An MDO Approach to NATO's Counter-IADS Strategy

Integrating Suppression of Enemy Air Defences and Cyber-Electromagnetic Activities

Lieutenant Colonel Athanasios Sdrakas, Hellenic Air Force, JAPCC

Introduction

Russia's war in Ukraine has shattered long-held assumptions about the ease of achieving air superiority. The conflict has demonstrated that even modern air forces struggle to dominate contested skies when faced with a dense, multilayered defence.[1] While much attention has been paid to the proliferation of unmanned aerial systems (UAS), the more enduring lesson for NATO is the resurgence of the Integrated Air Defence System (IADS). These systems now anchor adversary Anti-Access/Area Denial (A2/AD) strategies, posing a direct challenge to how air power is projected and sustained.[2]

NATO's ability to deter and defend against a modern, IADS-equipped adversary requires a multi-domain campaign of suppression that is continuous, adaptive, and resilient. Future suppression of enemy air defences (SEAD) missions cannot rely solely on the traditional air-domain-centric model of airborne SEAD platforms – such as dedicated electronic attack aircraft, Wild Weasel units, and 5th-generation strike

fighters-operating primarily against individual surface-to-air threats. It must evolve to utilise all assets and effects capable of neutralising a sophisticated IADS.[3] Persistent electronic attack (EA), cross-domain cyber operations (CO), and precision kinetic effects must be orchestrated to create and exploit windows of opportunity at scale. NATO should therefore develop a framework that enables these effects to be sustained. Developing a framework to do so is central to sustaining NATO's deterrence posture, freedom of action, and credibility in collective defence.[4]

This begins with the integration of air-delivered SEAD effects and Cyber-Electromagnetic Activities (CEMA). Far from being a mere mix of jamming and hacking techniques, CEMA provides an operational framework that treats cyberspace and the electromagnetic spectrum (EMS) as a unified manoeuvre space. Within this framework, electronic warfare (EW) and cyber capabilities converge to influence an adversary's Integrated Air Defence System (IADS) by manipulating the EMS, cyber terrain, and information environment.

'Integrating SEAD and CEMA is more than a procedural improvement; it changes how NATO defeats a modern IADS.'

Like traditional airborne SEAD, CEMA employs electronic attack techniques such as jamming, deception, and spoofing, but extends further to include cyber operations that penetrate radar software, command-and-control (C2) infrastructure, and air-defence networks.[5] True integration must go beyond coordination: it requires an offensive counter-air 'system-of-systems' approach in which CEMA operators are fully embedded in mission planning and execution alongside airborne SEAD specialists. When electromagnetic attack, deception, cyber intrusion, and kinetic fires are synchronised in time and purpose, NATO can generate the unified effects needed to suppress or neutralise a modern IADS.[6] This SEAD-CEMA coupling forms the foundation of a multi-domain strategy that achieves air superiority through the synergistic application of kinetic and non-kinetic effects across the EMS.[7]

The Operational Need for SEAD-CEMA Integration

Advanced air defence systems with sophisticated mobility, redundancy, and electronic countermeasures (ECM) can degrade the effectiveness of traditional air-employed SEAD.[8] Russia's IADS illustrate how a multi-layered defence architecture can quickly detect, track, and neutralise traditional aerial threats in a congested environment. The SA-21 Growler

An EA-18G Growler with AN/ALQ-99 pods on the deck of the USS Abraham Lincoln.

(S-400) and S-500 Prometheus can target aircraft, missiles, and satellites. Mobile systems like the Buk-M2 (SA-17) and Tor-M1/M2 (SA-15), together with powerful EW platforms like the Krasukha-4, Divnomorye, and Murmansk-BN, support these kinetic effects by disrupting, deceiving, and degrading adversary sensors. Their effectiveness is amplified through Russia's sensor-fusion and battle-management networks, Baikal-1M, Polyana-D4M1, Nebo-M, which provide shared tracking data and coordinated engagements.[9] When fully integrated, such an advanced IADS presents a high risk to traditional SEAD platforms unless they are supported by synchronised multi-domain effects, including cyber, space, and electromagnetic activities.[10] Without synchronised lethal and non-lethal effects to achieve a level of suppression against a modern IADS, creating even limited pockets of air superiority is nearly unachievable.

An Effects-Based Framework: Lethal vs Non-Lethal SEAD and the Role of CEMA

SEAD uses various means to produce both lethal and non-lethal effects that degrade, deceive, deny, disable, or disrupt adversary IADS, as shown in Table 1.[11]

Non-lethal SEAD effects, like those achieved with airborne electronic attack (AEA), rely on EMS jamming to defeat surveillance and fire control radars, and disrupt communications. Lethal SEAD effects use physical force or energy transfer, often via traditional kinetic weapons like anti-radiation missile (ARM) and precision strike weapons. In the future, emerging technologies, most notably directed energy weapons (DEWs), including high-energy lasers and high-power microwaves, could further expand the lethal effects arsenal.

CEMA offers a range of non-lethal effects, providing time-limited and reversible means to suppress adversary air defences. Traditional SEAD methods, such as employing ARMs and supporting EA, remain fundamental in disrupting IADS. However, the increasing complexity and resilience of modern IADS demand that these methods evolve. To remain effective, SEAD must incorporate the full spectrum of CEMA, which blends kinetic, electronic, and cyber capabilities into a unified operational concept. Integration of CEMA capabilities and effects from the earliest stages of operational design and campaign planning processes, co-locating cyber/EW planners within air tasking cycles, and synchronising target development, effects sequencing, and battle damage assessment across all domains rather than treating them as parallel or supporting activities.[12]

Category	Means	Description
Physical Destruction (Hard Kill)	Anti-Radiation Missiles (ARM)	Missiles that home in on radar emissions to destroy radar sites.
	Precision-Guided Munitions (PGMs)	Highly accurate bombs / missiles are used to strike IADS components.
	Directed Energy Weapons (DEW)	Lasers or high-energy beams are used to damage or destroy electronic systems.
	High-Power Microwaves (HPM)	Emits powerful microwave bursts to disable enemy electronics.
	Kinetic Strikes	Physical attacks on radars, SAM batteries, or C2 facilities.
	Special Operations Forces (SOF)	Covert missions to disrupt or sabotage IADS infrastructure.
	Support Jamming (SJ)	Jamming that degrades enemy radar and communications.
Sensor Denial (Soft Kill – EW)	Escort Jamming (EJ)	Jamming support from aircraft accompanying strike packages.
	Stand-In / Stand-Off Jamming	Jamming is conducted from near-target or distant positions.
	Digital Radio Frequency Memory Jamming	Generates coherent false signals.
	Radar Spoofing / Deception	Manipulates radars to display false tracks or ghost formations.
	GPS / PNT Denial	Denies accurate navigation / timing cueing to disrupt engagements.
Logic / Network Disruption (Cyber)	Cyber Intrusion into IADS	Gains access to modify, disable, or corrupt radar / C2 logic.
	Data Injection / Manipulation	Alter sensor feeds, track tables, or identification databases.
	Admin / Authentication Lockout	Blocks operator access or inhibits system configuration.
	C2 Node Disruption	Cyber effects degrade routing, fibre-optic networks, or SATCOM.
	Malware Targeting Sensor Firmware	Corrupts radar modes, ECCM routines, timing or processing algorithms.

***Table 1:** SEAD effects and CEMA contributions across lethal and non-lethal means.*

Accordingly, CEMA effects must be integrated from the earliest stages of operational design and campaign planning. This includes embedding cyber and EW planners within air tasking processes and synchronising target development, effects sequencing, and battle damage assessment across all domains. Such convergence underpins the future of SEAD: a cross-domain, layered approach that synchronises kinetic fires, EW, and cyber warfare (CW). Through SEAD-CEMA integration, NATO can generate decisive effects within contested electromagnetic environments, disrupting enemy air defences through destruction, deception, denial, and digital exploitation.

To illustrate how these dynamics unfold in real operations, the following case studies examine SEAD-CEMA integration across permissive, contested, and advanced IADS environments.

F-35 Lightning II aircraft flying in close formation. The F35 is ideal for stand-in SEAD asset in contested airspace.

Case Study 1: Operation Unified Protector (Libya, 2011) – SEAD in a Permissive Environment

NATO's intervention in Libya successfully enforced a no-fly zone and neutralised most of Libya's antiquated IADS. The rapid degradation of Libyan air defences, however, masked significant structural weaknesses in NATO's SEAD posture.

- **Doctrine–Reality Gap.** Existing Cold War-era SEAD doctrine was ill-suited to the decentralised and mobile Libyan defences. NATO lacked a doctrinal framework for dynamic SEAD in a fluid operational environment.[13]
- **Over-Reliance on US Enablers.** SEAD support to the Alliance depended almost entirely on US Navy EA-18G Growlers and US Air Force F-16CM Wild Weasels, supported by US Air Force intelligence, surveillance, and reconnaissance (ISR) assets (e.g. E-3 AWACS, E-8 JSTARS), aerial refuelling, and precision strike capabilities.[14]
- **Interoperability and C2 Challenges.** The transition from the US Secret network (SIPRNET – Odyssey Dawn) to the NATO Secret Wide Area Network (NSWAN – Unified Protector) resulted in delays and data loss, and Battlefield Information Collection and Exploitation Systems (BICES) was not fully integrated with US Africa Command AFRICOM. This was more than a C2 friction point: if NATO struggled to share basic targeting data in 2011, it would not be able to exchange far more complex cyber intelligence, EW mission libraries, or EMS threat files in a future SEAD-CEMA campaign. In Libya, we learned an important lesson: if the network is fragmented, CEMA is impossible.[15]

Assessment: Unified Protector's permissive conditions masked the Alliance's lack of indigenous European SEAD/Destruction of Enemy Air Defences (DEAD) capacity. The operation underscored the need for NATO to develop a joint, multi-domain SEAD doctrine that fuses EA, cyber, and ISR into a combined planning and execution framework.[16]

Case Study 2: The Ukrainian Crucible (2022–Present) – Attritional SEAD in a Contested Environment

The Russian invasion of Ukraine provided the first real assessment of SEAD against a modern and adaptive IADS. With no formal NATO involvement and few trained SEAD air operators, Ukraine relied on an attritional, multi-domain suppression, providing rare insight into degrading Russian IADS.

- **Innovative Tactics & Centrality of UAS.** Ukraine relied heavily on small military and commercial drones to identify Russian SAMs, radars, and EW units, enabling a simple but effective targeting cycle that quickly paired 'finders' (UAS) with 'shooters', such as artillery, missiles, and one-way attack OWA drones.[17]

Integrated cyber and electromagnetic activities (CEMA), showing how cyber intrusion, jamming, and precision strike effects combine to suppress modern IADS.

- **Multi-Domain Synergy: ISR–Enabled Precision Fires Against IADS.** ISR data from drones has been linked to precision fires from high mobility artillery rocket system (HIMARS), M270 guided multiple launch rocket system (GMLRS), and OWA drones, systematically degrading Russian IADS over time, including confirmed strikes on S-400 radars and launchers. This represents a genuine multi-domain SEAD construct, where air/space ISR enable land-based fires to suppress threats to the air domain.[18]
- **SEAD & CEMA Integration.** Ukraine rapidly improvised methods of suppression that blended kinetic, EW, and cyber effects. Pilots adopted 'Wild Weasel-style' tactics, exposing themselves to radar emissions to provoke Russian engagement and enable strikes with Western-supplied AGM-88 HARMs adapted for MiG-29 and Su-27 aircraft. The latter 'FrankenSAM' hybrids – Western missiles on Soviet launchers – demonstrated a high degree of battlefield innovation. However, these strikes alone could not permanently suppress a Russian IADS that remained mobile, resilient, and shielded by EW assets such as Krasukha-4 and Leer-3.[19]
- **The Virtual Dimension.** The KA-SAT/Viasat attack in February 2022 was not just a communications disruption; it was a counter-C2 strike that temporarily blinded parts of Ukraine's command network during the invasion's opening phase. Ukrainian CO targeted logistics and navigation networks, while tactical jamming, spoofing, and GPS denial created temporary windows that allowed drones and missiles to penetrate.[20] The conflict has thus evolved into a continuous fight for EMS dominance, with both sides employing increasingly low-cost CEMA tools.[21]

Assessment: Ukraine's attritional SEAD highlights the need for continuous, multi-domain suppression, rather than episodic strikes, utilising ISR, precision fires, cyber, and EW to degrade IADS steadily. The conflict also reveals the rise of democratised or 'guerrilla' CEMA, where inexpensive commercial tools – such as Software-Defined Radio (SDRs), open-source software, and improvised jammers – deliver real operational effects.

Case Study 3: Israel-Iran War (June 2025) – Advanced SEAD-CEMA Integration

Israel's networked integration of cyber, EW, and precision strikes demonstrated that sophisticated multi-domain effects can achieve strategic dominance with

The S-400 Triumf Russian air defence SAM/Transporter Erector Launcher (TEL).

relatively few assets. In contrast, Iran's reliance on mass-saturation tactics consumed vast quantities of munitions without achieving decisive results, illustrating that sheer volume cannot compensate for a lack of cross-domain coordination.[22]

- **CW–EW Opening Moves.** Pre-emptive CO reportedly degraded Iranian radar networks, satellite communications, and C2 nodes in the first hours, creating short windows for Israel Air Force (IAF) strike packages to enter contested airspace with reduced risk.[23] A Mossad-linked mission to sabotage fibre-optic lines and disrupt radar facilities inside Iran compounded the cyber effects, physically degrading Iranian network resilience.
- **IADS Resilience & Temporary Kinetic Windows.** Even after early blows, Iran dispersed and reconstituted air defence coverage within 24–48 hours, relocating its Khordad-15 and Raad SAM systems and command elements. This limited opportunities for HARM employment, forcing Israel to rely on persistent ISR and dynamic re-attack windows with UAVs.[24] Coordinated cyber actions and GPS jamming degraded air defence capabilities and enabled windows for kinetic missions to succeed.[25]
- **Massing Multi-Domain Effects.** Iran launched mixed salvos of ballistic missiles and Shahed drones, aiming to saturate Israel's layered defences. Although most were intercepted, the volume of fires forced the IAF to shift its efforts towards defending key military targets. This created a trade-off: every asset pulled into missile defence was an asset unavailable for SEAD tasks.[26] Israel countered with its own waves of UAVs, loitering munitions, and decoys to overload Iranian engagement zones, enabling F-35I Adir aircraft to strike Bavar-373 and S-300 sites protecting Natanz and Fordow. The use of inexpensive decoys to drain SAM magazines mirrors Russian concepts, as seen with Geran/Shahed drones.[27]
- **Layered Multi-Source Intelligence.** The use of national intelligence, satellite imagery, and open-source intelligence (OSINT) rapidly revealed movements on both sides. Both sides faced unprecedented transparency.[28]

Assessment: Iran proved relatively responsive following initial SEAD effects, but Israel maintained the advantage through synchronised cyber, EW, and kinetic actions that created recurring windows of vulnerability. Their persistent SEAD cycles – suppress, exploit, re-suppress – aided by both military intelligence and OSINT, ensured proactive suppression of adversary defences to enable other functional objectives (strike, ISR, pursuit of air superiority.

Recommendations

Operational Adjustments

- **Establish SEAD-CEMA planning cells.** NATO should form integrated SEAD-CEMA cells within Allied Air Command (AIRCOM) and especially at the Joint Force Command (JFC) level, integrating cyber, EW, ISR, and all components (air, land, maritime, and space), ensuring multi-domain planning and targeting. These cells must also begin developing detailed, 'on-the-shelf' SEAD-CEMA plans, since adequate cyber/EW preparation requires months or years of access, not last-minute tasking. The Alliance must address classification and releasability barriers that restrict multinational targeting and integration, delegate approval of non-strategic cyber effects to the JFAC Commander level to exploit fleeting SEAD windows. NATO should adopt a pre-approved library of generic cyber payloads for rapid deployment. CEMA must be fully integrated into the Joint Targeting Cycle and reflected in the ATO as a standard SEAD tool.

Capability Development and Investment

- **Build a layered, interoperable SEAD-CEMA capability portfolio.** NATO's Defence Planning Process should direct investment into both high-end, exquisite effectors and scalable attritable systems. This includes advanced ARMs, stand-in EW drones, survivable ISR platforms, long-range precision strike weapons, and affordable swarms of unmanned systems proven effective in Ukraine.
- **Enforce open architecture standards.** The Conference of National Armaments Directors (CNAD) should mandate that all new CEMA-related systems comply with open architecture and data standards. This could serve to break the cycle of proprietary, non-interoperable systems and ensure that future NATO assets are integrated by design.
- **Reduce over-reliance on US enablers.** Allies must develop and acquire EW, ISR, and SEAD assets to create a more balanced and sustainable defence capability.

Training, Exercises, and Professional Development

- **Evolve NATO training and exercises for MDO.** Flagship exercises (e.g., Ramstein Flag, Ramstein Guard) should stress SEAD-CEMA integration against an adaptive and advanced adversary. Scenarios should include contested EMS, enemy cyber intrusions, and adaptive red IADS. Advanced live virtual constructive (LVC) environments should be expanded to realistically simulate peer-level opposition.
- **Create a cadre of multi-domain practitioners.** NATO and its member states should establish and/or enhance recognised career paths for CEMA professionals. This includes expanding specialist training (e.g., Non-Kinetic Effects Coordination courses) and operational continuation training to provide qualified and proficient operators for SEAD-CEMA cells.
- **Educate commanders.** Senior leaders must be prepared to understand CEMA effects, assess non-kinetic risks, and confidently integrate capabilities into operations. This reduces cultural bias toward familiar kinetic tools and promotes genuinely multi-domain decision-making.

Doctrinal Development

- **Codify SEAD-CEMA within MDO.** NATO should formally embed SEAD-CEMA integration within its MDO doctrine. This doctrine must define authorities, command relationships, targeting processes, and escalation thresholds for integrated cyber, EW, and kinetic suppression. It will provide a common Alliance-wide framework, ensuring that CEMA is not treated as an adjunct but as an indispensable pillar of future SEAD campaigns.

Future Outlook

Integrating SEAD and CEMA is more than a procedural improvement; it changes how NATO defeats a modern IADS. The aim is not only to disrupt radars or individual sensors, but to pressure the adversary's entire decision-making chain – its data links, software logic, and C2 nodes. When CO, EW effects, and precision fires are synchronised, they create dilemmas the defender cannot resolve quickly, preserving NATO's freedom of action and supporting air superiority in contested environments.

Looking ahead, SEAD-CEMA will sit at the core of NATO's MDO model. Future IADS will be too mobile, networked, and software-driven for traditional SEAD to be effective alone. NATO will need earlier

cyber shaping, stand-in EW capabilities, resilient ISR, and integrated targeting processes that align effects across all domains. Embedding SEAD-CEMA teams into campaign design will help ensure the Alliance can challenge advanced IADS, maintain deterrence, and retain the initiative in future high-end conflicts.[29]

1. General Hecker, James B., 'Air Superiority: A renewed Vision', Summer 2024, (accessed 25 June 2025).
2. NATO, AJP-3.3 'Allied Joint Doctrine for Air and Space Operations', NATO Standardisation Office, 2021, (accessed 1 November 2025).
3. Generalleutnant Günter Katz, Commanding General of the German Air Force Forces Command, AOC Europe 2023 conference, (accessed 25 June 2025).
4. Stoltenberg, J., 'NATO Must Adapt for the Future: Deterrence and Defence in the Digital Age', NATO Review, 29 June 2023, (accessed 30 October 2025).
5. Brig. Gen. Sgamba, G., 'Electro Magnetic Spectrum Operation (EMSO)', EMSOPEDIA, 2020, (accessed 9 July 2025).
6. Scott Richard, 'I Feel the Need – the Need for SEAD', JED, November 2023, (accessed 25 June 2025).
7. Vasicek, R., & Oulehlova, A., 'Cyber and Electromagnetic Activities and Their Relevance in Modern Military Operations', 2021, (accessed 30 June 2025).
8. Ibid 3.
9. Sutyagin, I., 'Russian Air-Defence Networks: Structure and Modernisation', RUSI, 2021, (accessed 19 November 2025).
10. Bronk, Justin, 'Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Option', RUSI, January 2020, (accessed 1 July 2025).
11. Col Speed, J., & LtC Stathopoulos, P., 'SEAD Operations of the Future', JAPCC Article, June 2018, (accessed 9 July 2025).
12. NATO, AJP-3.5 'Allied Joint Doctrine for Air and Missile Defence', NATO Standardisation Office, 2020, (accessed 1 November 2025).
13. Maj Kassebaum, J., USAF, 'The Art of SEAD: Lessons from Libya.', JAPCC Journal, 2013, (accessed 1 November 2025).
14. Mueller, K., 'Precision and Purpose: Airpower in the Libyan Civil War', RAND, 2015, (accessed 27 August 2025).
15. Maj. Jason R. Greenleaf, USAF, 'The Air War in Libya', Feature, March-April 2013, (accessed 27 August 2025).
16. Phinney, T., 'Reflections on Operation Unified Protector', National Defence University Press, 1 April 2014, (accessed 27 August 2025).
17. Watling, J., & Reynolds, N. 'Ukraine at War: Paving the Road from Survival to Victory', RUSI, 2022, (accessed 29 August 2025).
18. Institute for the Study of War (ISW), 'Russian Offensive Campaign Assessments' (daily updates), (accessed 29 August 2025).
19. Bronk, J., Reynolds, N., & Watling, J. 'The Russian Air War and Ukrainian Requirements for Air Defence', 2023, RUSI, (accessed 2 July 2025).
20. Watling, J., & Reynolds, N., 'Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine', RUSI, November 2022, (accessed 2 July 2025).
21. Centre for Strategic and International Studies (CSIS). 'The Cyber War in Ukraine: Lessons for the Future of Conflict', 2022, (accessed 7 July 2025).
22. Cordesman, A. H., 'Israel–Iran: Lessons on integrated cyber-electronic warfare and strike operations. Centre for Strategic and International Studies', CSIS, 2025, (accessed 7 July 2025).
23. Saab, B., & White, D., 'Lessons Observed from the War Between Israel and Iran', War on the Rocks, 16 July 2025, (accessed 29 August 2025).
24. Clover, C., 'Military briefing: How Iran is preparing for Israeli or US strikes', Financial Times, 1 June 2025, (accessed 29 August 2025).
25. Ibid 15.
26. Beauchamp, Z., 'The Israel-Iran war hinges on three big things', Vox, 13 June 2025, (accessed 29 August 2025).
27. Sabbagh, D., 'Israel's air might, and Iran's nuclear bunkers may make for lengthy conflict', Guardian, 2025, (accessed 30 August 2025).
28. Ibid 20.
29. Laird, R., 'The Invisible Battle: Synchronising Non-Kinetic Effects in Modern Warfare', Second Line Defence, 22 July 2025, (accessed 30 October 2025).

ABOUT THE AUTHOR

Lieutenant Colonel Athanasios Sdrakas
Hellenic Air Force, JAPCC

Lieutenant Colonel Athanasios Sdrakas graduated from the Hellenic Air Force Academy with a Bachelor of Science in Aeronautics and holds two Master of Science degrees, in International Affairs (University of Nicosia) and Environmental, Disaster, and Crisis Management Strategies (National and Kapodistrian University of Athens). He has served in a wide range of operational, instructional, and leadership roles within the Hellenic Air Force, including positions in tactical aviation, flight training, and squadron-level command. His flying experience includes work on aircraft such as the RF-4E and T-6A, accumulating more than 4,000 total flight hours across operational and training assignments. He has held responsibilities in training standardisation, evaluation of aircrew and instructors, and operational oversight across the Hellenic Air Training Command. His professional military education includes graduation from the Hellenic Fighter Weapons School and the Hellenic Supreme Joint War College. Lieutenant Colonel Sdrakas is the Subject Matter Expert in Electronic Warfare (EW), including Suppression of Enemy Air Defence (SEAD) Operations at the JAPCC.