Timothy Compston investigates the world of Radio Frequency jamming in relation to IEDs and new security challenges like drones

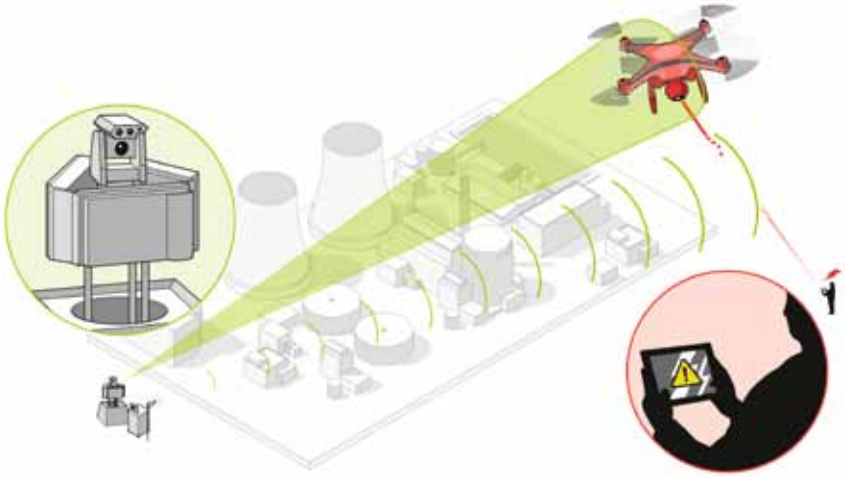
FROM BOMBS TO DRONES – RF JAMMERS ON THE FRONTLINE

In today's uncertain world with the ever-present threat posed by IEDs (Improvised Explosive Devices) in faraway trouble spots and, increasingly, closer to home, RF (Radio Frequency) jammers – or inhibitors – can provide an all-important safety bubble for troops on the move, bomb disposal teams, dealing with devices, and other first responders such as the police.

Speaking to Kier Head, operations director at Kirintec, who has a background of over 20 years as a British Army specialist in C-IED (Counter Improvised Explosive Device) and EOD (Explosive Ordnance Disposal) – including in Northern Ireland and Afghanistan – about his thoughts on developments on the RF jamming front in the context of IEDs, he is quick to underline the operational value of such systems: "Although jamming is actually a relatively expensive business I think that people are now seeing the absolute need for it. It is a life-saving capability and it enables you to travel on roads with force protection and hence a level of assurance that you are not going to be hit by these devices [Radio Controlled IEDs or RCIEDs]". Head adds that more and more countries are now keen to have this capability for themselves: "We are seeing a lot from the Middle East who are very interested in buying this [jamming capability] whereas before they may have waited for it to be gifted to them by the US or the EU, NATO, or even Britain itself," says Head.

The challenges faced by those looking to counter IEDs are constantly evolving, with Head admitting that it is a real battle to keep one step ahead of the terrorists: "The clue is in the name – Improvised Explosive Device. The fact it is improvised means how it is used is only limited by that bomber's imagination". One trend that is making life tougher on the IED jamming front, reckons Head, is the growing footprint of modern communications technology: "There are many different ways of communicating across the RF spectrum so there is really no limit to how people actually use that as the connecting link between the firer – the guy who is pressing the button – and the actual device".

The widespread take-up of mobile phone technology is also giving cause for concern: "Mobile phones are becoming the de facto method of initiating these sorts of things [IEDs]. People are very worried about that and there are a lot of technical challenges. It is the little things, like how much power mobile phone towers are giving out. In the UK this is restricted by law because people are worried about the effect of living next door to it, but those rules are not quite as hard and fast in other places". Head goes on to say that in some regions tower output strengths can be a magnitude higher, sometimes a thousand times more powerful, than in the UK: "So fighting the power output from that sort of tower can be a big challenge," he concludes.



Airbus DS' Counter-UAV System can be used to jam small drones

When using jamming systems, whether vehicle-mounted or man-portable, Head notes that there is always a battle between power and range. Given this he reveals that it makes sense, in scenarios like Iraq or Afghanistan, for electronic counter measures to be targeted at a known threat: "Different bomb making cells may use different technologies so you may look to program your equipment to jam those in a certain region". Head adds that a vehicle-installed jammer, by its nature, will always be more powerful than a man-portable system: "Man-portable systems, in the context of EOD, are really there to give the operator as they walk forward to a device a little 'bubble of protection' so the jammer distance is going to be less". Head notes that there are now solutions coming to market which are looking to combine the best of both worlds: "We have a portable system now, for example, which you can put into a dock on a vehicle to amplify it, doubling the power, although this is still not quite as good as a proper install".

In terms of other recent innovations, Head is enthusiastic about a Kirintec solution called REBUS, which he tells me is a 'quick to deploy' inflatable protective tent

©Kirintec

The Mercury man-portable RF jammer

which, he reckons, can be set up by first responders at the scene when a suspect device is discovered: "It is about five or six feet high and responders who are not trained in bomb disposal – the police or security personnel – can put this tent over the top of a device at an airport, for example, without touching it. There is jamming inside the tent and some ballistic protection as well".

For its part, Airbus DS (Defence and Space) – a division of Airbus Group – has come up with a 'Multirole Jammer' vehicle-fitted protection system which the company feels is industry-leading in the way it combines countering radio-controlled improvised explosive devices (RCIEDs) with the ability to comprehensively monitor the signal spectrum and offer tactical communication jamming.

Based on latest software-defined radio technologies, according to Airbus DS, the Multirole Jammer analyses the signal spectrum around a vehicle to jam the radio signals intended to ignite a roadside bomb in a target-efficient way. In an extended role, the device can be used for operational signal intelligence, thus contributing to the generation of a comprehensive picture of the signal situation, a task that Airbus DS reports previously could only be accomplished by separate systems. The Multirole Jammer also allows it to take over classic tactical jamming tasks, as well as supporting developing counter-UAV systems. "Lessons learnt from deployments such as

FROM BOMBS TO DRONES - RF JAMMERS ON THE FRONTLINE

Afghanistan have made more versatile and compact devices to monitor the electromagnetic spectrum indispensable", says Thomas Müller, head of the Electronics Business Line at Airbus Defence and Space.

Another area where there is certainly an increased appetite for RF jamming is to clip the wings of the soaring number of drones in our skies, especially when they start to pose a threat to security, safety or even those engaged in industrial espionage. One developer of counter-UAV (Unmanned Aerial Vehicle) solutions is British company K9 Electronics, including portable drone jammers, to disrupt R/C control signals and GPS navigation.

Glenn Darien, managing director at K9 Electronics, tells me more about the way the jammers work in practice: "The current systems we offer are hand portable. You have to see the drone first because it [the jammer] is manually operated then you can take action to jam the drone so the operator loses control. The jammers can disable the communication link between the controller and the receiver, therefore halting the drones intended mission. By jamming the GPS band the drone is unable to follow GPS coordinates".

Asked what happens next, Darien says it depends on the type of drone being flown: "Most will not fall out of the sky, but descend automatically to the ground in a controlled manner". On the subject of preventing interference with other non-drone communication systems, Darien says that using narrow beam radiation antennas pointed at the drone minimises such issues.

Regarding where he has found the most demand for jammers so far, Darien reports that there has been a real mixture of users: "There are the private individuals who are worried about drones flying over when they are in their backyards and we also have airports and palaces out in the Middle East on our customer list".

Turning to the next step for K9 Electronics on the counter-UAV stakes, Darien reveals that the business is expanding its horizons even further with the imminent launch of a solution to automatically identify the presence of a drone and then to track and jam it. Darien is working with a company in the US and is currently fine tuning some of the details of what he refers to as the 'Detect, Classify, Track, and Jam' solution: "It is more or less ready at the moment. We are developing it with a company in the States". Although full details of the solution are still under wraps, Darien was willing to sketch out a few of the elements: "This solution is for fixed-site installations where they want a constant system to monitor the perimeter. It uses microwave radar to actually do the detection and then for the tracking it is using video analytics to do the classification".

Airbus Defence and Space (Airbus DS) has also unveiled its own response to small drones in the shape of a 'Counter-UAV System' with first customer deliveries anticipated for Q4. This, says Airbus DS, has been designed to detect 'illicit intrusions' of UAVs over critical areas at long ranges backed up by electronic countermeasures 'to mimimise the risk of collateral damage.' Speaking when the company's Counter-UAV

©Kirintec

A vehicle-mounted RF jammer for mobile operations

©Kirintec

An inflatable inhibitor, it has radio frequency jamming inside of it as well as offering some ballistic protection in case the explosive goes off

FROM BOMBS TO DRONES - RF JAMMERS ON THE FRONTLINE

System was first announced back in September, Thomas Müller, head of the Electronics business line at Airbus DS started out by painting a picture of the existing threat landscape to explain the rationale for such a solution, pointing out: "All over the world incidents with universally available small drones have revealed a security gap with regards to critical installations such as military barracks, airports or nuclear plants".

In Müller's view, as a specialist in defence electronics, Airbus with all the technologies in its portfolio – and integration knowledge – was well placed to bring to market a quick-response protection system with, he underlined, extremely low false alarm rates. Drilling down into the specifics of how the Counter-UAV System operates, according to Airbus DS, it combines sensor data from different sources with the latest data fusion, signal analysis, and jamming technologies. Essentially the system uses operational radars, infrared cameras and direction finders from Airbus Defence and Space's portfolio to identify the drone and assess its threat potential, as well as to find the pilot, at ranges between five and 10km. In addition, based on an extensive threat library, and real-time analysis of control signals, a jammer interrupts the link between drone and pilot and/or its navigation.

When it comes to the jamming employed by the system, Airbus Defence and Space points out that because it is employing 'Smart Responsive Jamming Technology' the jamming signals are blocking only the relevant frequencies used to operate the drone while other frequencies in the vicinity remain operational. Since the jamming technology contains versatile receiving and transmitting capabilities, Airbus points out that, more sophisticated measures like remote control classification and GPS spoofing can be utilised as well. This allows effective and specific jamming and also a controlled takeover of the UAV.

So to conclude, whether the threat comes from a UAV or an IED it is clear that jamming by portable, vehicle-based, or site-specific solutions will remain an invaluable tool in the disruption of potential attacks.

©Kirintec

The Rebus is an inflatable protective tent, which can be deployed by first responders at a scene where there is a suspect device

RF Jammers – a brief history

Radio frequency jammers are certainly not a new phenomena, but their application has changed significantly over time. Up until very recently, the purpose of a jammer was to block, jam or interfere with more traditional forms of wireless communication and was used as early as during the Second World War. Ground-based radio operators would attempt to mislead enemy pilots by jamming the official line of communication and then replacing it with a spoof one, providing new instructions to throw the pilot off course. Meanwhile, in occupied Europe, the Nazis attempted to block broadcasts to the continent from the BBC and other allied stations. In turn, the allied forces fought back by increasing transmitter power, adding extra frequencies and even by leafleting cities with instructions providing listeners with the knowhow to construct their own directional loop aerial so that they could avoid the jammers.

The Cold War saw jamming continue as countries in the Soviet and Eastern Bloc increased their transmission power and utilised highly directional antennas to ensure that people wouldn't be able to watch or listen to undesirable broadcasts from abroad. Despite denying that it had been jamming out such frequencies, it wasn't until 1987 that the Soviet Union finally stopped jamming Western broadcasts.

©Kirintec

The Mercury VENTURA man-portable and Mercury Blade 5 radio frequency jammers

Timothy Compston is a journalist and PR professional who specialises in security issues. He studied International Relations and Strategic Studies at Lancaster University, is PR director at Compston PR and a previous chairman of both the National PR Committee and CCTV PR Committee of the British Security Industry Association (BSIA).