SETA Emerging Military Technologies Series .1.

Electronic Warfare:

Global Trends & Turkish Capabilities Report

Feridun Taşdan

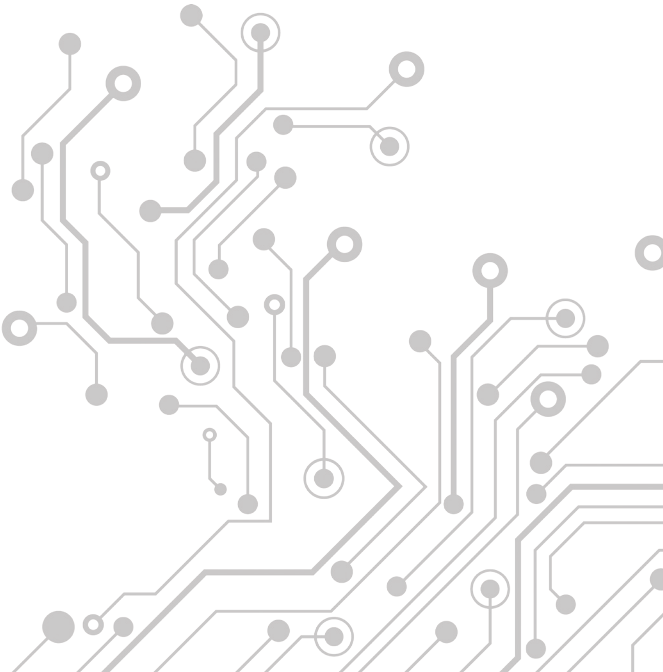
SETA

SETA Emerging Military
Technologies Series .1.

Electronic Warfare:

Global Trends & Turkish Capabilities Report

Feridun Taşdan



SETA

FERIDUN TAŞDAN

Dr. Feridun Tasdan is a professor in the Department of Mathematics at Western Illinois University in the United States. In addition to his academic work on robust estimation methods, and generalized linear models, he also has been writing articles related to air defense systems and their operational concepts in several defense and aerospace journals in Türkiye

Emerging Military Technologies Series is a SETA Project aims to shed light on the key aspects of new and developing key military technologies by elaborating on global trends and Türkiye's capabilities. A part of the Project is sponsored by STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş.

SETA Publications 201
First Published in 2022 by SETA
ISBN: 978-625-8322-11-8

The conclusions and recommendations of any SETA Foundation publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

Layout: Sema Türk Bayazit
Printed in Türkiye, Turkuvaz Haberleşme ve Yayıncılık A.Ş., İstanbul

SETA | FOUNDATION FOR POLITICAL, ECONOMIC AND SOCIAL RESEARCH
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312.551 21 00 | Fax :+90 312.551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüp İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Fax: +90 212 395 11 11

SETA | Washington D.C. Office
1025 Connecticut Avenue, N.W., Suite 1106
Washington, D.C., 20036 USA
Tel: 202-223-9885 | Fax: 202-223-6099
www.setadc.org | info@setadc.org | @setadc

SETA | Berlin
Kronenstraße 1, 10117 Berlin GERMANY
berlin@setav.org

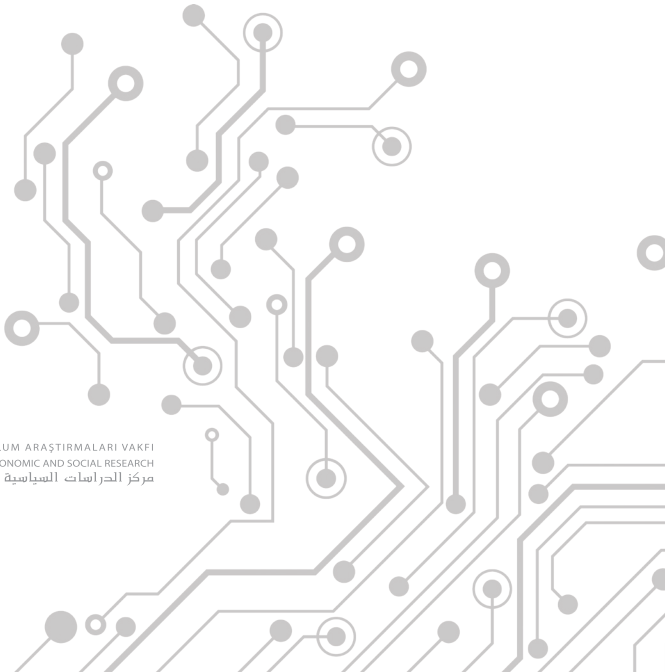
SETA | Bruxelles
Avenue des Arts 6, 1000 Bruxelles BELGIUM
Tel: +32 2 313 39 41

SETA Emerging Military Technologies Series .1.

Electronic Warfare:

Global Trends & Turkish Capabilities Report

Feridun Taşdan



SETA
SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
FOUNDATION FOR POLITICAL, ECONOMIC AND SOCIAL RESEARCH
مركز الدراسات السياسية والاقتصادية والاجتماعية

Contents

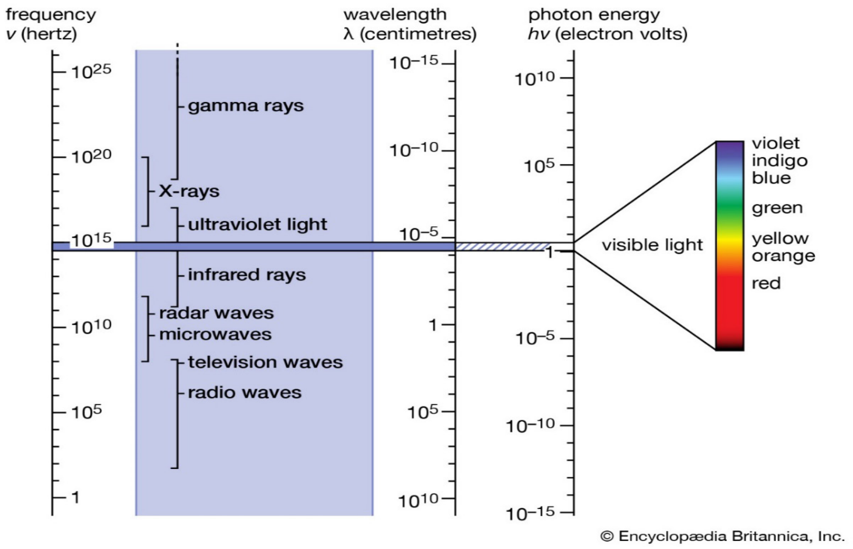
Introduction

A brief introduction to the electromagnetic spectrum (EMS) could pave the way to explaining EW systems' role in modern warfare. Not surprisingly, from cell phones to a simple TV remote control, many devices in our daily lives all use the EMS. What is the electromagnetic spectrum[1]? Basically, the EMS can be defined as electromagnetic waves that travel at the speed of light in certain frequency ranges and wavelengths. The full range of the EMS in frequency and wavelengths can be seen below in Figure 1.[2] The top of the frequency and wavelength portion of the EMS belongs to gamma and X-rays, which are commonly used in medical fields (medical imaging) and nuclear physics due to the nature of their high energy photons and very small wavelengths (ก=10-10 cm). We see the EMS's ultraviolet and infrared light portion right after the X-rays. This EMS is mostly invisible to the human eye but only in a small portion of this spectrum, the electromagnetic waves can be seen by humans and most animals. Infrared cameras (to detect the thermal image of objects) also work in this portion of the EM spectrum. The 1-300 GHz frequency (100 meter-0.5 mm wavelength) spectrum of the EMS field is mainly used by a wide range of radar systems that are mainly used for military applications, weather observations, and navigational aid purposes. The bottom of the EMS range is mostly used for radio communications and TV broadcasting purposes.

[1] "The Electromagnetic Spectrum", NASA, March 2013, https://imagine.gsfc.nasa.gov/science/toolbox/emspectrum1.html

[2] Christian Wolff, "Waves and Ranges", Radartutorial.eu, https://www.radartutorial.eu/07.waves/Waves%20and%20Frequency%20Ranges.en.html

***Figure 1:** Electromagnetic Spectrum's Frequency and Wavelength Scale*



***Source:** Britanica.com*[3]

Most radar/communication systems work within the 1 to 40 GHz frequency band (100 meter-0.5 mm wavelengths), based on the design purpose of the radar. These radar systems use a narrow portion of the full EMS. For example, most long-range search radars use L (1-2 GHz, 30-15 cm wavelength) and S bands (2-4 GHz with a 15-7.5 cm wavelength), and most fire control radars use X, Ku, or Ka bands with the respective frequencies and wavelengths to optimize their performance against their intended targets. The range of radar bands and their frequency and wavelengths can be seen in Figure 2 below.[4]

So, electronic warfare (EW) is defined as any action or capability of using EMS to detect, deceive and disrupt the opponent's weapon systems such as radars, communication systems, command control systems, data networks, or other digital infrastructures using EMS.

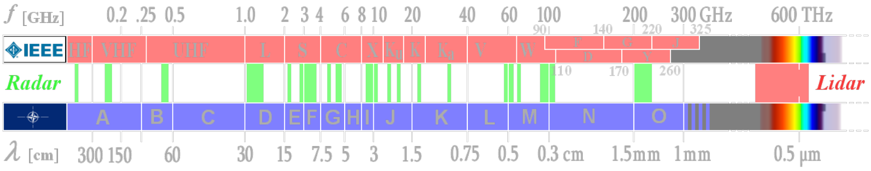
Why do militaries around the world place particular importance on developing and fielding EW systems? The most obvious answer is to control the EMS to gain superiority on the battlefield to defeat the enemy. The second answer would be

[3] The Editors of Encyclopaedia Britannica, "Electromagnetic Spectrum",Britannica, https://www.britannica.com/science/electromagnetic-spectrum

[4] Christian Wolff, "Waves and Ranges", radartutorial.eu, https://www.radartutorial.eu/07.waves/Waves%20and%20Frequency%20Ranges.en.html

to have the capability to upgrade or update EW systems' hardware and software whenever it is required. EW technologies can be placed at the top of the list of military technologies that are highly protected and controlled by the countries that developed these technologies. Usually, the EW systems come "as is," in other words, the countries that purchased these systems have no or very little control over the software or hardware architectures of the EW systems. Technically, the EW systems require continuous upgrades for their threat library since the operational environment of EW systems changes over time, and new weapon systems are introduced into the battlefield. To keep EW systems effective and functioning at maximum performance, militaries upgrade/update their EW systems to counter these new threats. The upgrades and updates are mostly done during peacetime operations but, when necessary, urgent upgrades and updates might be required during war times. If the EW systems are purchased "as is" and have no access granted to a threat library or jamming algorithms, users of these systems might face difficulties employing their EW systems effectively against an opponent who introduces a new radar or communication system or a guided missile that the relevant EW systems cannot recognize. Therefore, EW systems are strictly controlled technologies, and developing national EW systems indigenously comes with great security benefits.

Figure 2: Frequency and Wavelength Classification of Electromagnetic Spectrum in Military Applications Such Radars and Communication Systems



EW can be applied from all four domains (air, sea, land, space) by manned and unmanned systems and target the enemy's communication systems, radars, or other military and civil assets. The EW can be divided into three major subdivisions:

1. Electronic Support Measures (ESM):

The main task of ESM systems can be summarized as contributing to the preparation of the picture of the tactical situation by detecting and diagnosing the electromagnetic (EM) broadcasts (in the frequency band defined for the system) of the threat and target radar/radars in the operational environment where the platform is deployed. Traditionally ESM is used to perform the task of target identification and classification of threats that could come from all four domains. Moreover, electronic support measures (ESM) gather signal intelligence through passive "listening" to electromagnetic radiations of military systems.

2. Electronic Attack (EA):

It is also known as electronic countermeasures (ECM), and it involves the offensive use of EM energy, directed energy to attack command-control facilities, or electronic equipment with the intent of degrading, jamming, or confusing enemy combat capabilities. EA systems protect the platform on which they are used against RF broadcasting radars or missiles by actively jamming radar systems or missile seeker heads; on the other hand, they apply preventive active jamming techniques against threats or target radars broadcasting in the operational environment.

3. Electronic Protection (EP):

It is the set of technologies and techniques that protect the EW system against the effects of hostile electronic attacks (EA). When the enemy's EW system attempts to jam/degrade a friendly radar, the EP technology in the friendly radar would resist the jamming and other deception techniques. The EP technologies and techniques should be built-in features of a modern EW system.

A Survey of International Developments in EW Systems

Many military analysts believe that the electromagnetic spectrum will be at the forefront of future warfare while armed forces worldwide have been working on new EW technologies to dominate the battlefield and gain upper hand. USAF Col. Dan Javorsek, a Defense Advanced Research Projects Agency (DARPA) program manager in the Strategic Technology Office, describes the future of EW technologies and developments from a military decision maker's perspective:[5]

"Being able to maneuver in the electromagnetic spectrum is a fundamental tenant of all operations and has been for some time. You can't imagine any modern nation having a program without some expertise in the electromagnetic spectrum. Communications and EW all fit in the same part of the spectrum and you need to be able to manipulate that space.

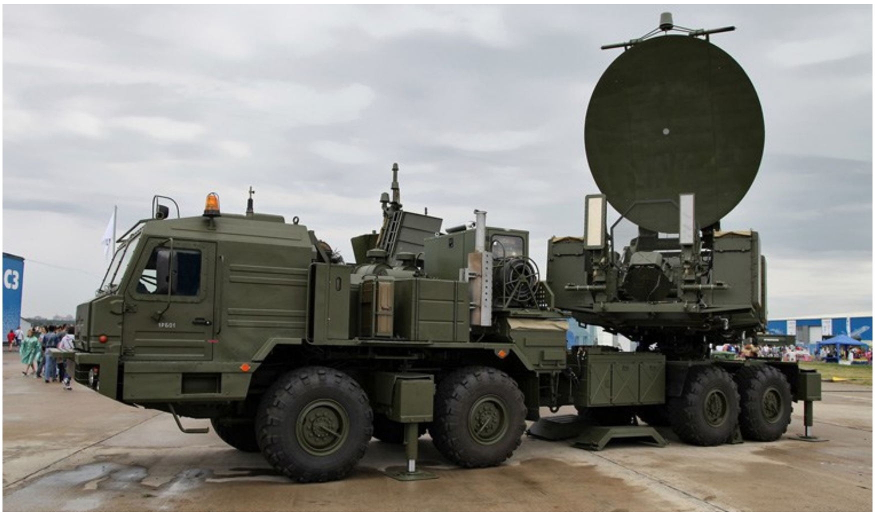
The transition to the digital world gives us a lot of new capabilities, but also a lot more things we need to manage. Most of the time there is an opportunity for the system user to modulate and control that, to use EW in an offensive and a defensive sense. If the user has maximum flexibility, which digital systems give us, that emphasis will move around a lot. The more we can control, manipulate and exploit the electromagnetic spectrum, the technology is really agnostic in terms of offense or defense."

While decades ago, legacy EW systems worked efficiently to counter threats that were also using similar generations of electronics technologies, now threats are evolving much faster than the EW systems. The newer EW systems need to stay ahead of emerging threats while avoiding a quick and costly obsolescence

[5] Stefano D'urso, "Let's Talk About the Digital Evolution of Electronic Warfare", The Aviationist, 26 October 2020, https://theaviationist.com/2020/10/26/lets-talk-about-the-digital-evolution-of-electronic-warfare/

issue that could be caused by the advancement in technologies. EW systems and related technologies are controlled mainly by developed countries but the evolution of semiconductor technology and the affordability of commercial off-the-shelf electronics with increased computing power has started to break the paradigm.

Figure 3: *Krasukha-2 EW System of the Russian Army*



Source: *https://static.themoscowtimes.com/image/1360/05/qmdzgyjftyjW.jpg*

Based on fully digitized, secure, and modular open system design principles, ultra-broadband digital receivers and exciters offer significant advantages over traditional systems. These new technologies enable enhanced frequency coverage, full spatial coverage, and faster response. They are designed to detect, identify, and defeat next-generation sensors and weapons with highly efficient broadband power amplifiers and countermeasure adaptive modulation.

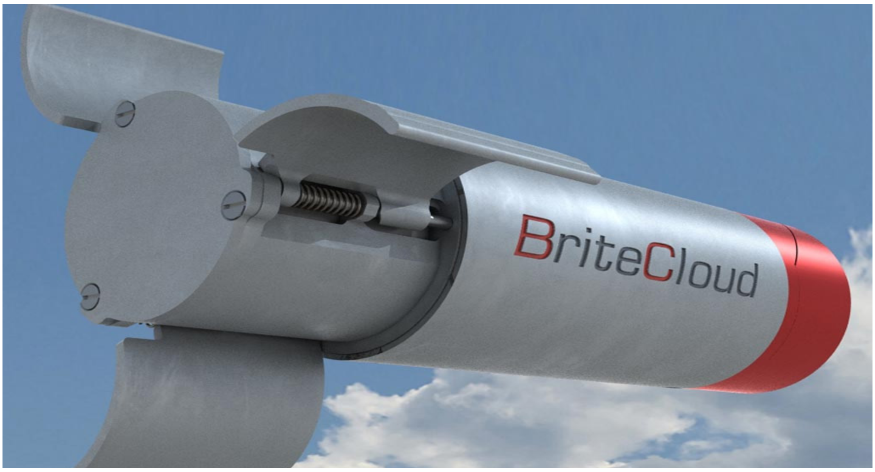
Digital systems are the solution to the problem of the obsolescence issue, as Northrop Grumman[6] stated on its website. Electronic warfare suites can now perform multiple functions, support different mission sets, and share components and software between a family of systems. This building block approach reduces development costs and timelines, accelerates upgrade cycles, and enables economies of scale during production. As new threats emerge, improvements can be quickly communicated throughout the product line. Often, only one

[6] "Why Digital Transformation Matters", Northrop Grummman, https://www.northropgrumman.com/what-we-do/digital-transformation/

software change is needed to add new features, minimize the risk of obsolescence, and reduce time in the field.

Another advantage of the new digital systems described here is the adoption of EW systems by a broader range of platforms, while until less than two decades ago they were exclusively used on tactical aircraft such as F-16s, F-15s, the Tornado, etc. This now includes cargo and air refueling aircraft, unmanned air vehicles (UAV), and intelligence assets. Opting for fully digital EW systems would allow for smaller and more compact systems, which will mean they could fit into smaller platforms. Moreover, using an open systems architecture will provide easy maintenance and software updates, which in turn will make the system cost-effective. A good example of scalability/miniaturization of EW systems can be seen in Leonardo's Brite Cloud Digital RF Memory (DRFM) Countermeasure, a smart chaff system miniaturized to fit into a chaff/flare cartridge launcher used by fighter aircraft such as F-15s, F-16s or even smaller UAVs. According to the producer (Leonardo[7]), the BriteCloud Expendable Active Decoy (EAD) is a compact, DRFM-based active RF countermeasure that can defeat the majority of RF-guided surface-to-air and air-to-air threat systems. BriteCloud is designed to be dispensed from standard chaff/flare dispensers and therefore requires minimal platform integration. Utilizing advanced techniques, it is effective against active and semi-active RF seekers, and fire control radars.

***Figure 4:** BriteCloud Smart Decoy System*



***Source:** https://electronics.leonardo.com/en/products/britecloud-3*

[7] "The BriteCloud Expendable Active Decoy (EAD)", Leonardo, https://www.leonardocompany.com/en/products/britecloud-3

The compact size of electronic countermeasures like the smart chaff system provides military aircraft protection against air-to-air missiles and ground-to-air missiles for self-defense. During air-air engagements, the smart chaff can give an extra layer of protection against beyond visual range (BVR) missiles by creating false targets around the aircraft. Similarly, there are towed decoys that are commonly used by the USAF and U.S. Navy aircraft. In towed decoy operations, the aircraft releases the decoy to a safe distance from the aircraft and then the decoy broadcasts jamming signals or presents itself as a real aircraft by giving off a larger radar cross-section compared to the aircraft. This solution protects the aircraft from home-on jamming capable Aim-120 AMRAAM type missiles or other radar-guided ground-to-air defense missiles. Raytheon's AN/ALE-50 Towed Decoy system is currently operational on F-16s, F/A-18s, and B1s. It has protected aircraft against radio frequency (RF) missile threats in Kosovo, Afghanistan, and Iraq.[8]

[8] "AN/ALE-50 Towed Decoy", Raytheon Technologies, https://www.raytheon.com/capabilities/products/ale50

Recent Developments of EW Technologies in Israel

Israel is the leading EW powerhouse in the Middle East and has been using EW systems extensively since the Yum Kippur War in 1973. Israel's defense companies produce a wide range of EW systems used in all domains of the battlefield and have also exported these systems to foreign armies. Currently, Israel maintains a range of locally built fleets of Airborne Early Warning and Control (AEW&C) and ELINT/SIGINT/EW aircraft based on Gulfstream G550 business jets, which are code-named Shavit (ELINT/SIGINT) and Eitam (AEW&C aircraft). These special mission aircraft allow the IDF (Israeli Air Force-IAF) to conduct missions far from Israel and to support strike missions carried out by the Israeli Air Force in Syria and other classified locations. All IAF jets, including F-16Is and F-15Is, have locally built advanced EW self-protection suits or EW pods carried externally. The capabilities of these jets and special mission aircraft have been constantly demonstrated in strike missions over Syria and Lebanon. Many of these missions are highly classified, and not much information has been released about the status of the aircraft used in those missions; however, it is known that the IAF lost one F-16I on Feb. 5, 2018, due to Syrian air defenses. The IDF's new F-35 Adir[9] is also expected to have an indigenous or customized EW suite (AN/ASQ-239 electronic warfare suite) to fit Israel's requirements.

In a recent news article[10], it was revealed that Israel has recently introduced a new electronic warfare system called Scorpius, which is designed and produced

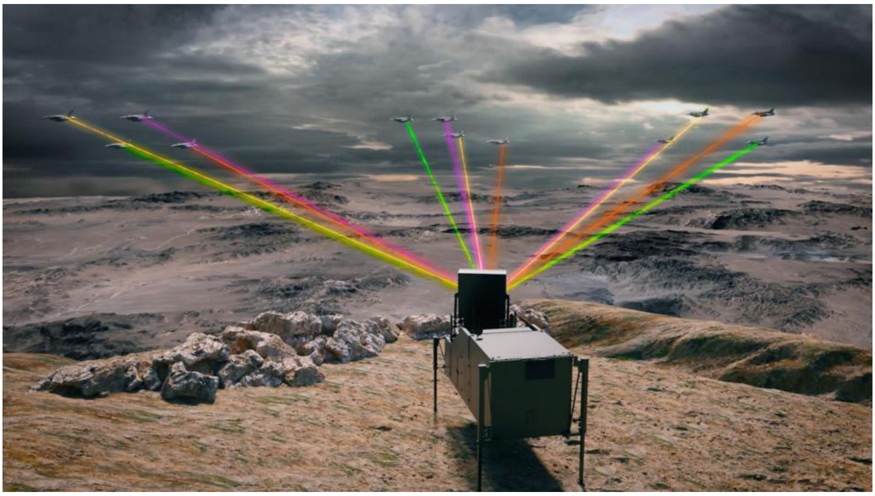
[9] Mark Episkopos, "Israel's F-35I Adir: The Most Dangerous Fighter on Earth?", The National Interest, 8 January 2021, https://nationalinterest.org/blog/buzz/israel%E2%80%99s-f-35i-adir-most-dangerous-fighter-earth-176008

[10] Paul Iddon, "Israel Unveils 'Revolutionary' New Scorpius Electronic Warfare System", *Forbes*, 11 December 2021, https://www.forbes.com/sites/pauliddon/2021/11/11/israel-unveils-revolutionary-new-scorpius-electronic-warfare-system/?sh=72d7a0ff2fdd

by Israel Aerospace Industries. The article states that Scorpius has capabilities that will revolutionize electronic warfare. Unlike older generation EW systems, Scorpius uses active electronically scanned array (AESA) technology to scan the airspace. It can also send narrowly targeted beams electronically formed at a specific wavelength and frequency in a specific direction against targets to disrupt hostile data communications, navigation systems, and radars without interfering with friendly forces.

Before the innovation of such narrow beams, operators of EW systems only had two options. They could either aim a single narrow beam around the sky in search of a target, which is very difficult to do, or use a wider beam. While prior EW systems can neutralize specific targets, or perhaps a couple of targets, Scorpius can take out anything in the sky and engage multiple targets simultaneously. Basically, Scorpius uses a wide beam to scan for potential threats in all directions and narrow beams to target specific threats thanks to the combined use of AESA, Microwave Monolithic Integrated Circuit (MMIC), Digital Frequency Radio Memory (DFRM), and artificial intelligence/adaptive machine learning (AI/AML) technologies used in the system design. Scorpius has land, air, and naval applications based on the operational needs of the military.

Figure 5: *Scorpius-G System from IAI (Israel Aerospace Industries)*



A Special Case EW; Israel’s Cyber Warfare Application

Cyberattacks are a common phenomenon in today’s highly networked business and internet environments. Attackers usually infiltrate the computer system of a company and then hack it or plant a virus to damage the computer systems or collect secret data or even ask for ransom money. Something similar to these real-life cyberattacks could be performed by the newer EW technologies. A land-based EW system or Stand Off Jammer/SIGINT aircraft will be fielding cyber-attack technologies that will allow it to hack or plant malware (virus) into the enemy's command and control networks.

In fact, open-source information provided by some researchers[11] suggests that IAF's Operation Orchard against a Syrian nuclear installation, near the Syrian city of Deir el-Zour in 2007, was largely attributed to a cyberattack carried out by the IDF's EW platforms that supported the strike mission and blinded the Syrian radar networks. According to U.S. aerospace industry experts and retired military officials, the Israelis utilized a technology similar to the U.S.-developed "Suter" airborne network attack system, developed by BAE Systems and integrated into U.S. unmanned aerial vehicle operations by L-3 Communications. Israel has long been adept at using unmanned systems to provoke and spoof Syrian surface-to-air missile (SAM) systems, as far back as the Beqaa Valley engagements in 1982.

Even though the details of IDF's operation are still unknown, either employment of cyberattack or effective jamming (the DRFM method could result in a similar outcome) would be among the possibilities.

[11] Fulghum & Barrie, "Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target", ABC News, 8 October 2007.

The Recent Developments of EW Technologies in the U.S.

The first paragraph of the U.S. Department of Defense's 2020 Electromagnetic Spectrum Superiority Strategy Document[12] starts with the following statement, which indicates the importance of controlling the electromagnetic spectrum (EMS) from the U.S. perspective:

"The Nation has entered an age of warfighting wherein U.S. dominance in air, land, sea, space, cyberspace, and the electromagnetic spectrum (EMS) is challenged by peer and near peer adversaries. These challenges have exposed the cross-cutting reliance of U.S. Forces on the EMS, and are driving a change in how the DoD approaches activities in the EMS to maintain an all-domain advantage.

The core of the U.S. Navy's EW capability relies on the EF-18G Growler, which became the standard EW aircraft of the U.S. Navy after retiring EA-6A Intruder electronic warfare aircraft in the early 1990s. EF-18G is purpose-built for EW missions and it is the derivative of the U.S. Navy's two-seat F/A-18F strike fighter. The Growler carries several EW pods for self-defense or offensive purposes. Its main mission is about escorting carrier strike packages against enemy air defenses or providing EW protection against enemy interceptors by jamming them from a long distance. The current EW pod ALX-99 is an older generation EW pod, but the U.S. Navy is in the process of accepting the ALQ-249 NGJ (Next Generation Jammer).[13]

[12] "Electromagnetic Spectrum Superiority Strategy," U.S. Department of Defense, October 2020.

[13] Tingley & Rogoway, "Navy's New Jamming Pods For EA-18G Growler Eyed for Air Force Fighters", The Drive, 28 July 2021, https://www.thedrive.com/the-war-zone/41727/navys-new-jamming-pods-for-ea-18g-growler-eyed-for-air-force-fighters

According to Raytheon, who developed the ALQ-249 NGJ, it can offensively reject, disrupt, and degrade hostile threats such as air defense systems and communications equipment. It also uses the latest digital, software-based, and Active Electronic Scan Array (AESA) technology to engage multiple targets over longer distances. The ALQ-249 NGJ can attack multiple targets at the same time and has a modular architecture that allows it to be quickly upgraded and expanded to a variety of missions and platforms.

The ALQ-249 NGJ has at least three versions with low band, medium band, and high band capabilities incorporated in each pod. The EF-18G can carry two pods in one mission depending on the threat radar's expectations to have full coverage for multiple band jamming (UHF/VHF to S, L, X bands).

Surprisingly, the USAF lost its escort/stand-off EW jamming capability after retiring the EF-111A Raven in 1998 and is currently operating the EH-130H Compass Call EW aircraft, which is designed for electronic signal intelligence (ELINT) and communications jamming from a long distance by listening and jamming radio communications (UHF/VHF/FM bands) and cell phones, if necessary. The USAF's current EW capability relies on the self-defense pods, such as the AL-131C, carried by F-15s and F-16s. The fifth-generation F-22s and F-35s have built-in, integrated, highly advanced EW suites like the AN/ALR-94[14] and AN/ASQ-239[15], respectively. The AN/ASQ-239 EW suit in F-35 provides comprehensive broadband protection against new-generation radar threats and also suppresses enemy radars via active jamming and DRFM capability. Its ability to operate in dense threat environments protects F-35s from radar or infrared seeker-guided missiles. Moreover, the platform-level design improves reliability and maintainability and also optimizes long-term life cycle costs.

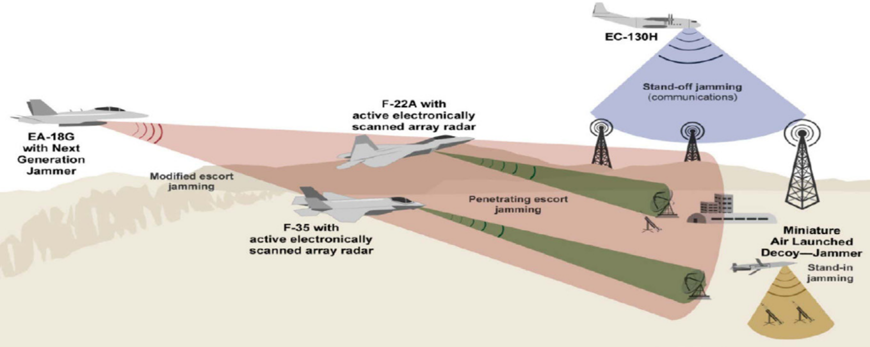
The F-35's AN/ASQ-239 EW system is also integrated with the Electro-Optical Targeting Sensor (EOTS) to have full (360-degree) self-defense EW coverage and also active electronic attack (EA/ECM) capabilities using the APG-81 AESA radar as part of the AN/ASQ-239 EW system. Even though the APG-81's main role is to detect air and ground targets (SAR/GMTI modes), it can also be used as a jammer as part of the integrated AN/ASQ-239 EW system. This capability gives F-35s a highly effective and long-range EW performance.

[14] "AN/ALR-94 F-22 Electronic Warfare System", BAE Systems, https://www.baesystems.com/en-us/product/an-alr-94

[15] Ibid.

In a recent development, in the House Armed Services Committee (HASC) press release issued on July 28, 2021, the Subcommittee on Tactical Air and Land Forces announced a proposal to include a provision in the Fiscal Year 2022 National Defense Authorization Act (NDAA)[16] that would require an assessment of Air Force airborne electronic attack capabilities and the feasibility of integrating the ALQ-249 Next Generation Jammer on Air Force tactical aircraft. This statement came as a surprise but considering the USAF's lack of an escort jammer platform, it would make sense to integrate the ALQ-249 Next Generation Jammer with F-15EX. The USAF is tailoring F-15EX to support future air campaigns to carry heavier bombs and air-to-air missiles in support of fifth-generation F-22s and F-35s. Integrating ALQ-249 NGJ pods on F-15EX will provide escort jamming/stand-off jamming capability. The figure below depicts the USAF's future jamming capability using several platforms.

***Figure 6:** A Joint EW Application Concept Using Several Aircraft; while the EA/18G and EC-130H provide stand-off jamming, F-35s and F-22s can provide EW capability in the close range alongside miniature decoy jammers.*


EC-130H
Stand-off jamming (communications)
F-22A with active electronically scanned array radar
EA-18G with Next Generation Jammer
Modified escort jamming
Penetrating escort jamming
F-35 with active electronically scanned array radar
Miniature Air Launched Decoy—Jammer
Stand-in jamming

***Source:** https://breakingdefense.com/2019/12/wholl-fix-ew-task-force-gropes-for-answers/*

There are published articles discussing the possibility of the ALQ-249 NGJ having artificial intelligence/adaptive machine learning (AI/AML) and cyberattack capability to complement the EW attack capabilities of the EF-18G Growler as well as performing SEAD/DEAD missions (using AGM-88 HARM anti-radar missiles), which would be giving the U.S. Navy three different mission profiles: jamming threat radars, SEAD/DEAD missions, and hacking enemy radar networks. With the 2022 NDAA bill, the USAF could be getting similar capabilities using the F-15EX as a 4.5th gen. platform.

[16] National Defense Authorization Act for Fiscal Year 2022, U.S. Congress, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text

Another recent example of using artificial intelligence (AI)/adaptive machine learning (AML) technology on an EW system is called the Angry Kitten EW pod, which is being integrated on USAF F-16s. The Angry Kitten EW pod uses adaptive machine-learning software and chooses the *"optimal jamming technique from available options in the library"* during an EW attack and finds the best possible jamming technique.

One of the Angry Kitten EW pod developers, research engineer Stan Sutphin[17], states they are currently developing fully adaptive and autonomous capabilities that are not available in legacy jammers. With a cognitive electronic warfare approach, based on machine learning algorithms and advanced hardware, they are confident that the Angry Kitten EW system can provide significantly higher levels of electronic attack and protection capabilities and enhance the security of U.S. fighters.

Similarly, the USAF's traditional tactical aircraft EW pod ALQ-131 has been upgraded with new EW technologies. The new pod has been designated as ALQ-131C[18] and incorporates fully digital DRFM, highly sensitive wideband receivers, and coherent and/or non-coherent jamming techniques. Mostly USAF and Allied F-16s will benefit from this capability since the ALQ-131C is carried on the center pylon of the F-16s.

[17] Inder Singh Bisht, "USAF Tests 'Angry Kitten' Electronic Warfare Pod on F-16", The Defense Post, 10 November 2021, https://www.thedefensepost.com/2021/11/10/usaf-tests-electronic-warfare-pod/

[18] Revolutionized through digital technology, The Northtop Grumman, https://www.northropgrumman.com/what-we-do/air/an-alq-131v-electronic-countermeasures-ecm-pod/

Russian Approach to EW Warfare

The electronic warfare (EW) capabilities of the Russian Armed Forces have been one of the prioritized areas of military modernization over the past decade for Russia. The domestic defense industry has continuously supplied the Russian Armed Forces with improved versions of a number of modern EW systems including Krasukha-4, which is a land-based, highly effective, modern EW system, and Borisoglebsk-2, which is designed to jam mobile satellite communications and radio-navigational units.

The Washington-based Center for Advanced Defense Studies (C4ADS) published a report[19] indicating that four Russian EW systems were identified as the well-known Krasukha-4 at the Khmeimim airbase, the R-330Zh Zhitel jamming station deployed at Aleppo airport, Samarkand and Rosevnik-AERO electronic warfare systems. The main purpose of these EW systems was to jam or degrade any threats that are aimed at Russian airbases in Syria.

Russia paid special attention to jamming Global Positioning System (GPS) signals to make them unavailable in the vicinity of the Russian operational areas. One of the reasons is to prevent swarming drone attacks that took place against Russian forces by the Syrian opposition forces several times in the past years. GPS spoofing is another technique used by the Russian forces. GPS spoofing is basically done by creating false positioning information for adversary aircraft or GPS-guided missiles. The fake GPS signals are broadcasted on the same frequencies used by the U.S. GPS satellites to prevent receivers from locking on to the real GPS signals. Once Russia's fake GPS signal is locked on instead of the real GPS signal, the EW system begins to transmit false positioning, navigation,

[19] Above Us Only Stars, (C4ADS Rapor, 26 March 2019).

and timing (PNT) data to give false location information, therefore, causing the adversary aircraft or missiles to miss their intended targets.

One of the well-written reports about the Russian EW capabilities can be accessed from the Georgetown Security Studies Review based in Washington, D.C. The report[20] states that the Russian forces modernized their EW capability in recent years and most importantly Russian operators have gained considerable EW experience in Ukraine and Syria in real-time war conditions. The report further argues that although the U.S. continues to possess military superiority in conventional weapons, Moscow now possesses a critical asymmetrical advantage that seeks to bridge this gap. In an age of renewed competition with Russia, the U.S. will need to increase its proficiency in EW missions or risk falling behind. This conclusion has also been supported by U.S. military officials on several occasions.

[20] Madison Creery, "The Russian Edge in Electronic Warfare", Georgetown Security Studies Review, 26 June 2019, https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/

China's EW Ambitions in the South China Sea

The Chinese military has been investing heavily in improving its electronic warfare (EW), communications, and intelligence-gathering capabilities in recent years. Many of the newly developed EW systems have started to be seen on Chinese military aircraft, naval or land platforms. Moreover, the Chinese military is in the process of improving its land-based EW, communications, and intelligence-gathering capabilities in the South China Sea. Open-source[21] satellite imagery reveals that China has built large EW complexes on Hainan Island and also on some of the reefs in the South China Sea. These land-based and island-based SIGINT/ELINT complexes provide the Chinese army with the ability to track and gather signal intelligence from foreign military forces operating in the region.

It can be said that the Chinese military is closely following the U.S. Navy's footsteps to develop its military force structure and military hardware. In this respect, we can even see very close copies of the U.S. Navy's MH-60R Seahawk and E-2D Hawkeye (AEW&C) in the inventory of the Chinese military. China's new KJ-600 Airborne Early Warning and Control aircraft (AEW&C) will be operated from Chinese-built aircraft carriers as well as the islands in the South China Sea. The KJ-600's main role is to provide early warning of aircraft and surface ships but its onboard ESM systems also provide signal intelligence.

On the airborne tactical jamming capability, the Chinese military has recently introduced a specially configured J-16D fighter jet, which is an equivalent of the U.S. Navy's EA-18G Growler, into their inventory. The J-16D can carry four standoff jamming pods, two on the wingtips and two on under-wing hardpoints. These

[21] Funaiole & Bermudez & Hart, "China Is Ramping Up Its Electronic Warfare and Communications Capabilities Near the South China Sea", CSIS, 17 December 2021, https://www.csis.org/analysis/china-ramping-its-electronic-warfare-and-communications-capabilities-near-south-china-sea

pods, designated as RKZ930-22 and RKZ930-32, respectively, detect, identify, locate, and analyze radio frequency emissions of hostile targets. According to Chinese sources,[22] these passive pods are heavier and larger than previous types. Covering the 0.05-20 GHz frequency range, a power level of 100 kW allegedly gives a range of more than 150 kilometers. The naval version J-15SD is expected to operate from Liaoning (Type 001) and Shandong (Type 002) aircraft carriers to provide airborne EW capability similar to the U.S. Navy's EA-18G. Both the J-16D and J-15SD will be the backbone of China's jet-based EW capability along with the 5th generation J-20 premium multi-purpose aircraft.

For ground-based systems, Chinese companies offer a range of EW systems for domestic and export markets from simple VHF/UHF band jammers to more advanced radar jammers. One of the new generation systems is the truck-mounted CHL-903 ESM/EA system, which performs wide frequency electronic signal intelligence and jamming capability over the battlefield. This system has been exported to Algeria.

On the naval side, China's new Type 052D and Type-55 destroyers and cruisers are integrated with advanced ESM/ECM systems. Details of these systems have not been made public but both ship classes are using mast-mounted Type 346A and Type 346B S-band AESA radars, respectively. The Type 346B is an upgraded version of the Type 346A model (used on Type 052D destroyers) and uses gallium nitride (GaN) technology with less cooling requirements and longer ranges. Even though the capabilities of the Type 346B haven't been released to the public, it could be similar to the U.S. Navy's new SPS-6 AESA radar, which will be replacing the decades-old SPS-1 PESA radars. Considering Type 346B's aperture size (the size of an AESA antenna), it is highly likely that Type 346B can also be used for jamming hostile radars if necessary.

As expected, China has adopted an information warfare (IW)[23] strategy, called "Integrated Network Electronic Warfare" (INEW), that consolidates the offensive mission for both computer network attacks (CNA) and cyberattacks via electronic warfare (EW). China's cyberattack strategy is considered a non-kinetic offensive attack tool to degrade opposing sides' war fighting capabilities. These attacks can be directed toward not only military command and control networks

[22] "China Shows off New Military Gear in Zhuhai", ANI, 5 Ekim 2021.

[23] Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare", *Journal of Defense Studies*, Volume: 4, Issue: 2, (2010).

but also the power distribution centers, financial institutions, weapon system production factories, etc.

Overall, China’s long-term investments in the microchip and electronics industry have started to show their value regarding military electronics production capability in terms of new military AESA radars and EW systems. Combining these high technology chip and semi-conductor production capabilities with China’s almost endless software development infrastructure, China could remain one of the top EW systems producers in the world.

The EW Capabilities of Türkiye

Türkiye's military threat perception is very unique and requires self-sufficiency in use and also in the production of military weapon systems. Even though Türkiye is a member of NATO and one of the most active participants in NATO missions, Türkiye has often faced problems purchasing or obtaining certain critical technologies from NATO allies. In addition to the difficulty of obtaining critical technologies and facing sanctions from allied nations, Türkiye's geographical location and historical rivalry with neighboring countries also dictate Türkiye develop its own military concepts of operations and investment in certain critical technologies such as EW, radar, guided missiles, electro-optical systems, and command-control systems, among others.

Türkiye's military electronic system development and production efforts gained speed right after the U.S. sanctions were placed on the Turkish Armed Forces because of the Cyprus Peace Operation in 1974. The establishment of Aselsan, the Turkish defense electronics company, in 1976 was an important step for Türkiye to become self-sufficient in military communications, radars, command control systems, and electronic warfare technologies in later years.

Through the years, Aselsan became the main supplier of the range of EW systems for the Turkish land, air, and naval forces as well as internal security forces such as the Turkish Police or the National Intelligence Organization. Aselsan has also exported indigenously developed EW systems to other friendly nations.

The Turkish Defense Industry's portfolio of EW systems ranges from a simple UHF/VHF direction finder/jammer to the most sophisticated ESM/SIGINT/ELINT and EA/ECM systems that incorporate modern electromagnetic signal detection and EW/jamming techniques, including Active Electronic Scanned Array (AESA) and Digital Radio Frequency Memory (DRFM) technologies.

A Review of the Turkish Defense Industry's EW Productions Capabilities

Naval EW Systems of the Turkish Navy

The naval platform ESM System called ARES-2N[24], produced by Aselsan, is the first ESM system to be integrated into the Turkish Navy onboard the first ADA Class Corvette, TCG Heybeliada. The name ARES is derived from the abbreviation of "Aselsan Radar ESM System." The system has the capabilities of detection, identification, classification, tracking, direction finding, geolocation, audible warning, platform-related parameters, and emitter parameters recording. The ARES-2N, which operates in the 2 GHz to 18 GHz frequency range, can detect radar signals in broadband and uses the mono-pulse direction-finding technique in broadband with a high signal processing speed. The system has sensitive parameter measurement and unique emitter identification capabilities and can automatically track the emitters detected and determine their locations. With its broadband feature, ARES-2N is claimed to have a very high probability of detection. The high processing speed and sensitivity level ensure the detection capability of low output power radars at long distances. Due to its band selectivity, the system is reported to be able to operate under CW or Pulse Doppler signals without the desensitization that broad frequency band systems are exposed to.

The ISTIF Class Frigate TCG İstanbul and LHD Anadolu are also being fitted with an updated ARES-2N(V)2 Radar ESM. The BARBAROS class frigates will be upgraded to ARES-2N(V)2 configuration during their MLU program. Contrary to the ARES-2N System, which operates in the 2 GHz to 18 GHz frequency range, the ARES-2N(V)2 can cover 2-40 GHz frequencies and can also be extended to cover 0.5-2 GHz, and it features new generation wide-band receivers improving instantaneous bandwidth and receiver parameters. To extend its frequency coverage, a pair of digital receiver (RX) antennas will be integrated (to be located just above the AREAS-2NC R-EA's TX antennas) on the mast of the BARBAROS Class Frigate.

According to Aselsan, the ARES-2N(V)2 Radar ESM will feature detection of LPI emitters, high POI, low probability of false alarm, and very high direction-finding accuracy.[25]

[24] İbrahim Sünnetçi, "Naval Electronic Warfare Systems & Turkish Naval Forces", *Defence Türkiye*, Issue: 110, (October 2021).

[25] Ibid.

Meanwhile, the ISTIF Class Frigates (the first ship of its class will be commissioned in 2023) will be integrated with the AREAS 2NC Radar EA/ECM System and a pair of sub-band and high-band TX antennas (jamming heads/steerable transmitter units).

Aselsan also developed the ARES-2SC ESM System to meet the requirements for the radar electronic support measure system to be used in Turkish Navy submarines. In the first phase, the system was integrated into two AY Class (Type 209/1200) Submarines (the TCG Doganay and TCG Dolunay) in 2013, and the ARES-2NS model of the system was selected for the REIS Class Type 214TN submarines. The ARES-2SC performs functions such as detection, identification, classification, and display (in the suitable format), automatic and manual recording, and replaying capabilities toward radar systems broadcasting in the 2-18 GHz band along with radars that have a low probability of detection. The system, with 360 degrees of horizontal azimuth coverage, has a compact antenna resistant to high pressure, high technology broadband digital microwave receivers, and high data processing capability. To reduce the acoustic signature, a liquid cooling system is used in the ARES-2SC, which meets the MIL-STD-810F environmental and MIL-STD-461E electromagnetic induction/electromagnetic compatibility (EMI/EMC) standards. The pressure-tight compact antenna structures, the high-tech wideband digital microwave receiver, and sophisticated design enable the ARES-2SC to perform ESM missions reliably and successfully within a short reaction time.

While the ARES-2SC with the single balcony compact antenna and wide-band microwave receiver structure for AY Class Submarines and ARES-2NS Radar ESM Systems with the twin balcony antenna structure for Type 214TN REIS Class Submarines are currently available, the ARES-2NCL ESM System (2-18 GHz) with the single balcony compact antenna structure and combining both Radar Warning and ESM antennas for the FPBs has also been developed. Aselsan also exported “ARES-2NCL Extended” RESM Systems to the Pakistan Navy. They are believed to be mounted/or already mounted on two platforms in the inventory of the Pakistan Navy. Moreover, Aselsan also delivers the ARES-2SC/P RESM System under the Pakistan Navy Agosta 90B MLU Project which is carried out by STM, the main contractor of the project.

For the land application, the ARES-2 Series Radar Electronic Support Measures (ESM) System of Aselsan will be integrated into the Naval Forces Command (TNFC) Long Horizon Maritime Surveillance System, which plays a critical role in protecting Türkiye's interests in the surrounding seas. The Long Horizon System was put into use in the Aegean Sea under Phase I of the project, then extended to cover the Eastern Mediterranean with two additional Suricate Mk2 Surface and Air/Coastal surveillance radars. A total of five Suricate Mk2 Radars supplied within the scope of the Long Horizon System were deployed at the related sites established in Gökçeada, Bozdağ, Kuşadası, Kaş, and Kantara (TRNC). Moreover, three units of DR3000S Radar Electronic Support Measure (ESM) Systems from Thales were supplied in Phase I.

To provide the active jamming capability for the Turkish Navy, the state-of-the-art AREAS-2N Radar EA/ECM System, which features AESA arrays that can generate RF energy (electronic attack waveform) in a very tight beam format (pencil beam) to attack the RF systems threatening the ship, has been developed by Aselsan. Since the system can move and steer beams within microseconds and can put multiple beams out simultaneously, the AREAS-2N can engage multiple targets/threats at the same time.

According to Aselsan, the AREAS-2C Radar EA System covers 8-18 GHz frequencies (but is extendable to various frequency coverages) and is capable of applying both Coherent and Non-Coherent jamming techniques, and it has similar and even better capabilities than the Scorpion II Radar EA System. Therefore, having two independent jamming antennas/steerable RF transmitter units, and employing the DRFM technology, AREAS-2NC is claimed to jam/degrade up to 16 simultaneous RF emitters.

The LHD ANADOLU, amphibious assault ship, will be fitted with a comprehensive integrated ESM and ECM suite including Aselsan's ARES-2N(V)2 ESM and new generation AREAS-2N Radar EA/ECM Systems. Featuring both wide and narrow band digital receivers, Digital RF Memory (DRFM, for modern coherent threats), and solid-state power amplifiers, the AREAS-2N will include a total of four AESA antennas (each covers a 90-degree field of view and incorporates over 1,000 T/R modules) of which two of them will be deployed on the port and the remaining two on the starboard side of the ships. Thanks to its directional RF radiation capability, which enables deceptive and noise jamming techniques in a dynamic threat environment, the AREAS-2N Radar EA/ECM System can jam/deceive up to 32 threats.

Developed by TÜBİTAK MAM Materials Institute, the MAM-TFDLS[26] is a ship-deployed anti-missile floating decoy system that will be able to seduce, distract, or confuse approaching RF-guided missiles. It complements other active and passive soft-kill and hard-kill countermeasures on board the ship. Floating decoys are used as off-board passive targets against RF-based threats (radar-guided missiles, surveillance and fire control radars, etc.) as part of electronic countermeasures (ECM), especially as part of the naval electronic warfare concept.

One of the Turkish Navy's most secretive projects is the TCG UFUK ship, which was commissioned in November 2021 and entered into service in January 2022. It is designed to provide stand-off ESM/SIGINT and possibly EA/ECM capabilities to the Turkish Navy. Even though not much technical information was released about the EW systems used on board the TCG UFUK, we can anticipate that all available EW capabilities of the Turkish defense industry, mainly Aselsan, were incorporated on the ship. With the commissioning of the TCG UFUK, the Turkish Navy can monitor warship activities around Türkiye's coastlines and gather RF signals (including communications and wide range radar bands), emitted by the hostile warships from long distances. We can anticipate that the TCG UFUK has advanced (and also powerful) versions of Aselsan's ARES-2 ESM/EA systems integrated with the ship's combat management system.

One of the futuristic projects of the Turkish Navy is called the NAZAR Project[27] which is carried out by METEKSAN Defense and ALTINAY within the scope of the Turkish Navy's requirements. NAZAR is a Directed Infrared Countermeasure (DIRCM or Laser Electronic Attack System) System that uses a low power (power requirement is less than 10 kW) laser system designed to blind adversarial electro-optical and infrared sensors by projecting a dazzler laser beam at them. The NAZAR Naval System was planned to be used in TF-2000 Destroyers. After the production is completed, this system is expected to be installed on the LHD Anadolu for testing purposes. The Lite version will operate in several wavelengths (depending on customer decision) and will be lighter, so it can be installed on smaller surface platforms such as fast attack crafts, corvettes, or frigates. Thanks to its longer engagement range compared to existing CIWS, the NAZAR system can also be effectively used in simultaneous, salvo, or swarm

[26] "TÜBİTAK MAM at IDEF", TÜBİTAK MAM, 24 August 2021, https://mam.tubitak.gov.tr/en/haber/tubitak-mam-idef

[27] Interview, "NAZAR Projenin Başından İtibaren TF-2000 İçin Uygun Bir Elektronik Karşı Tedbir Sistemi olarak Düşünüldü!", *Defence Türkiye*, Issue: 110, (October 2021).

attack scenarios. It can quickly deal with multiple threats by engaging in succession. After blinding the first threat, it can immediately engage the second.

Airborne EW Systems of the Turkish Air Force

The Turkish Air Force also operates several special mission aircrafts such as the E-7T AEW, CN235M SIGINT/ELINT, and C160D MILKAR. These aircraft are equipped with special electronic warfare and signal intelligence hardware and pods.

The TURAF received delivery of four Boeing E-7T AEW platforms between 2015 and 2017. The E-7T operates Northrop's MESA L-band AESA radar and is integrated with Elta's ESM/ELINT system. The L-band AESA radar provides a 400 km+ detection range against fighter-type aircraft, while its ESM/ELINT system can detect, classify and geolocate RF emitters from long distances. With this capability, the TURAF can actively or passively detect air targets, naval warships, and land-based air defense systems from long distances. The E-7T can automatically share this intelligence information with joint command centers and aircraft nearby via encrypted datalinks such as Link-16.

The TURAF also operates at least three CN-235 ELINT/SIGINT (named Goren-1) special mission aircraft with Aselsan-made MILSIS-II signal intelligence pods. CN-235 ELINT/SIGINT aircraft operate near the battlefield or enemy's positions to collect communications or radar frequency signals and classifies them according to their types and roles on the battlefield. The signal information is later analyzed and decrypted for later use. For example, if an enemy introduced a new type of radar on the battlefield, the Goren-1 aircraft can detect this new radar's RF signal and operational modes. Then this information is used to develop countermeasure algorithms to jam or for deception purposes as well as to update the threat library of the friendly aircraft's EW systems.

The TURAF's C-160 MILKAR-2U EA/ECM aircraft supports air operations by jamming/confusing early warning or air defense radars of the enemy forces. With this capability, the TURAF can jam or degrade enemy air defense radars' effective ranges and reduce the likelihood of interceptions by the land-based air defense systems. In the near future, C-160 MILKAR-2U EW platforms will be replaced by Stand of Jamming Air Craft (SOJ).

At the tactical level, TURAF F-16s and F-4E/2020 fighter aircraft are integrated with self-protection EW suits. All Block-30/40 F-16s (under the Peace Onyx-I project) have been internally installed and integrated with full ALQ-178V3 EW suits that provide radar warning, jamming, and countermeasure dispensers for flare and chaff. 60+ F-16C Block-50s (Under Peace Oynx-II) were more recently integrated with more advanced ALQ-178V5+ with added low band jamming and DFRM capabilities. The last 30 F-16 Block-50+ (Under Peace Oynx-IV) are installed with Harris ALQ-211 V4 internal EW suits. In most recent years, the TURAF also decided to purchase 21+19 Harris ALQ-211 V9 EW pods to equip F-16Ds (two seated) that were not installed with any EW suits due to smaller internal volumes of D versions. Most internally mounted EW suites require enough volume inside the airframe to install EW hardware, LRUs, wiring harnesses, antennas, etc. As a side note, F-16Ds have 13% less internal fuel capacity compared to a single-seat F-16C for the same reason because the second seat in the airframe reduces the availability of internal space. With the acquisition of the ALQ- 211 V9 pods from the U.S., F-16Ds can now be used in the frontline missions such as Escort, CAP or BARCAP, etc.

The Turkish F-4E/2020 operates with ALQ-178 V3 RWR suits (similar to the F-16s ALQ-178V3), but EA/ECM capability was added with Elta EL/L-82225 ECM pods during F-4E Phantom modernization in the early 2000s. The TURAF also obtained the in-house software upgrade and threat library upgrade capabilities of the EL/L-8225 pods.

To complement or replace foreign-made EW pods, the EHPOD[28] (Electronic Warfare Pod) project has been initiated for tactical aircraft in the inventory of the TURAF and it is in the final stages of its testing activities. The EHPOD project is a new generation electronic jamming pod that will be capable of smart jamming through its internal Digital Radio Frequency Memory (DRFM) technology. It will use the outer geometry of the F-16's 300-gallon centerline fuel tank. This pod will be capable of analyzing and geolocating RF emitters, and performing DRFM jamming, deception, and noise jamming. With its broadband, narrow and wideband RWR (Radar Warning Receiver) frequency band coverage, highly accurate geolocation capability, DRFM-based broad beam jamming, and deception/noise jamming capability are optimized according to its design criteria set by the TURAF. Its high RF power output, multiple engagement capability, and high-performance heating/cooling system (Environmental Conditioning System [ECS]) enable the system to operate in all flight profiles as required by the TURAF.

[28] İbrahim Sünnetçi, "Status Report: EHPOD & EDPOD Projects", *Defence Türkiye*, Issue: 99, (June 2020).

Obviously, the TURAF has already invested heavily in obtaining self-protection EW suits for all tactical fighter aircraft. Most importantly, the TURAF has obtained the capability to upgrade the threat library of these mentioned self-protection systems. Whenever a new RF threat is introduced into the battlefield, Türkiye's ELINT/SIGINT platforms can detect these new RF emitters' EM signals and decrypt them to classify the systems and their operational modes. When necessary, new jamming algorithms can be developed and tested before integrating into the fighter aircraft.

One of TURAF's most interesting and powerful EW systems is called KORAL[29], which is a land-based, full-spectrum radar electronic warfare system designed and produced by the Turkish EW powerhouse Aselsan. It became operational in 2015 and saw its first operation in Syria against a wide range of air defense systems, including the Russian S-400 or Syrian air defense systems. The system's architecture is based on the operational needs of the TURAF. The KORAL system consists of two 8x8 military trucks, each carrying Electronic Support (ES System) and a multi-band Electronic Attack System to cover the full electronic spectrum. According to open sources, KORAL uses a phased array antenna structure to perform multi-band electronic support and attack duties. The system also uses the latest Digital Radio Frequency Memory (DRFM) technology to digitally copy the RF threat signals and retransmit them back to the original radar source with fake signal returns by altering the actual radar returns. This way, the threat radar is spoofed with false targeting information, and the air defense systems can misidentify or cannot track real targets for a firing solution. According to open sources[30] again, KORAL is so powerful that it can perform electronic attacks up to a range of 150-200 kilometers against RF threats.

To complete its full EW spectrum of systems, the TURAF is in the process of receiving four units of Stand-Off Jammer (SOJ) aircraft (based on Bombardier's Global 6000 business jets), which will be delivered in the last quarter of 2023. Aselsan is the prime contractor of the project and Turkish Aerospace Industries (TUSAŞ) will be modifying and installing the mission systems on the G6000 aircraft with the help of Aselsan. The SOJ will enable the identification of the enemy's communications and radar systems (for land, naval, or air domains), accurately geolocate their positions, and jam/degrade/spoof them from stand-off

[29] Feridun Taşdan, "TURKISH EW SYSTEMS - The Unseen Force Behind Recent Turkish Drone Successes", *Defence Türkiye*, Issue: 106, (May 2021).

[30] "Koral System to Paralyze the Hostile Radar", *Defence Türkiye*, Issue: 67, (April 2016).

ranges. With SOJ capability, TURAF fighters and other supporting aircraft will be able to conduct their operations closer to the enemy air defenses or deploy their weapons more accurately under the EW protection of the SOJ aircraft.

The information about SOJ's capabilities is kept secret but we anticipate that the SOJ system will feature numerous new technology electronic warfare capabilities including powerful GaN-made AESA antennas and DRFM techniques similar to the EHPOD and KORAL systems. All of the required hardware and software systems to be integrated into the SOJ systems will be developed and manufactured by the Turkish defense companies locally. The modification and certification processes (after SOJ modifications) of the G6000 aircraft to be procured as part of the contract are aimed to be executed in Türkiye by TUSAŞ and other local companies.

One of Europe's extensive EW Testing and Training Range, called EWTTR/EHTES, is built by Havelsan, a Turkish software company in Konya, Türkiye. The range contains wide ranges of real air defense threats or RF emulators to simulate certain radar bands. Some of the air defense systems (ADS) in the range include SA-6 Gainful/Straight Flush Radar, SA-8 Gecko, SA-10B Grumble, SA-11A/B Gadfly, SA-15 Gaunlet/TOR, SA-19 Tunguska, D7 Super Fledermaus Radar, ZSU-23/4 Shilka, Skyguard/Sparrow, Rapier Mk2B, and I-HAWK systems. All of these ADS are instrumented (no real firing of missiles) and their radar engagements are controlled by the operators.

During the engagement phase of the air warfare training flights, EHTES ADS threat radars engage participating aircraft as if it is a real war. In the meantime, training aircraft use their EW systems to eliminate threats by applying jamming or deception techniques available in their EW systems. The results of the engagements are recorded and analyzed during debriefings. The records of all radar tracking and EW jamming data are evaluated to determine if the EW tactics used during the engagements against ADS' threat radars are a success. Thus, the EWTTR/EHTES system helps pilots in real-time if their mission is a success or a failure. EWTTR/EHTES' capability also helps the development of a national RF threat database/ECM jamming library against a wide range of air defense systems in near wartime conditions.

The TURAF's EHTES EW training capability is also very popular among NATO members and other friendly countries. The Anatolian Eagle Exercise takes place in Konya several times a year and invites countries to bring their aircraft/crew to practice air warfare training in predetermined scenarios, including flying in the EWTTR/EHTES range against ADSs to check their EW systems and train their pilots. This training is also necessary for the development of new updates for the EW hardware and software.

Land-Based EW Capabilities of the Turkish Land Forces

When the subject is EW systems, one might think that land forces won't be using EW systems as much as air and naval forces due to the character of warfare conducted by the land forces via tanks, artillery, or assault helicopters, among other platforms. However, the Turkish Land Forces have paid special attention to the employment of sophisticated electronic warfare (EW) systems. In fact, land-based Turkish EW assets are one of the lesser-known types of military hardware around the world and also very unique to the Turkish Armed Forces' operational concepts. Moreover, no other country in NATO, including the U.S., has an extensive land-based EW system like the one operated by the Turkish Land Forces, which has paid special attention to gaining land-based EW capability since 1990 or even before[31].

Throughout the 1990s and 2000s, the Turkish Armed Forces (TAF) have been continuously fighting asymmetric warfare against a separatist terrorist organization called the PKK in the southeastern part of the country. During these counterterrorism operations, the TAF used several locally developed VHF/UHF direction finders and other ELINT (Electronic Intelligence) systems to listen to the communications between PKK groups in northern Iraq or southeastern Türkiye near Syria and Iraq's borders. This capability of locating the PKK's radio broadcasting positions and deciphering its communications helped the TAF gain important intelligence about the PKK's moves and foiling possible attacks against TAF positions or soldiers operating in the region.

Toward the end of 2010, a new-generation threat appeared in the asymmetric warfare against terrorist groups. This threat is the improvised explosive device (IED),[32] which is an unconventional explosive weapon mainly used by terrorist organizations around the world to target soldiers and civilians. IEDs mostly use

[31] Dr. Feridun Taşdan, "Turkish EW Systems, Unseen Force Behind Recent Turkish Drone Success", *Defence Türkiye*, Issue: 106, (May 2021).

[32] "Improvised Explosive Devices", NATO, 12 December, 2018, https://www.nato.int/cps/en/natohq/topics_72809.htm

TNT, military-grade C4-type explosives, or sometimes fertilizers planted inside a propane tank, older bomb casings, metal pipes, cars, etc. Most IEDs are radio-controlled weapons that can be remotely detonated from several kilometers away. To counter remotely operated IEDs, the TAF quickly incorporated EW solutions produced by the Turkish defense industry. Counter-IED systems are now standard equipment of the TAF units on the field.

The Turkish Land Forces' first comprehensive EW system designed against threat radars is called the REDET. The first version of the system entered the inventory of the Turkish Land Forces Command in 2002. The system consists of two Electronic Support Measures (ESM) trucks (6x6) and one electronic attack (ECM) truck (6x6) and works as pairs against enemy radar systems operating on the battlefield. According to open sources, the system can perform electronic support and attack capability in the 0.4-40 GHz frequency band. The most recent version of the REDET-II system, an improved version of the REDET-I, was ordered in 2015, and the first systems entered the inventory of the Turkish Land Forces in 2019.

The REDET-II (named Vural) can simultaneously counter multiple hostile radar threats (for example, against artillery detections radars) by directing electronic beams through its active phased array jammer/transmitter antennas and active electronically scanned arrays, which are also used in the KORAL system operated by the Turkish Air Force. Ibrahim Sunnetci[33] from Defence Türkiye adds that although similar technologies are used in both systems, there are differences between the REDET II and the KORAL systems in terms of output power and detection/ jamming range capabilities. KORAL has larger ECM antennas and transmitting power than the REDET II system because it needs to detect and jam hostile radars from longer distances. Although the REDET II is designed to be deployed and operated near the operational areas of the Turkish Land Forces Command, the KORAL's system architecture (power and radar band coverage) is determined by the Turkish Air Force's tactical needs, therefore, it has the required output power and wide frequency bands against early warning and tracking radars that could be located hundreds of kilometers away from the KORAL.

For communications signal detection and jamming, the MILKAR-3A3, called ILGAR, is developed and produced by Aselsan. The system consists of two separate

[33] İbrahim Sünnetçi, "Redet-II Deliveries Completed!", *Defence Türkiye*, Issue: 96, (December 2019).

6x6 trucks with related system antenna assembly and generators. The system has been developed for electronic attack operations against UHF/VHF frequency band communication systems located on the battlefield. The system can either completely block the UHF/VHF frequency band or spoof enemy communications by sending incorrect information to the enemy forces on the battlefield.

Similar to the MILKAR-3 system, Aselsan's MILKAR-4A2 system, called Sancak, consists of two separate trucks, one for electronic support and one for the electronic attack on the high frequency (HF) band. The systems can intercept HF communications and jam/degrade the long-ranged communications of hostile forces.

MILKAR-3A3 ILGAR

***Source**: Aselsan*

To protect convoys and other military facilities against improvised explosive devices (IEDs), the MILKAR-5A5 system, which is called SAPAN, was added to the Turkish Land Forces' inventory. It is designed to protect land forces command's military convoys against IEDs (improvised explosive devices or radio-controlled drones, etc.). The system has a wide frequency coverage to disable remote-controlled IEDs and drones flying nearby.

Aselsan's GERGEDAN[34] portable jammer system against Radio Controlled Improvised Explosive Devices (RCIEDs) is designed to protect convoys, VIP vehicles in motion, and static infrastructure (e.g. entry control points, high-value assets, checkpoints, facilities) against the utilization of RCIEDs by jamming the communication between these devices and threats.

MILKAR-5A5 SAPAN IED Jammer

***Source:** Aselsan*

Turkish Armed Forces Joint Military Operations in Syria

The Turkish Armed Forces (TAF) have been at the forefront of new warfare employing unmanned air vehicles (UAVs) unconventionally in asymmetric/symmetric wars in recent years. We witnessed the TAF's Operation Spring Shield (OSS) (March 2020) in the Idlib region of Syria to counter Syrian forces attacking Turkish land forces positions in the region. During the OSS, the TAF heavily relied on armed UAVs, mainly Baykar's TB2 and TUSAŞ's ANKA-S, to conduct operations against Syrian forces where they inflicted heavy casualties. OSS was jointly managed by all forces of the TAF, including the Turkish Air Force (TURAF)

[34] "Gergedan - Portable RCIED Jammer System", ASELSAN, https://www.aselsan.com.tr/en/capabilities/electronic-warfare-systems/electronik-support-and-electronic-attack-systems/gergedan-portable-rcied-jammer-system-vehicle-type

and naval units. TURAF F-16s and AEW assets provided air cover by closing the airspace to Syrian fighters. In some instances, the TURAF shot down at least three Syrian warplanes (two Su-24 and one L-39 Albatros) that were trying to intercept Turkish drones operating over the Idlib region. TAF land-based EW systems (the REDET, KORAL, MILKAR 3 EW systems), as well as TURAF's CN-235 SIGINT special mission aircraft, were also supported the joint military operations during OSS.

After establishing air dominance, TB2 and ANKA-S (including the specially configured ANKA-I with special a SIGINT/ELINT payload) were able to operate freely and started their work on gathering information and targeting Syrian forces on the ground in the Idlib region. After losing air supremacy, Syrian forces tried to rely on their air defense systems (ADS), including SA-15 TOR, SA-22 Pantsir, SA-8 Gecko, and SA-10 Grumble (S-300), to protect the airspace over Idlib from TURAF warplanes, including TB2 and ANKA-S. Turkish F-16s and other AEW, AAR assets stayed out of the conflict zone, but the proximity of Idlib to Turkish borders made it easier for the TURAF to safely keep an eye on the airspace while staying about 35-40 kilometers within Türkiye.

ANKA-I UAS Using ELINT/SIGINT Payload

Source: *https://www.uasvision.com/2018/03/29/anka-gains-sigint-capabilities/*

The Turkish TB2 and ANKA-S needed to work around the Syrian ADS to provide real-time ISR to the Turkish command and control chain during the land operations. Turkish EW assets, which were also located on Türkiye's Idlib borderlines, continuously kept an eye on the Syrian ADS activities and provided real-time SIGINT/ELINT information about their operational conditions and geolocations to the TAF joint command centers. This information was very critical in the flight planning and tactical employment of the UAVs; otherwise, it would have been catastrophic to fly into the battlefield while many Syrian ADSs were actively looking for TAF drones.

A recent article by Lt. Col. Osman Aksu in the Journal of Joint Air Power Competence Center[35] stated that during Operation Spring Shield in Idlib, Syria, the airspace was highly contested, and friendly communications were heavily disrupted. Despite these vulnerable conditions for UAV operations, providing close air support (CAS) for ground troops was an urgent priority; therefore, the local commanders had limited options in terms of using attack helicopters and manned aircraft. The best option was to access the operations area with ANKA-S and TB2 UAVs under intensive EW support (especially against high GPS jamming) and hit predetermined or dynamic targets using detailed intelligence information verified by ELINT/SIGINT aircraft or Turkish Land Forces in the region.

Koral EW System (ESM and EA/ECM Vehicles) Deployment Near Syria Border

Source: *https://www.star.com.tr/teknoloji/elektronik-harp-sistemi-koral-suriye-sinirinda-haber-1299611/*

[35] Lt. Col Osman Aksu, "Potential Game Changer for Close Air Support Enhancing UAS Role in Contested Environments", *The Journal of the JAPCC,* Issue: 33 (Winter 2021).

Current Trends: Digital Evolution of the EW Systems

Though we are witnessing new developments in electronic warfare technologies, some of them are already operational and have been tested on the battlefield. There are several "key" technologies and capabilities that are currently included in the design and manufacturing of the new generation EW systems. It would be expected that the aforementioned technologies will be standard soon. So, according to a survey of the most recent EW system developments around the world, the following list of major technological breakthroughs are observed:

- Transitioning to higher-performance gallium nitride (GaN) semiconductor components from traditional gallium arsenide (GaAs) in the production of high-performance RF transmitters. GaN technology reduces cooling requirements and allows higher power output (kW) in the EW/Radar systems. By using GaN technology, the EW systems can perform long-distance jamming, require reduced cooling, and allow the engagement of multiple threats simultaneously.

- Use of artificial intelligence (AI) or adaptive machine learning (AML) algorithms to collect, analyze and implement countermeasures (adapting to the best jamming technique based on the threats) to the RF threats without changing/updating software or hardware. Currently, traditional EW systems provide automated responses to threats that are known and pre-programmed in their databases. AI/AML systems allow dealing with unknown threats based on available information from the database or newly collected data from the previous missions as they will be analyzed and elaborated by the AI/AML in real-time. This capability allows countering hostile software-defined EW systems that can be changed on the fly and may be unknown by the current threat database. The newer EW systems are easily reprogrammable to allow the best configuration for each mission, being able to switch in real-time from one function to another and integrate AI/AML, paving the way for a new generation of cognitive and adaptive EW systems.

- Use of Microwave Monolithic Integrated Circuit (MMIC) technology, which allows the development of miniaturized radio frequency (RF) transmitters/receivers that offer an increase in capabilities compared to older systems. Especially active electronically scanned array (AESA) radars and EW systems rely on MMIC. Moreover, these receivers are accompanied by high-quality and high-speed broadband analog-to-digital converters that overcome the signal quality degradation of analog receivers, and new interferometer antenna systems that now can determine the direction of a threat with an accuracy of 0.05 degrees instead of the 1-degree accuracy of older antennas. High accuracy and pinpointing the threat location increase EW systems' mission success by directing the RF energy in the right direction more efficiently.

- Digital Radio Frequency Memory (DRFM) technology provides a more complex approach to EW protection by modifying the threatening radar signal to create false target returns. DRFM involves the reception of a threat radar signal that is received, processed digitally, altered in real-time, and then retransmitted. The EW system has to avoid signal degradation and keep the altered RF signal coherent with the source of the original signal. DRFM is highly effective in jammers, for an instance. Described in simple terms, the system digitizes the received signal and stores a coherent altered copy in digital memory, replicating and retransmitting it when needed. Since this is a coherent representation of the original signal, the adversary's radar will not be able to distinguish it from other legitimate signals and will recognize it as a real target. DRFM can be used to create false range targets both behind (reactive jamming) and ahead of (predictive jamming) the asset that it's protecting.[36]

In addition to the listed technologies above, the introduction of new phased array antenna structures, and increased computing and transmitting power, the new generation of EW systems are now capable of simultaneously operating on multiple frequency bands, frequency hopping in real-time, and covering a wider range of frequency scale of the electromagnetic spectrum.

[36] Stefano D'urso, "Let's Talk About the Digital Evolution Of Electronic Warfare", The Aviationist, 26 October 2020, https://theaviationist.com/2020/10/26/lets-talk-about-the-digital-evolution-of-electronic-warfare/

Conclusion

It is not wrong to say that the future of conventional wars is heading toward the electromagnetic domain. Major military platforms, airplanes, air defense systems, missiles, UAVs, and warships are all integrated with electronic systems using the electromagnetic spectrum to see the environment around them, navigate, communicate, and engage with enemy forces. However, the enemy forces will also be using the same electromagnetic domain for all these activities. Thus, both sides will try to deny the other side the use of the electromagnetic domain. In this respect, the outcome of wars will be depended on the technological superiority, indigenous development of the EW systems (having full control of the systems), quick adaptation to surprises, and training of the personnel for either side.

The proliferation of the EW technologies is controlled by the export laws due to the national security concerns of the producers. Therefore, EW systems must be designed and produced indigenously to use the systems effectively and securely in wartime conditions. There could be always a possibility that an imported EW system may not be used as effectively as possible due to many circumstances, such as a new radar or a weapon system being introduced during a war. To keep the EW systems up to date against new threats, they are constantly updated by militaries to counter these new threats. In some cases, militaries (if they have the capability) use all available ELINT/SIGINT capability (or even spying) to gather signal information about the hostile countries' new weapon systems or threat radars to update their threat library during peacetime. This process is extremely critical to keep EW systems ready to use against new threats. Moreover, during active war times, the EW systems could also require software/hardware updates to counter new surprise threats as well. In reality, it would be almost impossible to receive any technical support from the original producer of the EW systems during an ongoing war.

The current trends in recent EW system developments are showing that AESA, MMIC, DFRM, AI/AML, and cyberattack technologies are being incorporated into the designs of the new generation EW systems. The newer EW systems are scalable and adaptable to multiple platforms for land, air, and naval applications.

As mentioned in the article, major military powers such as the U.S., Israel, Russia, and China are leading countries in the design and production of EW systems. To catch up with these countries, Türkiye's investments in locally designed EW systems have been paying off in recent years. Many indigenously developed EW systems are introduced into all domains of the Turkish Armed Forces (TAF). It is now obvious that controlling the electromagnetic spectrum is a key to winning conventional wars in the future and therefore, the TAF places special emphasis on the EW capability. More importantly, in addition to controlling the EW domain of warfare, Türkiye is close to reaching the level of sophistication and development of its operational concepts compare to the leading countries in the EW domain. Moreover, the TAF has gained considerable experience in using national EW systems in recent symmetric and asymmetric warfare in Syria, Libya, and even Karabakh, Azerbaijan. These experiences are highly valuable for future conflicts in terms of updating the capabilities of the current EW systems, determining future EW needs, and training the operators under real war conditions. Considering the number of ongoing domestic EW projects (already delivered and in the process of delivery) in all domains, the TAF will be using locally designed and produced EW systems that will provide advantages against regional countries that rely on using important EW systems.

As has been stated throughout this article, controlling the electromagnetic spectrum is key to the success of conventional wars in the future. Thus, we would expect that Türkiye's future EW projects will closely follow technological trends and, more importantly, make necessary investments in the domestic production capability of gallium nitride (GaN) modules, IIR detectors, and Microwave Monolithic Integrated Circuit (MMIC) technologies. These investments must be prioritized as the main goal to become fully independent in the designing and production of EW systems in Türkiye. These investments will also benefit other systems' design and production locally such as AESA radars, E/O systems, and RF/IIR seeker guided missiles since there are commonalities and similarities at the level of technologies used in these systems.

SETA Emerging Military
Technologies Series .1.

Electronic Warfare:

Global Trends & Turkish Capabilities Report

Militaries around the world place particular importance on developing and fielding electronic warfare (EW) systems. This is based on the fact that states believe controlling the electromagnetic spectrum (EMS) is key to gaining superiority on the battlefield to defeat an adversary. Electronic warfare is defined as any action or capability of using EMS to detect, deceive and disrupt the opponent's weapon systems such as radars, communication systems, command control systems, data networks, or other digital infrastructures using EMS. Due to their invaluable role on the battlefield, EW technologies can be placed at the top of the list of military technologies that are highly protected and controlled by the countries that developed the technology. Thus, developing national EW systems indigenously comes with great security benefits. Against this backdrop, this report sheds light on the key aspects of EW by focusing on global trends and analyzing Turkish capabilities.

SETA

9 786258 322118