Radio activity

Soldiers view a map during a training exercise at the Joint Multinational Readiness Center in Hohenfels, Germany. (Photo: US DoD)

Listening in to work out who is talking to whom, where they are, what kind of equipment they are using, whether they represent a threat and what they are saying is all in the realm of communications intelligence. **By Peter Donaldson**

Use of the RF portion of the electromagnetic spectrum for communication goes back to Heinrich Hertz and his experiments that proved the existence of radio waves in the latter half of the 1880s and will continue into the foreseeable future.

Communications intelligence (COMINT) is arguably the more demanding of the two major branches of signals intelligence (SIGINT), the other being electronic intelligence, which is principally concerned with radar signals.

COMINT is an expanding sector of the wider SIGINT market. Nicholas Cianos, senior director for products and process at DRS Signal Solutions, told *Digital Battlespace* that as wireless technology continues to evolve and become more pervasive, there will be a continuing need to support the COMINT market. DRS Signal Solutions makes key front-end components, including tuners and receivers, for larger COMINT systems.

In relation to use of commercial wireless and cellular systems by targets of interest, he said that COMINT provides a potential vehicle for identifying threats and developing an understanding of their intentions, indicating that there is still some way to go toward successful exploitation of their signals.

'Commercial communication technologies provide the enabling resources for efficient protected communications,' Cianos said. 'Modern waveforms can be especially challenging to process, especially in densely populated developed areas, where spectral densities are very large. The detection processes are further complicated with the use of commercial encryption methods. Hence, detection, location, identification and analysis of the signals is difficult.'

The ability to carry out traffic analysis, geolocation, transceiver identification and fingerprinting and cryptanalysis – or at least a subset of these jobs – simultaneously and in real time is a demanding task. James Kilgallen, president of COMINT Consulting, told *DB* that it is also one that industry and operators have fallen behind on, as adversaries of many kinds have adopted and adapted various combinations of software defined military radios, professional mobile radios and commercial cellular communication systems.

While it is fairly obvious that low probability of intercept (LPI) signals (which use techniques such as spread spectrum and frequency hopping to make them ▶

difficult to detect) present a serious challenge to COMINT systems, he argued that there are many others that can be received and recorded but still elude real-time analysis that would reveal their significance and enable them to be exploited, which he put down to weaknesses in signal classification techniques.

Decoding problems

Kilgallen explained that most of the wideband COMINT collection systems in operation today are hamstrung in both classification and decoding. Classification of energy, based on an old technique known as modulation recognition, he describes as crude and poorly suited to the needs of EW officers, who must have precise information in real time with little to no ambiguity.

He added that the technique does not provide full characterisation of the target because it only identifies a modulation type rather than a specific modem, has poor stability and only works in real time if channel conditions are good.

Taking aim at many collection systems' decoding capabilities, he said that they are not keeping up with the threat. 'In the three busiest areas of spectrum for communications – HF, VHF and UHF – the industry as a whole does not keep pace. The need is some 90-120 new waveform solutions per year, and the industry average is approximately 2.7 new decoders per year.'

While COMINT Consulting has developed new techniques that enable the company to produce more than 30 new decoders per year, he said, the need remains much greater. Kilgallen also argued that the market has focused on cellular communications to the detriment of other

FIGHTING THE LAST WAR

A particular challenge with HF is the variability of signal strength with propagation conditions, which vary between day and night and with the seasons. This means that COMINT systems that target HF radios must be able to handle signals with a high dynamic range, which is the difference between the strongest and weakest signals. Typically, today's receiver designers want to digitise as early as possible in the signal path to make the most of software-defined systems and use wideband direct digitising receivers.

Wideband receivers are particularly good for detecting LPI signals and use techniques such as digital down conversion, in which a wideband sampling analogue to digital converter (ADC) creates narrowband channels to target the signals of interest.

Shmulik Dahan, director, COMINT Systems at IAI's Elta Division, told *DB*: 'The increase in computing power of the processors allows the implementation of many processes in purely digital ways. This resulted in compact, sophisticated software-defined sensors. The same hardware can be programmed to fulfil different functionalities for various applications. The new and improved ADCs allowed direct sampling receivers, which simplify the receivers and reduced their physical size significantly.' However, the limited dynamic range of available ADCs means that this is not an ideal approach for HF.

CommsAudit argues that targeting low-power signals of interest in the presence of strong interfering signals requires a narrowband approach, with analogue filtering upstream of the ADC to exclude unwanted signals as early in the process as possible, and to make the most of a narrowband receiver's superior amplitude discrimination.

The company emphasises that the ability to pick out weak signals among strong interference is not determined by receiver sensitivity alone, and offers solutions based on combinations of wideband and narrowband receivers to monitor the whole RF spectrum year round, 24/7. While this kind of innovation shows what can be done with the right focus, Kilgallen expressed frustration over community priorities and procurement processes.

Procurement myopia

'The greatest problem is myopia,' he said. 'Over recent decades we (the intelligence community) have lost track of RF developments several times while focusing on the sexy technology of the moment. Unfortunately, narco-traffickers and terrorists don't follow our procurement trends and are continually a step ahead in deploying their communications technology.' Software-defined radio (SDR) technology has proven to be a double-edged sword, both challenging COMINT systems and providing them with new and improved capabilities.

Rapidly changeable

In particular, he told *DB* that SDR waveforms that are rapidly changeable have had the greatest negative effect on EW systems that cannot adapt to changes in threat systems rapidly enough to deal with them, adding that although there are some cognitive EW systems in operation, they still lack the kind of precise classification capabilities referred to above. 'Groups like ISIS use DMR handheld radios whose firmware can be downloaded and modified for $50. We don't keep up with that. Our Krypto1000 software has a solution to variant DMR waveforms that is market-leading, but it is still a challenge.'

He added that the aforementioned myopia is probably the greater problem, as the industry does not follow developments in communications technology as it should. 'Thus, COMINT systems remain fighting the last war, at best.' On the positive side, he emphasised, SDR technology has enabled higher quality capture and radically lower SWaP consumption. In turn, this enables the systems to capture what Kilgallen calls a higher resolution picture of the spectrum on more platforms, including clandestine and body-worn equipment and both manned and unmanned platforms in all environments.

important radio communications technologies, citing some very advanced HF systems in use today by targets of interest.

'One only needs to watch the evening news to see Boko Haram or ISIS terrorists with HF gear in their trucks or advanced VHF-UHF walkie-talkies, using modified DMRs.' [Digital Mobile Radios are capable of using RF or connecting over the internet.]

Monitoring HF

HF is playing a growing role in legitimate military, paramilitary and civilian operations, as well as in the nefarious activities of criminals such as smugglers, pirates and terrorists, all attracted by its ability to provide reliable BLOS communications using either sky wave or, for shorter ranges, ground-wave propagation, without the expense of SATCOM or the risk of interception as the data passes through SATCOM servers. This makes HF an increasingly important target for COMINT systems.

One innovative effort to target modern HF radios revealed last summer involves the combination of the ELK-7065 3D HF band COMINT interception and geolocation system from IAI Elta, with Schiebel's Camcopter S-100 rotary-wing UAV.

Packaging useful HF interception capability into a small vehicle was a tall order for many years because of the relationship between the wavelengths of the target signals and the size of the antenna required to receive them. With wavelengths from 100m to 10m, quarter-wave, half-wave and full-wave antennas made using traditional technology can be large, cumbersome things. However, the airborne antenna for Elta's ELK-7065 system measures just 30x50cm and, despite its size, provides very accurate direction finding, said the company.

Details of the antenna's construction have not been revealed, but the use of fractal geometry is a proven technique for packing very long antennas into very small spaces. According to IAI, the system tags and identifies signals in a multi-dimensional manner, using such tell-tale characteristics as power, centre frequency, modulation type, geolocation and polarisation. These techniques, said the company, enable swift labelling and identification of received signals and reliable generation of the electronic order of battle.

Other capabilities of the ELK-7065 include instantaneous azimuth and elevation measurement, fast and accurate waveform classification and identification, instantaneous geolocation, polarisation estimation and a high probability of intercept. The company also emphasises its ability to detect and analyse advanced HF signals rapidly, and to demodulate signals to extract voice and text data.

Hardware advances

While the smarts of modern EW systems, including COMINT suites, lie in the software, advanced hardware also plays key roles.

'Three technologies have been critical in the development of COMINT systems,' ▶

said Cianos. 'First, tuners and their corresponding digitisers are capable of instantaneously processing very large segments of the spectrum with processing bandwidths of up to 100MHz. Secondly, high-speed digital technology and open standards enable filtering and processing of the signals. Thirdly, high-speed back-end servers enable development of processing algorithms to process large volumes of digitised information.'

He said that DRS tuners offer high-performance wideband capabilities, operating from HF through the microwave spectrum. Flexible chips such as field programmable gate arrays (FPGAs) play their part with reconfigurable internal logic, enabling them to take on a range of specialised tasks much more efficiently than general-purpose microprocessors can, providing resources to process large volumes of wideband digitised data.

Kilgallen agreed: 'FPGAs are critical, allowing massive processing for cryptanalytics as well as more mundane tasks in signal processing, freeing critical CPU cycles for mission-critical tasks like decoding,' he said, while Cianos also emphasised the commonality among its tuners for air, sea and ground applications.

'DRS tuners are designed to provide high performance (noise figure, spur-free dynamic range) and, consequently, they can operate effectively in dense signal environments that air and land systems often experience. The tuners are also designed to stressing environmental parameters. Today, the tuners are created for temperature extremes between -40°and +70°C,' he said. For the future, he sees tuners evolving to cover the millimetre wave portion of the electromagnetic spectrum as commercial communication technology moves in that direction.

Artificial intelligence applications including cognitive radio are starting to make their presence felt, with machine-learning technologies providing tools to sort, process and identify signals of interest, according to DRS.

COMINT Consultants is working on predictive capabilities exploiting AI to improve classification and transceiver identification performance. 'The communications industry moves at a faster pace than we can train SIGINT, EW and IO officers, so AI and cognitive systems are our only hope of keeping up.'

Kilgallen cited a market average of 23 coarse classifiers in COMINT systems, pointing to the company's bid for leadership in this area, claiming to offer more than 4,000 precise, real-time classifiers, plus several hundred precise radio transceiver fingerprint IDs.

'These routines allow a more detailed picture painted of a communications environment that cognitive systems need to characterise them. It isn't enough to have them geo-located or lumped into benign categories based on their power, shape and where they are in the spectrum. All of those can be misleading and dangerously so. A combination of those techniques is the way forward.'

Traditionally, transceiver fingerprinting has relied on one-off solutions, but COMINT Consulting claims to have moved beyond this with a new software technique that allows any system to be instantly aware of any of several hundred transceivers.

In addition to classification and fingerprinting capabilities, the company's latest systems offer a growing number of software-based decoders for currently active targets, which are urgently needed in an industry in which, according to Kilgallen, between 40% and 60% of the decoders are obsolete, with many dating back to the Cold War.

Better decoders

Many deployed decoders are either inaccurate or incomplete, he told *DB*, elaborating that the names of the target radios and modes are often incorrect and the decoders don't address all the waveforms that these systems use. A typical modem may have four different Phase Shift Keying waveforms, but most COMINT solutions only offer solutions for two of them, he added.

In one case, a particular modem is wrongly named in all competitors' solutions, whose decoders process a vocoder (voice digitiser) that was last used by that modem almost 30 years ago, Kilgallen said.

'Worse still, the modem has been steadily replaced by more advanced modems over the past five or six years – a series of three new pieces of equipment issued to their military and certain governmental agencies – and none but COMINT Consulting has followed these developments and deployed solutions.'

The company is also adding to its inventory of parsers, tools that analyse signals on air extract information about alphabetic formats, transmission protocols, cryptographic systems etc. 'Our decoders are only as good as our customers' abilities

COMPACT COMINT

HF communications play an increasingly significant role in military, para-military and civilian applications. Dahan said that current HF DF COMINT systems are cumbersome and require very large antennas, rendering them impractical for compact and mobile applications. He cited the ELK-7065 with its compact HF COMINT and 3D-Geolocation system as revolutionary in that it provides the instantaneous and precise location of HF transmitters.

Measuring 50cm across, it is designed to be installed on board any airborne platform and can operate in the harsh electromagnetic environment characterising the HF band. The system tags and identifies signals characteristics in a multi-dimensional domain, composed of signal identifiers such as power, centre frequency, modulation, geo-location, polarisation and more. These techniques enable swift labelling of the received signals, identification and reliable electronic order of battle generation.

Dahan highlighted Elta's ELK-6060 radio location system as designed to address the need of ground combat units to collect on-the-move, real-time intelligence on hostile V/UHF communication transmission locations. The system includes an array of light-weight sensors carried by soldiers, combat vehicles, tactical UAV and, if necessary, installed unattended near an area of interest. Detected locations of hostile radio transmissions are displayed on a handheld C2 device of the commander or other C2 displays.

to extract the target's traffic. For us a decoder is a full demodulation-decode and parse chain.' He also stresses the importance of commonality, telling *DB* that the company has worked hard to ensure that its software can enhance any COMINT system.

'There is no place for proprietary or one-off solutions against targets that move and deploy faster than we do. We've also taken pains to ensure our decoders can be used in any active or passive (electronic attack or electronic support) system as well,' Kilgallen said. Ground troops in particular are not well served with lightweight, portable COMINT systems, with legacy systems essentially unchanged in their capabilities, despite lessons learned in the last two decades of conflict, he said.

'All, bar none, are still offering systems that can prosecute press-to-talk or cellular targets, but none of the other 10,000-plus target waveforms in ELF-EHF,' he continued. 'On a positive note, most have grown smaller (through SDRs) and have better geolocation, but that's it. Without exception, all need more processing power on board to host more advanced solutions like automated collection, classification and so on, and an external connection to a rugged tablet carry a SIGINT software suite to help them prosecute other-than-voice targets.'

Generally, he does not expect rapid improvements in the capabilities provided to warfighters in the field, with progress held back more by human factors than technological ones. 'I see industry myopia continuing, because specifiers do not know their targets as well as they should. They are comfortable with what they know and completely blind to what they do not know as their systems and software cannot help them learn more. I see procurement processes continuing to hamper rapid development.'

Enlightened agencies

He added that the highest priority developments are likely to be tackled, despite the above mentioned constraints, by what he called the more enlightened and forward-thinking agencies such as the DARPA, the Intelligence Advanced Research Projects Agency, the Air Force Research Laboratory, the Naval Research Laboratory and the National Security Agency in the US and the Defence Science and Technology Laboratory in the UK, which regularly reach out to small, innovative companies.

'There are plenty of small companies innovating that are under the radar. Witness the recent revelation that an Israeli company had a solution to the iPhone's encryption. But procurement processes and procurement contractors, typically large primes and long tails (at best 24 months from market survey to white paper to RFI to RFP to award) are our worst enemies against targets that make decisions in minutes.'

He added: 'The new NSA Director, Admiral Rogers, has begun an initiative called NSA21 that aims to address part of this – our fingers are crossed.' ■