defence for years. Now we have suddenly woken up, and we are throwing money at the defense industry. Europe is currently not prepared for a conflict, hopefully that will change in the future.'