

Thomas Withington

# COMINT on your back

Man-pack COMINT systems are separating the electronic wheat from the chaff.

According to the US Central Intelligence Agency, Signals Intelligence or 'SIGINT' gathering comprises the collection of ELINT (Electronic Intelligence) which is concerned with amassing data regarding friendly and hostile radar systems, and COMINT (Communications Intelligence); the collection of intelligence regarding telephone, cell phone, radio or online telecommunications.

The requirement for COMINT gathering across global intelligence and law enforcement communities has grown commensurate with the proliferation of cell phones across the world. According to figures published by the Statistica online statistics portal, in 2013 four billion people worldwide were in possession of a cell phone. The same organisation predicts that by 2019, this will have increased to five billion, while the number of people equipped with smart phones will have increased from almost 1.6 billion in 2014 to 2.7 billion by 2019. For those waging political violence cellular communications provide obvious attractions as a means of sharing written data, in the form of text messages, emails or messages on social media, and for the provision of voice communications, and the recording and sharing of photographs and video. Yet they have one important characteristic which it is impossible to overcome: To do all of these things, cell phones must use a telecommunications network. Every time a cell phone joins a specific network, or performs any of these functions, it electronically announces its presence to the outside world. This is thanks to a simple, yet essential, item of cell phone architecture known as the phone's International Mobile Subscriber Identity (IMSI) number.

Put simply, the IMSI is a unique numerical code which can include a series of digits representing the country where the phone is registered, the network it uses within that

country and the phone's Mobile Subscriber Identification Number (MSIN); the latter being the number assigned to that particular phone which is used to identify it to a cell phone network. Thus every time a cell phone joins a network it transmits its IMSI as a digital 'handshake'. The network responds by providing that phone with a Temporary Mobile Subscriber Identity code which is randomly assigned. The TMSI can be changed for that phone at any given moment with the intention of frustrating attempts by eavesdroppers to identify and track the phone using the IMSI. That said the IMSI still has to be used, albeit briefly, to perform the digital handshake and to rejoin the network if the connection between the phone and the network is lost. Moreover every time the phone moves out of the local coverage of one part of the network and moves into another, the IMSI is sent anew, and the process repeated.

Confidential sources have told S&SI that the IMSI can play a valuable role in tracking a person of interest. Consider this potential scenario: A terrorist suspect is known to be living and operating in a specific city and is placed under covert surveillance. Like millions of other individuals the suspect uses a cell phone and, like millions more, they move around the city moving between various local parts of a larger mobile network. Each time our target does this their phone transmits their IMSI and receives a TMSI. Once the suspect is under surveillance it will be possible for human operatives on the ground to see the suspect using their phone. At the same time a COMINT system can match their physical location with the IMSI emission of their phone as it joins the network. This can be captured by the COMINT system and although the TMSI may change every time the

target joins a new network, their IMSI will remain the same. Therefore by using a COMINT system to detect the IMSI every time the target joins the network, it becomes possible to track them around a city. The fact that suspected terrorists are mobile, makes it necessary that such COMINT systems are too, which can be greatly facilitated by enclosing such systems within a backpack, or onboard a vehicle. Man-pack COMINT systems have the added utility that they can be disguised as ordinary rucksacks thus preserving the surveillance operatives' low profile. As John Kilgallen, the founder and president of COMINT Consulting told S&SI: "Access to line-of-sight targets operating in difficult urban or challenging desert/mountain terrain or other harsh climates just about dictates a man-pack or small, remotely-controlled solutions to be used. Further, targets are mobile and thus COMINT systems must be correspondingly mobile."

*Artificial intelligence may aid the future development of man-pack SIGINT systems, greatly accelerating their speed of intelligence processing and dissemination.*  
(Photo: Elbit Systems)







**Rohde and Schwarz provide a number of COMINT systems including the firm's C-ESM system of which the PR-100 forms one part. (Photo: Rohde and Schwarz)**

Furthermore, by tracking a suspect's IMSI, in combination with human intelligence provided by operatives on the ground following the suspect, it is possible to detect and collect the IMSIs of their associates or other persons whom they may meet on a regular basis: "Man-portable COMINT systems, whether manned or unmanned, mobile or clandestinely-deployed for automated collection, offer the ability to collect more nodes of a target network with better fidelity and to understand and derive a picture of that organization's operations and key players," observes Mr. Kilgallen: "This in turn provides the basis for the ultimate steps in law enforcement operations; an arrest or preventive/disruptive measures being taken to avoid a drug shipment, kidnapping, or terrorist attack." As a written statement provided by Elbit Systems to S&SI observes: "In counter terror scenarios, both tactical and cellular arenas, the man pack operator is able to quickly detect the hostile targets' transmission, locate and track it while stationary or on the move." Like other companies mentioned in this article, Elbit provides man-pack COMINT systems, with the firm stating that these can cover a waveband of 25MHz to three gigahertz (GHz) encompassing the wavebands used by conventional tactical radio, cell phones and some satellite communications systems.

For the military, discerning the nature and complexity of the electromagnetic

environment at the tactical level also has clear benefits, in particular regarding intelligence gathering pertaining to an adversary's use of communications be those cell phones, conventional tactical radios or satellite communications. Confidential sources have informed the author that the Islamic State of Iraq and Syria have used cell phones as well as civilian standard handheld radios for battlefield communications. Once again, the man-pack COMINT system can help: "Often, operations are performed in areas, in which it is not possible to deploy vehicles adequately. In such situations, the proposed lightweight man-portable ESM (Electronic Support Measure) system with radio monitoring and Direction-Finding (DF) capabilities can detect and locate enemy activity," notes Guido Schwarzer, product manager monitoring and network testing division at Rohde and Schwarz. The company provides a range of battlefield COMINT products including the portable C-ESM COMINT system which its official literature states can monitor the nine kilohertz to 7.5 gigahertz segment of the electromagnetic spectrum. Crucially Mr. Schwarzer adds that such systems are passive, meaning that they can gather ELINT without revealing the user's position: "Such systems passively intercepts communications signals, provides the line of bearing and can locate the source of emissions."

Alongside assisting the collection of ELINT as part of the overall intelligence gathering

effort supporting counter-terror operations, such systems can contribute significantly to the tactical aspects of counter-terror operations. As Si Timewell, director of electronic warfare operations at Kirintec argues, man-pack SIGINT apparatus can be used: "Primarily as an intelligence tool to allow understanding of the situation, environment and enemy network prior to a strike or detention operation. Understanding the situation and environment allows the more surgical use of other assets such as communication denial or electronic attack (see below) system as well as understanding the enemies intent." Interestingly Mr. Timewell observes that manpack SIGINT can contribute to the efficacy of Counter-Terror (CT) operations in other, arguably less tangible ways: "An interesting development is the media and bystanders using social media who could unintentionally contribute to tipping off the enemy network either internal or external to the strike area. As this cannot be controlled understanding what is published and the impact is crucial to successful CT and law enforcement operations." Understanding what is happening regarding cell phone activity in the locale of an actual or potential operation is helpful. For example an arrest team may be less keen to apprehend a terrorist suspect in an area where many people using cell phones maybe present, for fear of having the operation recorded, or tip-offs being made on social media that a major police operation maybe underway. A man-pack COMINT system can help to determine if a particular area has less cell phone activity. If such activity is deemed excessive or could threaten the mission then the CT team may choose another site with less surrounding cell phone activity for the operation.

## ORBAT

On the battlefield, man-pack COMINT systems assist the drafting of the electronic Order-of-Battle (ORBAT); the list of friendly and hostile RF emitters, their location and transmission characteristics: "Often, when arriving in the mission area, (electronic warfare) operators know little about local communications. They start their operations by searching for signals. Then they exploit the radio spectrum step by step, thus tapping into the enemy communications," Mr. Schwarzer adds. Elbit's statement continued that one asset of man-pack COMINT systems is that the intelligence they collect can be sent up the chain from the tactical level to the operational level to build a consolidated picture of the friendly and hostile emitters in a particular theatre: "The man-portable SIGINT System objective is to provide full SIGINT situational awareness for dismounted forces dispersed in the field, utilising each soldiers' location to provide a complete SIGINT image transmitted to the tactical command centre." Building the electronic ORBAT forms a vital part of the overall electronic



support mission. In electronic warfare theory, electronic support (put simply, the gathering of ELINT) forms a key part of the overall electronic warfare effort of a deployed force, which also comprises electronic attack (the use of electromagnetic energy to attack hostile weapons) and electronic protection (the use of electromagnetic energy to protect friendly forces). This electronic support effort, Mr. Schwarzer states can include the *"Detection of signals and identification of targets in an area of interest where no information is available in advance is performed by searching for signals across wide frequency ranges, without any particular focus on communications channels."* Channels of interest, he adds, can then be logged and stored for further exploitation. Some COMINT systems can eavesdrop on analogue communications, if the signal can be demodulated, that is the information bearing


signal of the communication disentangled from its carrier wave. Where signals cannot be immediately demodulated and decoded then typically man-pack COMINT systems will allow these to be recorded for further analysis.

Battlefield man-pack COMINT collection has witnessed some important advances in recent years: In 2016 Chemring was awarded a contract by the Australian Department of Defence to provide the firm's Resolve-3 product to that country's army in a deal worth \$13.7 million, with deliveries of this system expected to be concluded by early 2018, according to a press release from the company announcing the news. Seven years earlier in September 2009, the UK Ministry of Defence awarded a contract to Roke Manor for the supply of the British Army's Project SEER land electronic warfare man-pack EW requirement which also saw the delivery of the Resolve

man-pack SIGINT system. Open sources state that this system was procured as part of an Urgent Operational Requirement to assist the British Army's deployment in support of US-led combat operations in Afghanistan, with the deployment of the Resolve occurring in 2010. Few details are publicly available regarding the capabilities of the Resolve-3 although the firm's official literature states that the system can perform wideband SIGINT and is operable at the halt or on the march using a tablet employing the Android operating system. Other improvements for the system *vis-à-vis* the preceding Resolve-2 manpack product include a weight reduction of 30 percent, with two batteries able to provide 24 hours' operation. Additional company literature states that the firm's Resolve Prefix SIGINT software which is used with the Resolve-3 can provide direction finding of radio frequency emitters across a two megahertz to three gigahertz waveband.

Kirintec sees promise regarding Artificial Intelligence (AI) and what it can offer to the SIGINT mission. The company is currently designing a man-pack SIGINT system utilising the expertise that it has carved out in the field of man-pack C-IED (Counter-Improvised Explosive Device) jammers telling the author that: *"the plan is that the system will use AI techniques to detect and characterise new threats"*. Broadly speaking, AI is defined in computer science as machines capable of perceiving their environment and taking this into account to orientate their actions to achieve a specific goal. Mr. Timewell continues that AI can be used to enhance a SIGINT systems' ability to accurately geo-locate emission sources, and that ensuring such systems are *"software defined"* is essential as it will make them comparatively easy to upgrade in the future as new threats are discovered, or new signal processing techniques are pioneered. Allied to this, he continues, is the use of *"open architecture to integrate with new technologies as they mature such as OSINT (Open Source Intelligence); material available in the public domain which might be useful for intelligence purposes."*

Visions of future manpack SIGINT system design have also been articulated by Elbit which, along with other man-pack SIGINT system manufacturers surveyed in this article, is working on reducing the size, weight and power consumption of their offerings while widening the bandwidth of the signals that they are capable of detecting. Mr. Timewell continues that he expects: *"future systems will have AI and machine learning algorithms at their heart. This will be the only way to keep pace with changes in threat, networks, targets and target sets."* Being able to easily share SIGINT with other users will also be essential as regards future system design: *"Timely dissemination in getting the right intelligence to the right person, at the right time by providing the ability to seamlessly exchange information with other datasets and repositories."*



**Chemring's Resolve man-pack COMINT system has been provided to the armies of Australia and the United Kingdom.**  
(Photo: Chemring)