# ADF LAND DOMAIN PUBLICATION

# LAND DOMAIN PUBLICATION - NOTE

# LNOTE 7.2.8 OLVANAN TACTICAL EMPLOYMENT OF ELECTRONIC WARFARE



This Land Domain Publication is issued on the authority of the Chief of Army pursuant to Army Standing Instruction (Knowledge Management) Part 2 – *Management and Governance of ADF Land Domain Publications*.

EDITION 1 2025

LN 7.2.8 Olvanan Tactical Employment of Electronic Warfare

Edition 1, 2025

ISBN: *XXX-X-XXXXXX-XX-X*

**Sponsor:** Chief of Army

**Release Authority:** Deputy G7 Army

**Content Adviser:** Director Information Advantage COE

**Lead Subject Matter Expert:** G76 – SO1 Signals Threat



This Land Publication is issued on the authority of the Chief of Army pursuant to Army Standing Instruction (Knowledge Management) Part 2 – *Management and Governance of ADF Land Domain Publications*.

**Sean D Parkes, DSC, DSM**
Brigadier
Deputy G7 Army
Department of Defence
Paddington NSW 2021
X Month 2024

[1] https://www.legislation.gov.au/Series/C1968A00063
[2] https://www.legislation.gov.au/Series/C2004A04868
[3] https://www.legislation.gov.au/Series/C2004A03712
[4] http://drnet/AssociateSecretary/security/policy/Pages/dspf.aspx

***This page intentionally blank***

## Preface

1. ADF Land Domain Publications (LPubs) describe the fundamental principles that guide land forces' actions, and provide the common frame of reference on how the Army achieves its mission. LPubs are the basis of the Army's training system based on time-tested, proven principles of war, combined with the critical analysis of contemporary lessons. LPubs have been shaped since 1901 by Army's proud history and culture, while being constantly adapted as required, thereby representing the sum of the Army's collective historical knowledge, presented into objective guides for action. In essence LPubs explain and guide 'who we are', 'what we do' and 'how we do it'.

2. ADF doctrine provides the framework that guides thinking but does not dictate what to do. While doctrine publications are written in a non-prescriptive style that allows latitude in interpretation and flexibility in application, they are specific enough to provide informed guidance. Doctrine is about fighting power and the integration of its three components: intellectual, moral and physical, applied through mission command and our manoeuvrist approach to warfighting.

3. Land procedural publications provide the authorised procedural and technical knowledge required for land forces to achieve their mission. Unlike doctrine, procedural publications convey information covering a range of activities based on best possible practice, in clear detailed steps that, depending on the publication, describe and/or prescribe how to perform specific tasks and drills. Whilst the majority of procedural publications are descriptive in nature, the decision not to follow the guidance contained in the publications should be justifiable. Land procedural publications are aligned and subordinate to ADF doctrine.

4. Land procedural publications include a number of publications that prescribe the procedures for the safe conduct of a range of tasks and activities required for delivering a range of lethal warfighting capabilities. Procedural publications which are safety in nature are written with an expectation of compliance, and therefore do not attempt to prescribe every 'do' and 'don't'. A number of land procedural publications are classified as Landworthiness Regulations in accordance with *Defence Landworthiness Management System Manual*. **LPubs constitute a lawful general order when written in mandatory terms and apply to all personnel**.

## Aim

5. LP 7.2.8 Olvanan Tactical Employment of Electronic Warfare, aims to provide an in depth understanding on how the training adversary, known as the Olvanan Peoples' Army, established under the Decisive Action Training Environment (DATE), construct will utilise Electronic Warfare in support of Combined Arms Brigade manoeuvre.

6. This publication provides philosophical and application-level doctrine on Olvanan Electronic Warfare. It describes the nature and scope of adversary tactics in support of operations. This publication aims to inform commanders and other key personnel about adversary electronic warfare operations, and to assist with operational and tactical joint planning; and to contribute to Defence education and training. Associated publications

## Land publication L-Library

7. The ADF Land Power Library (L-Library) is the single access point, and digital catalogue for Army's authorised land power artefacts, supporting resources, including other related publications. In addition to accessing all current and historical publications, the L-Library contains links to ADF doctrine, and other ADF domain publications, as well as approved international partner publications. The L-Library is accessible via ADF Land Power Library and Army Knowledge Online.

8. Additional printed copies of Land Publications may be ordered using the Defence Print Ordering Portal which can be accessed via this link: https://printportal/overview.web.

## Security

9. This publication contains Australian Defence information for the purposes of the *Crimes Act 1914* (Commonwealth) (the Act) and carries a protective marking in compliance with the Defence Security Principles Framework (DSPF). The publication and the information contained therein must be treated and secured in accordance with that protective marking. All Defence information, whether classified or not, is protected from unauthorised disclosure under the Act and may only be released in accordance with the procedures stipulated within the DSPF. Any requests for release of this publication or part thereof must be forwarded to Land Domain Publications. The publication must not be released to non-Defence agencies or persons without written authority from Land Domain Publications.

**Amendment record**

1. Amendments to this Land Publication are issued on the authority of the Chief of Army pursuant to Army Standing Instruction (Knowledge Management) Part 2 – *Management and Governance of ADF Land Domain Publications.*

| Number | Date of amendment | Authorised by |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |

2. All superseded amendment record pages should be retained at the rear of the publication for audit purposes.

3. Proposals to amend this publication may be emailed to: armybattlelab.landdomainpublications@defence.gov.au.

# Contents

Preface ..... 1-1
Aim ..... 1-1
Land publication L-Library ..... 1-1
Security ..... 1-1
Amendment record ..... 1-2
Chapter 1 Overview of Olvanan Information Warfare ..... 1-7
Section 1-1. Cyber Warfare ..... 1-7
Section 1-2. Olvanan Systems Warfare ..... 1-7
Section 1-3. Olvanan Modernisation of Electronic Warfare Capabilities ..... 1-8
Section 1-4. Command Diarchy ..... 1-8
Section 1-5. Integration of Artificial Intelligence (AI) ..... 1-9
Section 1-6. Cyber-EW Convergence ..... 1-9
Section 1-7. Learning from the modern battlefield ..... 1-10
Section 1-8. Integration with Joint and Multi-Domain Operations ..... 1-11
Chapter 2 Olvanan Tactical Employment of Electronic Warfare ..... 2-12
Section 2-1. Defining Electronic Warfare and Information Warfare ..... 2-12
Section 2-2. Education of operators ..... 2-12
Section 2-3. Olvanan Electronic Warfare Mission Sets ..... 2-12
Section 2-4. Electronic warfare in the 17th Group Army ..... 2-13
Section 2-5. The RISTA Battalion ..... 2-13
Section 2-6. The EW Company in the CA-Bde ..... 2-14
Section 2-7. The EW Platoon (EA) ..... 2-14
Section 2-8. The DF Platoon ..... 2-15
Section 2-9. The EW UAV Platoon ..... 2-16
Section 2-10. Olvanan Electronic Warfare Equipment ..... 2-16
Chapter 3 Principles of Employment ..... 3-20
Section 3-1. Command and Control ..... 3-20
Section 3-2. Layering of Electronic Warfare Effects ..... 3-20
Section 3-3. De-confliction of EW effects ..... 3-21
Section 3-4. Rigidity of Olvanan C2 and Release Authority ..... 3-21
Section 3-5. Delegation of EW capabilities ..... 3-23
Section 3-6. Role of the political officer ..... 3-23
Section 3-7. Exceptions to employment ..... 3-24
Chapter 4 Tactical Employment ..... 3-25
Section 4-8. EW in Offensive Zones ..... 3-25
Section 4-9. EW in Offensive groupings ..... 3-26
Section 4-10. EW in Defensive Zones ..... 3-26
Section 4-11. EW in Defensive groupings ..... 3-27
Section 4-12. Counter-drone Operations ..... 3-28
Section 4-13. Vignette 1 - Complex Envelopment ..... 3-29
Section 4-14. Vignette 2 – Advance ..... 3-30
Section 4-15. Vignette 3 – Positional Defence ..... 3-32
Section 4-16. Vignette 4 – Situational Attack (Urban) ..... 3-33

Section 4-17. Vignette 5 – Counter-Attack (Jungle) ..... 3-36
Section 4-18. Vignette 6 – Hard-Nut Diversionary Defence (Jungle) ..... 3-37
Chapter 5 Electronic Warfare Support to Deception Operations ..... 3-39
Section 5-19. EW Company Deception Tasks for CA-Bde Commander ..... 3-39
Section 5-20. Tactical Example 1: Phantom Battalion Manoeuvre in a River Crossing Operation ..... 3-40
Section 5-21. Tactical Example 2: Urban Assault Masking with EMCON and Decoys ..... 3-41
Section 5-22. Tactical Example 3: Counter-ISR Deception in Jungle Warfare ..... 3-42
Section 5-23. Tactical Example 4: Electronic Deception in Defensive Operations against Airborne Threats ..... 3-43
Chapter 6 Electronic Warfare TTPs ..... 3-44
Section 6-24. Fibre Optic Linking Procedure ..... 3-44
Section 6-25. Tethered UAS Procedure ..... 3-45
Section 6-26. Terrain Shielding during Electronic Attack ..... 3-46
Section 6-27. Leapfrog ..... 3-47
Section 6-28. UAS direction finding ..... 3-48
Section 6-29. Electronic Protection – Baseline Emission Control ..... 3-49
Section 6-30. Crew Responsibilities ..... 3-50
Chapter 7 Indicators and Warnings of Olvanan EW Operations ..... 7-51
Section 7-31. Indicators and Warnings Checklist: ..... 7-51
Chapter 8 Logistics Support ..... 7-53
Section 8-32. Power Requirements ..... 7-53
Section 8-33. Mobility Challenges ..... 7-53
Section 8-34. Resupply and Sustainment ..... 7-53
Section 8-35. Environmental and Operational Constraints ..... 7-53
Chapter 9 Conclusion and Future Trends ..... 7-54
Abbreviations ..... 7-55

**Abbreviations**

**List of figures**

**This page intentionally blank**

# Chapter 1
# Overview of Olvanan Information Warfare

## Section 1-1. Cyber Warfare

1.1 The Olvanan approach to cyber warfare is deeply integrated with its broader information and electronic warfare strategies, reflecting a holistic view of the electromagnetic and information domains. Cyber operations are viewed not as standalone activities but as complementary tools to degrade, disrupt, deny, deceive, and destroy enemy command and control, communications, and to gather intelligence. Olvanan doctrine emphasise s the offensive use of cyber capabilities to penetrate adversary networks, implant malicious software, exploit vulnerabilities and manipulate data flows to create confusion and delay enemy decision-making processes. Defensive cyber operations are equally prioritized, focusing on protecting critical military networks and infrastructure from intrusions and cyberattacks that could degrade operational effectiveness.

1.2 Strategically, the Olvanan People's Army (OPA) has developed specialised cyber units that work in close coordination with electronic warfare (EW), and intelligence formations to provide persistent cyber surveillance and exploitation capabilities. These units employ advanced cyber tools to conduct reconnaissance within hostile networks, identify vulnerabilities, and prepare the electromagnetic environment for synchronised attacks. Cyber and EW assets often collaborate to create multi-domain effects, such as simultaneous jamming and cyber intrusion against enemy command nodes, thereby overwhelming adversary defences. This fusion enhances the tempo and impact of operations and aligns with Olvanan principles of integrated warfare.

1.3 At the tactical level, cyber warfare is increasingly embedded within the operational planning cycle of the combined arms brigade, where cyber teams are tasked with supporting manoeuvre units by disrupting enemy communications and sensor systems in real-time. This includes targeting adversary battlefield management systems (BMS), logistics networks, and early warning radars to create windows of opportunity for kinetic strikes. Training for cyber operators stresses adaptability and rapid response, as cyber engagements often evolve quickly in response to enemy countermeasures. The OPA's cyber warfare capabilities also extend into psychological operations, where misinformation campaigns are coordinated to undermine enemy morale and cohesion.

1.4 However, Olvanan cyber doctrine acknowledges the risks and challenges associated with offensive cyber operations, particularly in maintaining plausible deniability and avoiding escalation into broader conflicts. Defensive cyber resilience is thus emphasise d, ensuring continuity of command and control (C2) even under sustained cyberattack. This is achieved through redundant network architectures, encryption, and rapid cyber incident response protocols. Ultimately, Olvanan cyber warfare is a vital pillar of the information age battlefield, tightly integrated with electronic warfare and kinetic operations to shape and dominate the electromagnetic spectrum.

## Section 1-2. Olvanan Systems Warfare

1.5 Olvanan systems warfare represents an evolved concept that integrates multiple warfare domains into a cohesive, interconnected framework designed to achieve rapid and overwhelming effects on the battlefield. At its core, systems warfare involves the synchronisation of kinetic, electronic, cyber, space, and information capabilities to disrupt, degrade, or destroy enemy systems. This holistic approach moves beyond traditional single-domain operations by targeting the interdependencies and vulnerabilities within the adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture. Olvanan doctrine views systems warfare as critical to gaining decision superiority and battlefield dominance.

1.6 The OPA's implementation of systems warfare leverages sophisticated C2, networks that link EW, cyber, and conventional forces under a unified operational picture. By fusing sensor data from multiple domains—including signals intelligence (SIGINT), electronic intelligence (ELINT), cyber reconnaissance, and human intelligence—the Olvanan command echelon can rapidly identify high-value targets and

coordinate cross-domain effects. For example, an enemy air-defence system can be simultaneously jammed, cyber-attacked to degrade software integrity, and destroyed by precision fires, demonstrating the power of integrated systems warfare. This synergy enhances both lethality and survivability.

1.7 From a doctrinal perspective, Olvanan training emphasise s joint exercises that replicate complex multi-domain scenarios, preparing commanders and operators to exploit systemic weaknesses in enemy forces. Interoperability between units and domains is achieved through standardized communication protocols and data sharing architectures. The Combined Arms Brigade (CA-Bde) serves as a primary platform for applying systems warfare concepts at the tactical level, where EW and cyber teams collaborate closely with manoeuvre and fire support units. This integrated approach fosters agility and resilience in dynamic combat environments.

1.8 Technological innovation and modernization underpins the success of Olvanan systems warfare, emerging capabilities such as artificial intelligence (AI), machine learning, and advanced analytics enhance decision-making and operational tempo. Systems warfare also prioritises the protection of friendly networks against adversary efforts to conduct counter-systems operations, including electronic attack and cyber intrusions. In this way, Olvanan forces maintain the initiative by ensuring their systems remain functional and dominant, while simultaneously degrading those of their opponents.

## Section 1-3. Olvanan Modernisation of Electronic Warfare Capabilities

1.9 The OPA has embarked on an ambitious modernization program to upgrade its electronic warfare capabilities in line with evolving multi-domain operational requirements. This modernization includes developing advanced EW vehicles such as the CTL-181 Menshi and ZBL08 EW variants, equipped with sophisticated jamming, direction finding (DF), and SIGINT suites. Furthermore, the OPA is investing in man-portable EW systems that enhance the flexibility of dismounted infantry units, enabling them to conduct localized electronic attack, protection, and deception. These enhancements increase the overall spectrum dominance capacity of the CA-Bde and improve operational adaptability across varied terrain.

1.10 Integration of these modernized EW capabilities into the CA-Bde structure reflects Olvanan doctrine that prioritises electronic warfare as a core enabler of manoeuvre and firepower. The EW Company within the brigade serves as the central node, orchestrating electronic attack (EA), and support missions in coordination with reconnaissance, infantry, artillery, and cyber elements. This tight integration ensures that EW effects are synchronised with kinetic actions, maximising combat effectiveness. For example, EW units may suppress enemy air defences ahead of an assault or protect friendly communications against enemy jamming efforts, demonstrating the operational utility of these modernized assets.

1.11 Training and doctrine have also evolved to support this integration, with increased emphasis on combined arms exercises that incorporate EW scenarios at the brigade and battalion levels. Operators and commanders are trained to exploit the new capabilities fully, such as deploying un-crewed aerial systems (UAS), equipped with EW payloads to extend sensor and jamming reach. Networked C2 systems enable real-time sharing of electronic order of battle information, enhancing situational awareness and responsiveness. These advancements enable the CA-Bde to operate effectively in complex, contested electromagnetic environments.

1.12 Looking ahead, further modernization efforts are expected to focus on AI-assisted EW systems, autonomous EA platforms, and enhanced cyber-EW fusion. The Olvanan military recognizes that maintaining superiority in the electromagnetic spectrum (EMS) is critical for operational success and survivability. By embedding these capabilities in every CA-Bde, the OPA is positioning itself to conduct sophisticated, integrated multi-domain operations against technologically advanced adversaries.

## Section 1-4. Command Diarchy

1.13 The command structure governing Olvanan EW operations is characterised by a dual or diarchic system that balances military operational command with political oversight. This command diarchy reflects the Olvanan political-military doctrine emphasizing party control and ideological reliability alongside professional military competence. In the context of EW operations, the operational commander—typically the brigade commander—holds responsibility for planning, directing, and executing electronic warfare missions with the EW Coy commander. However, political officers embedded within these units exercise parallel authority to ensure that operations align with party objectives and maintain morale and ideological discipline.

1.14 This dual-command system can lead to rigorous oversight and sometimes rigidity, but it also ensures that EW operations are conducted in accordance with broader strategic and political goals. The political officer plays a critical role in monitoring operational decisions, supervising adherence to doctrine, and influencing personnel management within EW units. Their presence guarantees that sensitive EW activities, which often involve covert or deceptive actions in the information environment, remain under strict political control. This arrangement underscores the strategic importance Olvanan leadership places on controlling the electromagnetic and information domains as instruments of state power.

1.15 At the tactical and operational levels, coordination between the military EW commander and the political officer is essential to maintain unity of effort and operational security. Political officers participate in mission planning and briefings, contributing to risk assessments and ensuring compliance with rules of engagement and propaganda objectives. They also oversee the welfare and ideological education of EW personnel, which is crucial given the technical and high-stress nature of EW tasks. This collaborative dynamic aims to balance operational effectiveness with political reliability, reflecting a uniquely Olvanan approach to C2.

1.16 However, the command diarchy can introduce challenges in decision-making speed and flexibility, particularly in rapidly evolving EW engagements where swift action is required. Olvanan doctrine attempts to mitigate these constraints by clearly delineating operational authority while preserving political oversight through structured communication and hierarchical control mechanisms. This balance seeks to maximize the advantages of political control without unduly hampering the responsiveness and initiative of commanders on the battlefield.

## Section 1-5. Integration of Artificial Intelligence (AI)

1.17 The OPA is actively integrating AI and machine learning (ML), technologies into all of its EW systems to automate and accelerate signal analysis, target recognition, and threat response. These AI-enabled capabilities allow EW units to process massive volumes of EMS data in real time, identifying patterns and anomalies that currently overwhelm human operators. By leveraging ML algorithms trained on vast datasets, Olvanan EW platforms can rapidly classify emitter types, locate troop concentrations, and recommend optimal jamming or deception measures. This automation enhances battlefield situational awareness and frees human operators to focus on higher-level decision-making.

1.18 Central to Olvanan doctrine is the concept of man-machine pairing, where AI systems operate alongside human controllers in “in-the-loop” configurations to combine computational speed with human judgment. In these setups, AI provides real-time recommendations, but humans retain authority to approve or modify actions, balancing rapid response with operational oversight. However, Olvanan doctrine also explores “out-of-the-loop” or semi-autonomous modes, especially for defensive EW functions requiring millisecond responses to incoming threats like drones or guided munitions. In such cases, AI algorithms may independently initiate countermeasures to protect critical assets, highlighting a shift towards greater autonomy in EW execution.

1.19 Despite the operational advantages, Olvanan commanders are mindful of the potential dangers inherent in heavy reliance on AI within the EW decision-making cycle. Overdependence on AI risks degradation of operator skills, reduces human situational awareness, and creates vulnerabilities to adversary attempts at AI deception or cyber-attacks targeting AI algorithms. Olvanan doctrine therefore emphasise s robust human-machine interfaces, continuous operator training, and multi-layered cyber defence of AI systems to mitigate these risks. Additionally, fail-safe protocols are embedded to allow manual override and rapid recovery from AI system failures or compromised data inputs.

1.20 The Olvanan military is investing in resilient AI architectures designed to operate effectively within contested and degraded electromagnetic environments. These system architectures integrate adaptive learning, anomaly detection, and collaborative AI nodes across EW units, enabling dynamic reconfiguration of electronic attacks and defences in multi-domain battlefields. Maintaining a balanced approach that harnesses AI’s power while safeguarding human control, will enable the Olvanan aim of achieving decisive information dominance in future conflicts against their adversaries.

## Section 1-6. Cyber-EW Convergence

1.21 The OPA recognizes that the EMS and cyberspace are increasingly intertwined battlefields. Cyber capabilities have also been integrated with traditional EW to enable synchronised operations across both physical and virtual domains. This convergence allows Olvanan forces to conduct operations that

simultaneously disrupt enemy electronic communications and information networks, degrade their C2, and manipulate data flows, achieving effects that neither domain could achieve independently. The OPA's cyber-EW units work closely to map adversary networks, identify vulnerabilities, and launch offensive operations that complement both kinetic, and electromagnetic strikes.

1.22 At the tactical level, this fusion means that electronic jamming and cyber intrusion operations are planned jointly to maximize surprise and operational impact. For example, an EW attack may jam enemy radar and communication frequencies while cyber teams infiltrate and degrade the enemy's data infrastructure, delaying their response and amplifying the overall effect.

1.23 The OPA also uses cyber operations to protect its own EW assets, safeguarding command nodes and data links from enemy hacking or electronic countermeasures. This holistic approach reflects the Olvanan understanding that future conflicts will be fought across a spectrum of interconnected environments. This integration improves situational awareness and decision-making speed, critical for dominating fast-moving multi-domain battlespaces. Furthermore, research efforts focus on developing AI-assisted tools to automate detection, targeting, and response coordination in cyber-electromagnetic operations.

1.24 The convergence of cyber and EW also presents unique challenges, including complex coordination demands and risks of escalation into the cyber domain with potentially strategic consequences. Olvanan planners mitigate these risks through strict C2 protocols, rules of engagement, and layered defensive measures. Despite these challenges, the cyber-EW fusion remains a cornerstone of OPA modernization, providing a significant asymmetric advantage against technologically advanced adversaries.

## Section 1-7. Learning from the modern battlefield

1.25 The Olvanan military closely studies ongoing conflicts around the globe in order to extract critical lessons on the rapid evolution and battlefield impact of EW. The high tempo of operations and extensive use of drones combined with both offensive and defensive EW has exposed vulnerabilities in traditional C2 systems. Olvanan analysts recognize the necessity of rapid EW adaptation cycles to maintain operational freedom in electromagnetic contested environments. To mitigate the sophisticated EW and intelligence, surveillance, reconnaissance (ISR), capabilities demonstrated by Western-backed forces, Olvana has accelerated its development of mobile, resilient EW systems capable of jamming, spoofing, and protecting key communications across dispersed units. This fast learning loop ensures their forces are better prepared for spectrum dominance in future peer-level conflicts.

1.26 In the Indo-Pacific region, the complex terrain and hybrid nature of conflict present unique EW challenges, which the Olvanan military uses to refine its approach to dismounted and small unit EW tactics. Observing how insurgent groups utilise low-tech jamming and signal interception to degrade government communications, the Olvanan focus has focussed on rugged, portable EW equipment optimised for rapid deployment alongside infantry in jungle and mountainous environments. By integrating these lessons, the OPA aims to close capability gaps seen in protracted low-intensity conflicts, thereby ensuring their forces can maintain communications and situational awareness while fighting both irregular adversaries and peer adversaries in the complex terrain of the Pacific.

1.27 Lessons from conflicts in the Middle East have further reinforced Olvanan recognition of the centrality of urban EW in future operations. The use of electronic deception and jamming against enemy forces revealed the disruptive potential of EW in urban terrain, while the rapid development of countermeasures highlighted the need for continuous EW innovation and spectrum agility. Olvanan doctrine has incorporated these findings by enhancing their urban EW training, and developing systems designed for quick repositioning, electronic protection, and close coordination with infantry and un-crewed aerial vehicles, (UAV) units in urban environments. This rapid learning and field experimentation cycle helps Olvanan forces build resilience and adaptability to counter sophisticated Western EW and counter-drone tactics in urban combat.

1.28 Across these conflicts, the Olvanan military is institutionalizing a faster EW learning loop by leveraging real-time intelligence, simulation exercises, and feedback from operational deployments. This process is further supported by enhanced EW training programs, more frequent field tests, and a doctrinal emphasis on multi-domain integration of electronic warfare with cyber, space, and kinetic operations. In accelerating their ability to learn and adapt from recent global conflicts, Olvana aims to close the technological and tactical gap against Western forces, ensuring their CA-Bdes can achieve information superiority and EMS dominance in future high-intensity warfare.

## Section 1-8. Integration with Joint and Multi-Domain Operations

1.29 Olvanan doctrine emphasises the seamless integration of electronic warfare within broader joint and multi-domain operations. At the CA-Bde level and above, EW capabilities are synchronised not only with ground manoeuvre forces but also with air force, naval, cyber, and space assets. This multi-domain approach enables the OPA to exploit the full spectrum of operational environments, creating coordinated effects that overwhelm adversary's sensors, command networks, and weapon systems. For example, EA from both ground and air EA assets could be used in tandem to degrade enemy radar coverage while naval forces conduct anti-access/area denial (A2/AD) operations, with air assets deliver precision SEAD, creating complementary layers of effect EW and kinetic effects.

1.30 At the operational level, mechanisms include centralised C2 nodes that manage EW effects in concert with joint targeting cycles, ensuring that electronic attacks support kinetic fires and reconnaissance efforts effectively. The OPA's use of integrated communications networks and data fusion centres allows real-time sharing of electronic order of battle (EOB) information across services, enhancing situational awareness and responsiveness. Such integration is critical in multi-domain battlespace, where speed and precision require synchronised action across disparate domains.

1.31 In emerging conflicts, space-based assets and cyber operations are increasingly assimilated into the EW framework, allowing Olvanan strategic forces to disrupt satellite communications, global positioning system (GPS), navigation, and adversary cyber infrastructure. This layered approach extends the reach of EW effects beyond the immediate battlefield, complicating enemy decision-making and reducing their operational freedom. Training exercises routinely incorporate joint and multi-domain coordination, preparing units to operate effectively in contested electromagnetic and informational environments.

# Chapter 2
# Olvanan Tactical Employment of Electronic Warfare

## Section 2-1. Defining Electronic Warfare and Information Warfare

2.1 For the OPA, EW is a key pillar across all military operations. EW involves the use of EMS operations to gain a strategic or tactical advantage. The core elements of EW include:

a. **Electronic Attack (EA) -** targets enemy systems via jamming and deception;

b. **Electronic Protection (EP) -** safeguarding friendly systems from interference; and

c. **Electronic Support (ES) -** detecting and analysing electromagnetic emissions.

2.2 Information Warfare (IW) in Olvanan doctrine is much broader and includes not only EW, but also cyber operations, psychological warfare, disinformation campaigns, as well as legal and diplomatic tools. The OPA views IW as essential for shaping the battlefield before kinetic conflict even begins. Their strategy often referred to as “informationalised warfare,” treats control of information as a decisive advantage equal to or greater than physical firepower.

## Section 2-2. Education of operators

2.3 **Foundational Training and Academics -** EW operator education begins with rigorous academic grounding at elite institutions such as the OPA’s Information Engineering University, where cadets earn degrees in radar engineering, signal systems, network command, or electronic countermeasures. Coursework covers the physical science of electromagnetic signals, electronic attack/protection/support techniques, and foundational cyber-electromagnetic integration. Students also engage in simulation labs and live-field exercises to reinforce theory with practical skills.

2.4 **Integrated War gaming and “Blue Force” Simulation -** EW trainees are immersed in advanced war-gaming exercises designed to replicate real-world electromagnetic complexity. Through simulated adversary “Blue Force” scenarios, operators learn to detect, jam, spoof, and neutralise hostile transmissions in a denied environment. These simulations are embedded in the Olvanan annual training cycle, and emphasise learning from forced errors and after-action review. This mirrors OPA practices of using “electromagnetic Blue Army” units—sometimes even with support from Olvanan defence industry partners—to build realistic training exercises.

2.5 **Continuous Certification and Professional Development -** After completing initial training, EW operators receive ongoing certification through a lifelong vocational education platform akin to the OPA’s Vocational Training Bureau. They complete a combination of long residential courses, micro-courses, and practical assessments in topics like intelligentised EW integration, AI-augmented jamming, direction finding, and the integration of effects from space-based EW tools. Course completion is tracked, and operators earn technical certifications that reflect evolving doctrine and technology—ensuring proficiency across emerging EW domains, and rising social credit.

## Section 2-3. Olvanan Electronic Warfare Mission Sets

2.6 The OPA has developed a robust set of EW mission capabilities to undermine adversary C2, disrupt precision navigation, and compromise sensor systems. These missions support key Olvanan tactical aims such as denying access to contested maritime and air domains and degrading enemy operational tempo.

2.7 Defensive measures include hardened communications, frequency agility, and electromagnetic shielding to resist hostile jamming and detection. These are routinely tested during large-scale training operations simulating high-intensity EW environments. Olvanan doctrine places equal emphasis on survivability and offensive disruption.

2.8 Key EW missions undertaken by the OPA include:

a. **Jamming –** Transmitting disruptive signals to interfere with enemy communications, radar, or GPS receivers. Used in both broad-area denial and targeted suppression.

b. **Spoofing –** Emitting false signals to deceive enemy sensors or receivers, particularly GPS, creating inaccurate location or targeting data.

c. **Direction Finding (DF) –** Locating enemy transmitters through triangulation of their electromagnetic emissions, enabling targeting or avoidance.

d. **Electronic Attack (EA) –** Active use of the EMS to degrade, neutralise, or destroy enemy equipment or capabilities.

e. **Electronic Protection (EP) –** Safeguarding friendly use of the spectrum through encryption, frequency agility, and shielding techniques.

f. **Electronic Support (ES) –** Passive collection of electromagnetic signals for threat detection, situational awareness, and battle management.

g. **Signal Intelligence (SIGINT) –** Interception and analysis of enemy communications and radar emissions for operational or strategic insights.

h. **Electronic Intelligence (ELINT) –** Technical analysis of non-communication signals, like radar, to understand enemy sensor and air defence capabilities.

2.9 These capabilities are tightly integrated with cyber and kinetic strike systems within Olvanan units and formations, enabling precision engagement and information dominance throughout the operational spectrum.

## Section 2-4. Electronic warfare in the 17th Group Army

2.10 As in all Olvanan Group Armies, the Olvanan 17th Group Army maintains a sophisticated and multi-tiered electronic warfare capability designed to support operational-level campaigns across both conventional and irregular environments. Its EW structure includes specialised electronic countermeasures units embedded within its Air Defence brigade (AD), and the Reconnaissance, Intelligence, Surveillance, and Target Acquisition Battalion (RISTA), technical reconnaissance elements responsible for long-range signal collection and analysis, and dedicated coordination cells at the Group Army headquarters level. These formations provide persistent electromagnetic support to subordinate CA-Bdes, integrating SIGINT, DF, and broad-area jamming to disrupt adversary C2 and surveillance systems. The group army can also mobilise spectrum denial assets on short notice to shape the electromagnetic environment prior to major offensive or defensive actions, particularly in urban or littoral settings.

2.11 In addition to its offensive jamming and targeting capabilities, the 17th Group Army is central to EMS management and de-confliction across brigades, ensuring that multiple manoeuvre elements can operate within contested spectral conditions without mutual interference. It provides operational-level electromagnetic orders of battle (EMOB), allocates time-frequency resources to subordinate EW companies, and conducts EMS war-gaming to rehearse synchronised effects. The Group Army works closely with cyber and space elements to ensure cross-domain integration, enabling the rapid fusion of cyber intrusion results with EW targeting data. In line with Olvanan doctrine, this orchestration of capabilities ensures that EW is not limited to tactical enablers, but instead functions as a decisive operational tool to fragment enemy networks, blind ISR assets, and impose friction across the battlespace.

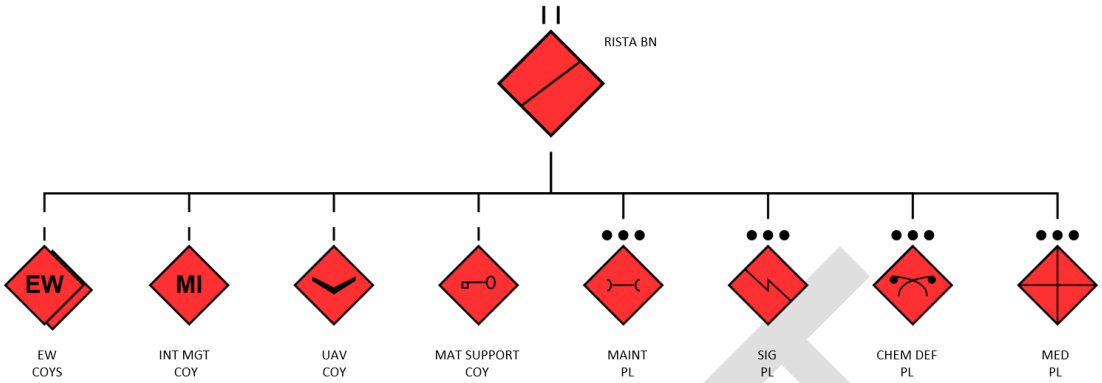
## Section 2-5. The RISTA Battalion

2.12 The Olvanan RISTA Battalion functions as the primary sensing and targeting element in the Group Army. It provides real-time electromagnetic situational awareness, cueing CA-Bde's EW Companies to threats, and enabling synchronised targeting of enemy C4ISR assets. This element integrates SIGINT, ELINT, and visual reconnaissance to map enemy positions and electromagnetic signatures.

2.13 Through the employment of organic UAVs, ground-based sensors, and mobile SIGINT teams, the RISTA Battalion supplies the CA-Bde with DF data, emitter geolocation, and cueing for jamming or

deception operations. It enables the CA-Bde's EW Company to execute distributed, coordinated effects across the EMS, enhancing tempo and lethality during shaping and decisive phases.

**Figure 2.1: RISTA Battalion**

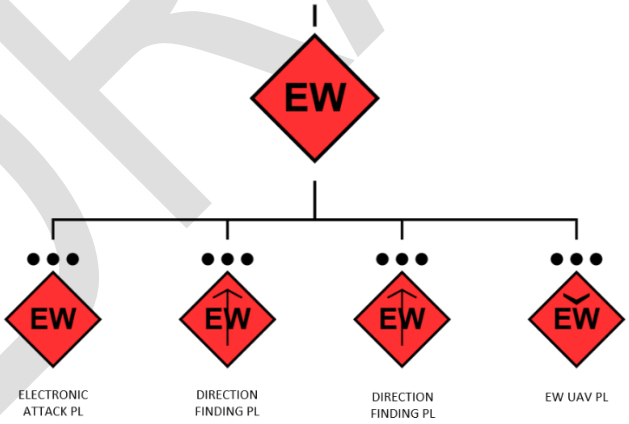



## Section 2-6. The EW Company in the CA-Bde

2.14 The Olvanan EW Company is the CA-Bde's principal EW force, delivering both offensive and defensive electromagnetic effects. It is tasked with degrading enemy communications, disrupting radar and sensor systems, and securing the brigade's use of the EMS. This element operates modular EW capabilities tailored to support manoeuvre, deep strike, and tactical protection.

2.15 Operating to the CA-Bde commander, the EW Company coordinates with manoeuvre battalions and artillery to deliver integrated jamming, spoofing, and signal protection. It maintains organic capability to conduct EA, ES, DF, and EP missions in support of the CA-Bde's objectives, enhancing decision dominance and survivability in contested environments.

**Figure 2.2: Electronic Warfare Company**



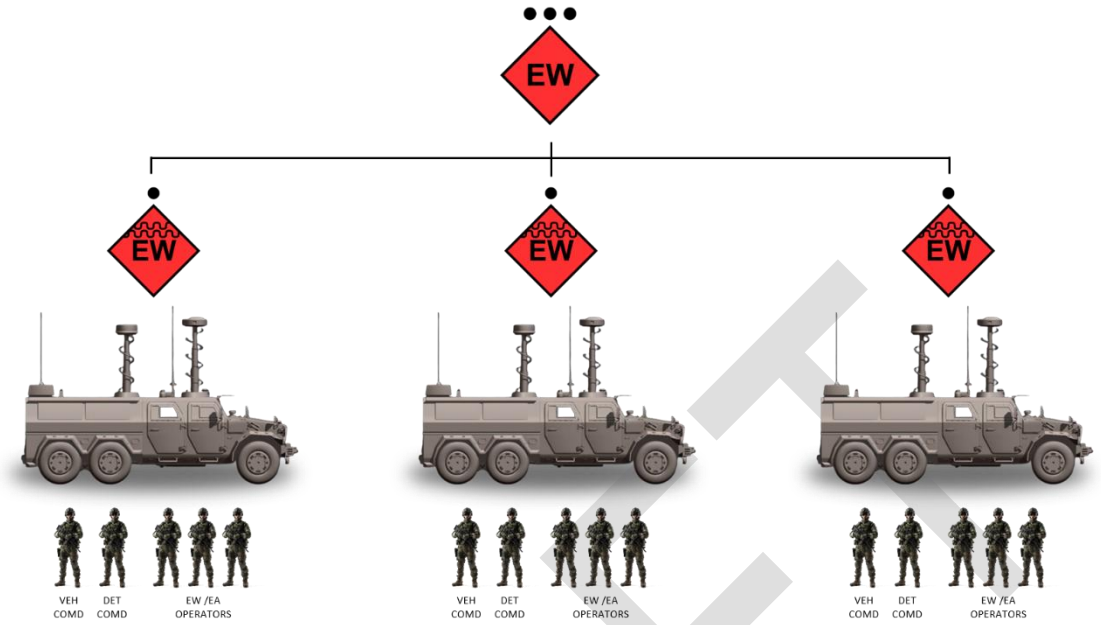

## Section 2-7. The EW Platoon (EA)

2.16 The EW Platoon forms the tactical execution-level element of the EW Company. It delivers localised, responsive EA support to manoeuvre elements, often forward deployed with combat units. It specialises in short-range jamming, signal spoofing, and real-time electromagnetic support, ensuring disruption of enemy networks at the tactical edge.

2.17 In addition to its offensive tasks, the platoon performs EP through the use of frequency agility, encryption support, and emission control (EMCON), procedures. It operates in close coordination with DF

and UAV Platoons, enabling agile responses to dynamic threats and adaptive countermeasures on a mission-by-mission basis.

**Figure 2.3: Electronic Warfare Platoon**

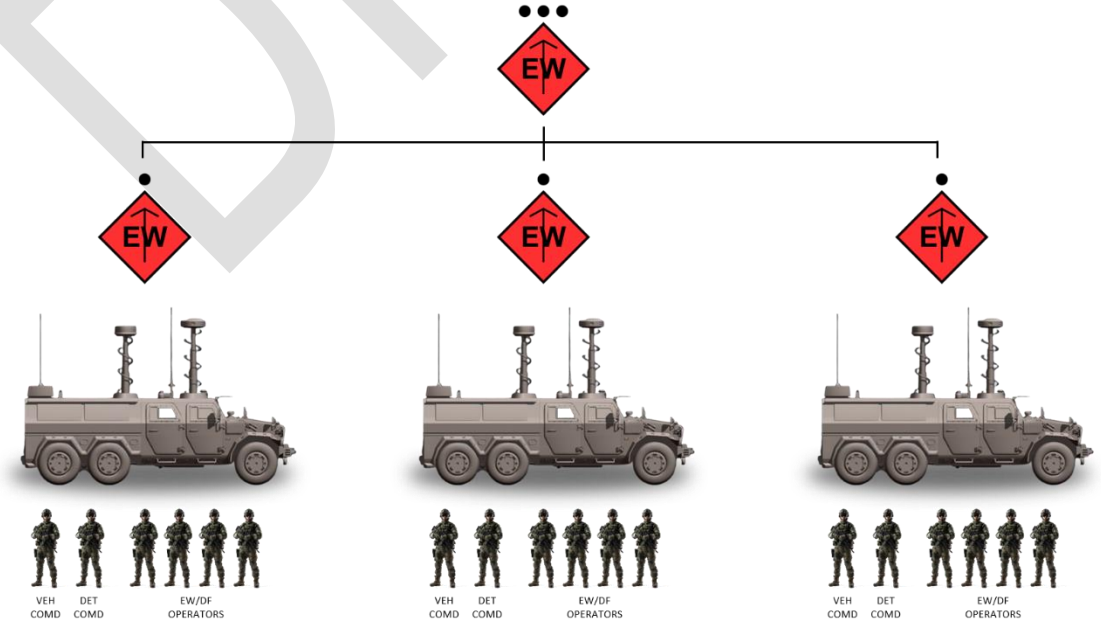



## Section 2-8. The DF Platoon

2.18 The DF Platoon is a specialised EW Company asset responsible for locating, tracking, and classifying enemy electromagnetic emitters. It performs emitter triangulation and signal analysis, enabling the brigade to geo-locate command posts, fire control radars, and communications hubs. This element is essential for cueing kinetic fires, jamming, or deception efforts.

2.19 Working in coordination with the EW UAV Platoon, the DF Platoon ensures rapid emitter identification and targeting, feeding critical data into the brigade's common operational picture (COP). It also supports EW de-confliction by identifying friendly vs hostile signatures in congested electromagnetic environments.

**Figure 2.4: Direction Finding Platoon**

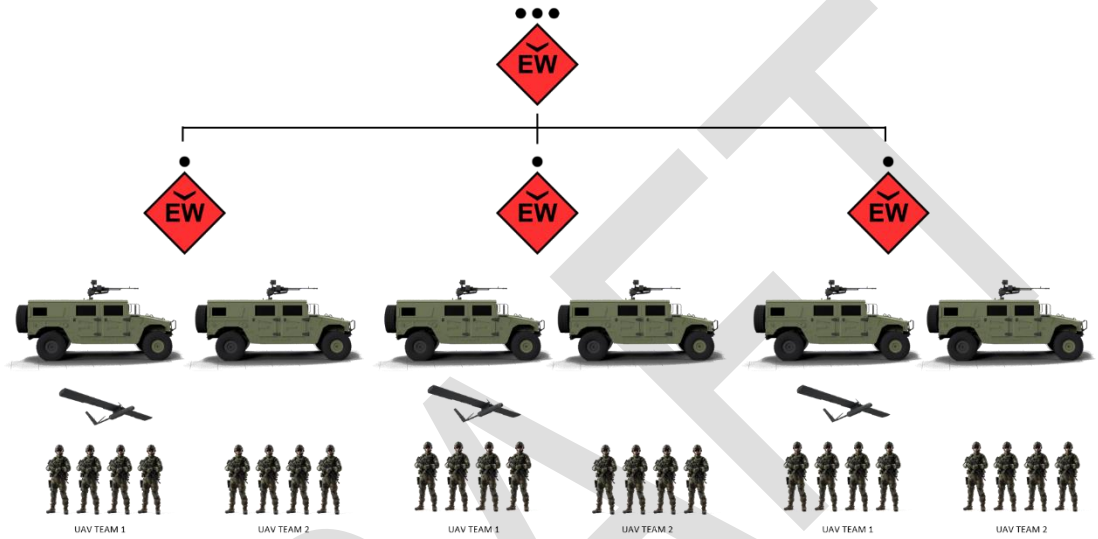


## Section 2-9. The EW UAV Platoon

2.20 The EW UAV Platoon provides airborne DF, EA, and ES via tactical UAVs equipped with EW payloads. This element offers extended reach and persistent electromagnetic coverage in denied or high-risk areas. Its primary mission is to conduct airborne SIGINT collection, and with changes to EW, payloads can conduct limited EA and spoofing operations across the brigade's area of operations.

2.21 Its mobility and standoff capability allow the EW UAV Platoon to operate in contested airspace with reduced risk to personnel. It also supports dynamic re-tasking, enabling the brigade to rapidly adapt its EW posture. Integrated with both the EA and DF elements, the UAV Platoon enhances the CA-Bde's ability to shape and dominate the electromagnetic battlespace.

**Figure 2.5: UAV Platoon**




## Section 2-10. Olvanan Electronic Warfare Equipment

2.22 The CTL-181A EW is a wheeled, mobile EW vehicle employed at the CA-Bde level to provide deep-spectrum EA, DF, and ES capabilities. It is built on a robust 6×6 chassis and equipped with modular antenna arrays, signal jamming suites, and direction-finding systems, enabling it to conduct offensive jamming, SIGINT, and EP roles with minimal reconfiguration. While it is typically deployed in support of motorised forces, it is the mainstay platform of many EW units.

2.23 The platform can conduct EA missions against enemy radio communications, radar emissions, and satellite navigation signals, effectively degrading adversary situational awareness and C2. The vehicle's integrated DF system allows it to geo-locate hostile emitters with high precision and pass target data to strike units or command posts. Its on-board encrypted communications suite enhances the resilience of Olvanan command networks when operating in contested electromagnetic environments.

2.24 The CTL-181A is often deployed in small teams to cover wide areas of the battlefield, working in tandem with reconnaissance units and UAVs to map the electromagnetic spectrum. With minimal reconfiguration, it can shift roles in real time depending on the operational requirement, and its high mobility allows it to reposition frequently to avoid detection and counter-fire. This adaptability makes it a key enabler for achieving electromagnetic superiority at the brigade level.

**Figure 2.6: CTL 181A Electronic Warfare Variant**

2.25 The ZBL-08 EW variant is a wheeled and armoured platform designed to provide EW support directly to manoeuvre elements. Based on the ZBL-08 chassis family used across Olvanan mechanised infantry formations, the EW configuration includes integrated systems for radar jamming, communications interference, and ELINT collection. It is operated by EW platoons organic to the brigade EW Company and supports close-in operations with armoured and mechanised units.

2.26 This vehicle is optimised for tactical-level EA, delivering targeted jamming against enemy surveillance radars and short-range communications systems. It also collects real-time signal data to identify and classify threat emitters on the battlefield. Its armoured protection allows it to operate in contested zones where lighter EW assets may not survive, and its mobility ensures it can keep pace with advancing mechanised forces.

2.27 The ZBL-08 EW vehicle is also equipped with systems for EP, including frequency-hopping and spectrum-shielding tools, which can help protect Olvanan forces from adversary jamming or electromagnetic intrusion. In combined arms operations, it enables the brigade commander to apply EW effects at the point of decision, supporting both offensive and defensive actions under armour.

**Figure 2.7: ZBL 08 Electronic Warfare Variant**

2.28 The CH-802 is a lightweight, hand-launched, fixed-wing UAV used by the EW UAV Platoon. Originally designed for battlefield reconnaissance, the platform has been adapted for EW by integrating modular payloads primarily in a signal interception, DF role, and localized jamming. Its small size, electric

propulsion, and low infrared signature make it ideal for use in contested environments where stealth and persistence are required.

2.29 As an EW asset, the CH-802 is typically deployed to map the EMS, identify hostile emitters, and collect SIGINT from frontline enemy communications and radar systems. Fitted with compact electronic support measure (ESM) payloads, it can geo-locate and classify transmissions across a range of frequencies. This data is relayed in real time to EW Company, enabling precision targeting and emitter exploitation. The platform can operate independently or be cued by other sensors within the CA-Bde's layered EW network.

2.30 It can be re-configured for an offensive role, and CH-802 variants may carry directional jamming pods capable of disrupting enemy radio links, UAV control signals, or short-range radar. While the power output is limited due to the airframe's size, its ability to deliver targeted jamming at low altitude and close range makes it valuable in EA missions against vulnerable or lightly defended targets—especially in urban and jungle terrain where ground-based systems have reduced effectiveness. It may also be employed for deception, broadcasting false emitter signatures to provoke enemy responses or mask friendly movements.

**Figure 2.8: EW UAS – CH-802**

2.31 Dismounted EW teams in the OPA are equipped with a range of portable electronic warfare systems designed to support tactical units in complex environments such as urban areas, dense jungle, and mountainous terrain. These teams are embedded with infantry or reconnaissance elements and provide localised EA and ES capabilities that complement the brigade's mounted assets.

2.32 Their standard equipment is mission dependant, however will include a mix of compact radio frequency jammers, capable of disrupting enemy communications within a defined radius, handheld DF units for locating hostile transmitters, and portable intercept systems for gathering ELINT. These tools allow small teams to map local electromagnetic activity, interfere with enemy C2 nodes, and feed emitter data back to higher headquarters for integration into strike planning.

2.33 Dismounted EW teams are highly valuable in terrain that limits line-of-sight or vehicle mobility. Their ability to set up quickly, operate covertly, and support deception or disruption missions makes them a flexible and important component of the CA-Bde's wider EW strategy, independent of larger vehicle platforms.

**Figure 2.9: Example of Olvanan dismounted EW equipment – DZ-9300**

# Chapter 3
# Principles of Employment

## Section 3-1. Command and Control

3.1 At the strategic level, the OPA employs a highly centralised C2 system for its EW capabilities. These units are typically subordinated to the Strategic Support Department (SSD), and operate under strict control from the national-level Commands. This structure ensures strategic coherence and unity of effort across multiple domains—including cyber, space, and EW.

3.2 Operational control is exercised vertically, with minimal delegation to tactical echelons. EW units receive mission directives that are tightly scripted, often accompanied by operational restrictions to ensure alignment with national messaging and political objectives. The C2 hierarchy prioritises tight coordination between EW, cyber operations, and kinetic fires, ensuring that effects are synchronised during both peacetime, and wartime activities.

3.3 However, this structure also reduces responsiveness on the battlefield. Since EW is considered an operational tool rather than a purely tactical enabler, its employment is subject to intense oversight. The result is a system optimised for long-term influence operations and pre-planned campaign-level engagements rather than fast-reacting battlefield support. Tactical commanders therefore often have limited freedom to initiate EW actions without higher approval.

## Section 3-2. Layering of Electronic Warfare Effects

3.4 At the Group Army level, the Olvanan RISTA Battalion plays a critical role in shaping the electronic battlefield by conducting broad-spectrum EW effects focused on operational objectives. The RISTA Battalion's EW assets, such as long-range signal intercept systems and ELINT platforms, provide the commander with a detailed EOB. This includes identifying enemy emitter locations, frequencies, and patterns of communication and radar usage.

3.5 Through continuous signal collection and direction finding, the RISTA Battalion can map enemy communication nodes and air defence radars across the operational area, enabling the commander to anticipate enemy movements and plan spectrum dominance strategies. This intelligence-driven EW layer is essential for building situational awareness and underpins the CA-Bde's ability to conduct synchronised EA and EP missions.

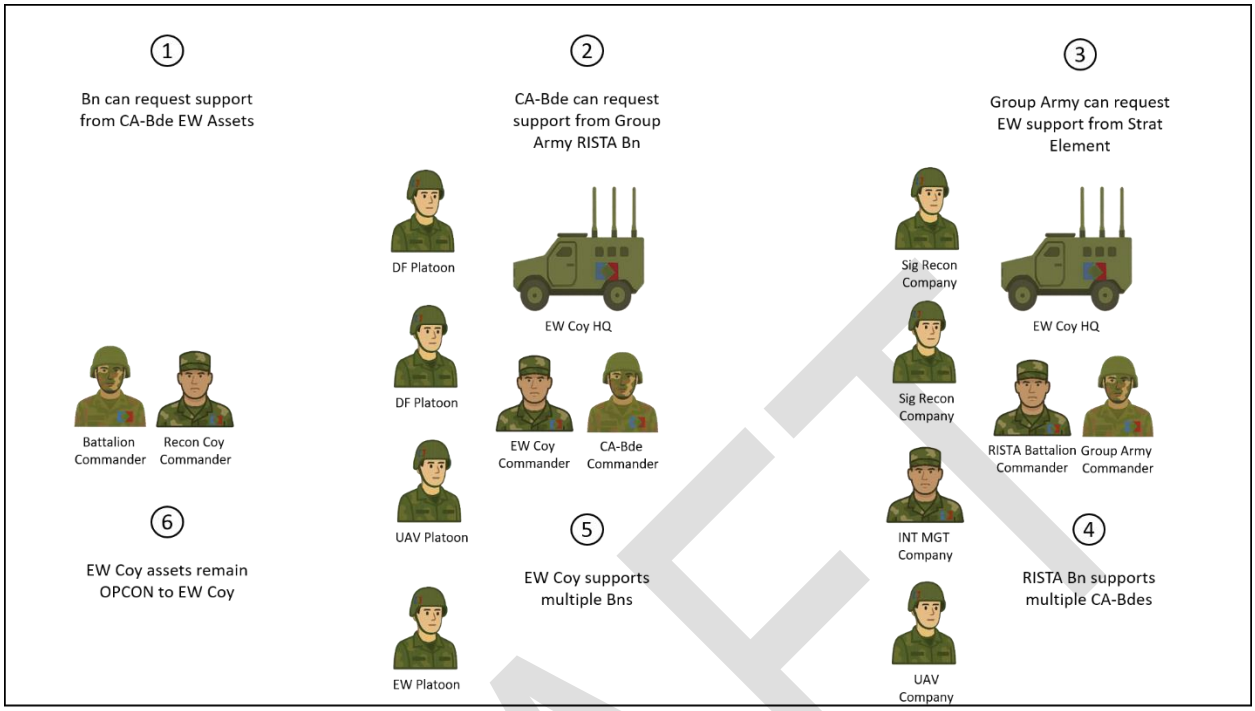
3.6 Within the CA-Bde, the EW Company operates at the tactical level to translate the RISTA Battalion's intelligence into actionable EW effects that directly support manoeuvre units. The company conducts focused EA, DF, EP, and deception operations. The integration of these capabilities ensures that EW effects degrade enemy situational awareness and communications at the point of contact, enhancing the survivability and effectiveness of friendly forces.

3.7 At the platoon level, the EW Platoon, DF Platoon, and EW UAV Platoon execute specialised and immediate EW tasks that contribute to the CA-Bde's mission and broader EMS control. The DF Platoon, for example, uses mobile sensor arrays and handheld equipment to pinpoint enemy emitters during engagements, facilitating rapid targeting decisions by artillery or air assets. Simultaneously, the UAV Platoon deploys unmanned aerial systems equipped with EW payloads to maintain persistent electronic surveillance over key terrain features or enemy assembly areas, extending the brigade's reach into areas inaccessible to ground forces. This tactical layering enables the Olvanan CA-Bde to maintain continuous EMS situational awareness and apply flexible EW effects dynamically on the battlefield.

3.8 The CA-Bde commander relies heavily on this multi-tiered EW framework to understand the enemy's EMS laydown—essentially, the distribution and activity of enemy electronic emitters across the operational environment. Integrating intelligence from the RISTA Battalion with real-time data from the EW Company and its platoons, allows the commander to construct a comprehensive and current enemy EOB. This enables informed decision-making on spectrum management, force protection, and offensive EW operations. The commander's situational awareness is further enhanced by pulling information from joint command centres where EW data is fused with other ISR inputs. This holistic understanding allows

the CA-Bde to anticipate enemy EW tactics, optimise their own spectrum usage, and maintain electromagnetic superiority across their zone of operations.

**Figure 3.1: Layering of Electronic Warfare Effects**




## Section 3-3. De-confliction of EW effects

3.9 Effective management and de-confliction of the EMS are essential for maximising the operational impact of Olvanan EW capabilities while minimising the risk of fratricide. The OPA employs a disciplined EMS control framework that assigns specific frequency bands and time windows to different EW and communications units. This structured approach prevents overlapping transmissions and interference between friendly systems, ensuring that jamming, DF, and reconnaissance efforts do not degrade each other's effectiveness. Coordination is maintained through a layered C2 system that disseminates real-time EMS usage data from higher authority, through the CA-Bde headquarters to EW Company and EW platoons.

3.10 Olvanan forces also leverage advanced spectrum monitoring and management tools to continuously assess the EMS environment. These systems allow EW operators to dynamically adjust frequencies, modulation techniques, and emission timing in response to adversary actions and environmental changes. In highly contested or cluttered EMS environments—such as dense urban areas or jungle terrain—this agility is crucial to maintaining operational superiority.

3.11 Despite these rigorous controls, managing EMS in a complex battlefield is inherently challenging. The OPA accounts for this by training specialised EMS management teams tasked with rapid detection and resolution of frequency conflicts, interference patterns, and emergent threats. These teams maintain detailed EOB updates and employ predictive analytics to anticipate adversary EW deployments, enabling proactive spectrum adjustments. This combination of doctrinal discipline, technological support, and continuous monitoring ensures that Olvanan forces exploit the EMS to its fullest while preserving the integrity of their own networks and sensor suites.

## Section 3-4. Rigidity of Olvanan C2 and Release Authority

3.12 One of the defining characteristics of the Olvanan C2 structure is its rigidity, derived from a dual-command framework that prioritises ideological control alongside operational effectiveness. Every EW or IO unit is subject to both military hierarchy and political oversight. This duality imposes an additional layer of coordination, often slowing down decision cycles during critical moments.

3.13 The Olvanan C2 model emphasises control over initiative. Units are trained to wait for direction rather than act autonomously, which can be effective for maintaining message discipline and strategic cohesion but often proves limiting under ever changing battlefield conditions. In environments where adversaries rapidly adapt, this rigidity can hinder the OPA's ability to exploit time-sensitive opportunities or respond to unforeseen disruptions.

3.14 Exercises and real-world engagements have highlighted this structural inflexibility; even when frontline commanders identify exploitable vulnerabilities in enemy electronic systems, the requirement to obtain political and operational clearance before acting often causes missed windows of opportunity. This rigidity is a systemic trade-off: it prioritises control and ideological purity over adaptability and rapid initiative.

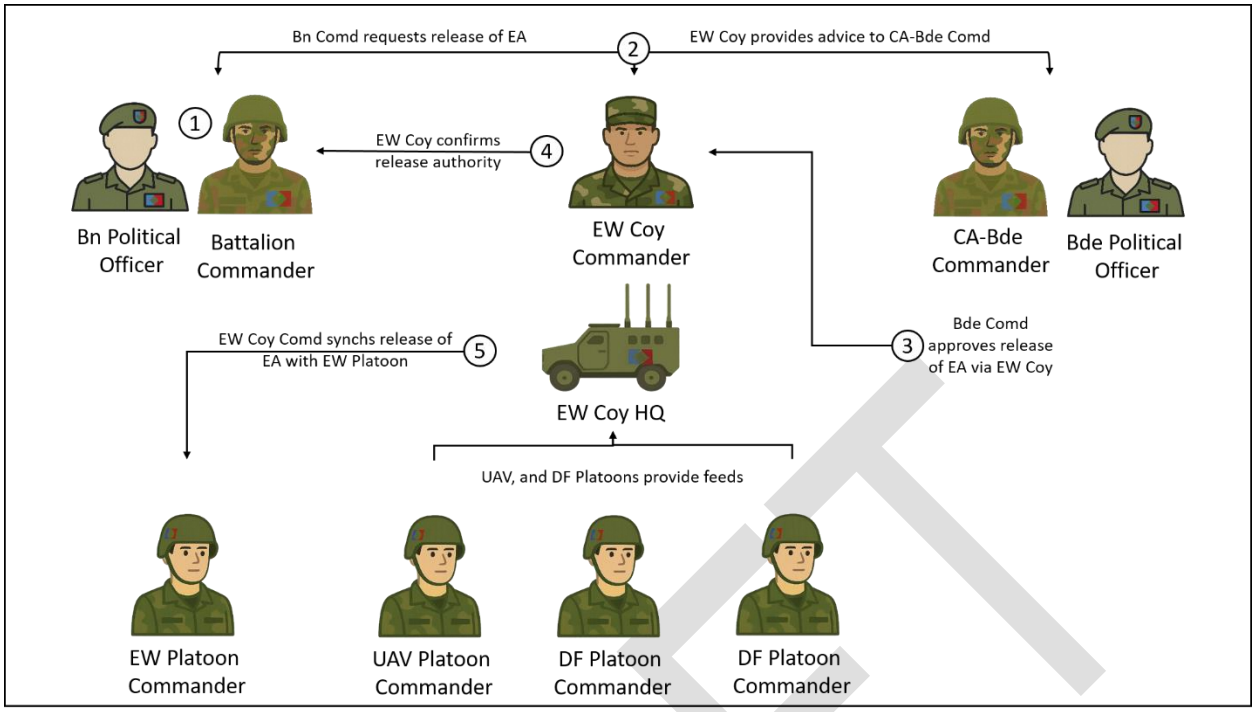
3.15 Release authority for EW effects within the CA-Bde is tightly controlled to balance operational effectiveness with risk in the EMS. Typically, the CA-Bde commander holds ultimate authority for approving any major EW missions, especially those with wide-ranging or long-duration effects such as area jamming or GPS spoofing. This centralised control ensures EW actions support the commander's intent, minimise fratricide and collateral disruption, and align with the broader operational plan. Tactical EW effects of limited scope—such as localised jamming or short-term deception—may be delegated to subordinate EW platoon or company commanders, provided they operate within established parameters and coordinated frequencies.

3.16 Coordination mechanisms within the CA-Bde staff are critical to managing release authority effectively. The brigade's EW Company Headquarters acts as the primary coordinating node, working closely with the Intelligence, Communications, and Fires cells to integrate EW activities into the brigade's overall battle rhythm. The EW Company commander advises the Bde commander on spectrum availability, de-confliction needs, and potential collateral effects before recommending release of specific EW effects. This process often includes dynamic reassessment during combat operations, with an emphasis on maintaining EMS situational awareness and adapting jamming or spoofing actions to evolving threats and friendly force movements.

3.17 At the Group Army level, release authority also requires synchronisation with higher-echelon commands, especially for EW missions that have cross-brigade or theatre-wide impact. For example, broad-spectrum jamming that could affect adjacent units or civilian infrastructure usually demands approval from Group Army or Theatre Command headquarters. This tiered command structure of centralised control over EW effects prevents unintended operational friction and ensures compliance with political and legal frameworks. The CA-Bde commander must liaise with these higher authorities to secure permissions and align tactical EW operations within operational objectives.

3.18 Finally, the complexity of modern EW necessitates robust C2 systems that enable rapid decision-making and release of EW effects under high-tempo conditions. Olvanan doctrine emphasises integrated C2 platforms that fuse real-time intelligence, EOB updates, and spectrum management tools to empower the CA-Bde commander and EW staff with timely, accurate data. This integration allows the delegated authorities to operate confidently within defined boundaries and supports the agile, decentralised execution of EW tasks while retaining centralised oversight. The command structure thus balances flexibility with control—crucial for effective EMS dominance in complex, contested environments such as urban or jungle warfare.

**Figure 3.2: Release Authority**




## Section 3-5. Delegation of EW capabilities

3.19 In Olvanan doctrine, the delegation of EW capabilities at the CA-Bde level tends to follow a “tasked in support” model rather than a full task-organised structure. While the CA-Bde commander retains command over the organic EW Company and its subordinate platoons, higher-echelon EW assets (such as long-range jamming systems, strategic SIGINT platforms, or passive detection systems are generally controlled at the Group Army or Theatre level, and placed in support of the brigade based on operational requirements. This centralised approach ensures strategic coherence and spectrum de-confliction across echelons, aligning with the Olvanan emphasis on tightly controlled, synchronised application of information domain effects.

3.20 In practice, this means that the CA-Bde commander can request EW effects or ISR support from higher headquarters through the brigade’s Electronic Warfare Coordination Element (EWCE), but does not normally gain direct control of those systems. Even within the brigade, the employment of organic EW capabilities is often pre-scripted in support of priority missions, such as deception during offensive operations or suppression of enemy C2 nodes during a penetration, for example. This method ensures that the use of EW is coherent with the wider operational plan. Thus, Olvanan commanders tend to employ their EW Company in support of manoeuvre or fires elements at key phases, rather than restructuring the force around temporary task groups.

## Section 3-6. Role of the political officer

3.21 The political officer—formally known as the Political Commissar—is a cornerstone of the Olvanan military system, including within EW units. These officers are embedded at every level of the OPA and wield authority equal to that of their commanding officers. Their primary role is to ensure that military operations are ideologically aligned with the ruling party’s objectives and values.

3.22 Within EW and IW formations, political officers serve dual functions. First, they are tasked with supervising the moral and political discipline of the unit, ensuring loyalty to the state and the central command. Second, they directly influence the operational planning and execution of information warfare campaigns. This includes guiding the tone, messaging, and target selection for psychological or electromagnetic effects.

3.23 Political officers also act as conduits for top-level narratives, ensuring that EW activities support broader strategic objectives such as regime legitimacy, regional influence, or deterrence messaging. Their presence ensures that EW is not simply a technical function, but a political act with consequences

beyond the battlefield. In many cases, they are responsible for approving the initiation of EW operations and serve as the final arbiter in any dispute between military urgency and political caution.

## Section 3-7. Exceptions to employment

3.24 **Jungle -** The jungle environment imposes severe constraints on the propagation of electromagnetic signals due to dense vegetation and rugged terrain, as outlined in Olvanan Jungle Warfare Doctrine. Thick foliage absorbs and scatters radio waves, severely limiting the range and effectiveness of communication and jamming systems. For example, the ability to conduct long-range EA is diminished; forcing operators to adapt by using relay nodes or low-frequency bands that better penetrate dense canopies. EW teams must carefully plan their positioning and timing, coordinating with ground forces to exploit natural clearings and high ground to maximisee signal effectiveness.

3.25 Mobility challenges are equally pronounced. Vehicles cannot traverse the narrow, muddy, and uneven jungle trails, compelling dismounted EW teams to carry lighter, man-portable systems. This shift increases the logistical burden, as operators must carry additional batteries and equipment to sustain operations. For instance, during jungle patrols or reconnaissance missions, dismounted EW operators may employ handheld direction-finding gear and tactical radio jammers, but their operational endurance is limited by the weight and power supply of these systems, complicating sustained EW support in remote areas.

3.26 The jungle's electromagnetic environment is cluttered creating a complex spectrum landscape. Olvanan EW doctrine stresses the use of advanced signal processing techniques and operator training to distinguish enemy communications from environmental clutter. The complexity of operating in this environment is compounded when enemy forces employ low power, frequency-hopping radios or short-range communications to evade detection.

3.27 Jungle EW operations require close synchronisation with infantry and reconnaissance elements to overcome visibility and communication challenges. According to the Olvanan CA-Bde Jungle Tactics Manual, EW teams operate within close proximity to manoeuvre units to ensure mutual support and security. This proximity exposes EW operators to greater risk, demanding rigorous training in jungle survival, camouflage, and threat evasion. Integrated operations using UAVs equipped with EW payloads can extend sensor reach, enabling detection beyond line-of-sight limitations, but must be carefully coordinated to avoid fratricide and maintain stealth in a heavily contested electromagnetic and physical environment.

3.28 **Urban -** The urban electromagnetic environment is characterised by extreme congestion due to civilian cellular networks, Wi-Fi, broadcast services, and multiple military emitters operating in close proximity. This creates a challenging signal discrimination problem. Olvanan doctrine mandates the use of advanced signal analysis and target identification protocols to prevent collateral disruption and ensure compliance with rules of engagement.

3.29 The EW Company therefore utilises detailed electromagnetic mapping and modelling to identify optimal jamming positions, often leveraging rooftops or elevated structures to maximise coverage while minimising unintended interference with civilian networks, and preserving essential civilian services, reducing the risk of civilian casualties and maintaining operational legitimacy.

3.30 Mobility for mounted EW assets can be highly restricted in urban terrain. Narrow streets, rubble, and the constant threat of ambush require vehicles to proceed cautiously or dismount EW teams to conduct their operations on foot. Olvanan urban doctrine prescribes the use of modular, lightweight EW equipment for dismounted teams, enabling them to move through confined spaces like buildings, alleyways, and subterranean passages. For example, during urban clearance operations, dismounted EW operators deploy handheld jammers and direction finders to disrupt enemy command posts concealed within building complexes, while maintaining mobility and minimising their electronic footprint.

3.31 Successful EW operations in urban areas requires tight integration with manoeuvre forces, intelligence units, and civil affairs to balance operational effectiveness with risk management. Training focuses on rapid target discrimination, adaptive tactics, and situational awareness in the fluid urban battlespace, enabling Olvanan EW operators to maintain electromagnetic dominance while supporting complex multi-domain operations.

# Chapter 4
# Tactical Employment

## Section 4-8. EW in Offensive Zones

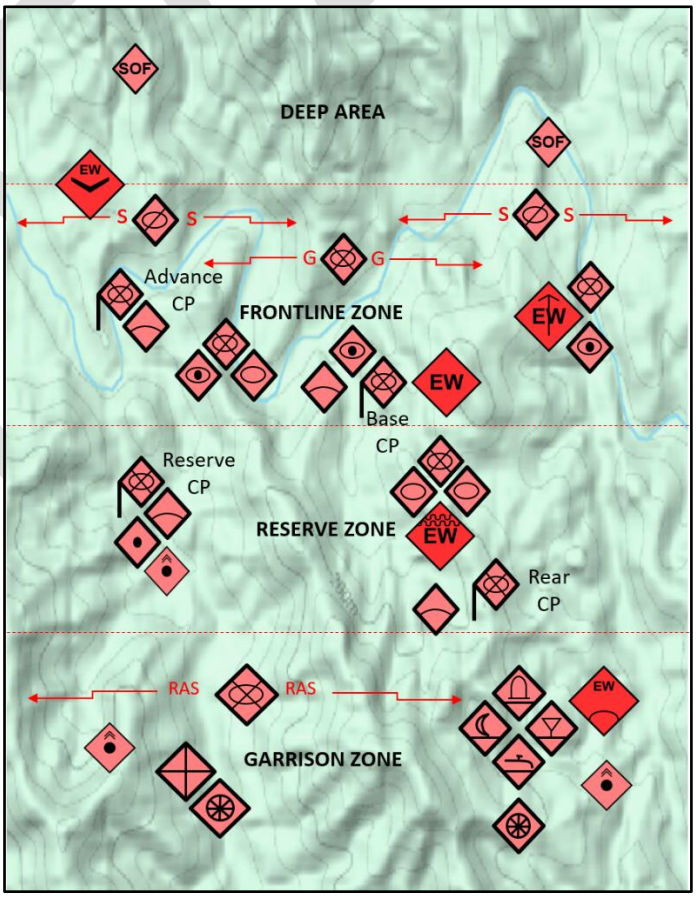
4.1 In offensive operations, EW elements play a key role in shaping the electromagnetic environment within the deep and disruption zones. Passive detection systems and EW-equipped UAVs are employed ahead of the forward edge of the battle area (FEBA) on the seam between the Deep Area and the Frontline Zone to detect and map enemy C2 nodes, radars, and communication infrastructure. This effort builds an enemy EOB used to identify critical emitters, degrade sensor coverage, and support strike packages. These shaping operations enable manoeuvre elements to retain the initiative by blinding enemy early warning systems and disrupting coordination prior to the main assault.

4.2 As manoeuvre formations enter the Frontline Zone, the organic DF elements are more likely to be deployed to provide early warning, add additional fidelity to the information being received from the EW UAVs, and to enable kinetic targeting of the enemy's frontline assets. They will also be utilised to enhance the CA-Bde's deception efforts.

4.3 In the Reserve zone, EA elements can be attached to Depth Attack Groups, in order to provide focused jamming in line at critical periods in the advance. These will be synchronised with direct and indirect fires, and deception operations. This controlled employment ensures that electronic effects remain scalable, dynamic, and tactically relevant, directly enabling penetration into contested enemy positions.

4.4 Also in the Reserve and Garrison Zones, higher level EW systems, potentially supplied from the Group Army may be seen. These will generally be utilised in a more defensive role at HQ locations, and key logistics nodes, and are more likely to be associated with AD EW.

**Figure 4.1: EW in Offensive Zones**

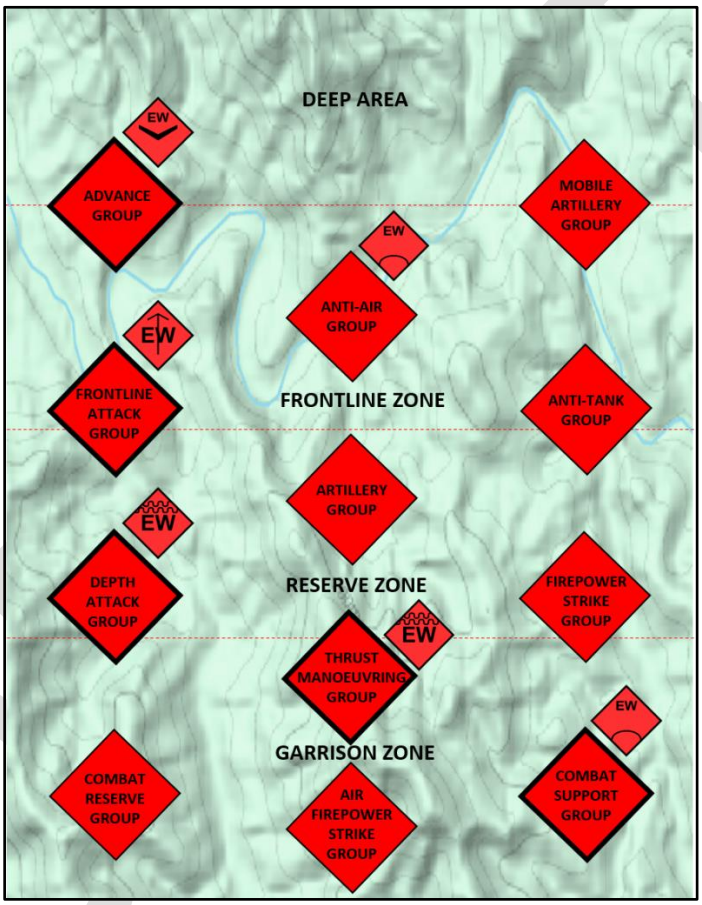


## Section 4-9. EW in Offensive groupings

4.5 Within offensive formations, EW elements are integrated into both the Advance and Frontline Attack groups. Their primary role is to suppress enemy coordination and degrade sensor coverage during the close fight. EA and DF platoons work alongside manoeuvre units to jam command nets, locate emitting headquarters, and cue precision fires, limiting the adversary's ability to coordinate a defence, EW forces can help set conditions which can be exploited by assault elements.

4.6 As the offensive progresses, EA capabilities shift toward support for Depth Attack groups. EW UAVs operate to the flanks, and further forward with the Advance Group to provide a more detailed intelligence picture, enabling the disruption of reinforcements, delay of logistical support, or to provide indicators and warnings on spikes in communications that might indicate enemy withdrawal, or the commitment of a reserve.

**Figure 4.2: EW in Offensive Groupings**



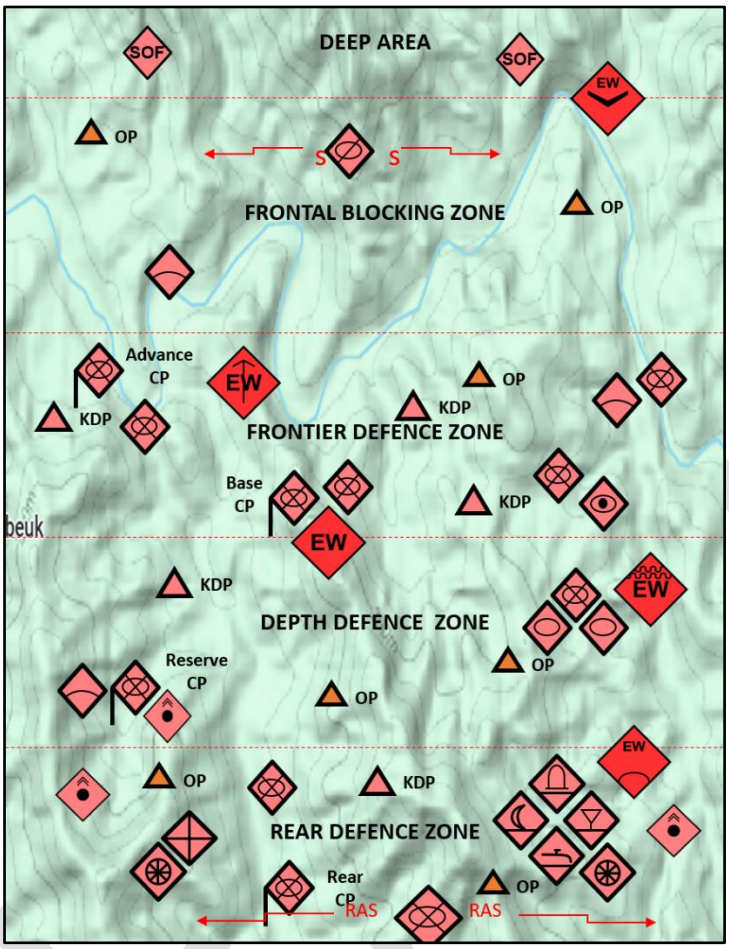

## Section 4-10. EW in Defensive Zones

4.7 In defensive operations, EW systems are generally deployed across the Frontal Blocking and Frontier Defence Zones to monitor enemy activity, detect approaching formations, and deny adversary situational awareness. Passive systems scan the spectrum continuously to identify enemy reconnaissance assets, and EA elements can be tasked with selectively disrupting the enemy's ability to coordinate fires or execute reconnaissance. These electronic effects are layered with decoy and deception efforts to delay the enemy and channel them into engagement areas.

4.8 Further in-depth, EA elements support reserve and counterattack forces positioned in depth defence zones. These units rely on EW to suppress enemy targeting networks and support force protection during manoeuvre. As enemy momentum slows or stalls, EW elements enable friendly forces to regroup, reinforce critical areas, or prepare for local counterattacks under the cover of reduced electromagnetic visibility.

4.9 Any higher level assets are more likely to be deployed in the Depth Defence Zones, and will be focussed on AD, or counter drone operations on larger logistics and reserve locations.

**Figure 4.3: EW in Defensive Zones**



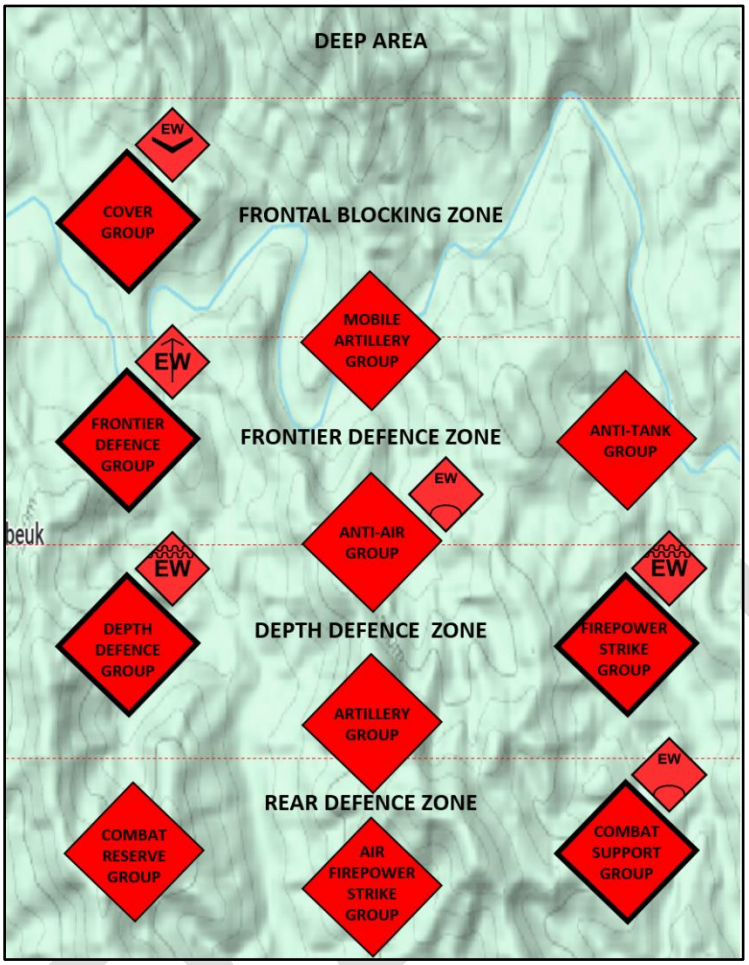

## Section 4-11. EW in Defensive groupings

4.10 Defensive groups rely on EW to delay, dislocate, and deceive enemy forces. EW UAVs will generally operate well forward of the main defensive positions with the Cover Group, with the majority of Direction finding capability also forward with the Frontier Defence Group. Provided a large enough ops box, the DF units can support multiple groupings, as they will also be required to aid with deception operations throughout the battlespace.

4.11 Depending on the level of release authority devolved to the commander, the EA elements can be found in either the Depth Defence Group, for use in localised counter-attacks, or within the Firepower Strike Group, when a more synchronised kinetic/non-kinetic effect is required.

4.12 Depending on the drone threat, EA elms may also be found in the Frontier Defence Group conducting a C-UAS function, however this limited resource will be quickly used up across a CA-Bde frontage.

**Figure 4.4: EW in Defensive Groupings**




## Section 4-12. Counter-drone Operations

4.13 The proliferation of drone technology on the modern battlespace has significantly altered the EW landscape, compelling Olvanan forces to develop specialised counter-drone capabilities as part of their tactical EW arsenal. EW units employ a combination of detection, tracking, and EA systems to deny enemy drones the ability to gather intelligence, conduct precision targeting, or provide battle damage assessment.

4.14 EW plays a central role in disrupting hostile drone swarms or individual UAVs by jamming C2 frequencies, spoofing navigation systems, and interfering with sensor payloads. These EW tactics are integrated with kinetic anti-UAV systems, and additional counter-measures creating a layered defence that complicates adversary drone operations and reduces the enemy's ISR and targeting advantages.

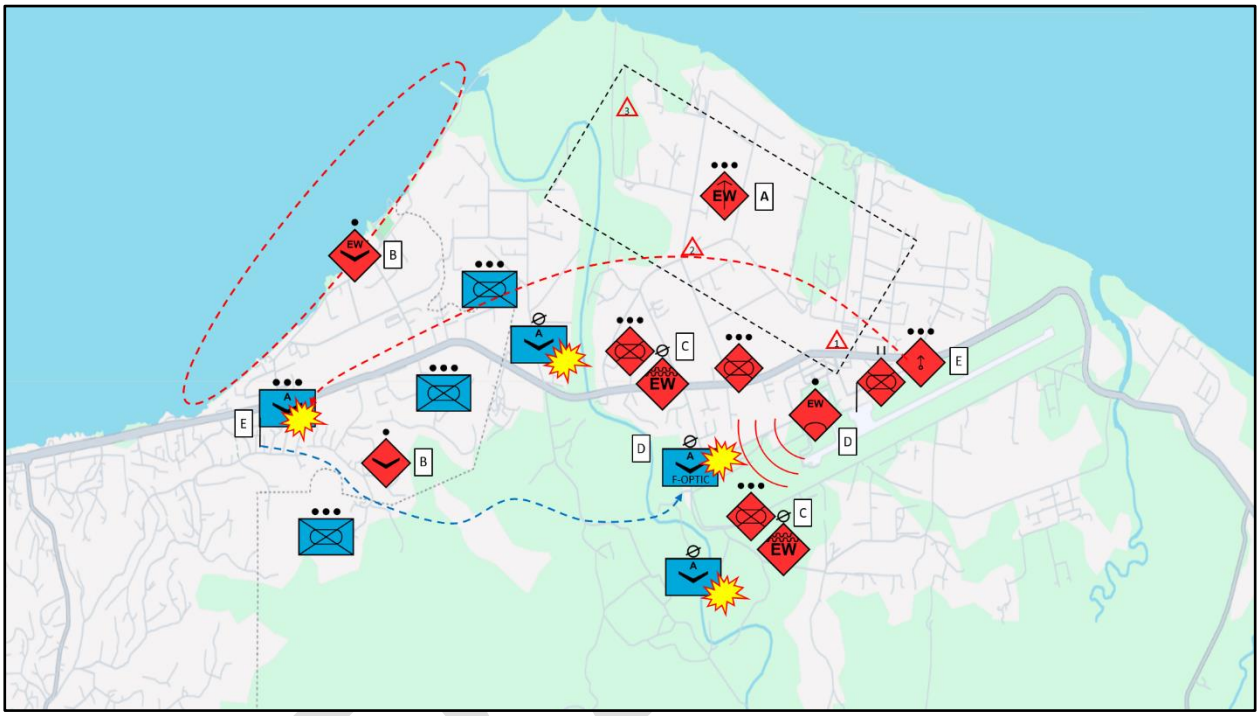
4.15 Olvanan doctrine emphasises the proactive use of EW to enable friendly drone operations while denying similar capabilities to the adversary. This includes EP measures for command links and sensor feeds, frequency hopping, and encryption, ensuring that friendly unmanned assets can operate effectively even within contested electromagnetic environments.

4.16 Counter-drone operations are incorporated into the broader multi-domain battle, reflecting the convergence of cyber, space, and EW domains. While the CA-Bde has a significant EW capability, coverage of an entire frontage is impossible, therefore Olvanan forces train EW operators to recognise emerging UAS threats, rapidly adapt EA profiles, and exploit enemy drone vulnerabilities.

4.17 The advent of large scale use of fibre-optic controlled First Person View (FPV) drones reduces the effectiveness of EW in a counter-drone capacity to zero. However, rather than focus on the drone itself, Olvana focusses on the drone command net, looking for spikes in the EMS consistent with C2 systems, allowing for targeting of both system, through EA, and of the operators through more traditional kinetic strikes.

4.18 At higher echelons, the Air Defence EW Battalion of the Group army fields large High-Power Microwave Weapon Systems (HPM) such as the Hurricane 3000, which leverages high-power microwave energy to disable or destroy drones by targeting their electronic components. These large systems are unlikely to be seen at the tactical level, however, the OPA is continuing to develop more, and smaller directed energy systems in answer to the proliferation of drones across the battlespace. As adversaries increase reliance on unmanned systems, Olvanan mastery of tactical EW against drones becomes a critical factor in maintaining operational superiority.

**Figure 4.5: EW in Counter-Drone Operations**




a. An Olvanan Battalion operating from a captured airfield is protected by a mechanised company. Due to the significant drone threat, the Bn has been augmented by a significant EW capability. A DF platoon is operating in an ops box to the North in an ops box tasked with conducting a baseline analysis of the EMS, and providing early warning for near ground aerial threats.

b. An EW drone operates to the flank searching for C2 nodes, drone launch locations, and troop concentrations, this is augmented by an EO/IR capable drone conducting visual search of likely launch and recovery sites.

c. The forward mechanised platoons have organic C-UAS guns, and an EA vehicle in support. These EA detachments can conduct jamming on likely UAS bands, as well as limited GPS spoofing to reduce the effectiveness of drone navigation systems.

d. A Hurricane-3000 HPM is co-located on the airfield, and is used against any drone swarms, and against fibre-optically controlled FPVs.

e. When the EW UAS, and DF elements detect and locate a likely drone C2 element operating to the rear, the position is engaged with mortars.

## Section 4-13. Vignette 1 - Complex Envelopment

4.19 In Olvanan doctrine, a complex envelopment requires that the commander should attempt to create multiple dilemmas for the enemy commander, attacking from multiple flanks, thus isolating them, and allowing for the defeat of enemy strongpoints in detail. A flank does not need to be physical, and to this end EW provides an additional means to both, understand where the enemy's strengths and weaknesses lie, and to provide an isolation effect at a critical point in the battle; a point that the CA-Bde commander will dictate.

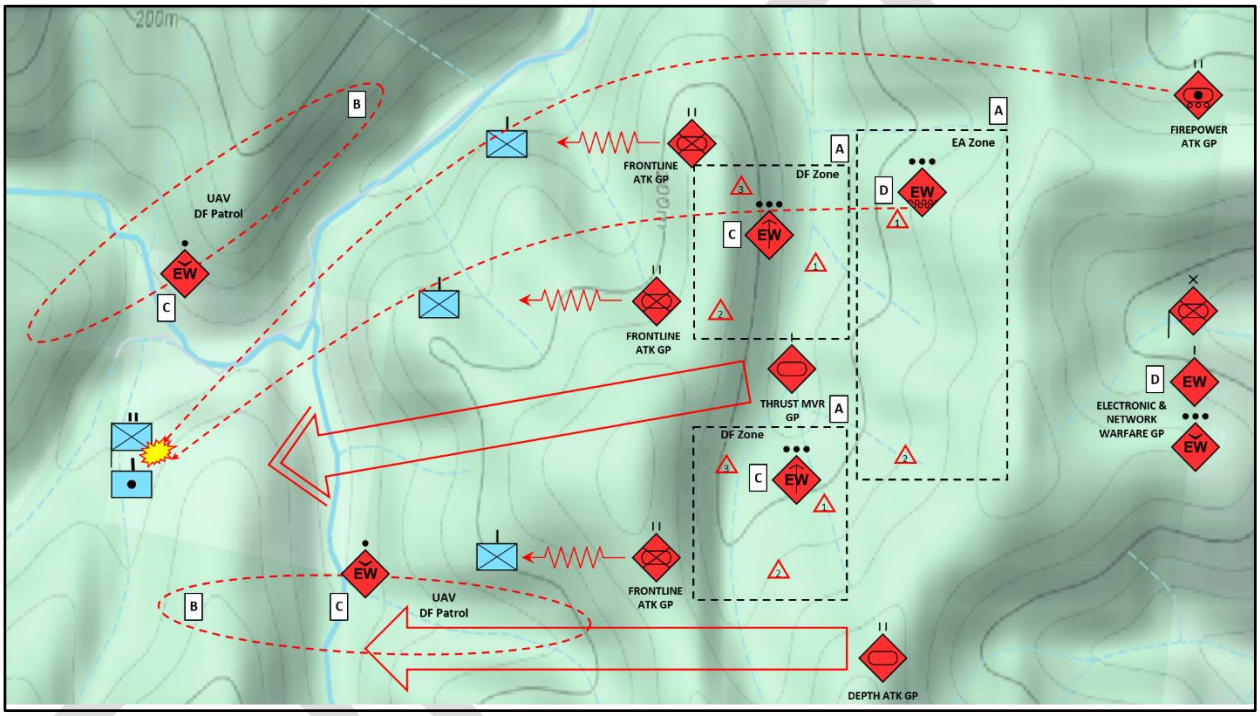
4.20 As this is a critical resource in terms of developing depth, the commander will ensure that each EW element is provided with an appropriate security element, of equivalent size. In this instance, this will require three Infantry Platoons to deploy in support of the two DF Platoons, and the EA Platoon respectively. These protection Platoons will likely come from the Bde reserve.

4.21 The EW Coy HQ and the UAV Pl will be co-located with the CA-Bde HQ in order to expedite information flow, and allow for faster release authority at the decisive point in the battle.

4.22 The three Platoons supporting the Bde manoeuvre plan are allocated zones of operation with the DF Platoons operating to the rear of the Frontline Attack Group. These zones will be terrain dependant, and are chosen in order to attain the best results from the available EW equipment.

4.23 Inside each of the zones, the Platoon will have pre-allocated primary, secondary, and tertiary operating points in order to improve survivability. *It is important to note that while working to the rear of the Frontline Attack Group, all EW elements remain under direct command of the EW Coy commander, and that RELAUTH remains with the CA-Bde COMD.*

**Figure 4.6: EW in the Complex Envelopment**




a. The DF and EA Platoons are allocated their zones of operation, with the DF Platoons conducting a baseline analysis of the EMS, identifying and locating enemy concentrations.

b. The UAV Platoon deploys two platforms. One to the rear of the forward enemy elements, and one in the deep area. These are tasked with providing greater fidelity on the locations of the enemy, identifying key C2 nets, and C2 node locations.

c. All DF Platoons and UAV assets will monitor for spikes in traffic, which may indicate enemy actions such as triggering the deployment of a reserve grouping, delivery of supporting fires and enemy EW effects, and the order to withdraw.

d. The EA Platoon is tasked with jamming enemy C2 and fires nets on command. This is likely to occur as the Depth attack groups conduct their attacks, or at a point when the commander sees an opportunity to further isolate the enemy, such as they commence a withdrawal.

## Section 4-14. Vignette 2 – Advance

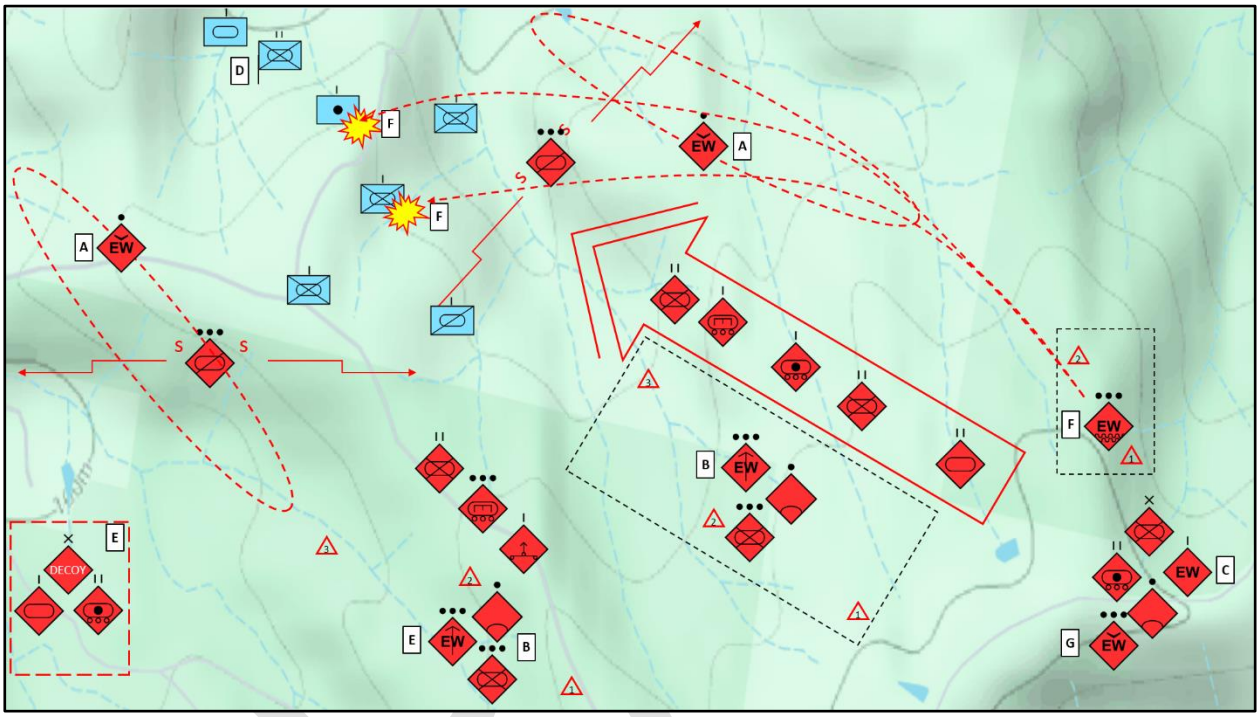
4.24 In the advance, the Olvanan commander will primarily use their EW assets in a passive manner, with the task of augmenting their organic reconnaissance assets to understand the enemy laydown and intent. However, there is a requirement for them to support deception and spoofing operations as a

means of masking and protecting the Bde's movement, and EA will provide both defensive and offensive effects in support of Bde manoeuvre when required

4.25 While the UAV Platoon will fly deep missions over the FEBA, the DF Platoons will move with the forward groupings tasked with understanding the baseline EMS, locating enemy troop concentrations, and gaining fidelity on enemy operational tempo. The EA Platoon will be kept in reserve until required.

4.26 Due to the vulnerability of the high emissions vehicles in the EW Coy, and the fact that they will likely be high priority targets for the enemy, the CA-Bde commander may provide additional protection on top of the normal infantry support, in the form of SPAAG.

**Figure 4.7: EW in the Advance**




a. UAVs fly on the flanks, overlapping with the Bde screen, with priority given to identifying and locating C2 nets and locations, enemy radar positions and artillery fire control nodes.

b. Deployed to the rear of the forward battalions, the DF Platoons will manoeuvre using the leapfrog method in order to maintain constant coverage. Their operational zones will move with them, and they will attempt to use their primary, secondary, and tertiary positions to increase survivability.

c. The EW CP will disseminate the information gained by the DF Platoons to the manoeuvring Battalions in order to provide them with increase situational awareness on likely enemy locations in their manoeuvre corridor.

d. Both the DF and UAV elements will monitor enemy voice and data nets in order to gauge operational tempo, detect command handovers/manoeuvre orders.

e. The DF Platoon may also be tasked with supporting deception operations, and may simulate traffic from larger scale formations, or move to the flanks to stimulate enemy actions in the wrong areas.

f. The EA platoon is kept in reserve and it prepared to initiate jamming of enemy VHF/UHF tactical nets and air defence radar when CA-Bde elements begin to shake out to conduct offensive manoeuvre.

g. The UAV platoon HQ conducts spectrum mapping and prepares transmission of information to CA-Bde HQ. On contact with the enemy, the UAV Platoon will deploy deeper behind the forward line of own troops (FLOT), in order to locate reserves, and any other high value depth targets.

## Section 4-15. Vignette 3 – Positional Defence

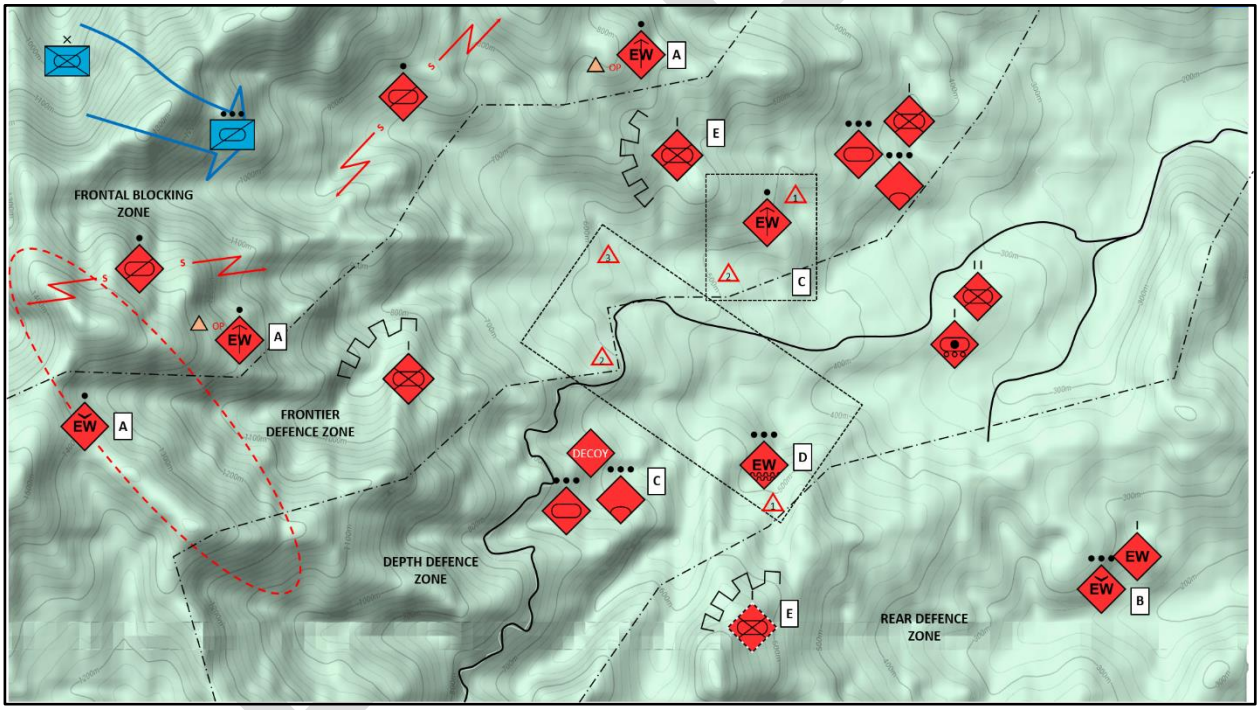
4.27 Olvanan doctrine dictates that prior to conducting a defensive operation, the CA-Bde commander must accomplish a number of key activities:

a. **Organise reconnaissance –** This will require the full integration of both the DF and UAV Platoons into the CA-BDE reconnaissance plan, with a view to understanding two of the three doctrinal Olvanan RFIs of disposition and intent of enemy forces, and the battlefield, specifically the electromagnetic environment. This will also see EW elements forward deployed in observation posts (OPs), in direct support of the Frontal Blocking Zone.

b. **Organise the defensive groupings –** Olvanan doctrine largely dictates that EW elements will operate in support of an element, however they are unlikely to be task organised as a Western military might. To that end, and while the bulk of the EW capability is in support of the cover group in a reconnaissance role, they will largely come under the authority of the CA-Bde HQ, and co-ordinate with the Firepower Strike Group for any EA.

c. **Spoil the Enemy's preparations –** While this phase of defensive preparation is focused on spoiling attacks and firepower assaults, it is unlikely that the CA-Bde commander will unmask their EA capabilities. What is more likely is that the DF Platoons will be used to enhance the Brigade deception plan by simulating the emissions of HQ locations, reserves, and fires elements to waste enemy effort and logistics prior to the defensive battle.

**Figure 4.8: EW in Positional Defence**




a. This Battalion position is the key to the CA-Bde's defence, therefore a UAV squad and a DF Platoon are in support of the recon screen in the Frontal Blocking Zone, with UAS flying on the flank of the likely enemy avenue of approach, and two squads of the DF Pl forward in static OPS.

b. The UAV Pl HQ is co-located with the EW Coy HQ in the Rear Defence Zone, co-ordinating assets in multiple Battalion AOs.

c. In the Frontier Defence zone the remaining DF squad operates from an ops box behind key defensive positions (KDPs), with pre-allocated primary and alternate positions. This supports both the ongoing reconnaissance during the defensive battle, but more importantly, the deception plan.

d. The EA Platoon is located in the Depth Defence Zone, however is enabled with a large Ops box, which encompasses areas in the Frontier Defence Zone. There will be multiple positions to

operate from, and while these will generally in support of the main effort position, they will be chosen in order to best enable support to the entirety of the Frontier Defence Zone if required.

e. As per the Olvanan requirement to wage simultaneous resistance, the EW Platoons will be used in support of both blocking and repositioning actions.

## Section 4-16. Vignette 4 – Situational Attack (Urban)

4.28 Olvanan Urban doctrine states that a situational attack is one launched into an urban area immediately and with limited regrouping. It is mounted when the CA-Bde commander judges that the enemy within the urban objective will be unable to offer effective resistance within the time it will take to secure that objective.

4.29 EW is a key pillar during all four doctrinal stages of this tactic, which include:

a. **Secern –** the conditions for a situational attack are either confirmed or created. Initial assessment is based on technical intelligence systems within the urban area.

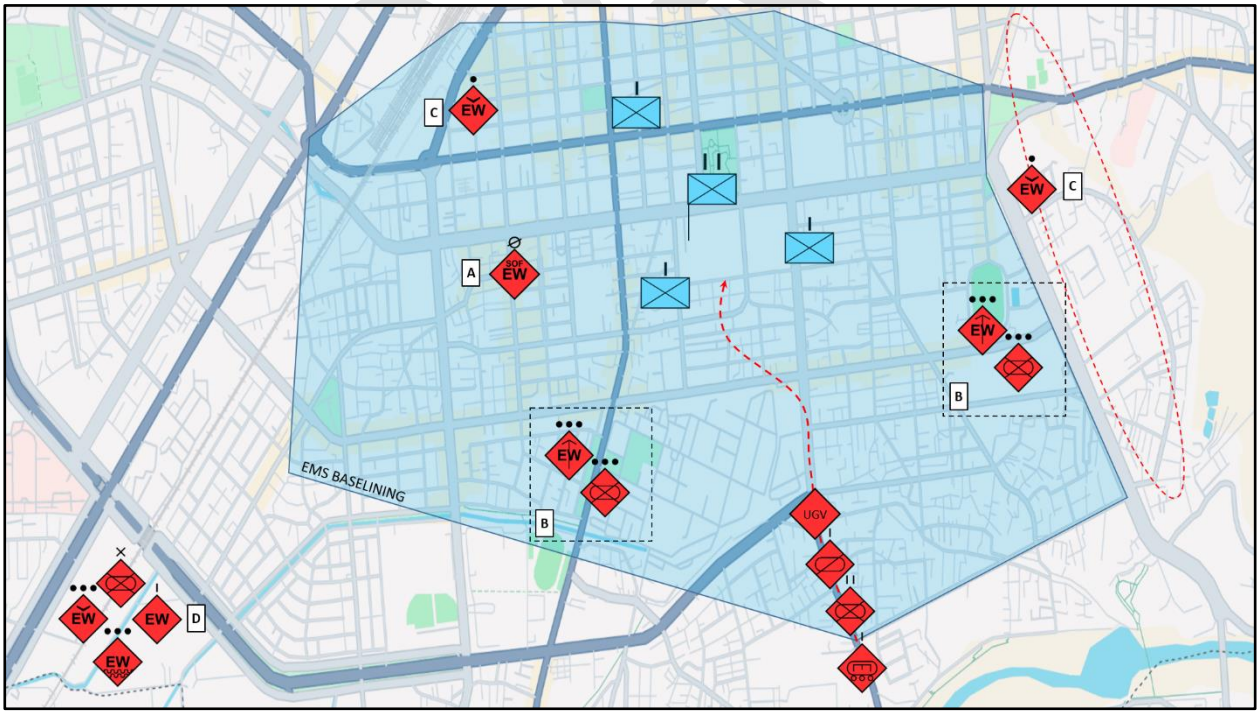
b. **Mask and penetrate –** The key enabler of the Olvanan situational attack is the capability of Olvanan AFV to 'transit' under obscuration.

c. **Seize –** The concept of the situational enclosed attack is to exploit obscuration, speed, and shock and drive right up to, or ram, breach and enter carefully selected objective buildings.

d. **Consolidate –** swift consolidation of key buildings and defensive positions, relying on shock and surprise to reduce the risk of swift counter-attack.

4.30 The EW Company will deploy all available assets in support of this operation, and will be required to liaise with, and fuse information from, special operations and elements from the RISTA Bn.

**Figure 4.9: EW in a Situational Attack (Urban) – Secern Phase**




4.31 **Secern phase -** EMS Baselining: Sensing and Mapping the urban spectrum.

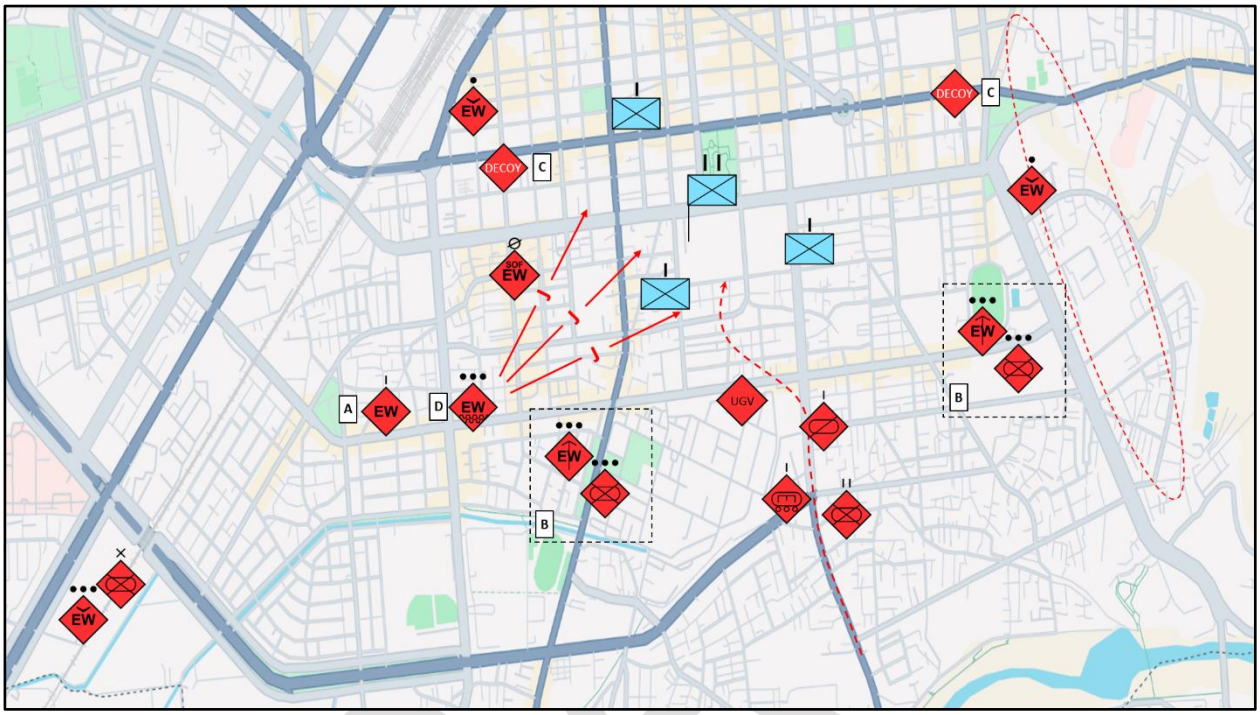
a. SPF EW team infiltrate ahead of the main force providing spectrum mapping, geo-location of key emitters, and can cue precision fires.

b. DF Platoon positioned on the urban fringe focusing on the EMS baseline, with the key task of differentiating military and civilian emitters.

c. EW UAVs overfly the objective & flanks, verifies enemy activity, possible safe lanes, and key enemy concentrations.

d. EW Coy HQ fuses information to provide an EMS baseline, EOB. It also uses enemy traffic to define and locate key C2 nodes, defensive locations, and to identify any uptick in traffic, which may indicate defensive preparations.

**Figure 4.10: EW in a Situational Attack (Urban) – Mask and Penetrate Phase**




4.32 **Mask and penetrate phase –** Obscure CA-Bde's high-speed approach - Cover own signature, blind enemy sensors.

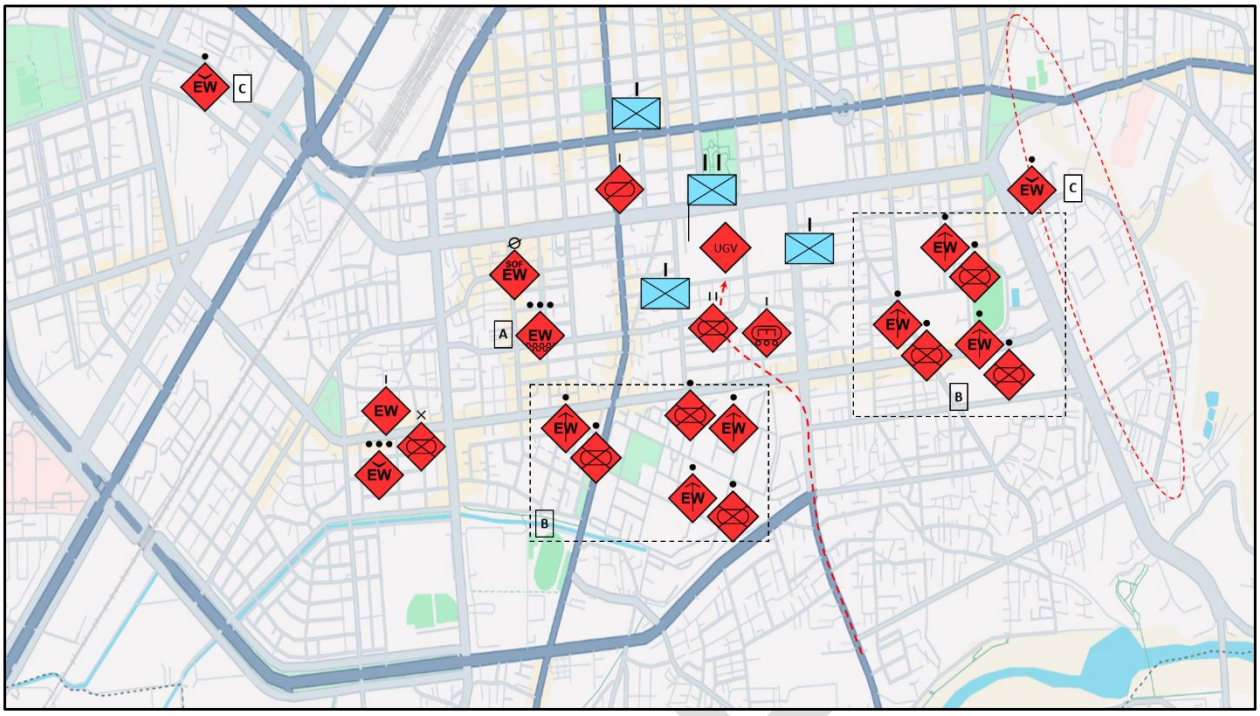
a. EW Coy HQ and EA Platoon push forward into pre-designated locations.

b. DF Platoon, supported by Mechanised elements, dismount and move to pre-identified high points within key buildings to support the wider penetration.

c. Conduct deception actions to focus enemy attention on false break in locations.

d. On command, the EA Platoon conducts pre-planned wide-band barrage spot jamming of fires and C2 nets for 6-10 min.

**Figure 4.11: EW in a Situational Attack (Urban) – Seize Phase**



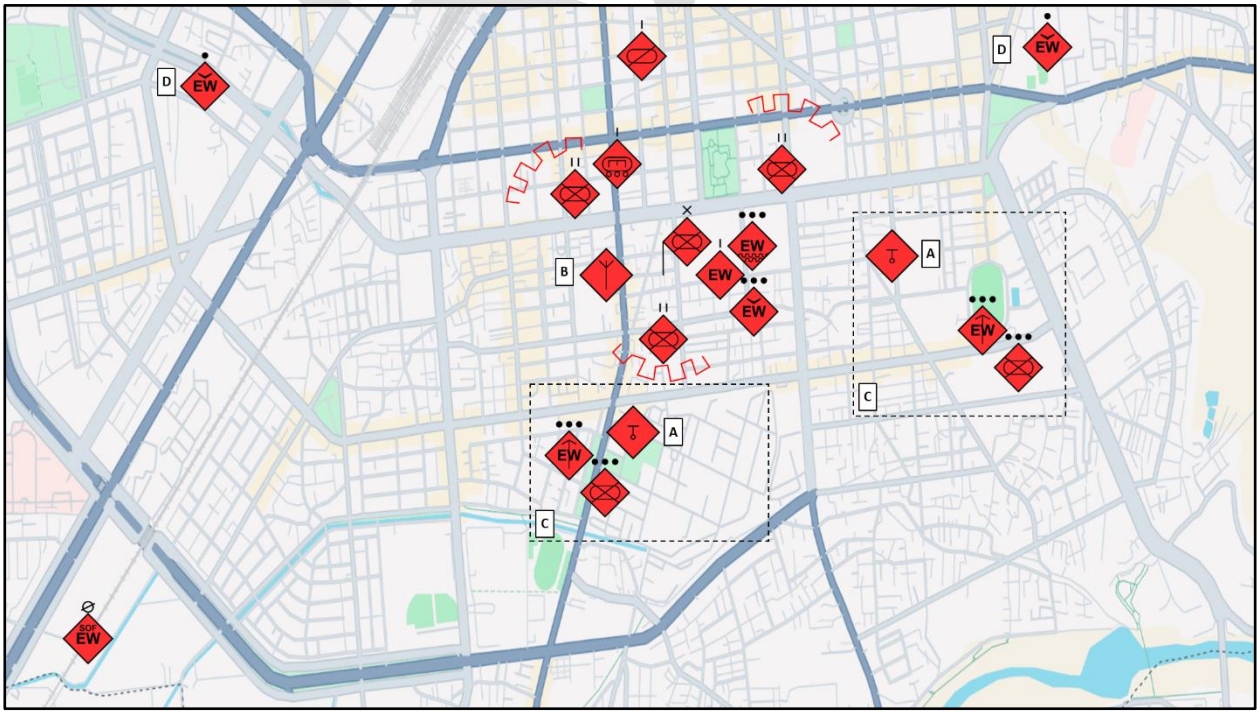

4.33 **Seize phase –** support early warning of enemy counter-attack operations

a. EA Platoon on notice to support main effort elements in the seizure of objective. Possible support to messaging, or penetration of civilian communications networks to broadcast messaging.

b. DF Platoon conducts mounted and dismounted SIGINT support in order to detect changes in levels of enemy traffic identifies further C2 nodes and troop concentrations.

c. UAV Platoon covers urban fringe, and likely reinforcement routes.

**Figure 4.12: EW in a Situational Attack (Urban) – Consolidate Phase**



4.34 **Consolidate phase –** support the setup of CA-Bde defensive preparations and posture, harden communications infrastructure, and enable EP of all supported elements

a. Under EW Coy direction, the Platoons deploy rooftop optical mesh to restore C2.

b. Activate Ku-band micro-SAT uplink for Bde fires nets.

c. Conduct ongoing spectrum monitoring to maintain OPFOR SA and detect potential enemy reconstitution.

d. UAV Platoon maintains coverage of likely reinforcement routes, assembly areas, and form up points.

## Section 4-17. Vignette 5 – Counter-Attack (Jungle)

4.35 The jungle counter-attack is an action that requires a detailed understanding of where the enemy is strongest, and where they are weakest. The commander needs to be able to confidently deliver a 'multi-dimensional penetration' with an appropriately sized force at the point and time of need while dealing with the fog of war, reduced visibility, and poor communications. To that end, having layered and persistent EW surveillance of the battlespace is a key force-multiplier.

4.36 This action is the culmination of the jungle defensive battle, and is conducted at a point in time where the commander believes that the enemy either is strung out too far, or has culminated against the forces resisting in the frontier defence zone.

4.37 While small tactical counter-attacks, and counter-penetration actions will be happening throughout the defensive battle the main counter-attack is co-ordinated by using one or more of the following four distinct phases:

a. **Concentrating fire –** focused on the enemy's strongest element

b. **Sealing off breakthroughs –** plugging any gaps in the line, which may be exploited by the enemy before the counter-attack starts.

c. **Using a multi-domain or multi-directional assault –** counterintuitively frontal assaults are preferred to flanking attacks due to speed of movement.

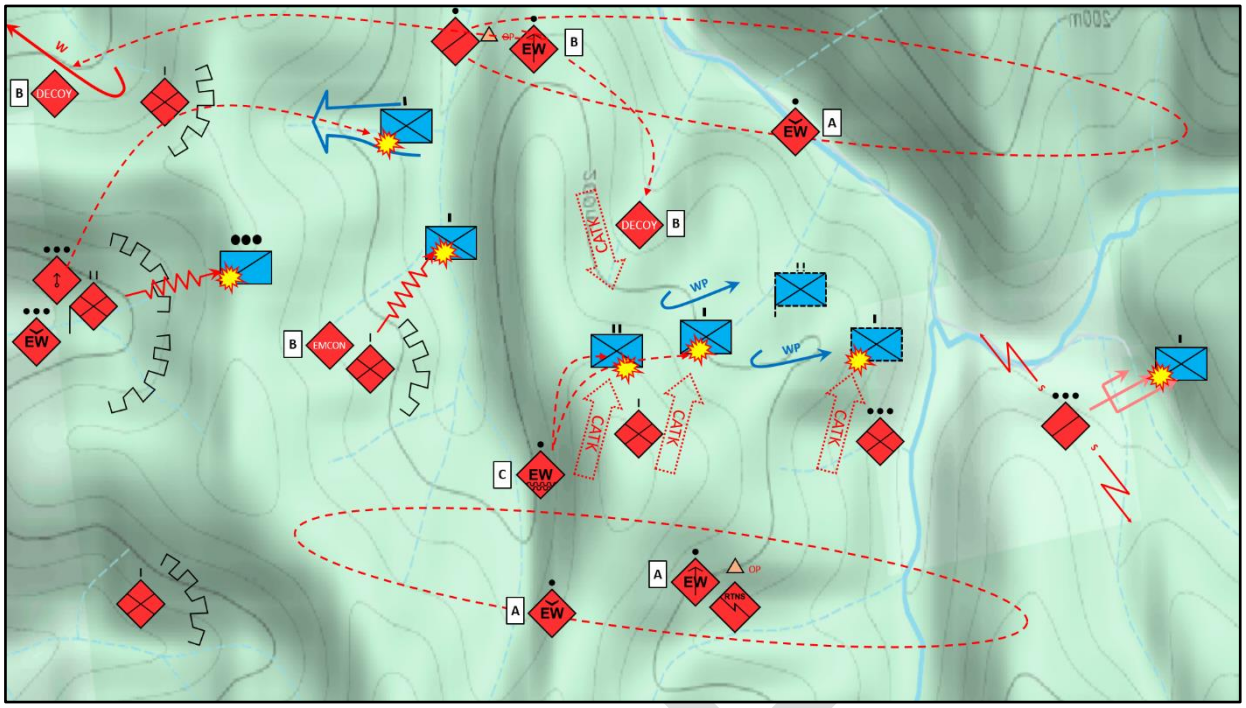
d. **Hold KDPs –** regardless of the success or failure of the counter-attack the KDPs are to be reinforced and held.

4.38 A DF Squad will be attached to a forward deployed SIG Retransmission element. This will enable them to leverage off the integrated security this provides, and will allow for good coverage of the likely enemy avenues of approach.

4.39 While the EW UAV Platoon is co-located with the CA-Bde HQ, their platforms will be pushed as far forward as possible, and on a constant rotation along the flanks of the Frontal Blocking and Forward Defensive zones.

4.40 The EA Squad will be co-located with the Frontline Attack Group in order to provide direct support upon the initiation and conduct of the counter-attack. It is likely that release authority may be delegated to the EW commander; however, this authority will only confirmed as the battle unfolds, and a counter-attack is ordered.

**Figure 4.13: EW in a Counter-Attack (Jungle)**




a. Throughout the battle, the UAV and DF elements provide layered coverage of the battlespace, providing feedback via the EW Coy to the supported commander on the ground. When this information is fused with organic reconnaissance and battlefield commentary, it allows the commander to synchronise the counter-attack in time and space.

b. If assets allow, these elements may also be employed to deceive the enemy commander regarding Olvanan intent through:

(1) Indicating that Olvanan forces are preparing to withdraw, forcing the enemy commander to commit their forces without preparation.

(2) Use EMCON to demonstrate a weak point in the Olvanan lines, whereas it is actually a strongly held or reinforced KDP.

(3) Employ decoy signals to show that the counter-attack is coming from an unexpected flank

c. The EA element will be pushed as far forward as practical, and when the time comes will provide the EW side of the 'multi-dimensional penetration' that Olvanan doctrine requires.

d. Due to power limitations, the EA is likely to be focused on reducing enemy cohesion by attacking C2 networks, and fires networks, particularly of supporting mortar lines.

## Section 4-18. Vignette 6 – Hard-Nut Diversionary Defence (Jungle)

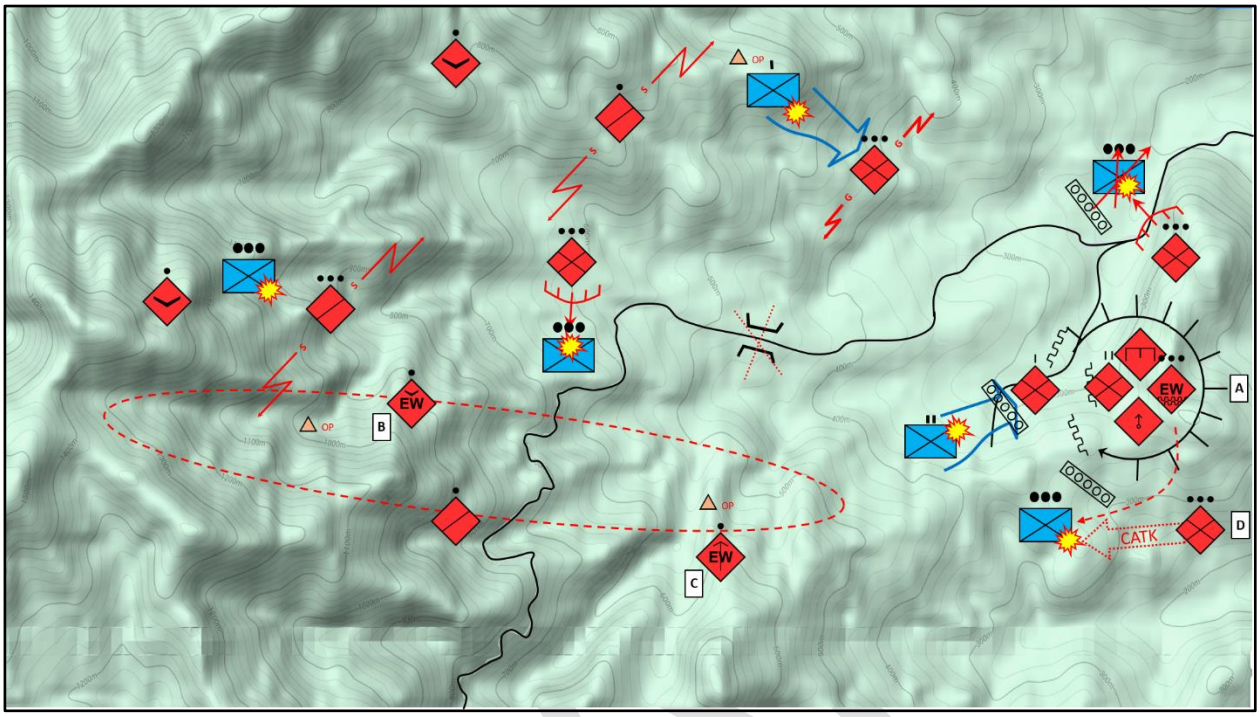
4.41 The hard-nut defence is another jungle specific example, the doctrinal aim of which is: '*to deploy as deep as possible into the enemy's rear, initially without being detected, and to establish a well-situated and suitably fortified defensive position. Once established, the fight is then taken to the enemy through the conduct of aggressive reconnaissance and counter-reconnaissance, well-resourced fighting patrols, demolitions, nuisance mining, artillery raids, any tactic at its disposal in order to pull ever more resources away from the enemy's main effort'.*

4.42 From an EW perspective, as the unit conducting this action will be the best trained, and most politically reliable in the formation, they will not only be augmented a considerable slice of the CA-Bde's EW capability, they **will be delegated release authority** for EA, something which is generally kept at the CA-Bde HQ level.

4.43 While there are questions about the efficacy of ISR drones in a jungle environment, drones with an EW payload are every bit as capable, and will be the mainstay of the reconnaissance support provided to the Bn commander for this tactic.

4.44 It is imperative to remember that for jungle operations the power output of any DF or jamming capability, less UAV, is significantly reduced due to the requirement to man-pack equipment and power. To this end, the distances involved in any EW activity will be dramatically reduced, and will require the deployed elements to be much closer to the enemy.

**Figure 4.14: EW in a Hard-Nut Diversionary Defence (Jungle)**




a. The HQ of the EW element in support of this action will be located with the BN HQ in the KDP, and will provide the commander with as much information on the enemy scheme of manoeuvre as possible.

b. On establishment of the hard nut, EW UAS are pushed forward early. These will remain on station over likely enemy avenues of approach for as long as possible.

c. The ground based DF element will be pushed forward into an OP on the most likely avenue of approach, and will be tasked with passive collection, and with deception tasks in order to waste enemy combat power attacking dummy positions.

d. Due to the issues with power and range, the EA element will only be used in support of any localised counter-attack. Release authority is delegated to the local commander, and the commander of the EW element will provide advice on the most appropriate time to utilise the EW capabilities under their command

# Chapter 5
# Electronic Warfare Support to Deception Operations

5.1 The EW Company plays a critical role in providing deception capabilities that enable the CA-Bde commander to manipulate the enemy's perception of the battlefield. By leveraging sophisticated electronic deception techniques, the EW Company can create false electromagnetic signatures, simulate fictitious force deployments, and disrupt enemy reconnaissance and targeting systems. These deception activities reduce the enemy's situational awareness and degrade the accuracy and timeliness of their decision-making processes.

5.2 Central to this deception role is the ability to generate controlled and credible false signals that mimic authentic Olvanan communications and sensor emissions. This includes creating phantom radio networks, spoofing GPS signals to mislead enemy navigation and targeting, and fabricating radar or sensor returns that suggest non-existent troop or vehicle formations. In doing so, the EW Company can mask the true disposition and movement of CA-Bde's units, increasing operational security (OPSEC), and enabling surprise.

5.3 The EW Company's deception function is closely coordinated with the CA-Bde's overall operational plan and intelligence efforts. Through integration with the brigade's ISR assets, the EW Company identifies key enemy ISR and targeting nodes vulnerable to deception. The company then tailors its electronic deception effects to exploit these vulnerabilities, aligning with the broader brigade-level scheme of manoeuvre and objectives.

5.4 In dynamic combat environments, the EW Company continuously adapts its deception tactics in response to enemy countermeasures. Using advanced electronic counter-countermeasure (ECCM) techniques, the company can modify signal characteristics, frequencies, and emission patterns in real-time to maintain the credibility of false signals. This agility helps sustain the effectiveness of deception throughout prolonged operations, continually pre-empting and wrong-footing the enemy decision cycle.

5.5 The EW Company supports deception not only through electronic means but also by coordinating with cyber and psychological operations (PSYOPS) elements from higher echelons. Combining electronic deception with cyber intrusions and targeted information campaigns, the CA-Bde can create multi-domain effects that compound confusion and misdirection within enemy ranks. This holistic approach to deception enhances the CA-Bde commander's ability to shape the electromagnetic environment to maintain the tactical advantage.

## Section 5-19. EW Company Deception Tasks for CA-Bde Commander

a. **Phantom Signal Generation:** Create simulated radio traffic and communications networks to suggest false unit locations and movements.

b. **GPS Spoofing:** Emit counterfeit GPS signals to disrupt enemy navigation and targeting accuracy.

c. **Radar and Sensor Decoys:** Fabricate false radar returns and sensor emissions to mimic non-existent troop formations or vehicles.

d. **Emission Control and Masking**: Manipulate and reduce emissions to conceal true force posture while presenting deceptive signatures.

e. **Vulnerability Targeting:** Identify enemy ISR and targeting nodes for focused deception efforts.

f. **Adaptive Signal Modification:** Employ ECCM techniques to adjust deception signals dynamically in response to enemy counter-EW activities.

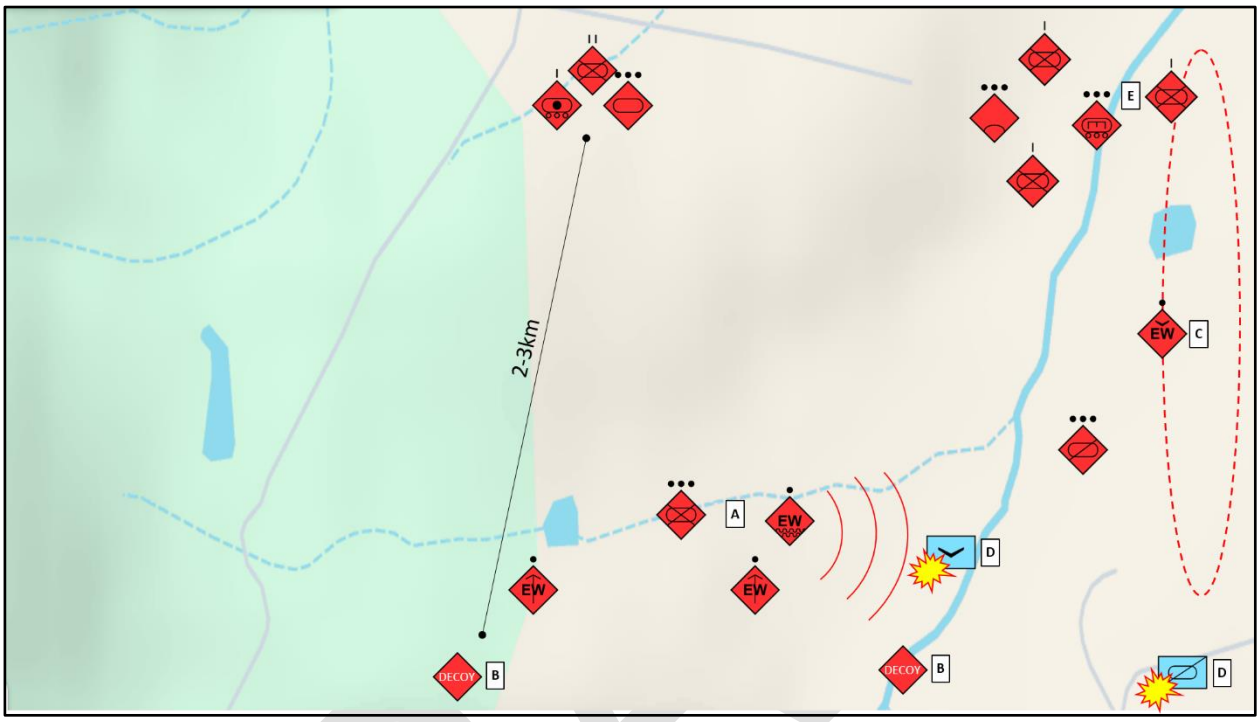
g. **Coordination with ISR and Cyber Units:** Align deception with intelligence gathering and cyber operations for synchronised multi-domain effects.

h. **Support to Psychological Operations:** Integrate electronic deception with PSYOPS to amplify enemy confusion and disrupt morale.

i. **Operational Security Enhancement:** Use deception to reduce enemy targeting accuracy and protect CA-Bde manoeuvre elements.

j. **Continuous Monitoring and Feedback:** Assess deception effectiveness via real-time SIGINT and ELINT, adjusting tactics as necessary.

**Figure 5.1: Phantom Battalion Manoeuvre in a River Crossing Operation**




## Section 5-20. Tactical Example 1: Phantom Battalion Manoeuvre in a River Crossing Operation

a. During a planned river crossing, an Olvanan Bn commander aims to conceal the true location and timing of the main crossing point. Supported by a security force, they push their attached EW elements between 2 and 3km to the south.

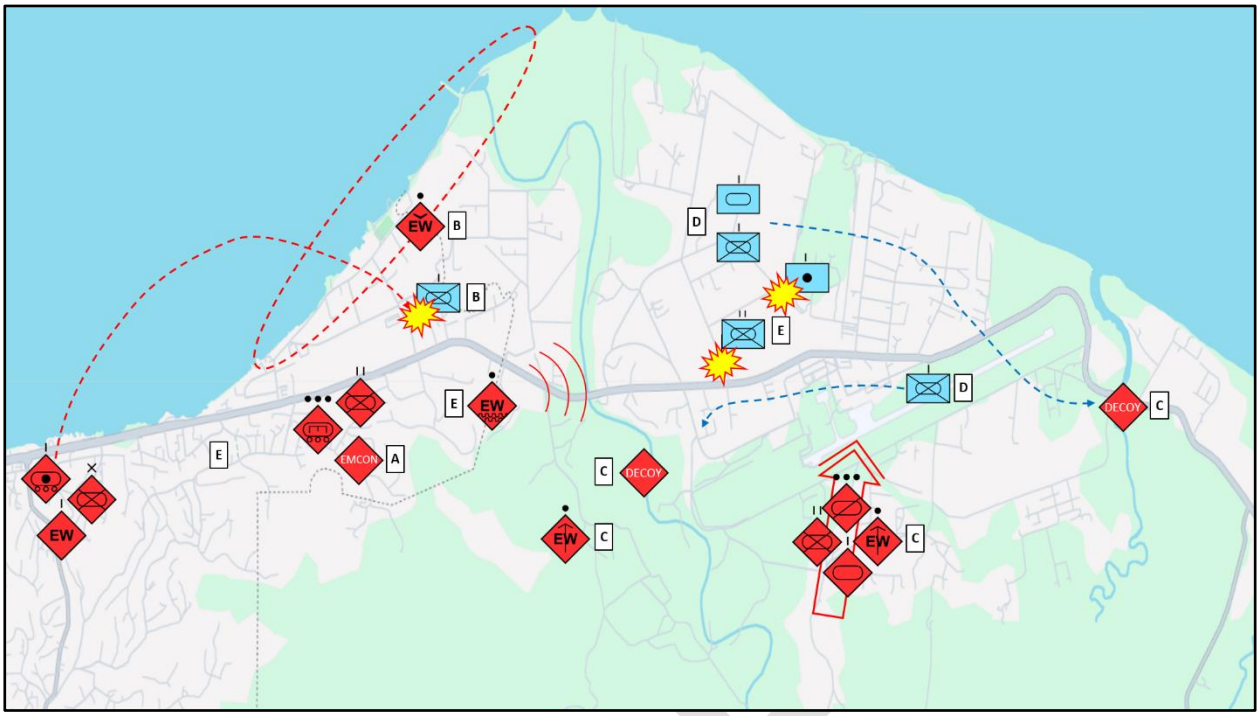
b. Two key decoy locations are emulated using software defined radios to generate traffic consistent with a full battalion's command net, engineer nets and SHORAD.

c. EW UAS provide an EMS soak on the far bank, and cue the EW elms in the south to approaching enemy UAS, and recon elements.

d. EW elms spoof the GPS signal which puts the enemy UAS and recon elms a further 3km north of their actual location, forcing them to turn further south to try and intercept the decoy Bn river crossing.

e. This provides additional time for the real crossing to take place., and the multi-layered approach delays enemy artillery and air strikes, allowing the CA-Bde's real crossing to proceed with minimal interference.

**Figure 5.2: Urban Assault Masking with EMCON and Decoys**




## Section 5-21. Tactical Example 2: Urban Assault Masking with EMCON and Decoys

a. In preparation for an urban assault, the EW Company works with the CA-Bde's intelligence and manoeuvre units to mask the brigade's true approach routes, by reducing electronic emissions from forward units through EMCON procedures.

b. EW UAS provide EMS overwatch from the flank, identifying C2 and fires nets, and geo-locating the western enemy positions.

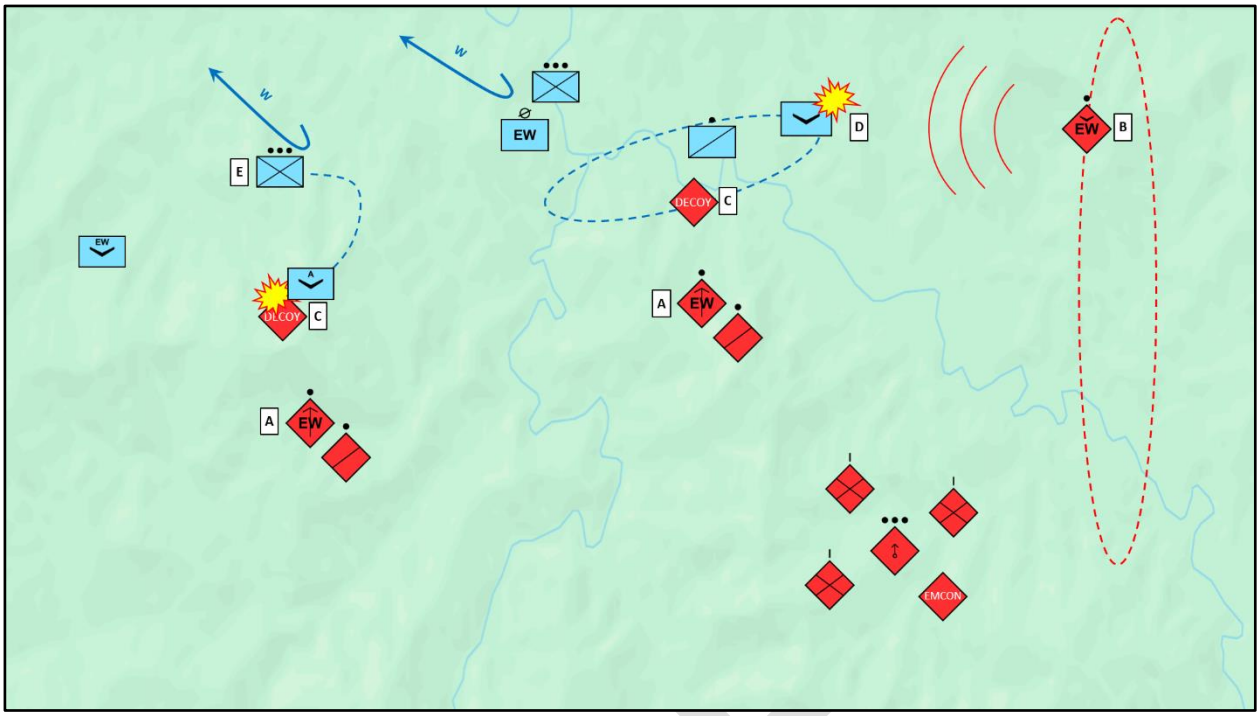
c. Two EW squads broadcast signals from decoy locations, simulating radio chatter and sensor emissions from multiple false, put possible, and entry points around the city's perimeter. The one to the east consistent with an armoured force supported by Engineers.

d. The enemy diverts reserves and surveillance assets to counter these perceived threats, thinning their defences at the actual point of attack.

e. At this key point in the battle the EA squad jams both the C2 and fires nets, as the CA-Bde's fires engage those forces identified on the Western. This enables the the seizure of the Airfield, and the western approaches.

f. The EW Company adapts these signals in real-time to maintain credibility despite enemy attempts to detect deception.

**Figure 5.3: Counter-ISR Deception in Jungle Warfare**




## Section 5-22. Tactical Example 3: Counter-ISR Deception in Jungle Warfare

a. Operating in dense jungle terrain, an Olvanan Bn faces enemy force heavily reliant on electronic reconnaissance and UAV surveillance. Attached EW dismounted EW elms are attached to recon patrols, and are pushed forward

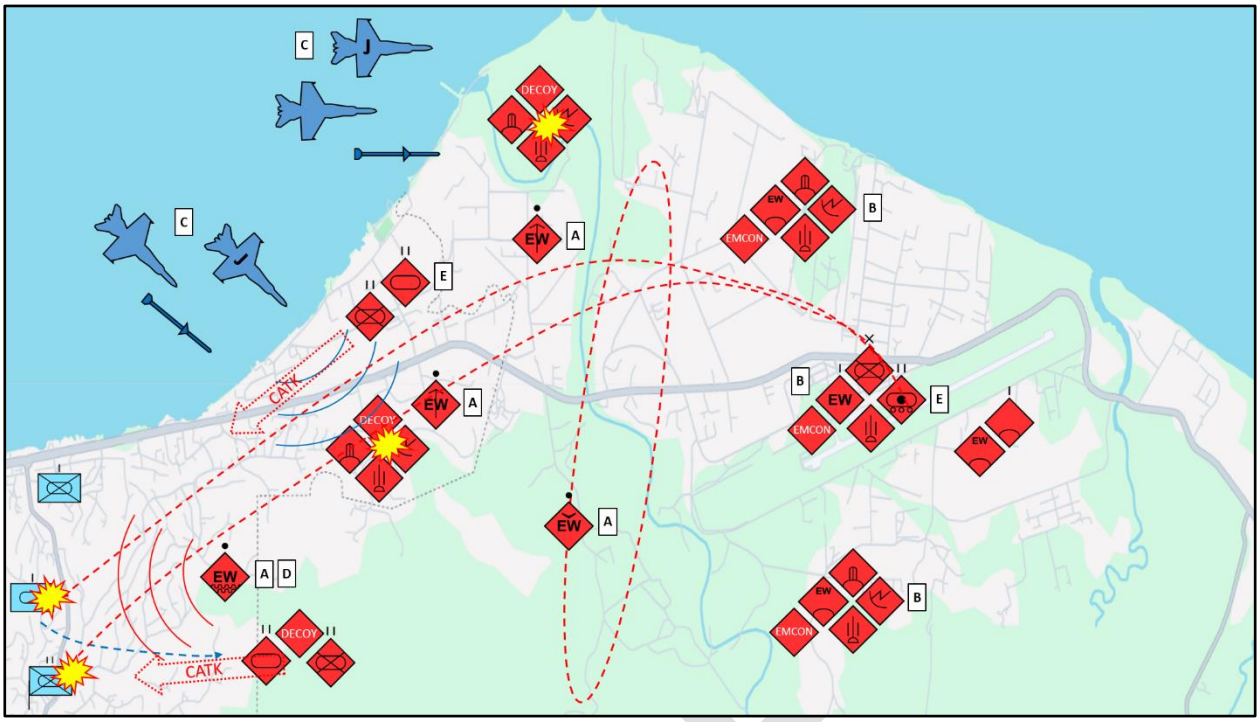
b. An EW UAV is launched to operate on the eastern flank out of visual and audiao range of likely enemy forces. This has been configured with a jamming pod.

c. The ground EW elms simulate appropriate traffic for two Battalion sized forces, with scheduled traffic back to a higher formation, as well as a fires net.

d. The enemy element not only utilises both its ground and aerial EW assets, but pushes recon elms forward with UAS in support. The Olvanan EW UAS is used to jam the controls of the enemy UAS, blinding them of visual confirmation. This then returns to base in order to avoid interdiction.

e. An enemy platoon attempts to engage one of the positions with an FPV, and the Olvanan EW operators increase the simulated communications to reflect the attack. However, without the ability to visually confirm the strike, and faced with contradictory signals indicating a much larger force than they are capable of dealing with, the enemy forces withdraw. This confusion enables Olvanan manoeuvre elements to exploit jungle cover for surprise flanking manoeuvres with reduced risk of interdiction.

**Figure 5.4: Electronic Deception in Defensive Operations against Airborne Threats**




## Section 5-23. Tactical Example 4: Electronic Deception in Defensive Operations against Airborne Threats

a. Facing an enemy supported by a significant air capability, the CA-Bde needs to deploy deception measures which limits the efficacy of this threat. As Engineers construct dummy positions, EW elms are pushed forward in support to establish an electronic pattern of life consistent with medium range SAM batteries. A further unit is sent to the South to simulate a reserve formation on a possible avenue of approach, and the EW UAS is deployed to gather information on the EOB, and geolocate enemy C2 nodes.

b. All Olvanan units, including the actual SAM batteries are put under strict EMCON conditions, this is co-ordinated by the EW Coy HQ, in conjunction with the Gp Army AD Bn.

c. The enemy undertakes multiple SEAD sorties against the decoy positions, wasting valuable ordnance, and flight hours for no result, with the actual SAM protection of the Air field left intact and operational..

d. The EW elm in the south begins simulating traffic, which forces the deployment of the enemy reserves, and spiking traffic on their C2 nets.

e. As the EW element jams the enemy C2 nets, the information gained by the EW UAS on enemy locations and dispositions is utilised to co-ordinate a fires, and the real deployment of the CA-Bde's reserves.

# Chapter 6
# Electronic Warfare TTPs

## Section 6-24. Fibre Optic Linking Procedure

6.1 In order to remain undetected by enemy sensors, the Olvanan EW Platoon avoids using radios and instead links vehicles using rugged, armoured fibre optic cable. This allows for fast, secure communication while keeping the unit's electronic signature extremely low.

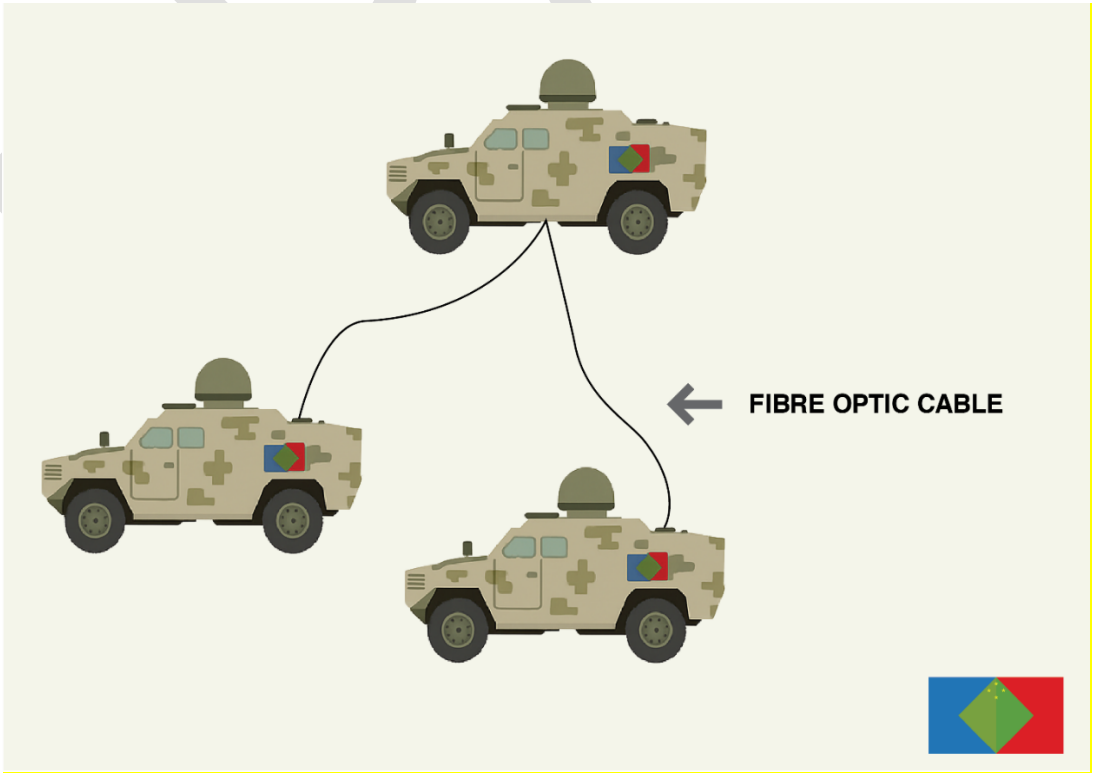
6.2 To link two or three vehicles quickly and quietly, the team lays a short length of fibre optic cable. After a quick walk-through of the area to avoid vehicle tracks, hot exhaust paths, or sharp rocks, a two-person cable team begins to unroll the fibre from a shoulder-mounted reel. As they move, they clip the cable low to the ground or hide it in shallow scrapes for camouflage. Care is taken to keep the cable gently curved with no sharp bends. A little slack is left at each vehicle so they can move slightly without damaging the cable.

6.3 Once the cable is in place, a technician checks the link by measuring the light level or sending a quick signal (called a "ping"). Once everything is working, the commander confirms that the link is live.

6.4 While the link is active vehicles must not move beyond the cable’s slack, and crew members must keep watch for anything that could pinch, cut, or melt the cable. When it is time to move again, the commander orders the disconnection and retrieval of the link. At this point all movement stops, the connectors are unplugged and capped, the cable is rolled up onto the reel and is wiped clean, checked for damage, and packed away

6.5 **Tactical Advantage of Fibre:** Because fibre optic cable gives off no radio energy, the entire vehicle cluster stays virtually invisible to enemy detection systems. All vehicles operate in a passive-collect mode — they listen for enemy signals but do not transmit anything themselves.

**Figure 6.1: Fibre-optic Linking Procedure**



6.6 As all collected data is sent through the fibre, this keeps the unit's position undetected, even when near enemy forces. There is a much lower risk of interception or geolocation, and the system is resistant to jamming.

6.7 The absence of radio links means that the EW node can sit closer to targets, that large amounts of raw signal and telemetry data can be moved securely, and that there is no lingering RF signal after the cable is removed

6.8 If a connection to the EW Command Post is needed, it can be made using a long fibre run to a remote antenna, or via scheduled radio communication bursts, keeping exposure to a minimum. This method gives the Olvanan EW Platoon a fast, secure way to stay hidden while sharing large amounts of data in hostile environments.

## Section 6-25. Tethered UAS Procedure

6.9 To create a reliable and low profile communication link between a forward vehicle cluster and the rear EW Command Post (CP), a tethered UAS can be launched from the platoon HQ vehicle. This is done in four steps

6.10 **Step 1: Site Survey and Setup -** before launch, the crew checks the area for overhead obstacles and ensures there is no direct line-of-sight for enemy observers. They then unroll a tough power and data cable that connects the drone to the vehicle. This cable powers the drone and allows two-way communication directly with the vehicle's radios.

6.11 **Step 2: Launch and Operation -** the UAS is launched and climbs to a height of 120–150 metres. This is high enough to get over terrain but still low enough to avoid most enemy radar. Once in position, it enters "kite" mode (a GPS-assisted hover), after which the operator switches on the on-board relay: a small software-defined radio which can rebroadcast VHF, UHF, or cellular signals toward the rear EW CP.

6.12 Because the connection from the shelter to the drone is through the cable (not wireless), there is no radio signal at ground level. The only radio signal comes from the drone's antenna high in the air, which can be adjusted to use the lowest possible power. The signal travels in a narrow vertical cone, making it very hard for enemies to detect from the sides.

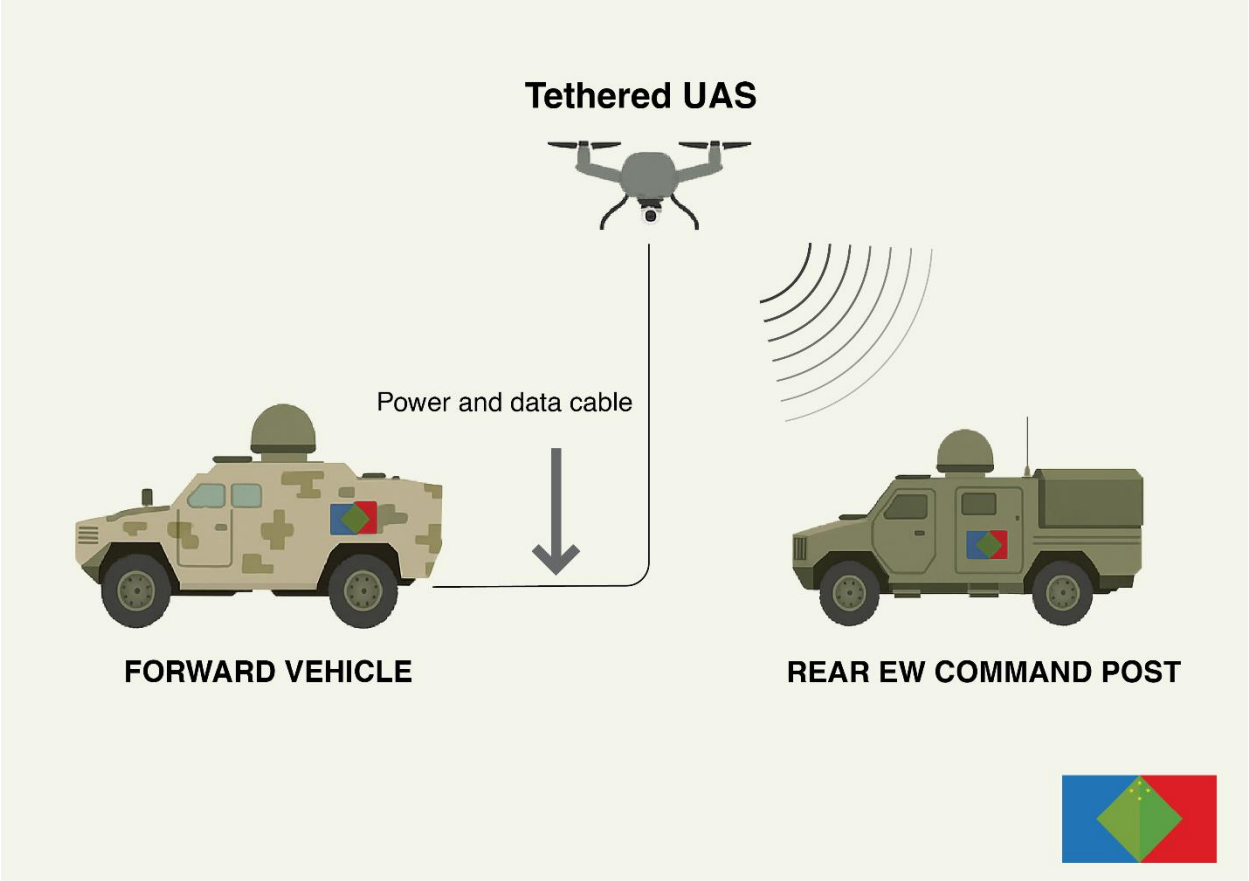
6.13 **Step 3: Safe Operation During Missions -**while active, the forward node remains radio-silent except for the UAS with the drone's signal pointing downward at a tight angle, helping to avoid detection or tracking. Wind and weather are constantly monitored (maximum safe gusts are ≤ 35 knots), and the vehicle must not move more than one metre without checking with the UAS operator.

6.14 If the team detects interference or jamming, then transmit power is shut off immediately, and the drone auto-descends to 30 metres using battery power. The plan is then adjusted to avoid the threat.

6.15 **Step 4: Recovery -** to pack up, the call "UAS retrieve" is given, and the drone lands safely back on its pad. The cable is reeled in carefully to prevent twists, with the entire system shut down and stowed in under six minutes.

6.16 **Tactical Advantage of the Tethered UAS**: This system allows the Olvanan EW Platoon to open a secure voice and data path to higher command without revealing their location. Because the uplink is controlled and focused, and there is no local radio signal on the ground, enemy forces find it very difficult to detect or geo-locate the team. The result is a low-risk method to stay connected while remaining hidden in a contested electromagnetic environment

**Figure 6.2: Tethered UAS Procedure**




## Section 6-26. Terrain Shielding during Electronic Attack

6.17 To carry out an effective electronic attack without revealing their position, the Olvanan EW Platoon uses the terrain to shield their jamming equipment from enemy detection.

6.18 **Step 1: Choose a Concealed Jamming Position –** the jamming vehicles are placed on the reverse slope of a hill or behind a tree-covered ridge, the goal is to stay hidden from enemy direction-finding systems while still maintaining a clear electronic line-of-sight to the enemy transmitter (the target).

6.19 **Before deployment -** a quick line-of-sight and RF sweep is carried out. This checks terrain profiles, antenna beam angles, and ensures there is a clear path to the target emitter. The jammer is then driven into position, usually onto a shelf just below the ridge, and the antenna is pointed through a gap or saddle in the terrain, enabling coverage of the assessed enemy transmitter. Transmit power is kept as low as possible, just enough to affect the enemy signal without drawing extra attention.

6.20 **Step 2: Set Up for Low Visibility -** all jamming vehicles remain engine-off during operation, and crews use cabled or shielded control lines to run the jammer remotely from a small control point at least 50 metres downslope. This reduces the chance of the enemy focusing fire or sensors on the main vehicle. A spotter team stays hidden near the ridge or crest, using handheld spectrum monitors to check that the jammer is working

6.21 **Step 3: End of Mission and Withdrawal -** once jamming is complete the antenna is collapsed and all RF transmissions are stopped immediately. The crew then withdraws under terrain cover, using a route that was scouted in advance

6.22 **Tactical Advantage of Terrain-Shielded Jamming:** By carefully using the landscape for cover, the Olvanan EW Platoon can launch focused jamming attacks without being easily detected or targeted, staying mobile with the ability to pack up quickly.

6.23 This method offers high effectiveness with low risk, making it ideal for operations in contested areas where stealth and survivability are critical.

**Figure 6.3: Terrain Shielding**

## Section 6-27. Leapfrog

6.24 To maintain continuous EW coverage while staying mobile and hard to detect, the EW Platoon uses a leapfrog method. This allows one vehicle to operate while others move forward in silence, creating a rolling chain of continuous support.

6.25 **Step 1: Role Assignment and Initial Deployment -** the detachment begins by assigning roles, with one Holding Vehicle (HV), and one or two Advance Vehicles (AVs) – depending on the unit composition

6.26 The HV sets up first, raisings its mast, and begins its allocated EW task. While the HV is active the AVs stay in receive-only mode (EMCON), moving forward a tactical bound along pre-planned, reconnoitred routes to the next pre-allocated position, EG. a ridge or terrain feature that provides cover

6.27 **Step 2: Advance Vehicle Setup -** once each AV reaches its new location the crew performs a 90-second “hot-start” drill, antennas are raised and passive system checks are run. GPS time is synced with all radios RF silent (no transmitting). When the senior EW Officer confirms the AVs are ready, he gives the command “Hand-over hot.”

6.28 **Step 3: Handover and Role Switch –** on receipt of this order the HV counts down and discontinues its task. A quick snapshot of the radio spectrum is sent from the HV to the AVs using a short radio burst, and one AV immediately takes over, going live and taking over as the main task element. The original HV then powers down, lowers its mast, and begins moving silently past the new hold position, preparing for the next leap

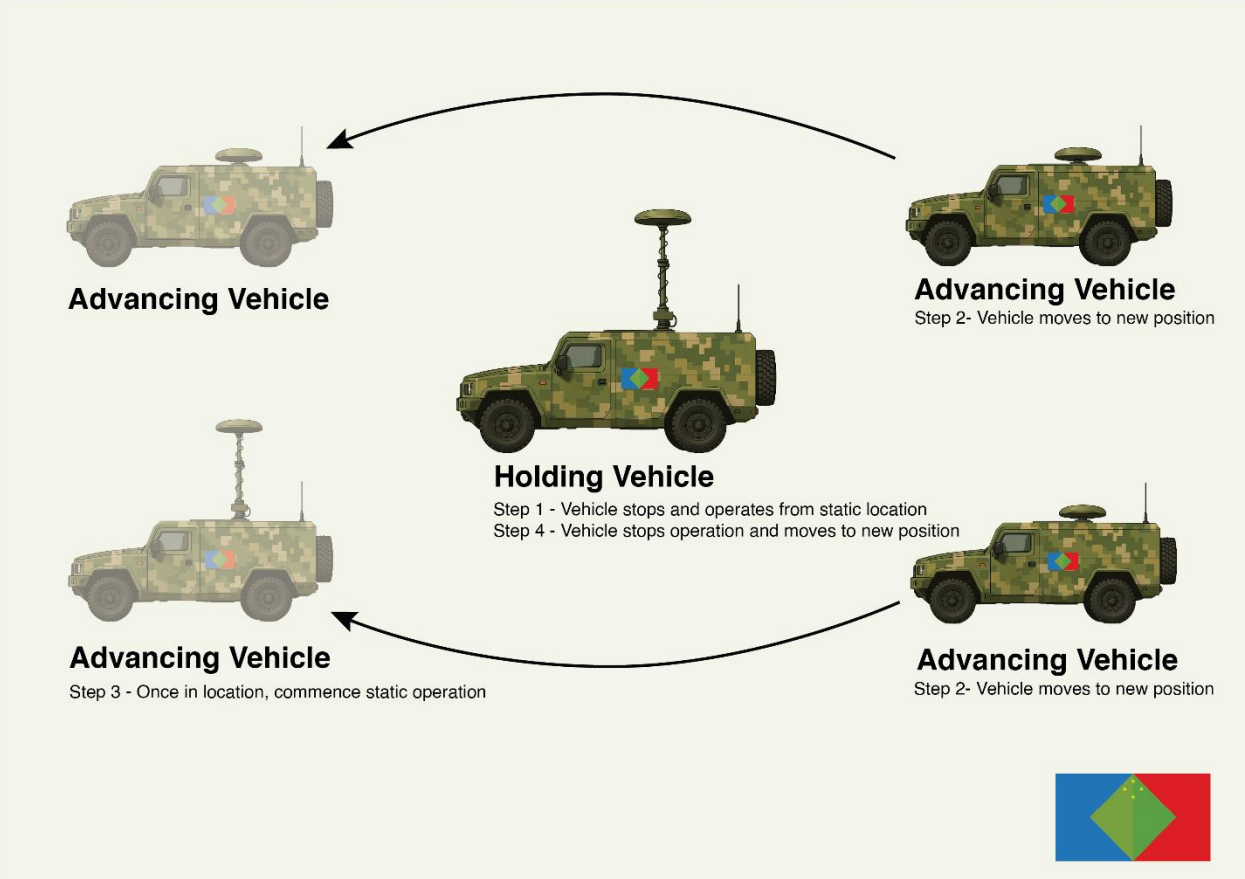
6.29 **Step 4: Maintaining Coverage and Reacting to Threats -** the Platoon conducts this procedure every 30 minutes, keeping coverage continuous and overlapping, with each handover including a five-second gap on a spare frequency to check for enemy counter-attacks or fake signals or spoofing.

6.30 If jamming becomes less effective or enemy threat levels rise, the commander can order a “double-barrage”, with both AVs going live for 30 seconds to flood the enemy’s frequency range, then one AV drops back to silent movement again. All power levels, antenna direction, and mast heights are recorded on a shared digital whiteboard. This helps all teams stay updated and avoid interference with friendly signals.

6.31 **Step 5: End of Mission -** the leapfrog process continues until the force reaches its final objective, or until the team is ordered to switch to an alternative tasking

6.32 **Tactical Advantage of the Leapfrog Method:** This “one-foot down” approach keeps at least one system active at all times while the rest of the team stays on the move. It provides constant EW pressure on enemy systems, reduces risk of detection, and by rotating roles and using terrain smartly, the Olvanan EW Platoon can dominate the spectrum without exposing its location for long.

**Figure 6.4: Leapfrog**




## Section 6-28. UAS direction finding

6.33 To locate enemy signal sources without putting ground vehicles at risk, the EW UAS Platoon uses a small, hand-launched UAS equipped with direction-finding sensors.

6.34 **Step 1: Preparation and Launch -** the EW vehicle parks under cover, powers down its own transmitters, and connects a battery to the UAS payload. The UAS operator uploads a pre-programmed racetrack flight path, designed to orbit 3–5 km away from suspected enemy emitters on a flank. The flight plan will dictate the maximum altitude, duration of the flight legs, the safe return route, and the landing location (this will be different to the launch location).

6.35 A two-person launch crew completes a 60-second start-up checklist which includes, GPS lock, inertial navigation alignment, spectrum sensor self-test, and an encrypted datalink check. The UAS is then launched into the wind from a clear, open area.

6.36 **Step 2: Direction-Finding in Flight -** once airborne, the UAS enters receive-only EMCON mode (no transmissions), and begins collecting bearing data on enemy signals, recording time and direction of arrival. As it follows its route, the UAS uses its on-board software to calculate where signal lines intersect, and when bearings from multiple waypoints match closely (within 100 m), the UAS automatically marks a “FIRM FIX” on the tactical map and sends a brief data burst to the ground operator.The operator can then instruct the UAS to focus on a certain area, or allow it to continue its pre-planned scan.

6.37 **Step 3: Threat Reaction and Recovery -** if the UAS detects hostile radar activity or its battery drops to a pre-determined level the operator initiates “HOME RECALL”, at which point the UAS climbs to maximum ceiling, aligns its directional antenna at the EW truck and sends a high-speed burst of data.

6.38 The UAS then goes silent again (EMCON), flying a deceptive return route to avoid enemy tracking, and performs a GPS-guided belly landing within 200 m of the EW vehicle at the alternate landing site.

6.39 After recovery -the crew removes the memory card and downloads available data sets, wipes the temporary memory, and resets all data to prevent information loss if captured.

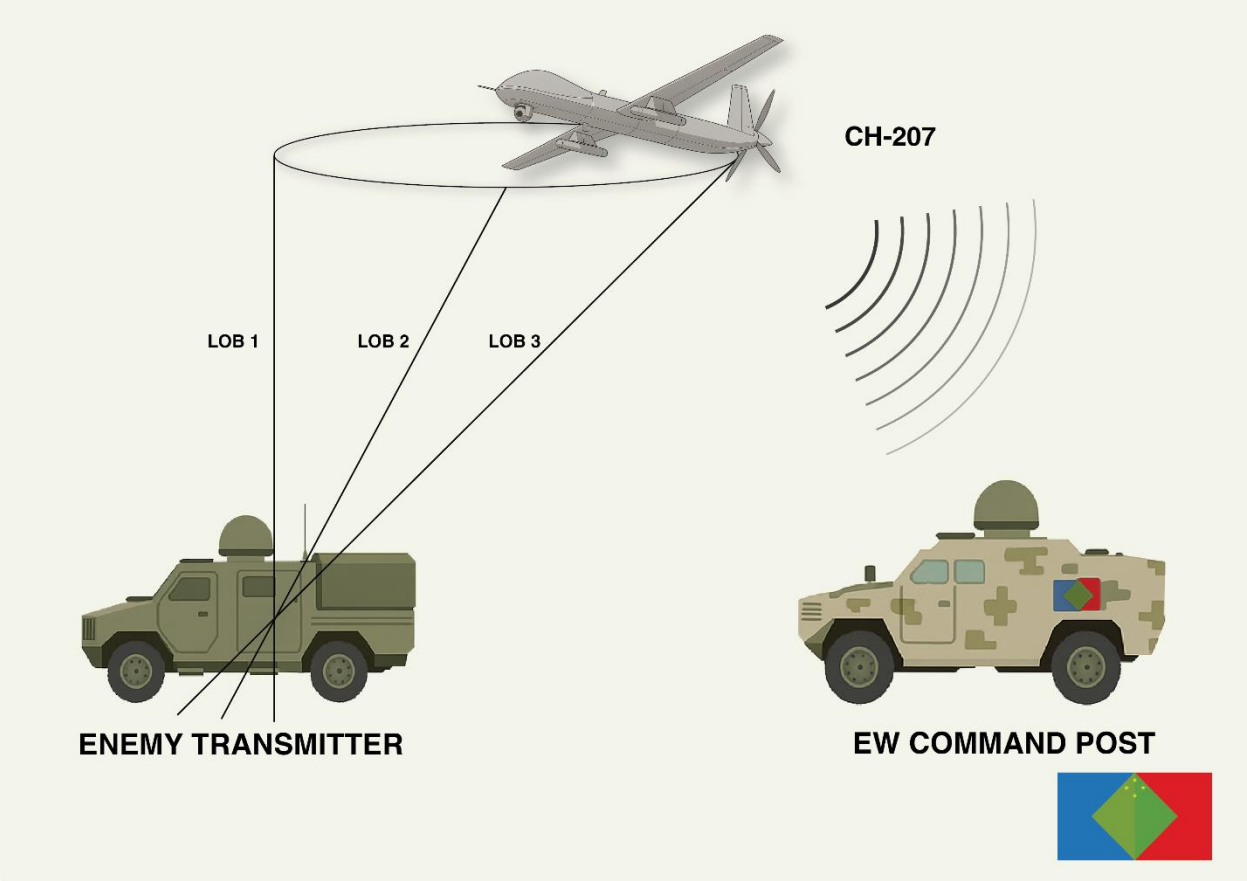
6.40 **Step 4: Ground Crew Safety and Counter - Detection Protection** - throughout the mission, the EW vehicle stays radio silent, except for receiving the short burst transmissions from the UAS. The antenna mast stays down to reduce visibility, while a second crewmember monitors the EMS for any signs of enemy DF attempts.

6.41 If enemy tracking is detected the team cuts all telemetry and the UAS is commanded to autonomously finish its mission and land at a pre-selected hidden landing zone (LZ). This ensures that the enemy is unable to obtain a fix on the EW vehicle's position, while signals data is preserved

6.42 **Tactical Advantage of UAS Direction Finding:** Using UAS-based direction finding extends the platoon's sensor reach while keeping the crew protected and hidden in the electromagnetic battlespace.

6.43 This method allows the Olvanan EW Platoon to detect and locate enemy emitters from a safe distance, reduces the chances of detection of ground based EW elements, maintain mobility and stealth, and allows for earlier detection of threats.

**Figure 6.5: UAS Direction Finding**




## Section 6-29. Electronic Protection – Baseline Emission Control

6.44 To avoid detection, resist jamming, and stay operational in a contested environment, the Olvanan EW Platoon follows strict EP practices. These help reduce the unit's RF signature and make it harder for the enemy to track, jam, or strike them. They do this by adhering to the following principles:

a. **EMCON** - transmit only when needed, use short, encrypted bursts of radio traffic, and send routine reports at the top of the minute with a random ±15 second offset to avoid patterns.

b. **Power Control** - always transmit at the lowest power setting needed to reach your target, increase power only when ordered by the net controller, and log every power increase, and reset to low after each successful message.

c. **Frequency Agility** - keep two pre-loaded frequency hop sets on all radios (a primary and a backup), and if jamming DF is detected, switch to "Hop Bravo" within 5 seconds—no permission needed.

d. **Antenna and Terrain Management** - mask, don't mast. Avoid raising antennas into the open sky, and park behind ridgelines and use shielded cables to connect to low profile antennas placed just below the crest.

e. **Control Azimuth** - after every stop, slightly rotate directional antennas downslope, this forces enemy jammers to overshoot and weakens their signal at your receiver.

f. **Drop-and-Shift Drill** - collapse mast in under 10 minutes, drive 200 m along the ridge, and reconnect using the spare hop set. This breaks enemy tracking and keeps their position unpredictable.

g. **Mobility and Signature Management** – one up, one down, in each section, keep one vehicle transmitting, one in receive-only, and one moving. This leapfrog pattern ensures constant pressure while staying mobile.

h. **Silent Bounds** - when moving keep all radios in receive-only, turn off headlights, limit engine RPM to stay quiet, and drone spotters check routes ahead for hostile signals or ambushes

i. **Deception Beacons** - leave small decoy transmitters behind for 15 minutes after moving out of a location. These fool enemy DF systems into targeting empty ground.

j. **Monitoring and Immediate Actions** - spectrum guard, one crewmember monitors the RF spectrum full-time using a wideband receiver. Any unusual signal triggers a quick alert using an appropriate code set.

k. **Fast Reaction** - within 30 seconds of detecting jamming or DF, send a report on the backup frequency set, drop transmit power by one level, rotate antennas 20° away from the threat, and resume operations as soon as practicable

l. **Hardening and Redundancy** – cable over the air,use fibre optic cables between vehicles whenever the distance allows (under 300 m). This removes the need for short-range radio links, reducing emissions

m. **Backup Paths** - every important report has a second option, whether HF, UHF SATCOM, or even courier with flash drive. If no RF path is available within 2 minutes, switch to the alternate. When every team member sticks to this discipline, the Olvanan EW Platoon becomes hard to detect, resilient against jamming, and costly for the enemy to track.

## Section 6-30. Crew Responsibilities

6.45 **Detachment Commander -** controls EMCON levels, approves power increases, tracks node positions, commands frequency changes, and links in with EW Company.

6.46 **EW Technicians** - maintain spectrum watch, checks antenna alignment, and trains the crew in drop-and-shift drills

6.47 **Vehicle Commander (Chief)** - manages mast operations, logs power levels, and makes sure decoy beacons are used and recovered

# Chapter 7
# Indicators and Warnings of Olvanan EW Operations

7.1 Detecting early indicators and warnings of Olvanan electronic warfare operations is vital for maintaining battlefield awareness and preserving the integrity of friendly C2 systems. The OPA employs sophisticated, layered EW tactics that often begin with preparatory electronic reconnaissance to map friendly electromagnetic signatures and vulnerabilities. Units should monitor for unusual or unexplained fluctuations in the EMS, such as sudden signal degradation, unexpected noise bursts, or the appearance of anomalous radio emissions. These signs often precede more aggressive jamming or spoofing attacks and can indicate that Olvanan EW teams are actively probing communications, radar, or navigation systems.

7.2 Another key indicator of OPA EW activity is the presence of advanced DF efforts targeting friendly emitters. Olvanan forces use mobile EW platforms and dismounted teams equipped with DF equipment to triangulate and locate critical command posts, radar sites, and communication nodes.

7.3 Observations of unfamiliar signature equipment consistent with Olvanan EW vehicles, such as the CTL-181A or ZBL-08 EW, or other EW equipped vehicle variants, should raise alarms, as should sightings of dismounted personnel operating EMS equipment, eg. with larger packs with multiple antennae.

7.4 Sudden losses or intermittent failures in GPS signals, unexpected navigation errors, or conflicting radar returns often indicate Olvanan GPS spoofing or electronic deception operations are underway.

7.5 Indicators of cyber intrusion attempts or unexplained data disruptions can serve as warnings of concurrent EW campaigns. Increased radio chatter from suspected EW units, coupled with suspicious network anomalies such as unauthorized access or degradation of friendly cyber infrastructure, may signal an integrated electronic attack in progress.

7.6 Furthermore, irregular electromagnetic emissions that do not conform to friendly patterns, especially pulsed or frequency-hopping signals, should be carefully analysed, as they are hallmarks of Olvanan electronic countermeasure systems attempting to mask or jam communications.

7.7 Finally, recognising the tempo and scale of Olvanan EW operations is essential for the employment of effective countermeasures. The OPA frequently employ short, high-intensity jamming bursts in contested zones to minimise detection and maximise surprise, as well as longer-duration saturation jamming during major offensive operations. Units should remain vigilant for recurring patterns of EMS interference coinciding with observed Olvanan movements or large-scale fires.

7.8 By institutionalising comprehensive spectrum monitoring, rapid reporting of anomalies, and continuous updating of the EOB, forces can gain crucial early warning, which can help to mitigate the operational impact of Olvanan EW, and maintain freedom of manoeuvre in the EMS.

## Section 7-31. Indicators and Warnings Checklist:

a. **EMS Anomalies**

(1) Sudden loss or degradation of radio and data communications.

(2) Unexplained bursts of noise or interference across frequencies.

(3) Appearance of unfamiliar or anomalous electromagnetic emissions, including pulsed, chirped, or frequency-hopping signals.

b. **Direction-Finding and Reconnaissance Indicators**

(1) Rapid fluctuations in signal strength consistent with triangulation attempts.

(2) Increased enemy radio chatter or suspicious transmissions near key friendly emitters.

(3) Sightings or intelligence of specialised EW vehicles

(4) Dismounted personnel operating equipment consistent with EW reconnaissance or electronic attack.

(5) Litter including significant deposits of batteries.

c. **Navigation and Radar Disruptions**

(1) GPS signal loss, spoofing, or erratic navigation fixes.

(2) Conflicting or false radar returns, multiple or phantom contacts.

(3) Unexpected sensor outages or degraded radar coverage in operational sectors.

d. **Cyber and Network Effects**

(1) Unexplained data corruption or network outages correlating with EMS interference.

(2) Increased unauthorised access attempts or cyber intrusion alerts during suspected EW operations.

(3) Coordinated cyber-electronic disruptions targeting C2 nodes.

e. **Operational Patterns and Tempo**

(1) Short, high-intensity jamming bursts designed for surprise effects.

(2) Longer-duration jamming during major OPA offensive or defensive operations.

(3) Correlation of EMS interference with observed Olvanan troop or vehicle movements.

(4) Repeated interference patterns focused on key terrain or infrastructure.

7.9 Early detection and reporting provide critical time to activate countermeasures such as EMCON, frequency hopping, redundant communications, and sensor realignment. Maintaining an up-to-date EOB and integrating SIGINT with tactical intelligence enhances situational awareness and reduces vulnerability to Olvanan EW effects.

# Chapter 8
# Logistics Support

## Section 8-32. Power Requirements

8.1 EW equipment, whether mounted on vehicles or carried by dismounted operators, demands a reliable and continuous power supply to function effectively. Mounted EW platforms benefit from vehicle-integrated power systems that can support high-energy jamming and signal processing systems for extended periods. However, these systems still require careful power management to avoid overloading the vehicle's electrical infrastructure, especially during sustained operations.

8.2 For dismounted EW teams, power supply becomes a critical constraint, as portable batteries must balance capacity, weight, and size. Limited battery life restricts operational endurance, necessitating frequent battery changes or recharging, which may be challenging in austere or contested environments.

## Section 8-33. Mobility Challenges

8.3 Mobility is a key factor influencing the deployment and effectiveness of EW assets. Mounted EW systems enjoy enhanced mobility by leveraging armoured vehicles' off-road capabilities, allowing them to keep pace with mechanised and combined-arms formations. Nonetheless, the size and weight of EW vehicles can limit their ability to manoeuvre in dense urban terrain or restrictive environments such as forests or mountainous areas.

8.4 Conversely, dismounted EW teams benefit from greater agility and access to difficult terrain but face physical limitations imposed by the weight and bulk of their equipment. Carrying multiple batteries, antennas, and electronic modules can reduce the endurance and speed of operators, potentially limiting their ability to rapidly reposition or evade threats.

## Section 8-34. Resupply and Sustainment

8.5 Sustaining EW operations over time demands robust logistical support, especially regarding the resupply of consumables such as batteries, spare parts, and electronic components. Mounted EW platforms typically rely on brigade or higher-echelon logistics to maintain their power systems, repair electronic modules, and replenish expendable supplies. However, the complexity of EW equipment and the sensitivity of electronic components require specialised maintenance personnel and controlled supply chains, which can be disrupted in high-tempo or contested operations.

8.6 Dismounted EW teams face greater challenges, as their small size and dispersed deployment make it difficult to establish consistent resupply points. Limited carrying capacity restricts how much spare equipment and power sources they can carry, often-requiring close coordination with support units or aerial resupply.

## Section 8-35. Environmental and Operational Constraints

8.7 Beyond power, mobility, and resupply, environmental factors impose additional logistical burdens on EW systems. Harsh weather conditions such as extreme temperatures, humidity, and dust can degrade electronic components and reduce battery efficiency, necessitating more frequent maintenance and replacement cycles. Mounted EW vehicles must also contend with terrain obstacles that limit movement and complicate resupply routes.

8.8 Dismounted operators are vulnerable to these environmental stresses as well, and must carry protective gear and maintenance kits to mitigate equipment failures. These factors collectively emphasise the need for thorough logistical planning and adaptive sustainment strategies to ensure EW capabilities remain operational during prolonged and dynamic combat engagements.

# Chapter 9
# Conclusion and Future Trends

9.1 The future of EW is increasingly defined by the integration of multi-domain operations, where cyber, space, and EMS operations converge to create layered effects. Drawing on doctrinal trends observed in the OPA, future EW capabilities will emphasise seamless interoperability between EA, EP, and cyber operations. This integrated approach will enable forces to disrupt adversary networks, not only through jamming and deception but also by exploiting vulnerabilities in software and data links. The expansion of AI and ML within EW systems promises faster signal identification, autonomous threat response, and dynamic spectrum management, allowing Olvanan EW units to operate effectively in increasingly contested and congested electromagnetic environments.

9.2 Another key trend is the miniaturisation and increasing mobility of EW platforms, reflecting the need to support dispersed fast-moving forces across varied terrains and operating environments. The OPA has invested in lightweight, man-portable EW systems that enhance the flexibility of dismounted troops, while simultaneously developing advanced vehicle-mounted EW for mechanised formations. This dual focus supports rapid deployment and multi-layered spectrum control, critical in complex battlefields such as dense jungles and urban centres. Additionally, the proliferation of small UAS equipped with EW payloads enhances persistent surveillance and targeted DF and EA capabilities, extending the reach of ground forces and complicating enemy countermeasures.

9.3 In the realm of spectrum management, future EW operations will rely heavily on sophisticated EMS and SIGINT systems to maintain real-time EOB awareness. Olvanan doctrine increasingly focuses on continuous monitoring of the EMS using distributed sensor networks, including UAVs, ground stations, and space-based assets. This networked approach enables rapid identification and classification of enemy emitters, facilitating dynamic reallocation of EA assets to exploit weaknesses and counter adversary EW efforts. Such real-time spectrum awareness is vital for both offensive operations and defensive EP, especially given the growing complexity and sophistication of adversary communications and radar systems.

9.4 Tactical EW systems are critical in counter-drone operations, as small, commercially available unmanned systems proliferate on modern battlefields. As a leader in the field of drone technology, the Olvanan military recognises that drones pose a significant threat at all levels, from reconnaissance, to precision strike capabilities, and as a main stay of the asymmetric kill chain.

9.5 Tactical EW units equipped with electronic jamming and spoofing technologies are essential to disrupt enemy drone control links and GPS navigation, effectively neutralizing hostile UAVs before they can inflict damage. This role requires EW operators to integrate closely with air defence and ground manoeuvre elements, rapidly detecting and engaging drones within contested environments. The development of adaptive, low-signature EW tactics ensures Olvanan forces maintain airspace control against increasingly autonomous and swarm-capable drone threats.

9.6 Future EW will be shaped by advancements in cognitive and adaptive EW systems that learn and evolve in response to enemy tactics. Through research into AI-enabled EW, Olvanan forces are likely to adopt systems capable of autonomously adjusting jamming frequencies, power levels, and emission patterns to counter frequency hopping, spread-spectrum, and other advanced enemy techniques.

9.7 This adaptive type of EW reduces operator workload, increases system resilience, and enhances mission success rates in dynamic electromagnetic environments. Moreover, integration with cyber operations and kinetic effects will enable Olvanan commanders to conduct synchronised multi-domain campaigns that leverage the full spectrum of EW capabilities to achieve electromagnetic superiority.

## Abbreviations

The source for approved Defence terms, definitions and abbreviations is the Australian Defence Glossary (ADG), available on the Defence Protected Network at http://adg.dpe.protected.mil.au/.

| term | definition |
|---|---|
| **AD** | Air Defence |
| **ADF** | Australian Defence Force |
| **AI** | Artificial Intelligence |
| **AV** | Advancing Vehicle |
| **A2/AD** | Anti-Access Area Denial |
| **BMS** | Battle Management System |
| **BN** | Battalion |
| **BDE** | Brigade |
| **CA-BDE** | Combined Arms Brigade |
| **CDF** | Chief of the Defence Force |
| **COP** | Common Operating Picture |
| **C2** | Command and control |
| **C4ISR** | Command Control Communications Computers Intelligence Surveillance and Reconnaissance |
| **COY** | Company |
| **DF** | Direction Finding |
| **EA** | Electronic Attack |
| **ECM** | Electronic countermeasures |
| **ECCM** | Electronic counter-countermeasures |
| **EMCON** | Emissions Control |
| **EMP** | Electro-magnetic Pulse |
| **EMS** | Electromagnetic Spectrum |
| **EOB** | Electronic Order of Battle |
| **EO/IR** | Electro-optical/Infra-red |
| **EP** | Electronic Protection |
| **EW** | Electronic Warfare |
| **EWCE** | Electronic Warfare Control Element |
| **FEBA** | Forward Edge of the Battle Area |
| **FLOT** | Forward Line of Own Troops |
| **GPS** | Global Positioning System |
| **HPM** | High Powered Microwave |
| **HQ** | Headquarters |
| **HV** | Holding Vehicle |
| **ISR** | Intelligence, surveillance, and reconnaissance |
| **KDP** | Key Defence Point |
| **LZ** | Landing Zone |
| **ML** | Machine Learning |
| **OP** | Observation Post |
| **OPCON** | Operational Control |
| **OPSEC** | Operational Security |

| | |
|---|---|
| **OPA** | Olvanan People's Army |
| **ORBAT** | Order of Battle |
| **PL** | Platoon |
| **PSYOPS** | Psychological Operations |
| **RF** | Radio Frequency |
| **RISTA** | Reconnaissance Intelligence Surveillance, Target Acquisition |
| **SEAD** | Suppression of Enemy Air Defences |
| **SOM** | Scheme of Manoeuvre |
| **TACON** | Tactical Control |
| **UAS** | Un-Crewed Aerial System |
| **UAV** | Un-Crewed Aerial Vehicle |
| **WIFI** | Wireless Fidelity |