

ELECTRONIC WARFARE

AN ARMADA INTERNATIONAL COMPENDIUM SUPPLEMENT



ARMADA : THE TRUSTED SOURCE FOR DEFENCE TECHNOLOGY ANALYSIS



The Partner You Can Count On™

Advanced Anti-Radiation Guided Missile


AGM-88E AARGM: An advanced weapon for multiple target sets embedded in anti-access and denied environments.



Destruction of Enemy Air Defenses: Advanced Anti-Radiation Guided Missiles (AARGM) strike their targets at China Lake, Calif. during live fire tests.

OrbitalATK.com

DefenseElectronicSystems.BDev@orbitalatk.com



An EA-18G Growler lands on the flight deck of the aircraft carrier USS Theodore Roosevelt (CVN 71). The Boeing EA-18G Growler is a carrier based electronic warfare aircraft.

ELECTRONIC WARFARE AND SIGINT COMPENDIUM

Signals Intelligence (SIGINT) is the demanding discipline on which the rest of Electronic Warfare (EW) depends, if a military commander is to take and hold the initiative in a wide variety of operational scenarios and if success is to be gained in the maritime, land, air, space and cyber domains.

Peter Donaldson

Electronic warfare (EW) is often described as the struggle to secure the use of the electromagnetic spectrum for one's own purposes and to deny it to one's enemies.

There is, of course, more nuance in EW than that, but it's a good place to start.

For many years, NATO defined the main branches of EW as Electronic Support Measures (ESM), Electronic Countermeasures (ECM) and Electronic Counter-Countermeasures (ECCM), with the Suppression of Enemy Air Defences (SEAD), using Anti-Radiation Weapons (ARW) tacked on as a kind of afterthought. These terms are still in common use, but the current official parlance divides EW into Electronic Support (ES), which is basically the old ESM category, Electronic Attack (EA), which encompasses the old ECM category plus SEAD and Directed Energy Weapons (DEW), while the old ECCM category is now known as Electronic Protection (EP).

These acronyms tend to pepper any discussion of electronic warfare, but they

are not very helpful without some definition and exposition. But before we get to that, it is worth noting that they all seem to leave out the intelligence gathering and analysis functions upon which these mission areas rely.

SIGINT FOUNDATIONS


This apparently orphaned, but actually central and fundamental, branch of EW is Signals Intelligence (SIGINT). The purpose of SIGINT is to collect technical information about signals of interest, analyse it and disseminate the results to the intelligence agencies and databases on which all other EW disciplines and systems must rely if they are to work properly. SIGINT encompasses the subdisciplines of Electronic Intelligence (ELINT) and Communications Intelligence (COMINT), the principal difference between them being the kind of signals they target.

The targets of ELINT operations are signals between machines (principally radar), while COMINT operations target communications signals between people. Both do this largely through intercepting their transmissions with

very sensitive and sophisticated receiving equipment, as this kind of direct method is one of very few ways of gaining accurate and comprehensive information about adversary military systems.

The purpose of COMINT is to extract information about adversary capabilities, force dispositions, plans and intentions from communications signals. This may be achieved either through the breaking of codes to read messages, overcoming encryption to listen to them or sometimes simply by working out who is talking to who, where and when and about what.

ELINT's purpose, on the other hand, is to receive, locate and identify and sometimes measure and analyse radar signals. Sometimes ELINT missions carry out electronic reconnaissance - simply aiming to compile an electronic order of battle for an enemy, or identifying where particular enemy systems may be deployed. At other times ELINT is a more deeply analytical tool, whose aim is to gather an electronic fingerprint so that particular sensors and systems can be quickly



Staff Sgt. Kristoffer Perez, Cyber Electromagnetic Activities section, 1st Armored Brigade Combat Team, 1st Infantry Division, points toward a nearby objective during the final day of training with his section's new equipment on Fort Riley, Kansas, 6 April 2018.

recognised when they are encountered in the field, and to assess their likely performance and capabilities – sometimes in order to develop more effective countermeasures to the sensors and the weapon systems associated with them.

ELECTRONIC SUPPORT

ES (formerly ESM) systems have the more urgent and more reactive purpose of receiving and recognising signals (and associated threats) so that the information can be acted on immediately. This may mean handing off the data to a defensive countermeasures system or to a more offensive system tasked with jamming or destroying the enemy system. It may mean adding an entity to the Electronic Order of Battle (EOB) and sharing it so that it appears on the digital maps used by all cooperating forces, though many would argue that this is primarily a SIGINT/ELINT function.

Such have been the advances in the contributing technologies of solid-state radio frequency electronics, digital receivers, antennas, software defined radio and computer processing power and information storage capacity, that the latest ES systems have capabilities that overlap with those of ELINT systems – although the way they are used is very different – and they can also

take on some of the roles of traditional Radar Warning Receivers (RWR).

Ideally, an ES system on an aircraft, for example, should be able to recognise the transmissions from a threat radar system, associate it with a hostile platform and weapon system, discern the operating mode it is using, whether that be search and track or weapon guidance, and hand the information off to, for example, a Defensive Aids Suite (DAS) controller to deploy countermeasures and issue the pilot with appropriate manoeuvre advice. It might also hand the information off to a data link for sharing over a tactical network. The problem is that modern radars are so smart and adaptable that countering them is becoming increasingly difficult, an issue that will be discussed in more detail elsewhere in this compendium.

PLATFORM SELF-PROTECTION

The above mentioned DAS, sometimes referred to as a Self-Protection System (SPS) or a countermeasures suite, is a set of integrated sensors, processors and effectors whose primary and usually sole purpose is to protect the platform to which they are attached from threats that exploit the electromagnetic spectrum.

These will include a set of radar warning antennas, probably shared with the ESM

system, a set of electro-optical Missile Launch Detectors (MLD) and/or Missile Approach Warners (MAW) that work in either the ultraviolet (UV) or infrared (IR) portions of the spectrum, or both. Sometimes, small active radar sensors and laser detection systems are used in the MAW role.

These sensors provide information to processors that control jamming transmitters and the launch of patterns of radar-reflecting chaff, and decoys – most likely based on Digital Radio Frequency Memory (DRFM) technology – IR decoy flares or laser-based Directional Infrared Countermeasures (DIRCM).

Naval vessels and, increasingly, armoured vehicles also have such systems, although with different combinations of sensors and effectors and with a growing emphasis on hard-kill countermeasures designed to destroy incoming missiles and projectiles.

The jammers increasingly fitted to ground vehicles and even carried by foot soldiers to block the signals that would otherwise detonate Remotely Controlled Improvised Explosive Devices (RCIEDs) can also be thought of in this way, as can jammers used against Global Navigation Satellite System (GNSS) receivers that may be integrated into, for example, precision guided munitions and UAVs.

ELECTRONIC ATTACK AND CYBER

In the old parlance, most of these systems would be labelled as ECM systems, but now, slightly awkwardly, they are grouped with the Electronic Attack (EA) systems, even though they are arguably defensive in nature.

In airborne systems, EA is usually associated with escort and support jamming systems fitted either to fast jets that accompany strike packages or dedicated special mission aircraft whose task is to protect potentially large numbers of aircraft tasked with penetrating enemy air defences.

On the ground there is an established role for powerful communications jammers that might target enemy deployed headquarters for example, perhaps forcing them onto an unjammed frequency that can be exploited in another way, such as geolocation or even code breaking. There is also an emerging role for jammers that target hostile UAV/drone command links, both on land and at sea.

Although some forces, notably the US Army, consider cyber and EW operations together because they can be used in mutually supportive ways and cyber attacks can be delivered over RF bearers, they are distinct disciplines so this compendium will refer to cyber systems only where they have a direct bearing on EW.



The US Air Force Boeing RC-135V/W Rivet Joint reconnaissance aircraft support theatre and national level consumers with near real time on-scene intelligence collection, analysis and dissemination.

INSIDE THE SHADOWY WORLD OF SIGNALS INTELLIGENCE

What is SIGINT, not to mention ELINT and COMINT? What technology is used in this closed guarded area of defence.

Peter Donaldson

It is difficult to overstate the importance of Signals Intelligence (SIGINT) to a nation's EW effort. If it is not done properly none of the other EW systems will be fully effective, while command authorities will be faced with sending their irreplaceable people and costly platforms into combat with little situational awareness and less protection against threats that exploit the electromagnetic spectrum.

SIGINT is divided into Communications Intelligence (COMINT), which targets adversary communications signals, and Electronic Intelligence (ELINT), whose targets are non-communications RF signal sources, principally radars.

With the growing power of computer and radio technologies, there is a convergence of core capabilities between SIGINT and ES systems, but there are still important differences in the equipment and, more importantly, a fundamental difference in the way they are used.

COMINT deals with the content of enemy communications signals, necessitating decryption and translation before full exploitation. It and supports strategic and high-level tactical decision making whereas Comms ES focuses only on the 'external' characteristics of communications signals: the type and level of modulation and the location of the transmitters. It tells us, in real time who is talking to who, and where, but not what they are saying.

ELINT systems are strategic assets tasked by intelligence agencies to gather information about radars for later use by tactical forces and the analyst-operator's in-depth knowledge is key. ELINT gathers as much data as possible, in order to support detailed analysis, recognising and analysing new threat emitters and their capabilities, as well as modifications or changes to old emitters. Its aim is to gather enough information to determine the detailed capabilities of enemy systems, and precise details of deployment, etc.

By contrast, radar ES (sometimes called RESM) systems are tactical assets (often carried by non role-dedicated platforms) and are tasked by operational commanders with providing information to support immediate force protection and situational awareness. Radar ES systems generally gather only enough data to quickly determine which of the enemy's known weapon systems is being deployed against a target at that moment in time, for immediate tactical application. The location of an emitter is determined with sufficient accuracy only to allow countermeasures or evasion. In some ES systems, unknown (and even known) threats may be recorded for later analysis – but this is really an ELINT function.

In essence, ESM is all about collecting relatively limited information for immediate use - principally warning, while ELINT is a reconnaissance task with tactical application and with a more strategic emphasis. ES systems rely on programmable on-board libraries – the contents of which come from ELINT operations – to identify intercepted signals, the relative bearings of which are then triangulated in order that hostile emitters can be geolocated.

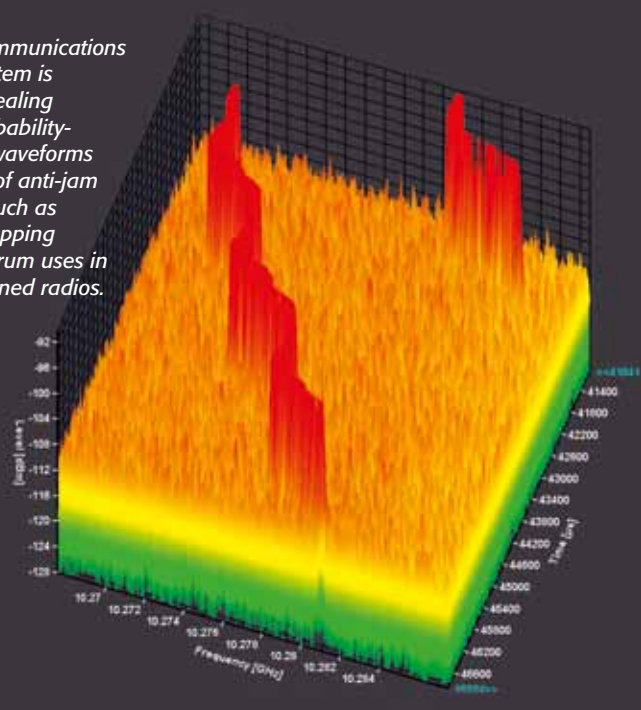
MODERN COMBINED SYSTEMS

Despite the different natures of ELINT and ES operations and the dissimilar skill sets of the respective operators, many modern systems combine these capabilities to a limited extent. Recorders and data links, in theory at least, enable some degree of remote or post-mission ELINT processing of signals collected by an ESM system, while some also boast COMINT and Communications ESM (CESM) while also providing warnings and cueing self-protection systems.

One family of systems that is designed to do all of this by combining modular elements is Elettronica's ELT/819, which is offered for both ground-based and large aircraft applications. As standard, it provides Radio Frequency (RF) spectrum coverage from the C band to the J band with optional extensions at the low and high ends, down to the A band and up to the K band for example. The dual receiver system is designed for high sensitivity, which is a key contributor to a high Probability of Intercept (PoI), along with a large instantaneous bandwidth for the Intermediate Frequencies (IF) into which – like most radio receivers – it converts the incoming signal to enable it to be processed. Elettronica emphasises that the system is capable of operating in dense, complex and unknown electromagnetic scenarios to create an Electronic Order of Battle (EOB) and

The Viper communications jamming system is capable of dealing with low-probability-of-intercept waveforms and the use of anti-jam techniques such as frequency hopping spread spectrum uses in software defined radios.

Rohde & Schwarz



displaying it on a digital map, aided by very accurate angle of arrival measurement.

It identifies emitter types through the automatic analysis of a wide range of signal parameters and modulation types. In the frequency domain, for example, it can cope with fixed, agile, hopping and burst transmissions. By examining Pulse Repetition Interval (PRI) characteristics, it can pick out pulse fixed, jittered, switched, staggered, coded, sliding and stepping PRIs, along with Continuous Wave (CW) signals, which are not pulsed at all. Other pulse characteristics that help identify radar functionality and type include pulse width, amplitude modulation on pulse, pulse modulation on pulse and frequency modulation on pulse. It also identifies a number of scanning patterns including circular, sectoral, track-while-scan, conical and steady.

The ELT/~819 also performs automatic and computer-aided fine analysis at the interpulse (between pulses) and intrapulse (within pulses) levels, and records all the data digitally and facilitates the programming, uploading and downloading of signal libraries.

The technical ELINT and tactical ESM displays are sometimes very different, the former showing an overview of the system's RF spectrum coverage along with selected portions in detail, the latter plotting targets on a map or simply giving an indication of bearing.

TOUGH ELINT CHALLENGE

While ELINT has benefited to some degree from advances in radio antenna, receiver and signal processing technologies, radar

has really taken hold of new technology and run ahead with it. Over the last 15 to 20 years, state-of-the-art radars and the signals they transmit have changed almost beyond recognition, German ELINT and radar ES specialist Rohde & Schwarz (R&S) points out.

Legacy radars used mechanically scanned antennas, simple interpulse modulation techniques and non-solid-state (vacuum tube type) RF amplifiers such as magnetrons and Travelling Wave Tube (TWT) devices. Cavity magnetrons, for example, have individually distinguishable resonances – they can be said to ring like bells but on radio frequencies. These resonances can be used like fingerprints, enabling ELINT analysts to recognise when a particular radar set has received a new magnetron. Legacy radars were also vulnerable to long established Electronic Attack (EA) techniques, and most operated on frequencies between about five and 18GHz.

Today's state-of-the-art radars feature either Passive Electronically Scanned Array (PESA) or Active Electronically Scanned Array (AESA) antenna/transceiver systems, signals with very complex modulations, unpredictable scan patterns and the ability to use different scan patterns simultaneously, multiple beams and multiple frequencies simultaneously. Their RF signal sources, increasingly, exploit solid-state gallium arsenide (GaAs) technology, which is difficult, bordering on impossible to fingerprint and can extend radar frequencies beyond 18GHz. Furthermore, a growing number of modern radars, such as Frequency Modulated Continuous Wave (FMCW) sets, operate at very low power levels, making them harder to detect.

Nigel Lawton, formerly a Royal Navy ELINT operator and mission manager and now ELINT and radar ESM systems product manager for R&S, explains that the radar environment has become much more difficult for ELINT, and by extension for ESM, over the last five to 10 years because such radars are now encountered almost everywhere.

LEGACY ELINT WEAKNESSES

Legacy ELINT systems, Lawton says, are not up to the job of intercepting and analysing the latest radars. Most are amplitude based and are not as sensitive as modern digital systems, he says. For example, systems based on Detector Logarithmic Video Amplifier/Instantaneous Frequency Measurement (DLVA/IFM) technology have a sensitivity of approximately -55dBm and a dynamic range of about 60dB. This, he says, is not enough to detect modern FMCW signals.

Furthermore, many legacy ELINT and COMINT systems employ wideband receivers that use 1GHz filters, which are blocked by high-powered Continuous Wave (CW) radar signals and similarly powerful communications signals. Also, many are not coherent in that they don't make use of IQ data that show the changes in both the amplitude and phase of a wave that are used to encode information on it. Phase information, Nigel Lawton says, is increasingly critical for the analysis of modern radars, as changes in phase often indicate a change in operating mode. "I need to be able to measure the phase on a pulse-to-pulse basis."

Rohde & Schwarz offers what it describes as a cutting edge digital ELINT system with market leading sensitivity (-85dB has been achieved), one that uses IQ data processing techniques for accurate identification and measurement of contemporary modulation techniques. A compact system that integrates the receiver, digitiser and analyser components, it is designed to provide both high sensitivity and a large dynamic range; the former enabling it to detect and process very faint signals and the latter allowing it to cope with both faint and powerful signals at the same time. Meanwhile, the software and user interface facilitate easy and reliable data handling throughout the ELINT cycle, the stages of which are observation, selection, collection, pre-analysis and storage.

The brains of the system are in the WPU500 wideband processing unit, which R&S says contains receiving, digitisation and pulse analysis capabilities in one. This operates over a frequency range of 20MHz to 18GHz, with optional extensions in both lower and higher bands from 8kHz to 40GHz, and covers a real

time instantaneous bandwidth of 500MHz.

EXPERT OPERATORS VITAL

While modern systems have many automatic features, the operators/analysts must still have the expertise and experience to recognise signals of interest when they appear on their screens among other signals and the inevitable noise and clutter. Expertise and experience are necessary if operators are then to select those signals – and only those – for detailed analysis by the software. To enable operators to see these signals, R&S presents them with a visual overview of the spectrum and a representation of the calculated noise level for each channel.

With these visual tools, the operator can decide whether the signal of interest is sufficiently stronger than the noise for the system to generate a meaningful analysis, the required margin being at least 12 to 13dB. Once the operator can see the bandwidth of the signal, they can set the width of the processing channel to match it exactly for analysis. This means that, for a given radar frequency and bandwidth, the system is as sensitive as possible because the noise is thrown away in the selection process.



Peter John Acklam

The Norwegian Navy's FS Marjata is an example of a purpose built naval electronic intelligence (ELINT) collection vessel.

FUTURE SHOCK

The future looks even more challenging. The resurgence of VHF long-range early warning radar with anti-stealth capabilities continues, while more short range – and therefore hard to intercept – gun and missile control radars exploit the 33 to 36GHz K-band window. Low power and solid-state radars proliferate

along with radars that use advanced and hard to unravel modulation techniques such as polyphase coding, a subject about which ELINT specialists could learn much from their COMINT cousins, according to Lawton. What the effect of exotica such as artificially intelligent cognitive radar will be is, as yet, unknown.

Total mission protection through full spectrum dominance

Leonardo has saved lives for over 100 years using the electro-magnetic spectrum, with equipment trusted to inform and protect aircrew worldwide. A market leaders in EW, Leonardo supports its customers to get the most out of their equipment; also providing advice and training in all areas of the EW, ESM and countermeasure life-cycle.

Inspired by the vision, curiosity and creativity of the great master inventor – Leonardo is designing the technology of tomorrow."

70
1948 • 2018

CS-3030 subsystems consists of omni and high gain direction finding (DF) antennas, receivers, signal processors and operator workstations and may be used for ELINT or ESM applications.



WARNING OF ELECTROMAGNETIC THREATS

ESM systems provide commanders and platform crews with a constantly updated picture of all electromagnetic signals in the battlespace, highlighting and identifying the threats in order to provide tactical warning and to cue appropriate countermeasures.

Peter Donaldson

Informed by ELINT, Electronic Support Measures (ESM) systems are operational assets whose role is to provide timely answers to crucial questions about the electromagnetic environment. They give force commanders and individual platform crews a detailed picture of signals and emissions, identifying and locating their sources and helping to work out what

their intentions are and whether they represent a threat. ESM will identify any weapon systems associated with a particular signal, and will flag up what they are doing, based on the operating modes that are discernible from the behaviour of that signal.

URGENT PURPOSE

ESM also has a more urgent purpose in helping

forces to identify, prioritise and respond to threats in real time. This means that it must work entirely automatically, putting detected, geolocated and identified emitters onto digital maps for operators with responsibilities broader than EW, and at platform level cueing integrated defensive aids suites and electronic attack systems. Whereas SIGINT tends to be the prerogative of dedicated platforms, ESM



A 360° PARTNER

ELECTRONIC WARFARE
 CYBER EW
 INTELLIGENCE
 EDUCATION & TRAINING



Saab's ESTL self-protection pod fits missile interfaces on high-performance aircraft and support modular sensors and effectors, while MIL-STD-1553 or RS-485 data links enable integration with ESM systems and EW controllers.

equipment is commonly carried by aircraft tasked with quite different primary roles.

The miniaturisation of receivers and processing equipment has made the use of ESM systems practical on more platforms, with UAVs and other unmanned systems prominent among them, so that their information gathering capabilities now permeate the battlespace.

Antennas, receivers, processors and –

crucially – databases are key components of an ESM suite, which is essentially a radio receiver that measures signals and compares them against a database containing previously analysed signatures. Requirements include 360 degree hemispherical or – for aircraft – spherical coverage, high sensitivity to detect low power signals, sufficient selectivity to separate the signals it wants from those that it doesn't, and a high Probability of Intercept (PoI).





IAI Elta's ELL-8385 is a 30kg ESM/ELINT system designed for use on IAI's Heron UAV and comparable vehicles.

CERTAINTY OF INTERCEPTION?

A full 360 degree of coverage is typically provided through the use of multiple staring antennas with overlapping coverage volumes. A PoI of 100 percent is routinely claimed by suppliers, but rarely defined. In a nutshell it is the probability that the ESM system will detect a particular threat signal between the time it reaches the system and the time at which it is too late for the system to do its job. That PoI figure applies to each signal on a threat list under specified set of conditions that define a scenario and a time limit. The threat list is in the ESM system's database, without which it is of little use. If a particular emitter is not in the database, the ESM system won't recognise it.

These databases are sovereign intelligence assets that do not come with the equipment, but have to be created through collection and analysis by ELINT operators or by other intelligence means. This is why leading ESM system suppliers, Leonardo for example, make a point of offering EW Operational Support (EWOS) packages including training, to enable nations to populate their threat databases and keep them up to date.

Nigel Lawton, ELINT/RESM systems product manager for Rohde & Schwarz, is emphatic. "Until an ELINT operator goes out, intercepts that radar, analyses it and stores it in his database, the ESM guy does not have any data for his onboard library."

He stressed that the systems need high quality data about what a radar is doing on a pulse-by-pulse basis, which means collecting a lot of data.

SIMILAR TECH, DIFFERENT MISSIONS

Despite the overlap in capabilities in modern

systems that are marketed as both ELINT and ESM systems, the two types of operation are very different. While an ELINT collection mission will often have a very specific target in mind, perhaps a new surface-to-air missile system and its associated radars and communications links, for example, ESM contributes to all-round situational awareness during missions of all kinds. Both can be used for both immediate threat recognition (the primary function of ESM) but also to support the kind of detailed analysis required for longer-term operational planning (a handy definition of SIGINT's main purpose). Naturally, SIGINT aircraft platforms also need an ESM system to help the crew maintain situational awareness while the specialists on board focus their equipment on the target radar or communication system.

BROADER PLATFORM BASE

Miniaturisation has brought very capable ESM systems to a broader range of platforms, including tactical UAVs, enhancing their ability to contribute to force situational awareness. For example, IAI Elta's ELL-8385 is a 30kg ESM and ELINT system that draws 400W of power and is designed for use on IAI's own Heron and comparable vehicles.

Leonardo's SAGE is another example. This 20 kg basic system is scalable for different platform sizes, from UAVs and helicopters to large maritime patrol aircraft. With frequency coverage from 0.5 to 40GHz it covers the upper extension into the K band but not the low end VHF "anti-stealth" radars that are increasingly widely available. As a communications ESM system, it can detect and characterise signals from VHF frequencies of 30 to 300MHz up to the 1 to 2GHz D band.

Leonardo emphasises its ability to

geolocate targets from a single platform, which enables accurate sensor cueing at what it calls tactically significant range, thanks to a claimed Direction Finding (DF) accuracy of 1 degree RMS. It is also designed to identify and characterise complex emitters while also providing an advanced radar warning capability, with the aid of an emitter library that can hold up to 16,000 mode lines.

In characterising the radar, it can recognise and exploit a wide range of Pulse Repetition Frequency (PRF) schemes, including fixed, jittered, slide, stagger, random stagger, drift batch, irregular and nets, for example. It can also measure pulse widths from 50 nanoseconds right up to CW, along with pulse width agility schemes including fixed, agile and agile discrete.

SHARED TECHNOLOGIES

As the core technology in ELINT, ESM and Radar Warning Receiver (RWR) systems is increasingly shared, in spite of the operational differences, industry offers tailored combinations of modules and operational software for different roles. One such product is the BOW family from Saab, which forms the basis of a number of systems including the Electronic Warfare Core System (EWCS) aboard the swing-role Gripen fighter.

The Gripen's BOW is described as an advanced radar warning system and is integrated with a high performance RF jammer to form the EWCS. The wing tip unit contains the antennas and receiver front-end for the E to J bands (two to 20GHz) and the K/L bands (20 to beyond 40GHz). With spare capacity for growth, the electronic warfare central unit contains the wideband and narrowband receivers for E-J Band, as well as the pulse processor, the radar warning/EW

computer and aircraft interfaces.

Modern ESM systems need wideband receivers for threat warning, and BOW uses an Instantaneous Frequency Measurement (IFM) receiver for this. IFMs cover the necessary wide frequency range, offer good sensitivity and selectivity and, as the name suggests, measure the frequency of received signals with useful accuracy – Saab quotes 5MHz.

The wideband IFM is coupled with tuneable narrowband receiver for detection of weak signals at longer range, better selectivity in dense signal environments, better measurement performance for more demanding applications, such as detailed parametric analysis of CW signals. Saab quotes an accuracy of 1MHz for the narrowband receiver, a super-heterodyne device. Such receivers are very flexible and provide very high sensitivity thanks to their pre-detection bandwidth and post-detection processing gain.

The narrowband receiver continuously searches by scanning through the frequency range available to it, but the chances of coming across a particular signal of interest this way is low, so it can also be cued by the wideband receiver or by external systems that tell it where to look.

UNBLOCKING RECEIVERS

A major challenge with wideband ESM receivers is dealing with blocking, says Nigel Lawton, a problem that occurs when, for example, an AESA radar transmits two pulses simultaneously. The receiver processes the peak power/amplitude at an instant in time, meaning that the more powerful of the two pulses is processed but if their relative power changes the receiver will switch to processing the other pulse, so that the processed waveform that comes out of the receiver will not be representative of either.

Multiple signals from different emitters on the same frequency can also block wideband ESM receivers, which is a major problem with all the civil, commercial and private wireless communications systems around harbours, for example. However, R&S has a solution for this from an ELINT perspective using a two-stage detection process involving visual pre-detection of signals in the spectrum overview and by matching the processing bandwidth to the bandwidth of the signal, as described in the SIGINT section.

R&S is now in the process of creating an ESM system that makes use of its latest ELINT capabilities to give operational forces a better

chance of success and survival in the modern electromagnetic environment.

DISRUPTIVE FUTURE

Another vision of the future of such systems is represented by the Disruptor SRX technology under development by Harris, which takes the idea of multi-function systems such as those that can be used in ELINT, ESM and RWR roles and radically extends it. Disruptor SRX is touted as a platform-agnostic, software defined system in multiple form factors that is able to switch between ELINT, ESM, electronic protection, communications jamming and electronic attack, in real time and according to mission need.

One of its key promoted capabilities involves radically compressing the ELINT-to-ESM cycle, which with current technology can take months of potentially dangerous collection and analysis work to completely characterise one new radar. Based on a few measurements of signals from a previously unknown emitter, Disruptor SRX is intended to decide in real time whether it is a threat or not, and even create a countermeasure on the fly. This is an application of artificial intelligence sometimes referred to as cognitive EW and will be one to watch.

Under the Management and Responsibility of Turkish Armed Forces Foundation

Eurasian Meeting

IDEF'19

14th International Defence Industry Fair

April 30 - May 3, 2019

www.idef.com.tr

TÜYAP
www.tuyap.com.tr



The Laser Weapon System (LaWS) technology demonstrator temporarily installed on the destroyer USS Dewey. Built by the Naval Sea Systems Command from commercial fiber solid state lasers, it can be directed onto targets from the radar track obtained from a MK 15 Phalanx Close-In Weapon system or other targeting source.

DEFENSIVE AIDS – THE FINAL LINE OF DEFENCE

With ever-more-sophisticated guided missiles, active and passive countermeasures face a progressively more difficult task, and increasingly rely on being integrated within advanced defensive aids systems.

Peter Donaldson

To cope with the full range of threats to military platforms, Defensive Aids Suites (DAS) have to be integrated systems that detect, identify and respond in real time, often within fractions of a second. Most threats exploit the electromagnetic spectrum for guidance, usually in the radar or optical/infra-red bands, and this provides an opportunity for effectors to disrupt the process.

Stealth aside, the technologies relied upon to protect against radar guided threats are chaff, decoys and jammers, all of which rely on detection of the threat radar and recognition of its operating mode to trigger the most appropriate response.

Ranging from long strips of metallic foil

to myriad short fibres, chaff is cut to length to match the wavelengths of the threat radars and serves to mask the platform or even an entire formation from search, tracking and weapon guidance radars and active missile seekers. With aircraft it is usually deployed in pre-programmed patterns from dispensers around the airframe, while ships often rely on rockets to deploy large, persistent chaff clouds to fool threats.

DRFM DECOYS

The go-to technology for radar jamming is Digital Radio Frequency Memory (DRFM), which records and stores intercepted threat radar signals and retransmits them with a delay and/or some kind of modulation to

prevent a radar from achieving a lock on the platform or to break that lock if it has been achieved.

One of the most innovative uses of DRFM jamming technologies has been Leonardo's packaging of DRFM hardware into its BriteCloud expendable active radar decoy, which is designed to be deployed from standard chaff/flare dispensers on fixed-wing aircraft, including fast jets, to minimising the requirement for greater integration with the platform.

The battery-powered device comes in two sizes that respectively fit into circular and rectangular cells in different types of launcher, these being the BriteClouds BC55 and BC218. The 1.1kg BC55 measures 55mm in diameter,

while the 0.5kg BC218 is 2in wide, 1in high and 8in long, and both cover the H to J radar bands (6 to 20GHz) used by surface-to-air and air-to-air missiles. The company emphasises that BriteCloud eliminates the 'home-on-jam' vulnerabilities of on-board jammers, and that its very quick deployment creates a large miss distances.

Jamming hardware can be semi-permanently integrated into a vehicle, or jostling for space with other RF emitters and receivers on the masts or superstructure of a warship, or in the fuselage of an aircraft. Alternatively jammers can be housed in more self-contained accommodation in a pod suspended from an aircraft's wing or belly. It can even be incorporated into towed, ejected or rocket-launched decoys, the latter including the BAE Systems Nulka hovering rocket decoy/seduction jammer.

In October 2016 the destroyer USS *Mason* fired a Nulka and three surface-to-air missiles (two SM-2 Standards and an Evolved Sea

Sparrow) to defend itself and the amphibious transport USS from two suspected cruise missiles reportedly fired by Houthi rebels at the ships, which were in the Red Sea off the coast of Yemen. Both incoming missiles struck the water, one reportedly without being hit. It is not clear whether the other was hit, but it is possible that both were sent off course by the Nulka.

EXPLOITABLE SIGNATURES

Detecting threat missiles doesn't exclusively rely on their radar emissions as they have other exploitable signatures. Missile launch detectors typically rely on the ultraviolet component of the weapon's rocket motor exhaust, with the latest systems being "solar blind" to prevent confusion from reflections of the sun on water.

There is also an infra-red component to the rocket motor signature, while missile airframes heat up through air friction and rocket motor combustion, which infra-red

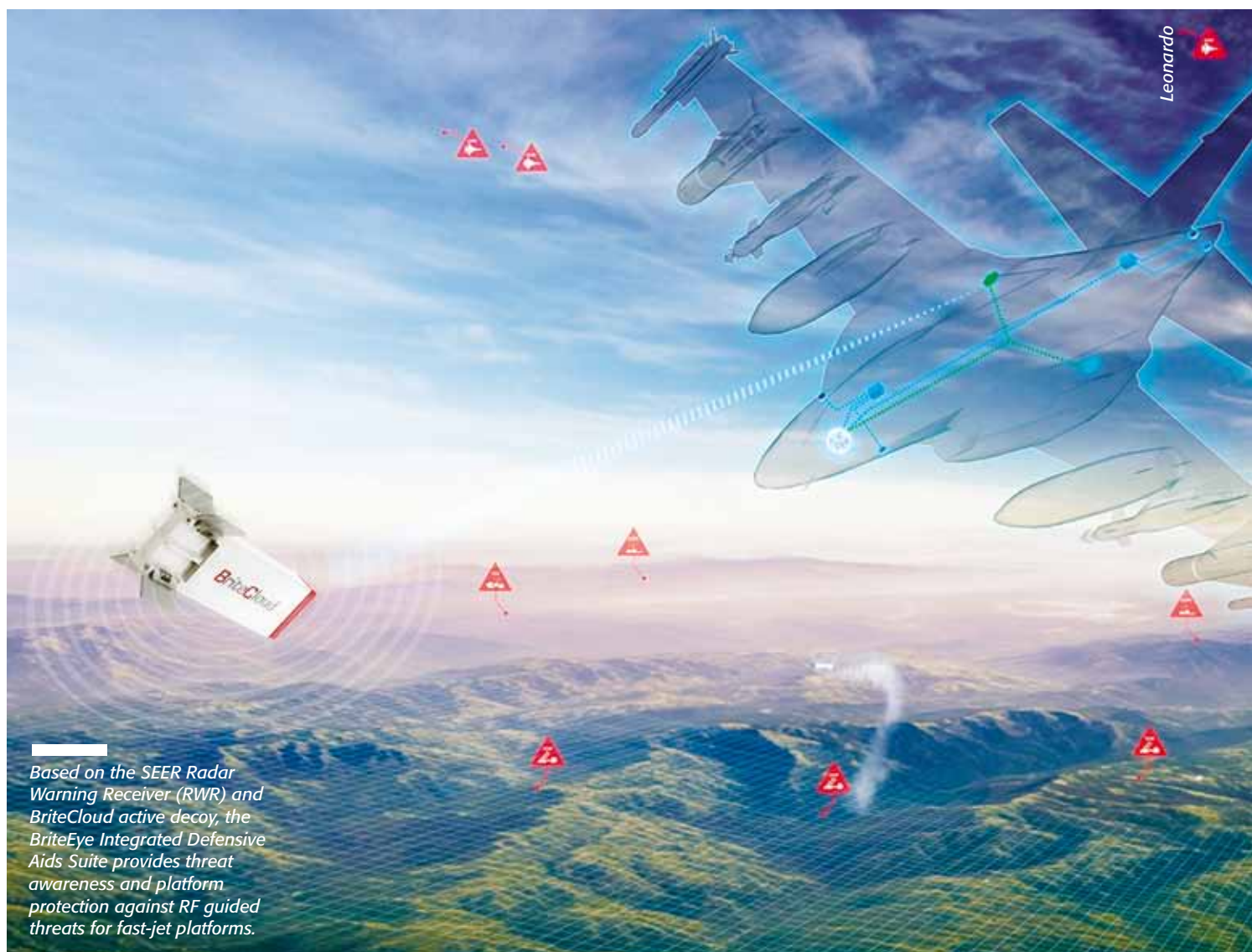
missile detectors and approach warning systems can exploit.

The latest IR homing missiles use imaging seekers that can choose the most vulnerable spot to strike. Defences against them can be divided into decoy flares and jammers that transmit modulated IR radiation to disrupt the seeker's tracking logic.

IR decoys have evolved from simple, individual, manually-fired flares, to automatically-fired patterns of flares, whose use is accompanied by carefully-calculated evasive manoeuvres. The flares themselves are carefully engineered to emit the most effective spectra, some emitting IR only to preserve covertness, and have precisely-controlled rise and burn times. They often share dispensers with chaff cartridges, both supplied by a range of companies including Chemring, Esterline and Lacroix.

JAMMING WITH LASERS

IR jammers began as omnidirectional devices,





Iron Fist detects, tracks, and neutralises anti-tank rockets, anti-tank guided missiles, kinetic energy and high explosive anti-tank (HEAT) rounds with two layers of active protection.

with modulation controlled by revolving shutters. They later evolved into directional jammers that target the missile seeker with a focused and encoded beam of IR light and, more recently, using encoded lasers that increase the Jamming-to-Signal (J/S) ratio by putting more energy into the missile seeker. Known as Directional Infra-Red Countermeasures (DIRCM) systems, they rely on missile launch detectors/approach warners to cue their fine tracking sensors that aim the laser. Leading developers of DIRCM technology include BAE Systems, Elbit Systems, Elettronica Leonardo, Northrop Grumman and Lockheed Martin.

Elettronica's ELT/572 is an example of one of the latest generation of these systems. It is claimed to be effective against the latest generation of IR-guided SAMs, and is based on fibre-laser technology. ELT/572's three main modules are the mirrored turret, the laser generator unit and the electronic unit. Two of them can be controlled by a multi-turret manager module and each can cope with multiple simultaneous threats, says the company.

SOFT-KILL, HARD-KILL

Platform defensive measures can also be divided into soft-kill and hard-kill varieties. Soft-kill measures seek to make the incoming weapon miss the target, while hard-kill measures try to shoot it down.

Hard-kill measures are long established aboard warships and consist of medium/long range missiles, point defence missiles and their associated sensors and control systems. In some cases, these are the principal missile systems of a warship.

The latest generation of Russian and Chinese supersonic anti-ship missiles are a major challenge to soft-kill systems because the window in which they can be detected and countered is so short and their radars are hard for ESM systems to detect, while some have additional passive electro-optical and/or IR seekers that transmit nothing. This means that hard-kill defences are likely to be increasingly essential to counter these weapons.

VEHICLE PROTECTION

Armoured vehicle DAS evolution is following a similar trajectory to that of ships, with the additional need to defend against Remotely Controlled IEDs (RCIEDs), which can be triggered by a wide range of RF devices including cellphones. RCIED jammers have become essential equipment on vehicles deployed to war zones, spawning a vast new industry which includes specialists such as Bombjammer and Shoghi plus international multi-technology defence companies such as Airbus, Cobham, Elbit, Harris, Hensoldt, Leonardo, L-3, Northrop Grumman and more. The most advanced are software-defined "smart jammers" that provide protection while leaving friendly and neutral communications unaffected.

Early vehicle countermeasures centred on the use of smoke dischargers and smoke grenade launchers. These were used to mask the vehicle or a formation of vehicles from threats that used optical tracking to aim or guide guns, rockets or missiles.

The next step beyond that was infra-red jammers that targeted the optical/infra-red goniometers (precise angle measurement

devices) used to track the flares in the tails of command-to-line-of-sight missiles, which rely on steering commands from the launcher sent down a wire or over a radio link.

As the latest generation of anti-tank guided missiles (ATGM) is increasingly difficult to jam, while rocket propelled grenades and unguided projectiles from tank guns are fundamentally unjammable. Hard-kill solutions tend to involve tracking them with radars and cameras then deflecting or destroying them with interceptor munitions or directional explosive charges.

The best known of these systems is the combat proven Trophy, developed by Rafael and IAI/Elta and offered in two variants. One version is tailored to heavy and medium armoured vehicles, the other is intended for light armoured vehicles. Both variants detect and track incoming projectiles, RPGs and ATGMs with small solid-state radar sensors. The heavy version destroying these with explosively formed projectiles, the lighter version using downward firing 'energetic blade' charges.

FUTURE DIRECTIONS

In an effort to match Israeli achievements in vehicle Active Protection Systems (APS), the UK MoD initiated the Icarus technology demonstration programme in 2017. It chose Leonardo to lead a team of UK companies and academic institutions including BAE Systems, Lockheed Martin UK, Ultra Electronics, Frazer-Nash, Vetronics Research Centre, Abstract Solutions, Roke Manor Research and SCISYS.

One of the programme's primary objectives is to develop and demonstrate a UK sovereign electronic architecture for a Modular, Integrated Protection System (MIPS) that enables "best of breed" APS sensors and countermeasures to be selected, integrated and deployed across the British military vehicle fleet.

Lasers have already proved their worth in soft-kill countermeasures in the form of DIRCM systems, and the growing capabilities of threat missiles means that they are also likely to play an important part in the future of hard-kill defensive systems. Lasers that can kill incoming missiles, inevitably, must be much more powerful than those designed to jam seekers, but after a series of successful demonstration programmes in the US, Germany, the UK and Israel in particular, such high energy lasers are looking increasingly mature, in shipboard and ground-based use at least. The next challenge is to make them light, compact and power-frugal enough for tactical aircraft.



INDO DEFENCE 2018 EXPO & FORUM

INDONESIA'S NO.1 OFFICIAL TRI-SERVICE DEFENCE, AEROSPACE, HELICOPTER AND MARITIME SECURITY EVENT

"BUILDING GLOBAL DEFENCE PARTNERSHIPS TO SECURE THE FUTURE"

INDO
AEROSPACE
2018 EXPO & FORUM

featuring
INDO
HELICOPTER
2018 EXPO & FORUM

INCORPORATING WITH
INDO MARINE
2018 EXPO & FORUM

*Make sure you don't miss out on
a prime position at 2018 by reserving
your space TODAY!*

CONTACT:

LOCAL INDUSTRY (INDONESIA)

MS. LISA RUSLI

Project Manager

M : +62 815 1822 716

E-mail : yulisa@napindo.com

INTERNATIONAL

MS. ERIKE BRIGITHA MALONDA

Project Manager

M : +62 815 9254 215

E-mail : erike@napindo.com

7 - 10 NOVEMBER 2018 | JAKARTA INTERNATIONAL EXPO KEMAYORAN, INDONESIA

www.indodefence.com | info@indodefence.com

OFFICIAL PUBLICATION
AND SHOW DAILY



OFFICIAL ONLINE PUBLICATION



OFFICIAL ONLINE SHOW DAILY
NEWS AND WEB TV



ORGANISED BY



PT NAPINDO MEDIA ASHATAMA
Tel: +62-21 865 0962, 864 4756 / 85
Fax: +62-21 865 0963
Email: www.napindo.com

[f Indo Defence Expo & Forum](https://www.facebook.com/IndoDefenceExpo)
[@IndoDefence](https://twitter.com/IndoDefence)

SUPPORTING PUBLICATIONS





Royal Australian Air
Force Boeing EA-18G
Growler electronic
attack aircraft.

BLINDING THE ENEMY – WITH SCIENCE!

Previously known as Electronic Counter Measures, Electronic Attack uses electromagnetic energy, directed energy, or anti-radiation weapons to attack enemy personnel, facilities, or equipment.

Peter Donaldson

Electronic Attack (EA) uses the transmission of radio frequency energy to disrupt the operation of other radio frequency systems. This is the essence of jamming, whether it is part of a radar or a communications system, and the purpose of which is to ensure that the receiver does not get the signal it needs. Like the other branches of electronic warfare, EA is evolving to counter smarter threats.

Classic applications include airborne escort jamming, a role in which aircraft accompany a strike package, carrying powerful jammers to blind the radars upon which enemy integrated air defence systems rely to mask the approach of the formation.

An alternative approach is used in stand-off jamming, where a larger aircraft with greater endurance will target air defence radars and their communications links from outside the engagement envelopes of enemy air defence systems. For these applications, ESM systems with very accurate geolocation capabilities are essential because the jamming power must be concentrated in relatively narrow beams to ensure that they can put sufficient jamming power into the target receivers at long range.

ESCORT/SUPPORT JAMMERS ADVANCE

While the best known of these jammers is the Northrop Grumman AN/ALQ-99, a podded

system that has been through many upgrades over several decades of service on platforms such as the EA-6B Prowler and subsequently the EA-18G Growler, it is due for replacement by the AN/ALQ-249 Next Generation Jammer (NGJ) that is designed to provide 10 times the power and handle four times the number of assignments. The NGJ is intended to provide EA capability that is more precise and powerful and with faster reactions and greater directivity, using Active Electronically Scanned Array (AESA) transmitters – akin to those in AESA radars – to create agile jamming beams.

In 2013, the US Navy chose Raytheon to lead the first increment of NGJ development

– the mid-band system – beating the ALQ-99's prime Northrop Grumman, which is reportedly targeting the low- and high-band increments that will be developed later to deal with emerging threats.

Investments planned for fiscal year 2019 are focused on the production of gallium nitride monolithic microwave integrated circuits and wideband circulator technologies. Both are essential for cutting edge AESA systems, the first in components such as transmit/receive elements, the second in all high-power microwave systems and antenna networks in which energy must be directed and isolated.

Saab is in the late stages of development of a podded escort and support jamming system for the Gripen E and other fast jet platforms. Developed with the same core technology as the Arexis EW system integrated internally into the Gripen E, the system is designed to screen the approach and departure of entire strike formations against low-frequency anti-stealth radars. The core technologies are ultra wideband digital receivers and DRFM (Digital Radio Frequency Memory) devices, gallium nitride solid-state AESA transmitters and interferometric direction finding systems.

EA against low-frequency radars requires very high power, and the equipment is too bulky and heavy to be integrated permanently

into a tactical fast jet, so it has been podded to make it a role-specific solution, says Saab, with self-contained power generation in the pods. It is designed to defeat these radars with DRFM-based jamming techniques such as smart noise, coherent false targets and saturation techniques. Two pod-equipped strike fighters can protect an entire formation, said Petter Bedoire, sales and marketing VP for the company's EW and surveillance systems business.

He told the author that to jam these surveillance radars effectively, attacking the main lobes is not sufficient and that the side lobes must also be jammed. "That means we need a lot of power, and that is why we have used two pods, because they are on different frequency bands, one covering the VHF and the other the UHF L-band."

Petter Bedoire wouldn't go into the sensitive subject of how to tell whether the aircraft is in the main beam or the side lobe of the radar it wants to target, as that's where the company believes it has an edge, but he emphasised that the use of two aircraft equipped with the pods is important.

"You can use smart coordination of jamming techniques that can overcome the side lobe suppression algorithms in modern radars."

ATTACKING FREQUENCY HOPPERS

One of the most demanding aspects of EA against communications systems is jamming the most modern equipment in dense EM environments. Such equipment includes software defined radios with Low Probability of Intercept (LPI) waveforms using high-speed Frequency Hopping Spread Spectrum (FHSS) techniques.

Guido Schwarzer, R&S product manager for COMINT/EW systems, explained that all communications jamming has three goals. The first is to interrupt or interfere with the enemy's communications links to temporarily disable their C4ISTAR capabilities, the second is to screen or camouflage friendly C4ISTAR assets against enemy COMINT/CESM, with broadband noise, for example, while the third is to deceive the enemy, perhaps by re-transmitting or imitating their signals.

For jamming to be effective, the signal strength from the jammer must be higher at the target receiver than the signal from the transmitter that it wants to receive. The relative signal strength of the jamming signal and the desired signal at the target receiver is known as the jamming margin or J/S ratio, and depends on many parameters including the power of the two transmitters and their distances from the target receiver.



Rohde & Schwarz

Frequency Modulated Continuous Wave (FMCW) radars transmit very low power signals that are hard to distinguish from noise, but the latest ELINT systems are sensitive enough to look into the spectrum before processing the signal.

Achieving this against radio systems that use FHSS techniques is hard because they switch carrier frequencies very rapidly and they use pseudo-random hop sequences. Key parameters of these schemes are the range of frequencies over which they hop (the hop range), channel spacing, the number of channels they use, hop length and bandwidth and their modulation and error correction schemes. Additionally, they use self-organising networks and automatic back-up links.

The legacy approach to attacking them involves wideband noise or barrage jamming, but this cannot achieve a large enough J/S ratio because the jamming energy is spread over a broad spectrum, while the transmitters in the target system can concentrate their energy at specific frequencies. Target radios also have effective error correction capabilities and use anti-jam waveforms. Also, barrage jammers are easy to detect and inevitably affect friendly and neutral comms with so-called collateral jamming.

Today, the mainstream approach to attacking FHSS radio systems relies on narrowband follower jamming. In turn, this typically depends on a monitoring receiver and spectrum analyser, narrowband processing in a PC, which loses time in processing and format conversion. The computer then commands an exciter to generate jamming signals, with more latency and frequency settling time before sending the jamming signals to a power amplifier and an antenna for transmission. Additionally, these systems are limited in hop rate to about 300 to 500 hops per second and have no multi-target capability, says R&S.


TARGETED COMMS EA

The company calls its alternative approach targeted comms EA. This uses a combination of wideband monitoring and detection and narrowband jamming. It also incorporates ultra-fast wideband digital IQ baseband signal processing and parallel jamming signal generation, with an emphasis on a very fast jamming response. The system is designed to keep the processing time as short as possible. This is achieved by carrying out the target signal detection and identification, and the generation of the jamming signal, in a single unit, Guido Schwarzer said.

This is the integrated wideband detector and exciter unit, which uses Field Programmable Gate Array (FPGA) chips to carry out ultra-fast wideband digital IQ baseband signal processing and parallel generation of the jamming signal. Unpacking this a little, FPGAs can have their circuitry configured to carry out specific jobs, so they do those jobs faster than a general purpose processor would, IQ refers to the phase and amplitude characteristics of a signal, while the baseband is the original frequency range of a transmitted signal before modulation. Amplitude, frequency and phase are the three basic parameters of any RF signal that can be changed (modulated) to carry information, so being able to measure them all, practically instantaneously, is crucial to understanding and countering it.

R&S claims that there is virtually no time loss in this system, enabling the wideband monitoring receiver to find the frequency in use by the target radio, set the narrowband jammer onto it, stop the jamming at regular but tiny intervals to make sure the target signal is still there – this is look-through jamming – and if it has moved it starts the search-to-jam cycle again. This multi-pulse approach ensures that every target hop will be jammed multiple times, says the company, while friendly/neutral comms remain unaffected thanks to the use of the Joint Restricted Frequency List (JRFL).

These capabilities have been embodied in the company's new ground-based Viper system, which is integrated into trucks and shelters.

Although major military forces, including the US Army, have established a philosophy of integrating cyber and EW operations, they are fundamentally different but potentially complementary. Jammers, as radio transmitters, are fully capable of transmitting cyber attacks, but this is not as reliable a means of attacking either a comms system or a radar as jamming because it relies on exploiting uncorrected vulnerabilities in enemy systems. Knowledge of these is hard to obtain and their value can be fleeting as they are quickly patched. In contrast, once the operating principles of target radars and communications systems are understood, Electronic Attack methods will remain effective for much longer. 



ON THE COVER: An EA-18G Growler, assigned to the Cougars of Electronic Attack Squadron (VAQ) 139, flies over the flight deck of the aircraft carrier USS Theodore Roosevelt (CVN 71). (US Navy)

Electronic Warfare Compendium
Supplement to **ARMADA** Issue 3/2018
Volume 42, Issue 3, June/July 2018

ARMADA

is published bi-monthly by Media Transasia Ltd.
Copyright 2012 by Media Transasia Ltd.
Publishing Office: Media Transasia Ltd.,
1603, 16/F, Island Place Tower, 510 King's Road, Hong Kong

Editor: Andrew Drwiega
Chairman: J.S. Ubersi
President: Egasith Chotpakditrakul
Chief Financial Officer: Gaurav Kumar
General Manager: Jakhongir Djalmetov
International Marketing Manager: Roman Durksen
Digital Manager: David Siriphonphutakun
Sales & Marketing Coordinator: Wajirapran Punyajai
Graphic Designer: Khakanaa Suwannawong
Production Manager: Kanda Thanakornwongkul
Circulation Assistant: Yupadee Seabea

Advertising Sales Offices

■ **FRANCE/SPAIN**
Stephane de Remusat, REM International
Tel: (33) 5 3427 0130
E-Mail: sremusat@rem-intl.com

■ **GERMANY**
Sam Baird, Whitehill Media
Tel: (44-1883) 715 697, Mob: (44-7770) 237 646
E-Mail: sam@whitehillmedia.com

■ **TURKEY / EASTERN EUROPE / UK**
Zena Coupé
Tel: +44 1923 852537, zena@expomedia.biz

■ **NORDIC COUNTRIES/ITALY/SWITZERLAND**
Emanuela Castagnetti-Gilberg
Tel: (46) 31 799 9028
E-Mail: emanuela.armada@gmail.com

■ **RUSSIA**
Alla Butova, NOVO-Media Ltd,
Tel/Fax: (7 3832) 180 885, Mob: (7 960) 783 6653
Email: alla@mediatransasia.com

■ **USA (EAST/SOUTH EAST)/CANADA (EAST)**
Margie Brown, Blessall Media, LLC.
Tel: (+1 540) 341 7581
Email: margiespub@rcn.com

■ **USA (WEST/SOUTH WEST)/BRAZIL/CANADA (WEST)**
Diane Obright, Blackrock Media Inc
Tel: (+1 858) 759 3557
Email: blackrockmediainc@icloud.com

■ **ALL OTHER COUNTRIES**
Jakhongir Djalmetov
Tel: +66 2204 2370, Mob: +66 81 6455654
Email: joaha@mediatransasia.com
Roman Durksen, Tel: +66 2204 2370, Mob: +66 9 8252 6243
E-Mail: roman@mediatransasia.com

Annual subscription rates:

Europe: CHF 222 (including postage)
Rest of the World: USD 222 (including postage)
Controlled circulation: 25,118 (average per issue)
certified by ABC Hong Kong, for the period
1st January 2016 to 31st December 2016.

Printed by Media Transasia Ltd., 75/8, 14th Floor,
Ocean Tower II, Soi Sukhumvit 19, Sukhumvit Road,
Bangkok 10110, Thailand.

Tel: 66 (0)-2204 2370, Fax: 66 (0)-2204 2390 -1

Subscription Information: Readers should contact the following address: Subscription Department, Media Transasia Ltd., 75/8, 14th Floor, Ocean Tower II, Soi Sukhumvit 19, Sukhumvit Road, Bangkok 10110, Thailand. Tel: +66 2204 2370 Fax: +66 2204 2387
Email: accounts@mediatransasia.com

www.armadainternational.com

I INDEX TO ADVERTISERS

INDO DEFENCE	15	LIMA	COVER 4
IDEF	11	MODERN DAY MARINE	COVER 3
ELETRONICA	9	ORBITAL ATK	COVER 2
LEONARDO	7		



MODERN DAY MARINE®

**SEPTEMBER 25-27, 2018
QUANTICO, VA**

Come See The Future!

300+ displays, product demonstrations and industry briefings covering the latest in emerging military equipment, vehicles, technology and training systems.

NEW! DEMONSTRATION ZONE OF TACTICAL TASKS AND GROUND SYSTEMS

To showcase your products and services, please contact:

Jaymie Nielsen at 980.328.8801 or jaymie.nielsen@emeraldexpo.com

Sponsored by



Marine Corps League

Register to attend or learn more at marinemilitaryexpos.com

FOLLOW US:



Facebook:
facebook.com/moderndaymarine



Twitter:
[@moderndaymarine](https://twitter.com/moderndaymarine)

Show is not open to the general public. Appropriate attendees include U.S. military, law enforcement, industry and consultant representatives. Foreign military and student organizations are also welcome with prior registration.



THE LANGKAWI INTERNATIONAL MARITIME & AEROSPACE EXHIBITION

The essential platform to showcase best-in-breed emerging technologies and equipment. Secure your space now. Don't miss it.

26-30 March 2019
Langkawi, Malaysia
#LIMA19

Supported by :



Government of Malaysia



Ministry of Defence



Ministry of Transport



Malaysian Armed Forces



Royal Malaysian Navy



Royal Malaysian Air Force



Malaysian Army



Royal Malaysia Police



Malaysian Maritime Enforcement Agency



Malaysia Industry Council for Defence, Enforcement and Security

For more information please contact



EN PROJECTS (M) SDN BHD

Suite 2.02, Level 2, Wisma E&C, No 2, Lorong Dungun Kiri, Damansara Heights, 50490 Kuala Lumpur MALAYSIA.

T: +603 2011 7233

F: +603 2011 7235

E: sales@limaexhibition.com

Connect with us



fb.com/lima.langkawi



@lima_exhibition



@LimaExhibition



www.limaexhibition.com