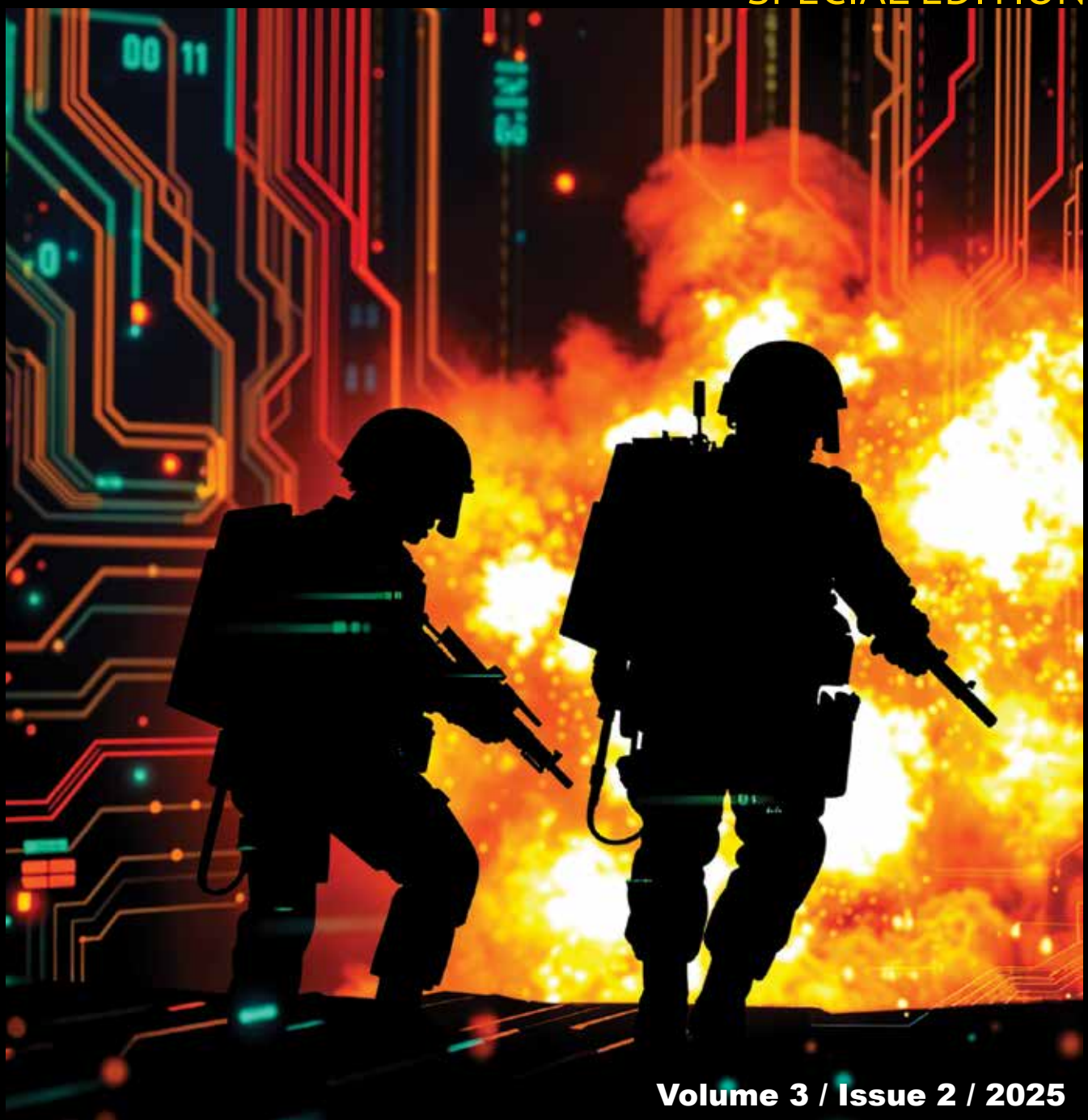
Electronic Warfare by ARMADA INTERNATIONAL

SPECIAL EDITION



Volume 3 / Issue 2 / 2025

TACTICAL DIRECTION FINDING

COMPACT DF HEAD SYSTEMS & RAPID DEPLOYMENT KITS

(30MHz to 40GHz)

CRFS' Compact Direction Finding (DF) Heads are lightweight, modular systems designed for spectrum monitoring, SIGINT, COMINT, and ESM operations. They are fully interoperable with CRFS' V-Track vehicle solution, can be deployed as part of heterogeneous distributed sensor networks, and support missions ranging from signal detection and interception to precise geolocation and intelligence gathering.

CRFS
EXTRAORDINARY
RF TECHNOLOGY

a Motorola Solutions Company

www.crfs.com

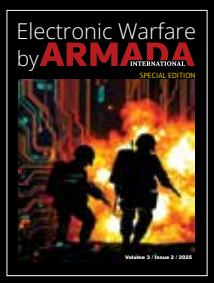
TACTICAL & COMPACT · LIGHTWEIGHT & SWAPPABLE · USE ANY RFEYE NODE

INTRODUCTION

Thomas Withington

"The convergence of cyberwarfare and Electronic Warfare (EW) represents one of the most complex challenges facing modern military command and control (C2) systems," says Suzanne Button, a cybersecurity strategist and Elastic's field chief technology officer.[1] This supplement has been produced to coincide with Tangent Link's EW Live event in Tartu, southern Estonia this September.[2] The publication will note that cyberwarfare and electronic warfare effects are increasingly complementary. EW cadres can employ Radio Frequency (RF) delivered malware alongside their traditional jamming effects as part of their tactical toolkit.[3] Ms. Button argues that "as warfare evolves beyond traditional domain boundaries, the integration of cyber and electromagnetic effects across land, sea, air, space, and cyber domains creates unprecedented operational advantages". This brave new world brings its own challenges, notably "significant command and control complexities that require innovative solutions".[4]

This supplement will seek to ascertain the extent to which the EW and cyberwarfare communities should converge, coalesce and/or coexist. The publication will chronicle how developments in military sensing and communications technology have occurred alongside advances in computing and digitisation. It will then detail examples where RF-delivered cyber effects may have been employed for tactical and/or operational advantage. It will conclude by discussing the technical, Command and Control (C2) and doctrinal challenges EW and cyberwarfare complementarity bring.[5] By tackling this question, it is hoped that this publication can contribute in a small way to ongoing discussions concerning the complementarity of cyber and electromagnetic effects to support military operations. E



ON THE COVER
The use of cyber warfare and electronic warfare effects in support of military operations at all levels of war are now a reality, yet challenges exist in coordinating these effects to ensure their utmost efficiency.

Published bi-monthly by Media Transasia Ltd.

Publishing Office: Media Transasia Ltd.,
1603, 16/F, Island PL Tower, 510 Kings Road, Hong Kong

Electronic Warfare Editor: Dr.Thomas Withington
General Manager: Jakhongir Djalmetov
International Marketing Manager: Roman Durksen
Digital Manager: David Siriphonphutakun
Art Director: Rachata Sharma

Global Offices

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

SOUTH KOREA
Jaeho Chinn - JES Media
Tel: + 82-70-7730-2905
Email: corres3@jesmedia.com

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

USA / CANADA / SOUTH AMERICA
Margie Brown,
Tel : (+1 540) 341 7581
Mobile: +1 703 622 2130
Email: margiespub@astound.net

TURKEY
Zeynep Özlem Baş
Mobile: +90 532 375 0046
Email: media@oz-ist.com

ALL OTHER COUNTRIES
Jakhongir Djalmetov
Media Transasia Limited
Tel: +66 (0) 661 6832, Mobile: +66 81 6455654
Email: Publisher@mediatransasia.com

Roman Durksen
Media Transasia Limited
Tel: +66 (0) 661 6833, Mobile +66 83 6037989
E-Mail: roman@mediatransasia.com
www.armadainternational.com

TABLE OF CONTENTS

ROHDE&SCHWARZ

Make ideas real

The frontline of security

EMBRACING TECHNOLOGY FOR SAFER BORDERS

Explore advanced solutions for electromagnetic warfare, intelligence, and counter-drone operations. Discover how Rohde&Schwarz can help in achieving true spectrum dominance while prevailing in the evolving landscape of EME/CEMA operations.

Delve into cutting-edge SIGINT/EW systems by Rohde&Schwarz at EW Live 2025, September 23–26

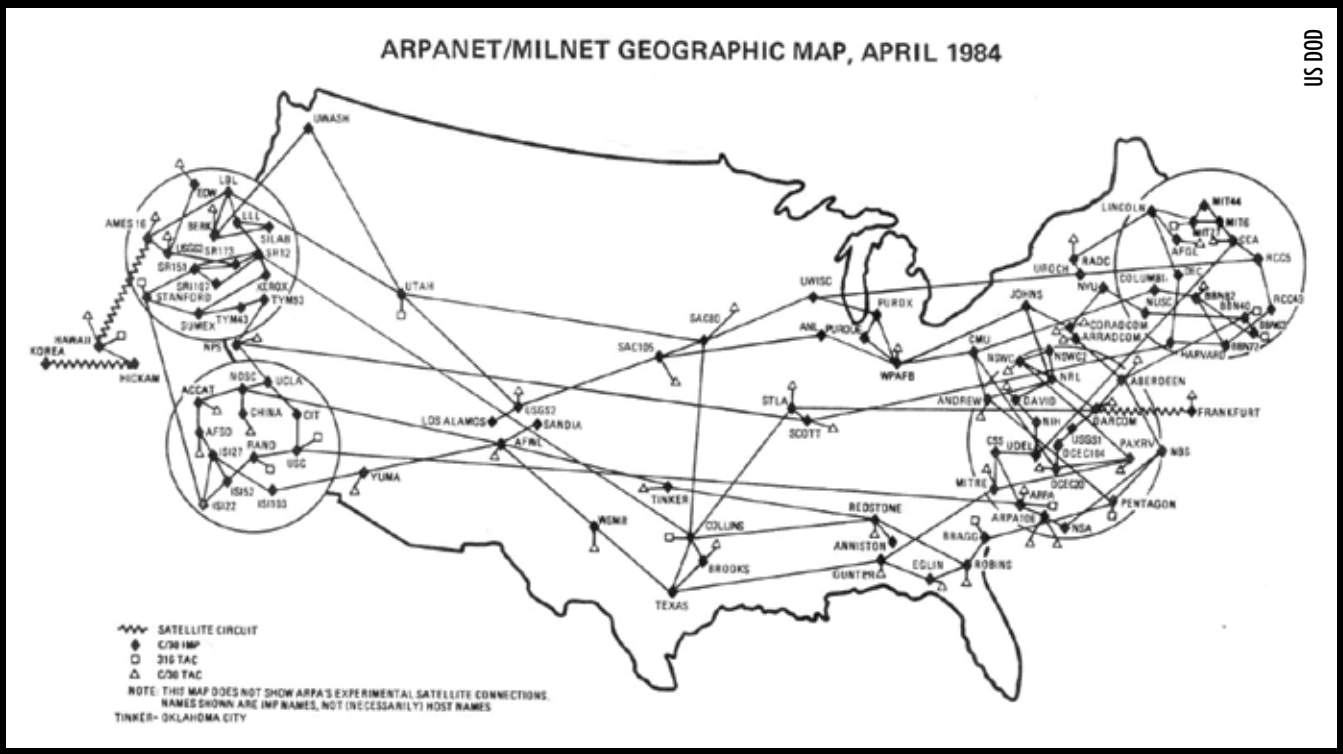
This graphic produced by the flightradar24.com website shows the effects of GNSS spoofing. United Airlines UA84 was a scheduled flight from New York's John Fitzgerald Kenedy International Airport in the United States to David Ben Gurion International Airport in Tel Aviv. The graphic appears to be showing the aircraft being diverted to Lebanon. This diversion never occurred and may have been due to the aircraft's GNSS receivers unintentionally relaying false PNT signals.

A BRAVE NEW WORLD?

Computers, digitisation, the primacy of data and networking have revolutionised how militaries communicate, navigate and improve situational awareness, but have also created new vulnerabilities.

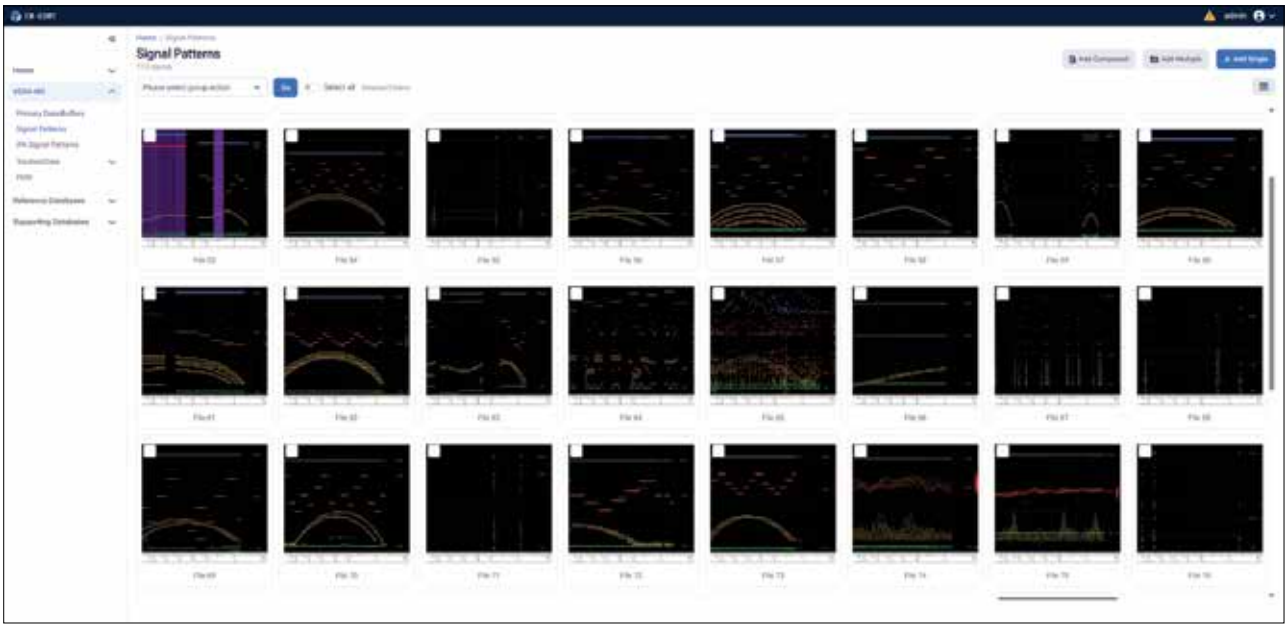
By Thomas Withington

Electronic Warfare (EW) practitioners have hitherto had two options when choosing to engage a Radio Frequency (RF) target. Such targets can include conventional radios and their networks, radars, Satellite Communications (SATCOM) and/or Global Navigation Satellite Signal (GNSS) Position, Navigation and Timing (PNT) signals. These targets could either be jammed or spoofed: Jamming focuses on inundating an RF receiver with enough noise to prevent it 'hearing' the intended signal. Noise can be thought of as interference. Imagine being at a concert and someone is trying to talk to you over the sound of the band. Their voice is the transmission



This diagram shows the nodes and links which underpinned ARPANET, the forerunner of today's internet. Several military sites can be seen such as Andrews airbase in Maryland, the Pentagon in Washington DC and the Redstone Arsenal, Alabama. ARPANET also linked academic and research facilities like the University of California and Sandia National Laboratories, New Mexico.

EW-EDMT - DATA MANAGEMENT TOOLKIT FOR ELECTROMAGNETIC WARFARE



ERA new product showcased currently within EW Live in Tartu called EW-EDMT (an abbreviation of Electromagnetic Warfare ERA Data Management Toolkit) is a comprehensive tool for processing ELINT/ESM data throughout the entire intelligence cycle with an emphasis on post-mission analysis. Its main purpose is determining targets' identification such as platform, emitter and emitter mode.

EW-EDMT works with all kinds of incoming data from the ESM (Electronic Support Measure) systems. The systems´ users try to extract as much information from collected data as possible and then convert, process, filter, identify and store them. The identification can be assigned manually based on user´s knowledge or automatically based on the comparison of parameters with the reference database.

During the live operation it is not possible to fully extract all available information, therefore post-mission analysis is needed. The aim of such analysis is to build and expand reference database to improve target identification and therefore further increase automation of the process.

Application consists of 4 Tools, where each is designed to perform specific tasks:

E mitter Tool - is used for managing and updating reference databases used in signal identification. It ensures consistent, accurate emitter data for ESM/ELINT systems.

D ata Mining Tool - is used for post-mission analysis to store, process and evaluate data collected by ESM/ELINT systems in order to identify new emitters and their modes.

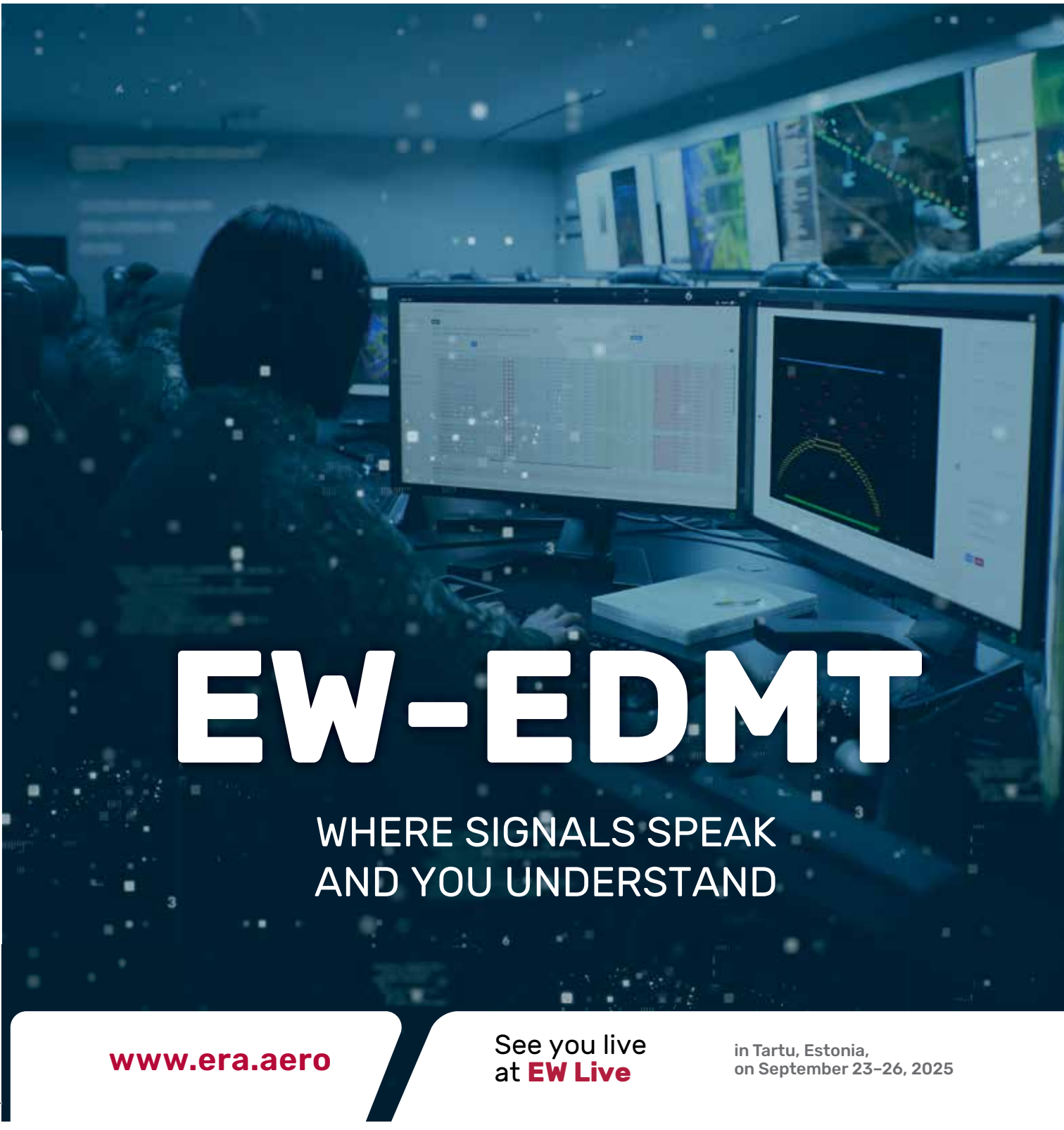
M ission Tool – is used to maintain situational awareness of detected priority targets during missions and to support the creation of regular activity reports within the area of interest.

T arget Tool - is used to provide detailed information on military platforms, emitters, weapon systems, and their deployment across countries.

The typical end users of EW- EDMT application are mission planner, intel analyst, signal analyst, database administrator responsible for the creation and management of national ESM database, and last but not least platforms´ operator as additional source of information to support the target/signal identification.

EW-EDMT Key Features:

- Advanced platform for multi-source electromagnetic intelligence data processing
- Capable to integrate and evaluate data from various ESM/ELINT platforms
- Full intelligence cycle end-to-end
- Supports building and maintenance of national reference database
- Input data comparison with the reference database
- Tactical data presentation in the map, 100% data utilization – no loss, no waste
- Reduces manual workload, saves expert capacity



www.era.aero

See you live
at **EW Live**

in Tartu, Estonia,
on September 23–26, 2025

Operation Desert Storm saw an unprecedented level of digitisation and connectivity, both of which were factors contributing to the US-led coalition's decisive victory.

that you are trying to hear, and the music is the jamming signal.

Spoofing is an arguably more sophisticated approach to electronic attack and can involve sampling an incoming radio signal. The modulation of that signal can be manipulated to have a particular effect. Modulation is the process of altering a radio signal in a particular way so that the signal performs a specific task. Consider a radar transmitting a pulse of RF energy every second. The pulse zooms out of the radar at the speed of light, 299,792 kilometres-per-second/161,875 knots-per-second. All radio signals travel at, or near, the speed of light. It takes that radar pulse 0.0025 seconds to travel through the ether, hit a target and be reflected to the radar as an echo. The radar operator is interested in the range to the target. By halving the time the pulse takes to perform this journey, given the speed of light, they can determine the target is circa 126 nautical miles/nm (374 kilometres/km) away. The Electronic Support Measure (ESM) onboard a combat aircraft samples the incoming pulse, copies the pulse's characteristics, such as its frequency and strength, and starts transmitting these to the radar. The ESM transmits seemingly identical pulses every 0.0012 seconds. The radar still receives the

0.0025 pulse echoes, but is now also receiving echoes every 0.0012 seconds. Do these two sets of pulses mean the radar now has two targets, one of which appears to be half the distance away from the first? A more sophisticated approach is to gradually increase or decrease the time during which the fake pulses are transmitted to the radar by the ESM. This can create the appearance that a new target is moving towards or away from the radar. Once again, which is the actual target and which is fake? The radar operator has been handed a dilemma.

There are many more sophisticated spoofing techniques which could fill a book by themselves. Another favoured tactic is to transmit fake PNT signals into GNSS receivers. Spoofing in this regard is often achieved by simply transmitting a fake time signal. GNSS constellations transmit a time signal derived from powerful atomic clocks onboard their satellites as part of their PNT signal output. Navigation measures speed and time to determine distance and direction. PNT signals are very weak by the time they have travelled tens of thousands of kilometres through space. Like a long-distance runner at the end of a race, the further a signal travels the less energy it has when it reaches its destination. The weaknesses of these signals make them relatively easy to 'wash out' with fake, but more powerful, spoofing signals transmitted into the GNSS receiver from a jammer within range. As above, the GNSS receiver no longer hears the true signal. Instead the receiver processes information from the spoofed transmission thus causing potentially serious timing and navigational errors.

Spoofing is a popular tactic used against hostile radios and their networks. In its simplest form, fake and misleading traffic is injected into a communications network via the radios connected to it. Once inside the network this false traffic can create confusion and dislocation causing serious errors. These errors may have profound ramifications at tactical, operational and even strategic levels.

Digitisation

Until the advent of the

digital age, the EW practitioner was largely restricted to employing jamming and/or spoofing electronic attacks. To be fair, jamming and spoofing contained a myriad of tactics which the discussion above has barely articulated. However, the advent of military digitisation is adding another effect to the EW practitioner's tactical repertoire they can increasingly exploit.

Digitisation has had a profound effect on how militaries share information using radio, how they exploit PNT signals and how radars do their work. Broadly speaking, digitisation "is the process of changing from analogue to digital".[6] What this means in practice is that a computer, which handles binary data in the form of zeros and ones within a radar or radio, is used to compose an RF signal. The signal must have certain properties to perform a particular mission. As articulated in the previous chapter perhaps a radar is sending out pulses to ascertain the range of potential targets? The radar's computers will send a series of instructions in the form of zeros and ones to compose an RF signal to perform that desired task. The signal is composed, transmitted towards a target and received as an echo. Now the process works in reverse. This incoming analogue echo is digitised, i.e. turned back into zeros and ones. Converted into data, the echo is depicted on the radar operator's screen. Radios will work in much the same way. Voice or data traffic enters the radio, is digitised, transmitted as an analogue signal, redigitised and presented to the recipient. Likewise, incoming PNT signals are digitised so that they can be processed by the GNSS receiver and displayed to the user.

Two major innovations paved the way for digitisation: The first was the invention of solid-state electronics in the 1960s with the perfection of the semiconductor or 'chip' after the Second World War. Semiconductors largely replaced the vacuum tubes in systems like computers, radios and radars. Chips were comparatively small, more robust and demanded less energy than vacuum tubes. The smaller semiconductors became, the more could be housed in a particular system and the more functions that system could perform. This is why your smartphone is a fraction of the size of the rotary dial phones formally ubiquitous in homes and offices. Electronics miniaturisation also explains why your smartphone performs umpteen tasks.

Digitisation has impacted military communications too. The first digital military radios began to be deployed by navies, armies and air forces in the late twentieth century.[7] Like their civilian telecommunications counterparts, digital radios are easier to use as much of the tuning burden is done by the radio's computer. Unlike the fragility of vacuum tubes, solid state radios are more robust. The latter also boast lower Size, Weight and Power (SWAP) burdens than their analogue predecessors.

Digitisation, which commenced in the 1950s, would arguably not have been possible without the arrival of the semiconductor.[8] The onward march of the zeros and ones eventually paved the way for another vitally important, and related technological revolution, in the form of the internet. The Advanced Research Projects Agency Network (ARPANET) commenced in the 1960s as a way for government researchers to share information.[9] APRANET was a child of the Cold War and was envisaged as a way in which information could be shared during and after a nuclear conflict.[10] As long as two computers were connected via telecommunications information could be shared. The more connected computers, the more recipients of information there would be and the more survivable the network. Some computers and

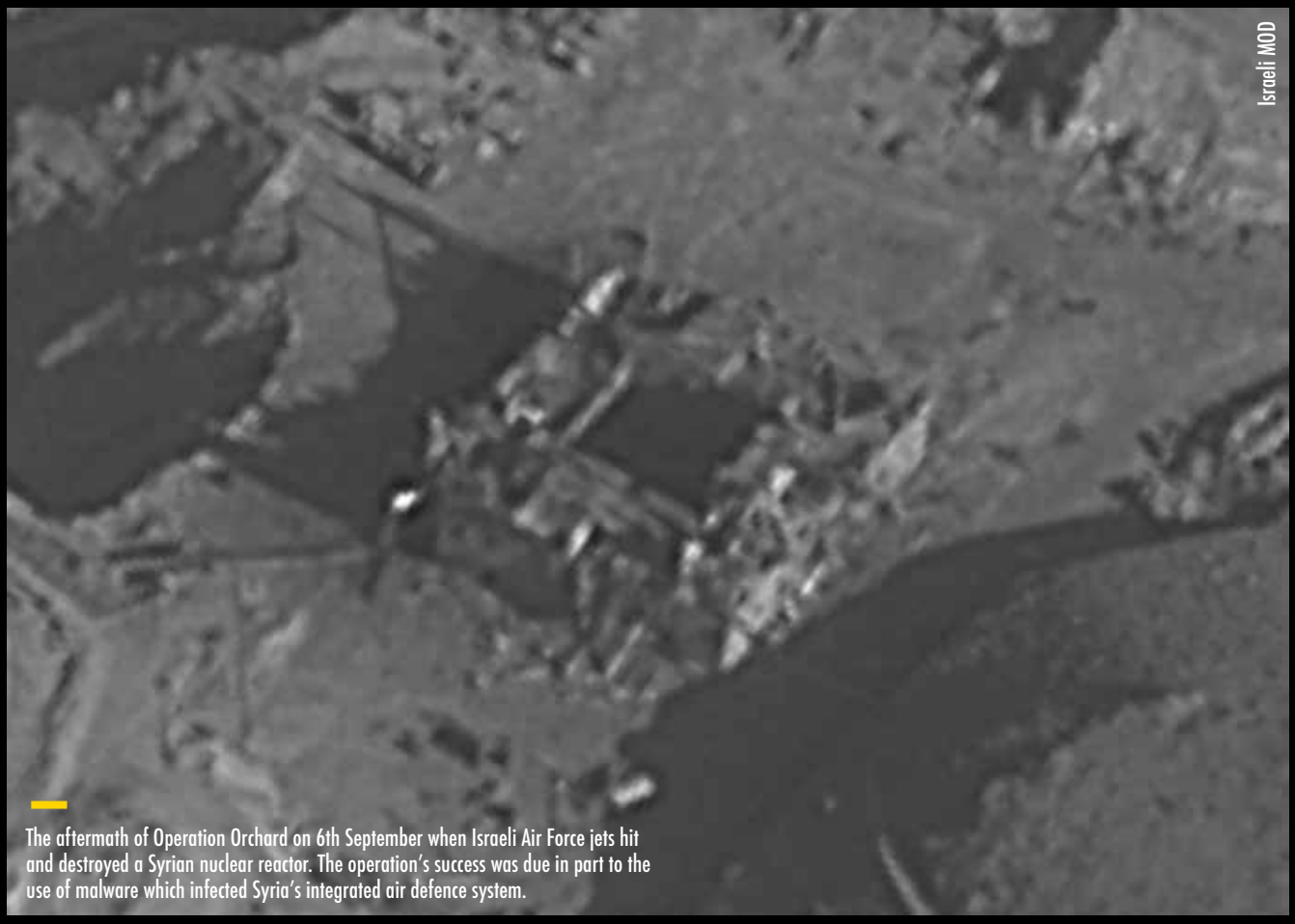
telecoms would inevitably be destroyed in the nuclear exchange, but some would not, hence making the network survivable even if badly damaged. The problem with ARPANET was that computers using the network did not have a single language to send and receive data. This created obvious problems: If English has become the international lingua franca, then it is the Transfer Control Protocol/Internet Protocol (TCP/IP) which has become that language's equivalent in cyberspace. The potential of IP as a standard protocol to move data was not lost on the military. The US defence community was an early adopter of IP networking to link military assets.

Digitisation had also impacted Command and Control (C2). C2 systems used by armed forces at all levels of war have undergone a similar revolution. Previously physical maps, typed, written and/or spoken orders and situation reports, written data and imagery were integral to C2 and battle management. These command and control components became digitised as computers found their way onto the battlefield. The US Army Ballistic Research Laboratory developed a computer to help calculate artillery fire control solutions during the Second World War.[11] Such nascent systems were relatively restricted in their applications, in this case confinement to artillery fire control.

It was in the early 1950s that the routine adoption of computing into command structures began to gain momentum.[12] At first, the physical size of computers restricted them to performing these functions in a static capacity. The US Department of Defence's Worldwide Military Command and Control System (WWMCCS), which entered service in the 1960s was a case in point. Intended to assist the operational/strategic level C2 of US forces, the WWMCCS was spread across 81 locations. It used 30 different types of software in almost 160 different systems.[13] While electronic miniaturisation played its part in reducing the size of the computers commanders could use to assist C2, so did ruggedisation. Ruggedised laptops began to equip militaries from the 1990s.[14] Computers could now be taken into the field in a package with a fraction of the SWAP burden inherent in systems like WWMCCS.

Digitisation and its IP sibling was first used to devastating effect by the US military during Operation Desert Storm in 1991. Desert Storm was mounted to expel Iraqi forces occupying Kuwait.[15] Voice and data traffic could be moved around the battlefield using wired and wireless communications at the speed of light. Forces were not only highly responsive to the unfolding battle, but could read it with a level of detail never previously experienced. This empowering movement of information, intelligence, C2 traffic and situational awareness was arguably a decisive factor in the victory of the US-led coalition during that war. The military digitisation trend has only deepened since and will continue to do so.

Nonetheless, as digitisation has brought untold benefits in terms of speed of battle, decision superiority and situational awareness, so too it has created potential vulnerabilities. Every military innovation will bring a riposte. The advent of airpower was directly responsible for the development of air defence. The emergence of the submarine spurred the realisation of sonar. Digitisation is likewise creating a similar reaction. Any military asset relying on computing is at risk of cyberattack. Cyberattack is a subdiscipline of cyberwarfare alongside cyber defence. While the EW practitioner has long had jamming and spoofing as means of electronic attack, they can now increasingly exploit cyberattack for tactical, operational and even strategic effect. E



Israeli MOD

The aftermath of Operation Orchard on 6th September when Israeli Air Force jets hit and destroyed a Syrian nuclear reactor. The operation's success was due in part to the use of malware which infected Syria's integrated air defence system.

BITS, BULLETS AND BOMBS

The use of radio frequency-delivered cyber effects in support of the tactical, strategic and operational battle is a relatively new phenomenon shrouded in secrecy, but some notable examples are in the public domain.

By Thomas Withington

The ground shook in Syria's eastern Dier ez-Zor governate in the early hours of 6th September 2007 as Israeli Air Force (IAF) combat aircraft performed Operation Orchard. The warplanes were attacking a nuclear reactor in the governate. This facility was suspected by the Israeli government of being a key component in Syria's nascent nuclear weapons programme. Israeli jets ingressed and egressed to and from Syrian airspace and destroyed the reactor undetected. This success may have been owed in part to the use of a cyberattack which infected Syria's Integrated Air Defence System (IADS).

It has been alleged that, prior to the operation which occurred on a Thursday, IAF intelligence operatives hacked into the Syrian IADS. This had been achieved either with Israeli agents operating covertly in Syria, or by hacking into the system from Israel. Several Thursdays' worth of air traffic was recorded from the radars serving the IADS. These Recognised Air Pictures (RAPs) covered the time of day

Russian land forces deploy the RB-341V Leer-3 electronic warfare system in independent EW brigades at the operational level. These systems use Orlan-10 UAVs, like the aircraft pictured here, to create a fake cellphone node in the sky. These nodes can be used to collect communications intelligence from devices which connect with it, or to transmit false and/or demoralising IP traffic.

when the expected raid was to occur. New, but fake, RAPs were created mimicking what Syrian air defenders would expect to see on their screen at that time on an average Thursday night.

These fake RAPs were thought to have been transmitted as code via an RF signal into the Syrian IADS exploiting either radar or radio antennas serving the IADS and its networks. It has been suggested that the IAF used one of its Gulfstream G-550 aircraft configured for electronic warfare to transmit the malware. The code may have deactivated the RAP feed from radars watching the airspace above and around the area where the raid was to occur. Instead new, but fake, RAPs were presented to Syrian air defenders. The data comprising these RAPs was probably drafted in ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange) format. ASTERIX is a standard radar language that can be moved with ease around an IADS. As far as the air defenders were concerned, they were watching a standard Thursday evening's movement of aircraft above their country. Unbeknownst to them, the reactor in Dier ez-Zor was being attacked. It is likely that the use of the malicious code was not the only measure taken to protect the IAF aircraft, nonetheless, it was highly effective.[16]

Ukraine's battlefields

The IAF's Operation Orchard cyberattack marked the beginning of such tactics forming an integral part of the Suppression of Enemy Air Defence (SEAD) mission set. The ongoing war in Ukraine has also illustrated the potential for RF-delivered cyberattacks to have tactical and operational effects. Russia invaded Ukraine in February 2014, seizing Ukraine's southern Crimea region, and parts of the eastern Donetsk and Luhansk areas. Ukrainian artillery experts had developed a digital fire control system for their 2A-18/D-30 122mm towed howitzers. Known as Correction D-30, the system could be used on devices employing the Android operating system like smartphones and tablets.

Russia's GRU military intelligence agency has a

cyberwarfare group called Fancy Bear. It was this group that created a malware called X-Agent. Once inside the Android devices Ukrainian gunners were using for fire control X-Agent created havoc. The malware altered target locations meaning that false coordinates could be unwittingly issued to Ukrainian gunners. Fire control errors caused ordnance to arrive some distance from intended aimpoints. X-Agent could hop easily from one device to another in proximity increasing the number of infected systems. As if this was not bad enough, it was possible to determine the locations of the infected devices: Find the device and you find the gunner; find the gunner and you probably find the artillery emplacement. From a Russian counterbattery fire perspective, this tactic proved devastating against Ukrainian artillery. A 2017 assessment by Henry Boyd, senior fellow for military capability and data assessment at the International Institute of Strategic Studies thinktank in London, estimated that Ukraine may have lost between 15 and 20 percent of her pre-war artillery strength.[17] The impactful role of X-Agent in this regard cannot be discounted.

How was X-Agent delivered? Anecdotal evidence suggests that Russian Land Forces units used RB-341V Leer-3 EW systems to deliver the attack. Each Leer-3 is equipped with a command and control vehicle and three Orlan-10 Uninhabited Aerial Vehicles (UAVs). These UAVs carry payloads capable of detecting signals from cellphones across wavebands of at least 900 megahertz to 1.9 gigahertz, the author understands. The same payload can act as an airborne cellphone tower transmitting traffic into cellphones within range. The Orlan-10 operates at altitudes above 16,000 feet (5,000 metres) with a stand-off range of up to 205 nautical miles (380 kilometres).[18] This is likely how X-Agent entered these android operating devices disguised as seemingly innocuous traffic, or perhaps entering in an entirely invisible fashion.

Suter

The digitisation of radar, and the networked, data-dependent nature of IADS and Ground-Based Air Defences (GBAD) makes these ideal targets for RF-delivered malware. Operation Orchard may have been the overture for this comparatively new SEAD tactic, but it is one which has been of interest for some time. There may even be synergy between IAF cyberwarfare tactics and techniques, and recent similar work in the United States.

The United States Air Force (USAF) is believed to have contracted BAE Systems to develop a cyberwarfare system called Suter to support the SEAD mission. Suter is thought to have been developed via the USAF's Big Safari programme which rapidly provides small-scale, niche and highly classified capabilities. Using malware transmitted over a radio frequency link, Suter has been developed in three versions: Once inside a hostile radar or IADS, Suter-1 lets users see RAPs developed by that radar or IADS. Users can gain access to, and control of, the capabilities furnishing an IADS or GBAD network using Suter-2. Meanwhile Suter-3 lets users disrupt the communications IADS and/or GBAD depend on. All three variants of Suter are understood to have been deployed by the USAF from 2006. It is possible that Suter malware can be transmitted into these targets via RF signals from USAF Lockheed Martin EC-130H and Gulfstream/L3Harris EA-37B Compass Call electronic attack aircraft, among other platforms.[19]

Details of the extent to which Suter has been deployed operationally are scant. The malware may have been used against the Islamic Republic of Iran's IADS after the downing of a US Navy Northrop Grumman RQ-4A Global Hawk UAV on 20th June 2019. The Iranian government claimed the UAV was shot down because it had violated Iranian airspace, which was denied by the US government. US President Donald Trump initially ordered a military response to the shoot-down but changed tack amidst reported concerns for Iranian casualties. Instead, US Cyber Command performed cyberattacks on computer systems controlling Iran's ballistic missile launch capabilities.[20] The extent to which these attacks used Suter malware, and their vector of delivery, remain unknown.

Rocking the Casbah

It is possible that Suter, or similar malware, may have been employed by both Israel and the United States during the short war between Israel and Iran between 13th and 24th June 2025. The IAF mounted a major air campaign to attack Iranian Weapons of Mass Destruction (WMD) sites, and other military facilities. Attacks were also performed by the IAF, and covert ground elements in Iran, against Iranian politico-military

targets and individuals. The US commenced a limited series of airstrikes against Iranian WMD targets on 22nd June. These hit the Fordow and Natanz uranium processing facilities, and the Isfahan Nuclear Technology Centre. All these targets are in the centre of the country, south of Tehran.

Recent analysis of the conflict noted that cyberattacks were used in conjunction, and in close coordination, with the EW efforts of the Israeli Defence Force. EW targeted Iranian military and government radio communications. Other EW targets included Iranian Global Navigation Satellite System use and Iranian ground-based air surveillance and fire control/ ground-controlled interception radars. Cyberattacks were employed against government and military IP networks and military databases. Other cyberattacks hit politico-military targets and critical national infrastructure.[21] These cyberattacks may have been perpetrated by Israel's Unit-8200 which specialises in cyberwarfare and cyberespionage.

How the attacks were delivered is unknown. It is entirely possible that some may have been facilitated via IAF aircraft such as the G-550 platforms mentioned above. This aircraft could have accompanied IAF strike packages but may have flown at a stand-off range from Iranian air defences, conferring important tactical advantages: Israeli cyberwarfare operatives could have infected the Iranian IADS, and accompanying GBAD systems, shortly before the packages' arrival. As per the attack on the nuclear reactor in Syria RF-delivered cyberattacks could fool Iranian air defenders into seeing a benign RAP on their radar screens.

Once the Iranian military was certain that attacks were taking place, Israeli malware could have greatly hampered the ability of Iran's air defenders to protect their skies. It would be highly likely that cyberwarfare was also used as a SEAD tactic to protect the US aircraft attacking Iranian targets on 22nd June. Once again, confirmation as to whether such tactics were used by US and Israeli forces does not appear to exist in the public domain. Nonetheless, the fact that neither Israel nor the US lost any inhabited aircraft during the recent conflict speaks volumes. It is possible that the coordinated use of cyber and electronic effects may have played an important role to this end. B

The advent of Anti-Access/Area Denial strategies by several countries around the world have been instrumental in spurring the development of the Multi-Domain Operations philosophy which has emerged from the previous revolution in military affairs and network centric warfare concepts.

CONVERGENCE, COALESCENCE OR COEXISTENCE?

The efficient use of cyber effects delivered by electronic warfare systems depends on addressing serious technical, command and control, and doctrinal challenges.

By Thomas Withington

Armed forces' stovepipes are breaking down: Successive Revolutions in Military Affairs (RMAs) culminated in the early 1990s with the stunning victory of US-led forces over Iraq during Operation Desert Storm. Iraq's forces had invaded and occupied Kuwait in August 1990.[22] The RMA subsequently morphed into the concept of Network Centric Warfare (NCW).[23] NCW was underpinned by a deepening 'jointness' across national militaries. Network Centric Warfare was conceptually adopted by the militaries of the United States, North Atlantic Treaty Organisation and allied nations.

The emergence of Anti-Access/Area Denial (A2AD) doctrines in the Democratic People's Republic of Korea, the Islamic Republic of Iran, Russia and the People's Republic of China (PRC) has prompted further change. NCW has morphed into the Multi-Domain Operations (MDO) philosophy. Definitions differ but MDO can be perceived as the intra- and inter-force connectivity of all military assets at all levels of war across the entire spectrum of conflict. This connectivity will facilitate synchronous operations aided by better quality, and faster, decision making than one's adversary.[24] The goal of MDO is to ensure that the side practicing it is continually pre-emptive to force their adversaries to be continually reactive.

As Ms. Button notes, A2AD postures challenge traditional domain-specific approaches. For example, Russia's A2AD posture, which includes a sophisticated, networked strategic Integrated Air Defence System (IADS), cannot be challenged solely by an air force, army or navy. Instead, all forces would have to work in a synergistic and synchronic fashion to overcome such threats. The reliance that complex targets

Estonia's CR14 cyber range provides bespoke facilities where NATO and allied cyber operations cadres can hone and develop their skills through dedicated training and regular exercises.

like IADS have on the radio spectrum to provide networking and communications, and computing power, means that "cyberspace and the electromagnetic spectrum now form one continuous, coherent environment".[25] However, Ms. Button sounds a note of caution: "Each domain operates under different physical laws, organisational structures, and operational timelines, making unified command exceptionally challenging".[26]

As the previous chapter explained, EW cadres have hitherto had jamming and spoofing tactics at their disposal when targeting hostile military assets. Increasingly, they can also use RF signals to transmit malicious code to convey a cyberattack. Much as Radio Frequency (RF) signals have been modulated, i.e. changed or augmented, to carry noise or false information in support of spoofing, so they can be modulated to carry malware. The transmitted signal may be able to gain access to a radio, its network and any asset connected to that network through an antenna. Likewise, a cyberattack could be delivered via an RF signal into a hostile radar. Once again, the radar itself may be the target. Alternatively, the target may be the communications networks connecting the radar to other assets. A cyberattack

Russian MOD

Russia is one of several countries which has exploited anti-access/area-denial postures to increase the *materiel*, and hence political, costs to any potential aggressor. The use of sophisticated ground-based air defence systems, such as the S-400 (NATO reporting name SA-21 Growler) high-altitude, long-range surface-to-air missile system depicted here.

may also gain entry via a GNSS receiver. The cyberattack will of course have to overcome whatever cybersecurity provisions and protocols the enemy has employed precisely to prevent and frustrate such tactics. Cyberattacks tend to be delivered across standard IP networks which include both wired and wireless connections. EW cadres are already sending jamming and spoofing RF signals through the ether. It is logical that they will also exploit the cyberwarfare-over-RF option.

In terms of the complementarity of cyberwarfare and EW, Dr. Kareel Piip, an electronic warfare expert at the University of Tartu, says that the two disciplines have much to offer. Initially, "cyberattacks could be used to gain information" about enemy capabilities like radar, communications and their networks, alongside other military assets depending on these capabilities.[27] He continues that "cyberattack can open ground for EW and vice versa". For example, if an enemy force tends to reply on IP networks for communications, but uses conventional radio networks as back-up, a cyberattack can close these IP links. If the enemy then decides to fall back on conventional radio communications they may put themselves at risk. Blue force EW cadres could detect, identify and locate red force radios

Alongside her NATO allies, the UK is bringing together her cyber and electronic warfare capabilities under a new CEMA command which will lead the new Digital Warfighter Group.

BAE Systems

carrying this traffic. Once this electronic support process is complete, these radios, and their networks, may then be jammed.[28]

Using electronic and cyber effects, while providing an additional useful arrow in the EW cadres' quiver does bring challenges that will need to be addressed as both effects are increasingly used in a complementary fashion: "Delivering cyber effects through EW vectors like RF (Radio Frequency) waveforms is technologically demanding and operationally complex," says Silver Andre, chief executive officer of Estonia's CR14 cyber range. "Such waveforms much be custom-engineered to the target's specific hardware, firmware and protocol stack," he continues.

As with conventional electronic attack environmental conditions, obstructions to a radio signal's line of sight and radio spectrum congestion, may all affect the efficacy of the transmission and hence its cyberattack payload, Mr. Andre emphasises. Any signal, including an RF transmission of malware, risks detection by the enemy. By detecting this signal, hostile actors may be able to pinpoint the signal's point of origin and retaliate using kinetic effects against the transmitter: "In contested environments, the challenge is not only in transmitting the waveform, but in ensuring its successful execution on the target system". These realities are complicated by the fact that it may not be immediately possible to determine whether an RF-delivered cyberattack has been executed successfully against the intended target.[29] An additional challenge, observed by Dr. Piip, is that an RF-delivered malware attack may have a short shelf life. Once the enemy realises their systems and networks have been hacked, they will take measures to ameliorate the damage, and reduce potential vulnerabilities to similar future attacks.[30]

The C2 challenge

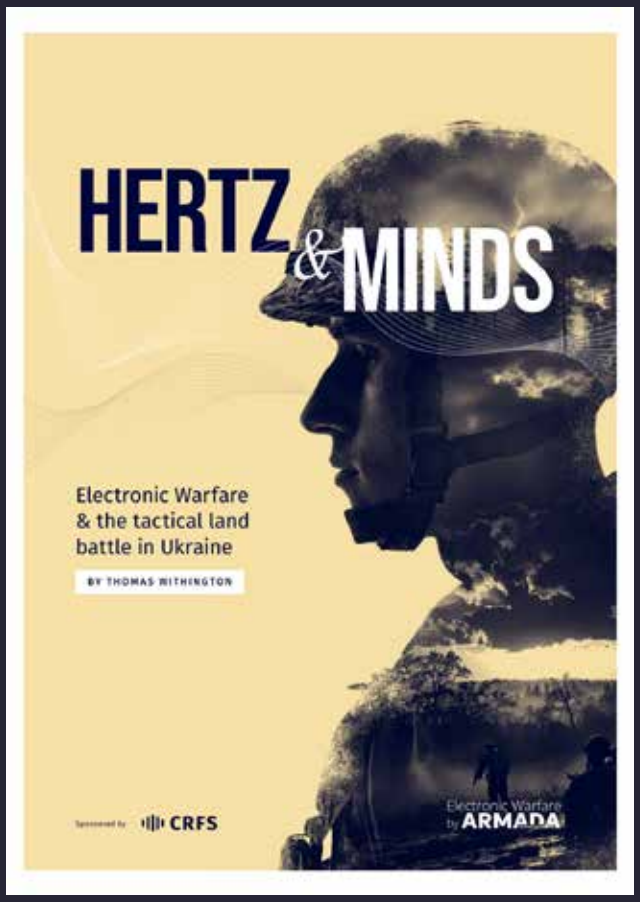
Coordinating cyber and EW effects brings additional challenges from a Command and Control (C2) perspective. Although examples of RF-delivered cyber effects are rare in the public domain, what stands out regarding the examples mentioned in the previous chapter is that they were used at the operational level to have a tactical effect. This is the case for the cyberwarfare tools supporting SEAD, and the X-Agent malware which was delivered by an operational-level EW platform, the Leer-3, with the intention of also having a tactical effect. Using cyber effects at the operational level, and above, may necessitate "high level legal and political approval," Mr. Andre observes. Alternatively, EW actions "may be delegated to tactical levels". He warns this mismatch "can result in delays or friction during fast-moving operations". To further complicate matters, cyber and EW warfare cadres may report through different levels of command. Classification levels, cultures and planning processes may differ between the two disciplines.[31] C2 arrangements for using cyberwarfare and EW synergistically should be carefully planned "not just for mission success, but to avoid fratricide, spectrum conflict and/or legal overreach".[32]

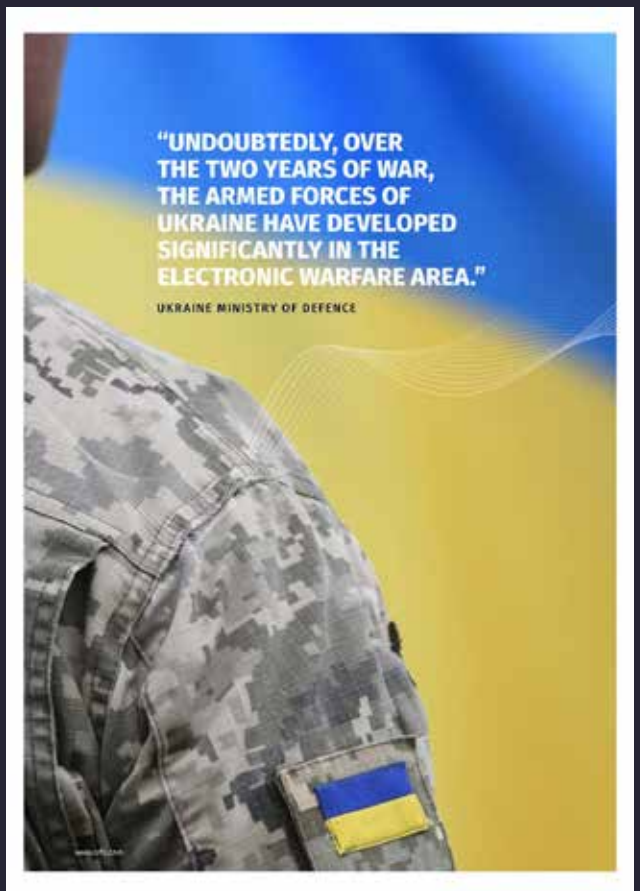
Timing forms a key element of coordinating EW and cyber effects. Ms. Button notes the "temporal mismatch" between the employment of kinetic, electromagnetic and cyber weapons: "Cyber battles typically occur in seconds to minutes, while traditional kinetic warfare unfolds over hours to days". As a result, C2 structures developed for kinetic warfighting may struggle to match the rapid decision-making cycles cyberwarfare demands. EW C2, which demands real-time spectrum management to avoid electromagnetic fratricide, and to exploit and counter rapid frequency agility, may provide a useful template for cyberwarfare command and control. Nonetheless, "coordinating these different operational tempos within a unified command structure presents a fundamental challenge to traditional C2 paradigms".[33]

The future, but not yet?

The RF-delivered cyberattacks which have emerged in the public domain discussed above may constitute the initial examples of what could become a widely adopted tactic in the future. Nonetheless, Mr. Andre cautions that it maybe sometime until cyber and EW effects are routinely used to support the tactical, operational and strategic battle. Cyberwarfare payloads must be optimised to ensure they can be delivered through the radio frequency vector: "Challenges include the miniaturisation of cyber payloads for constrained RF transmission," Mr. Andre explains. Moreover, the payload will need to be unaffected by rapid frequency changes performed by the RF carrier signal to avoid detection. A second consideration is ensuring that the cyberattack is absorbed by the intended target and does not spill over into unintended targets with attendant risks of collateral damage. Mr. Andre believes that Artificial Intelligence (AI) offers a path forward in this regard "allowing systems to respond dynamically to spectrum changes or target behaviour". AI forms the bedrock of cognitive radio and EW techniques which automatically configure signal propagation according to prevailing electromagnetic conditions.[34]

Mr. Andre argues that doctrine remains the "most critical enabler, or obstacle, for integrating EW-delivered cyber effects into mainstream military operations". In 2018, the United Kingdom's Ministry of Defence (MOD) published its





Electronic Warfare by ARMADA INTERNATIONAL

READ THE LATEST

SPECIAL REPORT ON

ELECTRONIC WARFARE &

THE TACTICAL LAND

BATTLE

IN UKRAINE

Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities document. The note explained how the MOD would bring together national Cyber and Electromagnetic capabilities collectively known as CEMA.[35] The UK's Strategic Defence Review (SDR), published on 3rd July, provides more details on the country's CEMA posture. The SDR outlines the UK's strategic priorities, and the capabilities she will adopt to address these, and stated that these capabilities will be the responsibility of a new CEMA Command. The CEMA command will be accompanied by a new Digital Warfighter Group.[36] As this supplement makes clear, there are challenges in using EW and cyberwarfare tactics in close coordination. Nonetheless, Ms. Button argues that the CEMA approach makes sense because "doctrinal division hinders the development of unified operational concepts and complicates the integration of cyber-electronic effects in multi-domain operations". Doctrinal divisions can cause "fragmented situational awareness and suboptimal employment of converged capabilities".[37]

While the steps of NATO and alliance members like the UK should be welcomed, there is still work to be done: "Many armed forces still lack joint frameworks that define how cyber and EW units should train, plan and operate together," says Mr. Andre. "Legal ambiguities about when RF-delivered cyber effects constitute use of force, and who must authorise them, further complicate integration". Additional obstacles include compartmentalisation which may be present in national military and civilian intelligence organisations: In essence, who owns the cyberattack mission? This maybe further hampered by national EW and cyberwarfare cadres working at different levels of classification inhibiting smooth, coordinated C2.[38]

Keen eyed readers will have noted that this supplement has tended to focus on the use of RF-delivered cyber effects in support of the land and air battle. Cases of cyberwarfare being used in support of maritime operations do not seem to have emerged in the public domain. One area Mr. Andre expects to see the increased employment of RF-delivered cyber effects is "for spoofing or disabling satellite navigation at sea". GNSS disruption seen in the Baltic, eastern Mediterranean, Black Sea and Persian Gulf over the last decade maybe indicative of this trend. RF-delivered cyberattacks may also have relevance in the space domain for "disrupting or deceiving satellite links". That said, legal and strategic sensitivities over utilising such effects may have retarded the widespread introduction of these tactics.[39]

As this supplement has shown, RF-delivered cyber effects vastly increase the capabilities which can be brought to bear at the tactical, operational and strategic levels of war. The advent of RF-delivered malware could represent the single biggest evolution of electronic warfare since the invention of radar. RF-delivered cyber effects are not the stuff of science fiction: Previous, and ongoing, conflicts in the Ukrainian and Middle Eastern theatres show that these tactics are already being used. Challenges remain in terms of cyber effect payload design vis-à-vis RF waveforms, C2, legal constraints and doctrinal provision. All these potential impediments must be addressed if RF-delivered cyberattacks are to be used effectively, ethically and legally in war: "Without such evolutions, even the most advanced tools may never leave the sandbox".[40]

This supplement sought to ascertain the extent to which the EW and cyberwarfare communities should converge, coalesce and/or coexist. Both missions are clearly complementary, yet they have key differences in terms of their dynamics. At present, the two missions are not coalescing in the sense that they are not merging into a single entity, despite the emergence of CEMA doctrines due to their significantly different characteristics. Whether coexistence is an apt description is also a moot point: Cyberwarfare and EW ostensibly do their work in different environments: EW primarily works in the radio spectrum, cyberwarfare in cyberspace. The missions overlap when the radio spectrum is employed to deliver cyber effects. Perhaps convergence is a more appropriate term, as noted in Ms. Button's quotation at the start of this supplement. The two disciples of cyberwarfare and EW have similarities and, in some cases, are coming together. The effectiveness of this process will depend on adequately addressing the challenges this convergence will bring. E

ASIAN MILITARY REVIEW

Reach Your Target Through Asian Military Review!

The Only Audited Defence Magazine in the Asia-Pacific Region with a Circulation of 21,379 copies (CAB Audit)

For advertising opportunities contact:

Joha Djalmetov: joha@mediatransasia.com (+66) 2 204 2370 ext 125
Roman Durksen: roman@mediatransasia.com (+66) 2 204 2370 ext 123

ENDNOTES

[1] Interview with Suzanne Button, field chief technology officer, Elastic, 8th July 2025.

[2] EW Live will be held in Tartu, southern Estonia, between 23rd and 26th September. The event will include a conference, an exhibition and a live demonstrations of electronic warfare capabilities.

[3] Malware is a generic term for software that can disrupt, damage and/or gain unauthorised access to a computer system, according to the *Oxford English Dictionary*.

[4] Interview with Suzanne Button, field chief technology officer, Elastic, 8th July 2025.

[5] Convergence can be defined as two or more things or ideas becoming similar or coming together, according to the *Cambridge English Dictionary*. The same publication defines coexistence as the act of living or existing together at the same time and in the same place whereas coalescence is defined as the process of coming or growing together to form one thing or system.

[6] Bloomberg, J, 'Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril', 14th April 2018 @https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/, accessed 16th July 2025.

[7] Frackiewicz, M, 'From Field Phones to 5G: The Evolution of Military Radio and Telecommunications', 20th June 2023 @https://ts2.tech/en/from-field-phones-to-5g-the-evolution-of-military-radio-and-telecommunications/, accessed 16th July 2025.

[8] Tarpey, M, 'A Brief History of Digitisation', 19th August 2022 @https://www.exelatech.com/blog/brief-history-digitization, accessed 16th July 2025.

[9] ARPANET was conceived by the Advanced Research Projects Agency (ARPA). ARPA was the forerunner of today's Defence Advanced Research Projects Agency based in the United States.

[10] 'A Brief History of the Internet', @https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=ARPANET%20and%20the%20Defense%20Data,connected%20by%20a%20universal%20language, accessed 16th July 2025.

[11] Malone, DK, 'The Commander and the Computer', in *Military Review*, (Fort Leavenworth, KA: US Army Command and General Staff College, 1967).

[12] 'The Evolution of Military Command and Control Systems Through History', 22nd August 2024 @https://legacyoflegions.com/the-evolution-of-military-command-and-control-systems/#The_Introduction_of_Early_Computers_in_Military_Command, accessed 16th July 2025.

[13] Hosaka, MI, *Army WWMCCS Information System: A Strategic Command and Control System*, (Carlisle Barracks, PA: US Army War College, 22nd March 1990).

[14] 'History of Toughbooks: How They Took Off', 15th August 1990 @https://www.ocruggedlaptops.com/blog/history-of-toughbooks-how-they-took-off/?srsltid=AfmBOoqeQe36_BFXIQCSICv9BaMBuwDa-aiIHEMhj6ZX6-9dF0Kc-eOd, accessed 16th July 2025.

[15] 'Evolution of Military Tactical Radios', @https://rockwellcollinsthoughtleadership.wordpress.com/wp-content/uploads/2017/08/evolution-of-military-tactical-radios.pdf, accessed 16th July 2025.

[16] Conversation with senior American scientific intelligence expert, March 2020.

[17] 'Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units', 22nd December 2016 @https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/, accessed 17th July 2025.

[18] Withington, T, '68 Guns', 2nd December 2021 @https://www.armadainternational.com/2021/12/russian-cyber-warfare/, accessed 17th July 2025.

[19] Dean, SE, 'Killer Code: Cyber-Supported SEAD', 16th August 2001 @https://euro-sd.com/2021/08/articles/exclusive/23246/cyber-supported-sead/, accessed 6th August 2025.

[20] Pomerleau, M, Eversden, A, 'What to make of US cyber activities in Iran', 25th June 2019, @ https://www.c4isrnet.com/dod/2019/06/25/why-trump-may-have-opted-for-a-cyberattack-in-iran/, accessed 6th August 2025 and Withington, T, 'Error 404', 4th March 2020 @ https://www.armadainternational.com/2020/03/error-404/, accessed 6th August 2025.

[21] Makowski, J, 'Israel-Iran War Cyber and Electronic Warfare Operations', June 2025 @ https://www.scribd.com/document/887673595/Israel-Iran-War-Cyber-and-Electronic-Warfare-Operations-2025, accessed 6th August 2025.

[22] A Revolution in Military Affairs occurs when a fundamental change happens in warfare. RMA examples include the use of railroads to move troops and materiel at speed during the 1861 to 1865 American Civil War; the introduction of armour, airpower and submarines during the First World War, and the use of atomic weapons to end the Second World War. The 1991 Persian Gulf War is considered the culmination of the RMA given the heavy use of technology such as precision-guided weapons, and satellite communications and navigation, by the US-led coalition.

[23] NCW can be defined "as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronisation. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace." Source: Alberts, DS, Garstka, JJ, Stein, FP, *Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition*, (Washington DC: United States Department of Defence, 1999), page 2.

[24] For this definition, military assets can include, but are not limited to, personnel, platforms, sensors, weapons, networks, bases and capabilities. The entire spectrum of conflict covers low intensity operations like counter-insurgency, and military operations other than war, up to and including high-intensity all-arms battle.

[25] Interview with Suzanne Button.

[26] Ibid.

[27] Interview with Dr. Kareel Piip, electronic warfare expert, University of Tartu, 25th July 2025.

[28] Ibid.

[29] Interview with Silver Andre, chief executive officer of Estonia's CR14 cyber range, 2nd July 2025.

[30] Interview with Dr. Kareel Piip.

[31] Interview with Silver Andre.

[32] Ibid.

[33] Interview with Suzanne Button.

[34] Interview with Silver Andre.

[35] Ministry of Defence, *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*, (Ministry of Defence: London, February 2018).

[36] Withington, T, 'Commanding Presence', 3rd July 2025 @ https://www.armadainternational.com/2025/07/uk-strategic-defence-review-electronic-warfare/, accessed 6th August 2025.

[37] Interview with Suzanne Button.

[38] Interview with Silver Andre.

[39] Ibid.

[40] Ibid.

EW LIVE

tangentlink

EWLive 2025:
Prevailing in EME/CEMA OPERATIONS

23-26 September 2025
Tartu, Estonia

EWLive has become a 'must attend' event for Defence and Security Industry stakeholders to gain knowledge through a live demonstration setting

EVENT OVERVIEW

- 23 September – CEMA/Cost Effective EW practitioners' day
- 24-26 September – live demonstrations

LIVE DEMONSTRATIONS

- Each demonstration lasts 50 minutes and is delivered to each participating military delegate group on a one-on-one basis
- Live RF and UAS detection environment allowing military delegation groups to immerse themselves in the operation of the equipment in a live setting
- Hands-on experience, not a simple sales pitch at a trade show
- Understanding the technology available and how it can address capability requirements

EXHIBITION

All companies giving a live demonstration will also have a booth at the exhibition hall for continued discussion. In addition, companies that are not ready or able to demonstrate live will showcase their equipment and capabilities within the exhibition.

WHO SHOULD ATTEND

- Senior EW/CUAS and CEMA practitioners and procurement decision-makers
- Registration deadline 31 July 2025

EME CAPABILITIES TO BE DEMONSTRATED

Please scan the QR code for the event website and the list of confirmed demonstrating companies

Please contact Kate Niven at kniven@tangentlink.com for further information and participation details.