

FM 34-45
Tactics, Techniques, and Procedures
ELECTRONIC ATTACK

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

TACTICS, TECHNIQUES, AND PROCEDURES FOR ELECTRONIC ATTACK

Contents

		Page
PREFACE	iv
Chapter 1	OPERATIONS AND ELECTRONIC WARFARE	1-1
	The Potential.....	1-1
	Methodology.....	1-2
	The Environment.....	1-2
	Electronic Warfare	1-2
	Tactical Electronic Attack.....	1-4
	Current and Future Threat Electronic Warfare Capabilities.....	1-4
Chapter 2	ELECTRONIC ATTACK IN INFORMATION OPERATIONS	2-1
	Information Operations	2-1
	Information Superiority.....	2-1
Chapter 3	ELECTRONIC ATTACK IN TARGETING: KEY PERSONNEL, ORGANIZATIONS, AND COORDINATION	3-1
	Electronic Attack in The Targeting Methodology	3-1
	Key Electronic Attack Personnel and Organizations	3-3
	Key Electronic Attack Coordination	3-8
Chapter 4	DECIDE	4-1
	Intelligence Preparation of the Battlefield	4-2
	Target Development	4-3
	Requirements Management	4-7

*This publication supersedes FM 34-40-7, 23 November 1992.

	Page
Mission Management.....	4-8
Asset Management.....	4-12
Chapter 5 DETECT.....	5-1
Electronic Support Data.....	5-1
Deploy Electronic Support and Electronic Attack Assets	5-1
Collect Electronic Support Data.....	5-13
Collection for Database Development	5-15
Search Techniques.....	5-15
Cross Cue.....	5-16
Process Signals Intelligence Data	5-17
Situation Development.....	5-17
Electronic Attack Effectiveness.....	5-18
Chapter 6 DELIVER.....	6-1
Tactical Decisions.....	6-1
Technical Decisions.....	6-1
Conduct Electronic Attack.....	6-2
Jumping EA Assets After EA Missions	6-5
Report Electronic Attack Results	6-6
Summarize Status of Electronic Attack Results	6-8
Chapter 7 ASSESS	7-1
Operator Evaluation	7-1
Unit Combat Assessment	7-3
Reattack Recommendation.....	7-5
Appendix A THE ELECTROMAGNETIC ENVIRONMENT	A-1
Military Electromagnetic Spectrum	A-1
Military Operations and Electromagnetic Environment.....	A-1
Principal Electronic Warfare Activities	A-3
Appendix B SIGNAL-TO-NOISE RATIO REFERENCE	B-1
Ratio Formula	B-1
Future Trends	B-2
Appendix C ELECTRONIC DECEPTION	C-1
Types of Electronic Deception	C-1
Electronic Deception Planning.....	C-2

	Page
Electronic Deception Techniques	C-4
Appendix D MESSAGE FORMATS	D-1
Appendix E EXAMPLE FORMATS AND TARGET REPORT	E-1
General	E-1
High-Payoff Target List	E-1
Target Selection Standards	E-2
Attack Guidance Matrix.....	E-2
Sensor or Attack Matrix.....	E-3
Optional High-Payoff Target List and Attack Guidance Matrix	E-4
Target Sheets	E-6
Electronic Warfare Annex	E-7
Appendix F DIRECT SUPPORT TO THE BRIGADE	F-1
Task Organization.....	F-1
Organization and Operations.....	F-2
Appendix G MILITARY OPERATIONS ON URBANIZED TERRAIN	G-1
Appendix H BRIGADE COMBAT TEAM	H-1
Organization.....	H-1
Operations	H-1
Glossary	Glossary-1
Bibliography	Bibliography-1
Index	Index-1

PREFACE

The purpose of this manual is to—

- Address the deployment and employment of electronic attack (EA) assets at division and brigade.
- Discuss concepts and principles unique to EA.
- Describe how to integrate EA into the targeting effort.
- Address specific tactics, techniques, and procedures (TTP) when applicable.

This manual is a guide for Army commanders, staffs, and operators who plan and/or execute EA. It applies equally to the Active Component (AC), US Army Reserve (USAR), and Army National Guard (ARNG).

This manual complies with FM 34-1 and is consistent with current joint doctrine. It assumes the user has a fundamental understanding of the doctrine in FM 100-5, FM 101-5, FM 34-1, FM 6-20-10, and FM 34-130.

The proponent for this publication is Headquarters, US Army Training and Doctrine Command (TRADOC). Send comments and recommendations on DA Form 2028 directly to Commander, US Army Intelligence Center and Ft Huachuca, ATTN: ATZS-FDC-D, Ft Huachuca, AZ 85613-6000.

This manual does not implement any International Standardization Agreements.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

Operations and Electronic Warfare

Division targeting teams and electronic warfare (EW) personnel work together to ensure that EW is integrated into targeting, is thoroughly planned, and is vigorously executed. The use of standard EW targets without thorough analysis and planning significantly limits the potential of EW as a true combat multiplier. Inadequate planning leads to the uncoordinated use of EW and limits the effects of both EW and fire support (FS) as a whole. On the other hand, if EW is adequately staffed, trained, integrated into targeting, planned, and executed, it helps the commander reach his targeting objectives by dominating the electromagnetic environment (EME).

EW can attack the threat when it is most vulnerable through a quick, accurate, timely, and responsive means that can also provide a fast assessment of the operation. Additionally, EW is important because it is a responsive tool to perform suppression of enemy air defenses (SEAD); it is also one of the integrated tools used to conduct information operations (IO). However, EW is effective only when the commander decides there is more value in conducting EA (for a specific high-payoff target [HPT] at a specific point) than performing additional collection in order to produce more intelligence.

THE POTENTIAL

1-1. The potential for EA is unlimited especially within the information age.

- **Offensive** operations often provide the friendly forces the element of surprise. Prior to units crossing the line of departure (LD), EA assets begin their missions. EA may focus on the scout or reconnaissance net to ensure intelligence indicating friendly forces attacking is not passed to the threat command post (CP). As units begin to engage the threat, EA assets then shift their effort onto the threat's counterbattery, command and control (C²), and artillery. The suppression of these targets denies the enemy the ability to effectively control his forces and also disrupts the flow of information to his artillery and counterbattery, thus rendering them useless. At this point, EA systems engage specific targets. A unit near a bridge that was destroyed is jammed to prevent the requesting of engineer support. This will cause a delay in maneuvering an enemy unit that would protect a vulnerable flank.