Mikael Westerlund looks at the need for deep covert communications in the hunt for terror suspects hiding among migrants and asylum seekers

COVERT COMMS IN HIGH-RISK SCENARIOS

From the shores of North Africa to landfall in Italy and Greece, the tragic scenes of migrants taking their lives in their hands in unseaworthy boats just to reach the relative safety of European shores has been front-page news for far too long. While there are those genuinely seeking asylum from the hellish conditions in their own homelands, European and international security services have known from the start that such masses of migrating people offer a perfect opportunity for terror suspects to mingle with the crowds and pretend they are ordinary asylum seekers fleeing persecution. Identifying, keeping track of and communicating intelligence on such threats requires dedicated individuals to infiltrate these migrating groups and pose as just another desperate refugee. How they then communicate the information they gather becomes a challenge for which supporting team members need

©Getty Images

to be in place and properly equipped with the right comms tech to make any such mission successful.

Any market that has a surveillance requirement for teams to observe a certain person or groups and, while doing so, communicate regularly to a central HQ or control about immediate actions that need to be taken will require an effective covert team communications solution set. A narcotics team – as part of a police force keeping a drug dealer under surveillance – would be a typical scenario where deep covert communications of the kind that a team keeping watch over the flow of immigrants through Europe would also need to consider. Such teams typically comprise between three and five operatives or agents. Some might need to be in close using as little kit as possible other than, perhaps, a normal-looking mobile phone. Other members of the three to five man team might be close by on foot, or in cars. Whatever the setup determined to be appropriate for a given scenario, the agents will need to be in continuous communication and because each member of the team can't follow a suspect the whole time they might need to anticipate where the suspect is headed and send different team members to that location in a system of repeated changeovers. This constant, on-the-move type of operation makes continuous communications essential, which is where deep covert communications solutions and accessories can be employed to deliver regular updates about movement, action and what's happening on the ground.

Migrants, such as these ones rescued off the coast of Libya, provide an ideal cover for insurgent attackers

Wearing any kind of communications device, no matter how unobtrusive, presents a risk that in some scenarios is too high to consider safe, such as when an agent infiltrates a sleeper cell or moves within a group of refugees in a permanent or temporary camp. Such an inserted agent might simply rely on a normal smart phone, while his/her colleagues, unseen beyond the group, will each be equipped with a deep covert system. They keep surveillance up from a safe distance and then locate their colleague infiltrator through his smart phone, even being able to take silent control of the device using an app. They can then listen to his conversation through the microphone, (but without being able to talk to him), and even be able to switch on the video without an indicator light showing.

These undercover agents around the inside man need to be coordinated through communication so that they can remain close to the target group, in turn giving the infiltrator a sense of security. Even in an urban counter-terror (CT) scenario, such as those that and which so this says: such as those that unfolded earlier this year in Brussels, the CT team observing the apartment of a sleeper cell can benefit from the use of deep covert devices. Earpieces, communications loop-type products, some disguised as ordinary everyday devices, can connect to cell phones or radios to pass real-time information back to control – observing and communicating all the time, these operatives will appear to be more 'civilians' just hanging around.

One growing problem is that terror groups are becoming as sophisticated in their communications and IT skills as many of the agencies trying to scupper their efforts and destroy their networks. They are trying to stay one step ahead of the security services, which in turn are trying to stay one step ahead of them. Teams on the ground tasked with identifying terror suspects from within a large group of migrating people, need to be aware that any such suspects will know that they are likely to be among them and looking for them. Such suspects may themselves be equipped and prepared technologically with readily available smart phones and sniffer apps and other means of 'watching' for signs of those watching them.

The case for a migrant scenario will include deep covert communications equipment, devices and accessories not dissimilar to those needed in already tried and tested security and policing situations. These might include the likes of the Clarity LTE range from Savox Communications, a new covert accessory set that can handle the dual role of simplex and duplex audio required as users switch from carrying a radio and mobile phone to a mobile phone with a radio client. The Savox Clarity interference-free and interception-free covert neck-loop/microphone system and covert base unit (CBU) are two-way radio accessories that provide totally discreet personal communications. They can be concealed under clothing and include a built-in microphone and a wireless PTT disguised as a car key fob. The key fob PTT also provides tones functionality as standard for situations where speech is impossible. Once connected to the user's radio, the solution is completed with miniature earpieces and an in-line PTT fall-back solution.

The CBU allows both verbal and non-verbal communications. Non-verbal uses tones that the team will have agreed on before they go into the field, such as a simple series of beeps to convey a message: two beeps may mean "I am close to the target now I can't talk" and so on. A handful – but not too many – of such signal messages will be useful. Clarity is interference-free and communicates with a specific earpiece – the RCR 7 – with the earpiece loop around the neck creating an electromagnetic (EM) field around the wearer's body above and below the equipment. The earpiece picks up any EM signal, that normally causes interference problems particularly in an environment with high EM noise. However, the Clarity neck loop and the earpiece operating together are immune from such interference. The wearer can stand right next to a power transistor or high-voltage lines without any adverse effect. Even inside a police car, the ultimate connected-car environment with lots of communications and sensor technology mounted on the interior, Clarity can operate without being impacted by EMI.

This system actually creates its own EM field, not only making it interference-free, but also interception-free. The EM field around the body of the wearer is created using such a low frequency that the field is very tight. This is a crucial differentiator in a scenario where, for example, several people are all in one room, perhaps a gymnasium holding large numbers of asylum seekers. Where other systems might be detectable by someone using a simple radio to pick up their signal out to a range of 3m or more from the user, a radio/detector will need to be no more than 1m from a Clarity user to pick up any signal.

While these accessories rely on the creation of an EM field at a very low frequency, the car key fob works using a Zigbee signal, (a wireless technology developed as an open global standard for low-cost, low-power wireless M2M networks), which has been modified with a proprietary Savox protocol that is more secure than the open standard itself. This means it can't be hacked. The only long-range transmission comes from the mobile device to which the accessory is connected. There are, however, covert solutions that use Bluetooth, with a transmission range of at least 10m and much further than a covert agent would typically want to risk.

©Savox

Connected to a smart phone, and hidden under a jacket, this Clarity solution will attract minimal attention

Added to that is the fact that Bluetooth is an open protocol and that means anyone can look into a solution and try to crack it. With simple Bluetooth 'sniffing apps' available from iTunes, anyone can see the Bluetooth traffic going on around them. The risk is something to be considered when adopting covert comms technology. It's perfectly feasible that a terror suspect within a group of refugees might have an iPhone with a sniffing app on it. Every time someone pushes the PTT Bluetooth button, or talks into the Bluetooth device, the suspect will be able to see some traffic going on regularly and the result for the agent is potentially disastrous.

To communicate with a command and control centre, such covert solutions as this connect to regular PMR radios, such as units from Motorola, Hytera and Airbus among others. They can also be used with mobile phones; this latter point is crucially important as it's much easier for an agent to hide a small mobile phone than a PMR radio. No matter how small the PMR radio is, a mobile phone will always be smaller. The connection to the phone or radio is wired.

Another advantage in the refugee scenario of a solution like Clarity is its ability to use the civil mobile LTE networks, as long as a data plan and mobile phone connection exist for the phone involved. Crossing countries in Europe will offer good LTE coverage and often better than a PMR radio might experience. Add to that the fact that refugees are using their own mobiles all the time, and an agent with a phone will simply fit in.

Being able to provide the communications that will operate reliably in a situation that might 'go bad' and where an operative in trouble might have to say "Get me out of here" is critical. Professional agents have said that no one should ever be left behind or without connection because of poor communications. By ensuring they have the right equipment to do their job, the most important thing in any operation is for everyone to get home safe.

Mikael Westerlund is CTO of Savox Communications, a leading provider of deep covert communication solutions for government and public safety agencies, as well as the manufacturer of C4i intercom and communications systems for defence, security and professional public safety users.