



202

EW

WAR

FARE

David L. Adamy

A Second Course

in Electronic

Warfare

EW 102

A Second Course in Electronic Warfare

For a listing of recent titles in the *Artech House Radar Library*,
turn to the back of this book.

EW 102

A Second Course in Electronic Warfare

David L. Adamy



Artech House
Boston • London
www.artechhouse.com

Library of Congress Cataloging-in-Publication Data

Adamy, David.

EW 102: a second course in electronic warfare /David L. Adamy.

p. cm. — (Artech House radar library)

Includes bibliographical references and index.

ISBN 1-58053-686-7 (alk. paper)

1. Electronics in military engineering. I. Title. II. Series.

UG485.A3322 2004

623'.043—dc22

2004050666

British Library Cataloguing in Publication Data

Adamy, David

EW 102: a second course in electronic warfare. — (Artech House radar library)

1. Electronics in military engineering

I. Title

623'.043

ISBN 1-58053-686-7

Cover design by Igor Valdman

© 2004 Horizon House Publications, Inc.

All rights reserved.

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 1-58053-686-7

10 9 8 7 6 5 4 3 2 1

Like EW 101 which came before it, this book is dedicated to my colleagues in the EW profession—in and out of uniform. Some of you have gone repeatedly into harm's way, and most of you have often worked long into the night to do things that are beyond the comprehension of the average person. Ours is a strange and challenging profession, but most of us can't imagine following any other.

Contents

	Preface	xv
1	Introduction	1
1.1	Generalities About EW	3
1.2	Information Warfare	5
1.3	How to Understand Electronic Warfare	6
2	Threats	9
2.1	Some Definitions	9
2.1.1	Threats Versus Threat Signals	9
2.1.2	Radars Versus Communication	10
2.1.3	Types of Threats	10
2.1.4	Radar-Guided Weapons	11
2.1.5	Laser-Guided Weapons	11
2.1.6	Infrared Energy: Guided Weapons	12
2.1.7	Lethal Communications	12
2.1.8	Radar Resolution Cell	13

2.2	Frequency Ranges	13
2.3	Threat Guidance Approaches	15
2.3.1	Active Guidance	15
2.3.2	Semiactive Guidance	16
2.3.3	Command Guidance	16
2.3.4	Passive Guidance	17
2.4	Scan Characteristics of Threat Radars	17
2.4.1	The Radar Scan	17
2.4.2	Antenna Beamwidth	18
2.4.3	Antenna Beam Pointing	19
2.5	Modulation Characteristics of Threat Radars	22
2.5.1	Pulse Radars	22
2.5.2	Pulse Doppler Radars	25
2.5.3	Continuous Wave Radars	25
2.5.4	Threat Radar Applications	26
2.6	Communication Signal Threats	26
2.6.1	The Nature of Communication Signals	27
2.6.2	Tactical Communication	27
2.6.3	Digital Data Links	29
2.6.4	Satellite Links	30
3	<u>Radar Characteristics</u>	33
3.1	The Radar Function	33
3.1.1	Types of Radars	34
3.1.2	Basic Radar Block Diagrams	35
3.2	Radar Range Equation	36
3.2.1	Radar Cross Section	39
3.2.2	Radar Detection Range	40
3.3	Detection Range Versus Detectability Range	42
3.3.1	Estimating the Sensitivity of the Radar Receiver	43
3.3.2	Example of Radar Detection Range Calculation	44

3.3.3	Detectability Range	44
3.4	Radar Modulation	48
3.5	Pulse Modulation	48
3.5.1	Unintentional Modulation on Pulses	50
3.5.2	Pulse Compression	51
3.5.3	Chirped Pulses	51
3.5.4	Digital Modulation on Pulses	53
3.6	CW and Pulse Doppler Radars	54
3.6.1	Doppler Shift	55
3.6.2	CW Radar	56
3.6.3	FM Ranging	56
3.6.4	Pulse Doppler Radar	58
3.7	Moving Target Indicator Radars	58
3.7.1	Basic MTI Operation	59
3.7.2	MTI Data Rates	61
3.7.3	Airborne Moving Target Indicator (AMTI) Radar	62
3.8	Synthetic Aperture Radars	63
3.8.1	Range Resolution	63
3.8.2	Azimuth Resolution	64
3.8.3	Focused Array SAR	66
3.9	Low Probability of Intercept Radars	67
3.9.1	LPI Techniques	67
3.9.2	Levels of LPI	68
3.9.3	LPID Radars	68
3.9.4	Detection Versus Detectability	70
3.9.5	LPI Figure of Merit	71
3.9.6	Other Factors Impacting Detection Range	72
4	Infrared and Electro-Optical Considerations in Electronic Warfare	77
4.1	The Electromagnetic Spectrum	77

4.1.1	Infrared Spectrum	78
4.1.2	Blackbody Radiation	79
4.1.3	IR Transmission	80
4.1.4	EW Applications in the IR Range	80
4.1.5	Electro-Optical Devices	82
4.2	IR Guided Missiles	82
4.2.1	IR Sensors	82
4.2.2	IR Missiles	83
4.3	IR Line Scanners	87
4.3.1	Mine Detection Application	87
4.4	Infrared Imagery	90
4.4.1	The FLIR	90
4.4.2	IR Imagery Tracking	93
4.4.3	Infrared Search and Track	93
4.5	Night-Vision Devices	94
4.5.1	Types of Devices	94
4.5.2	Classical Night Operations	95
4.5.3	History of Development	95
4.5.4	Spectral Response	96
4.5.5	Implementation	96
4.6	Laser Target Designation	98
4.6.1	Laser Designator Operation	98
4.6.2	Laser Warning	99
4.6.3	Countermeasures Against Laser-Homing Missiles	100
4.7	Infrared Countermeasures	101
4.7.1	Flares	101
4.7.2	IR Jammers	103
4.7.3	IR Decoys	104
4.7.4	IR Chaff	105
5	EW Against Communications Signals	107
5.1	Frequency Ranges	107

5.2	HF Propagation	108
5.2.1	The Ionosphere	109
5.2.2	Ionospheric Reflection	110
5.2.3	HF Propagation Paths	111
5.2.4	Single-Site Locators	112
5.2.5	Emitter Location from Airborne Systems	112
5.3	VHF/UHF Propagation	113
5.3.1	Propagation Models	113
5.3.2	Free Space Propagation	113
5.3.3	Two-Ray Propagation	114
5.3.4	Knife-Edge Propagation	116
5.4	Signals in the Propagation Medium	116
5.5	Background Noise	120
5.6	Digital Communication	121
5.6.1	Digital Signals	122
5.6.2	Digitization	122
5.6.3	Digitizing Imagery	124
5.6.4	Digital Signal Format	125
5.6.5	RF Modulations for Digital Signals	126
5.6.6	Signal-to-Noise Ratio	128
5.6.7	Bit-Error Rate Versus RFSNR	128
5.6.8	Bandwidth Required for Digital Signals	129
5.6.9	Impact of Signal Bandwidth on Electronic Warfare	132
5.7	Spread Spectrum Signals	133
5.7.1	Frequency-Hopping Signals	134
5.7.2	Chirp Signals	135
5.7.3	Direct Sequence Spread Spectrum Signals	136
5.8	Communications Jamming	137
5.8.1	Jamming-to-Signal Ratio	138
5.8.2	Operation Near the Earth	139
5.8.3	Other Losses	140
5.8.4	Digital Versus Analog Signals	140

5.9	Jamming Spread Spectrum Signals	141
5.9.1	Jamming Frequency Hop Signals	141
5.9.2	Jamming Chirp Signals	147
5.9.3	Jamming DSSS Signals	147
5.9.4	Impact of Error-Correction Coding	149
5.10	Location of Spread Spectrum Transmitters	150
5.10.1	Location of Frequency-Hopping Transmitters	150
5.10.2	Location of Chirped Transmitters	153
5.10.3	Location of Direct Sequence Transmitters	153
5.10.4	Precision Emitter Location Techniques	153
6	<u>Accuracy of Emitter Location Systems</u>	155
6.1	Basic Emitter Location Approaches	156
6.2	Angle Measurement Techniques	157
6.2.1	Rotating Directional Antenna	157
6.2.2	Multiple Antenna Amplitude Comparison	158
6.2.3	Watson-Watt Technique	159
6.2.4	Doppler Technique	159
6.2.5	Distance Measuring Techniques	160
6.2.6	Interferometric Direction Finding	162
6.3	Precision Emitter Location Techniques	164
6.3.1	Time Difference of Arrival Method	164
6.3.2	Precision Emitter Location by FDOA	167
6.3.3	FDOA Against Moving Transmitters	169
6.3.4	Combined FDOA and TDOA	170
6.4	Emitter Location—Reporting Location Accuracy	171
6.4.1	RMS Error	171
6.4.2	Circular Error Probable	173
6.4.3	Elliptical Error Probable	174
6.5	Emitter Location—Error Budget	174
6.5.1	Combination of Error Elements	175

6.5.2	Impact of Reflections on AOA Error	176
6.5.3	Station Location Accuracy	176
6.5.4	Error Budget Items for Angle-of-Arrival Emitter Location Approaches	177
6.5.5	Error Related to Signal-to-Noise Ratio	178
6.5.6	Calibration Errors	179
6.5.7	Combination of AOA System Errors	179
6.6	Conversion of AOA Errors to Location Errors	179
6.6.1	Measurement Accuracy	179
6.6.2	Circular Error Probable	182
6.7	Location Errors in Precision Location Systems	183
6.7.1	TDOA System Accuracy	183
6.7.2	Location Errors in FDOA Emitter Location Systems	187
7	Communication Satellite Links	191
7.1	The Nature of Communication Satellites	191
7.2	Terms and Definitions	192
7.3	Noise Temperature	195
7.3.1	System Noise Temperature	195
7.3.2	Antenna Noise Temperature	196
7.3.3	Line Temperature	197
7.3.4	Receiver Noise Temperature	197
7.3.5	A Noise Temperature Example	199
7.4	Link Losses	200
7.4.1	Spreading Loss	200
7.4.2	Atmospheric Loss	201
7.4.3	Rain and Fog Attenuation	202
7.4.4	Faraday Rotation	204
7.5	Link Losses in Typical Links	205
7.5.1	A Synchronous Satellite	205
7.5.2	Low-Earth-Satellite Link	208

7.6	Link Performance Calculations	209
7.6.1	Synchronous Satellite Links	210
7.6.2	Low-Earth-Orbit Links	212
7.7	Relating Communication Satellite and EW Forms of Equations	214
7.8	Jamming of Satellite Links	215
7.8.1	Downlink Jamming	216
7.8.2	Uplink Jamming	217

Appendix A: Problems with Solutions **219**

Part 1	Problems from the <i>EW 101</i> Book	219
Part 2	Problems from the <i>EW 102</i> Book	239

Appendix B: Cross-References to *EW101* Columns in the *Journal of Electronic Defense* **255**

EW 101	255
EW 102	256

Appendix C: Selected Bibliography **259**

About the Author **263**

Index **265**

Preface

EW 101 has been a popular column in the *Journal of Electronic Defense (JED)* for 10 years now—covering various aspects of electronic warfare (EW) in two-page bites on a month-to-month basis. The first 60 of those columns were reorganized into chapters with added material for continuity to become the book *EW 101*. The book, like the columns, has been very popular, but, since then, there have been almost 60 more *EW 101* columns. Some have provided deeper information on subjects covered in the first book and some are on entirely new EW areas. It was clearly time for another book—thus *EW 102*.

The target audiences for this book are the same as that for *EW 101*: new EW professionals, specialists in some part of EW, and specialists in technical areas peripheral to EW. Another target group is managers who used to be engineers—who now must make decisions based on input from others (who may or may not be trying to break the laws of physics). In general, the book is intended for those to whom a general overview, a grasp of the fundamentals, and the ability to make general-level calculations is valuable.

I sincerely hope that this book helps you be a better EW professional. The free world needs the best you have to offer in this important field of endeavor.

1

Introduction

This is the second book in the series, and like other books in that position it is intended to have stand-alone value—but not be redundant with the first book (in this case, *EW 101*). Like the first book, this one collects the material presented in many months of *EW 101* columns, organizes the material into chapters, and adds introductory and supplementary material for completeness—so it reads like a book rather than a collection of columns. It also has a feature requested by many readers of both the book and the columns: Solved problems.

This book comprises almost entirely new material that was not in the *EW 101* book. The exceptions are the sections which provide additional scope to material covered in *EW 101*. In those cases, there is a brief overview of the relevant *EW 101* material. The subjects covered in the rest of the book are:

- Chapter 2: Threats, from a functional and signal point of view. *EW 101* talked about threats in context, but never really focused in on them.
- Chapter 3: Radar Characteristics, is a functional discussion of the different kinds of radars—with emphasis on their significance to electronic warfare.
- Chapter 4: Infrared and Electro-Optical Considerations in Electronic Warfare, including heat seeking missiles, IR imagery systems, night vision devices, laser designators, and countermeasures.
- Chapter 5: EW Against Communications Signals, including radio propagation, digital communication, jamming, and various issues

regarding emitter location. Discussions are also extended to the EW impact of spectrum spreading.

- Chapter 6: Accuracy of Emitter Location Systems, including emitter location techniques (a brief review), error statistics, and circular error probable for all common emitter location techniques.
- Chapter 7: Communication Satellite Links, including the way satellite link performance is predicted, and link jamming.
- Appendix A: A large appendix of problems with solutions. These problems cover the subjects in both *EW 101* and *EW 102*, and the solutions are real solutions, with all of the important steps—not just answers.
- Appendix B: A cross-reference of the chapters of both the *EW 101* and *EW 102* books to the *EW 101* columns covering the same material.
- Appendix C: A list of reference books in electronic warfare and associated disciplines. Although not an exhaustive list of the books available on the subject, they are an excellent starting point for further, in-depth study of the field.

Like the first book in the series, and like the monthly tutorial articles from which both sprang, this book is intended to provide a top-level view of the broad, important and fascinating field of electronic warfare. Here are some generalities about the book:

- It is not intended for experts in the field, although it is hoped that experts in other fields and experts in subfields within electronic warfare may find it useful.
- It is intended to be easy to read. Technical material (contrary to popular opinion) does not need to be boring to be useful.

The coverage of technical material in this book is intended to be accurate as opposed to precise. The formulas, in most cases, are accurate to 1 dB, which is accurate enough for most system level design work. Even when much greater precision is required, almost all old-hand systems engineers run the basic equations to 1 dB first, then turn loose the computer experts to drive to the required precision. The problem with highly precise mathematics is that you can get lost down in the details and make mistakes of orders of magnitude. These mistakes are sometimes incorrect assumptions or (more often) an incorrectly stated problem. Order of magnitude errors get you (and probably your boss) into big trouble; they are worth avoiding.

When you work the problem to 1 dB, using the simple decibel form equations in this book, you will quickly derive a set of approximate answers. Then, you can sit back and ask yourself if the answers make sense. Compare the results to the results of other, similar problems...or just apply common sense. At this point, it is easy to revisit the assumptions or clarify the statement of the problem. Then, when you apply the considerable facilities, staff time, money, and (perhaps) stomach acid required to complete the detailed calculations they have an even chance of coming out right the first (or nearly the first) time.

1.1 Generalities About EW

Electronic warfare is defined as the art and science of preserving the use of the electromagnetic spectrum for friendly use while denying its use to the enemy. The electromagnetic spectrum is, of course, from dc to light (and beyond). Thus electronic warfare covers both the full radio frequency spectrum, the infrared spectrum, the optical spectrum, and the ultraviolet spectrum.

As shown in Figure 1.1, EW has classically been divided into:

- Electromagnetic support measures (ESM)—the receiving part of EW;
- Electromagnetic countermeasures (ECM)—jamming, chaff, and flares used to interfere with the operation of radars, military communication, and heat-seeking weapons;
- Electromagnetic counter-countermeasures (ECCM)—measures taken in the design or operation of radars or communication systems to counter the effects of ECM.

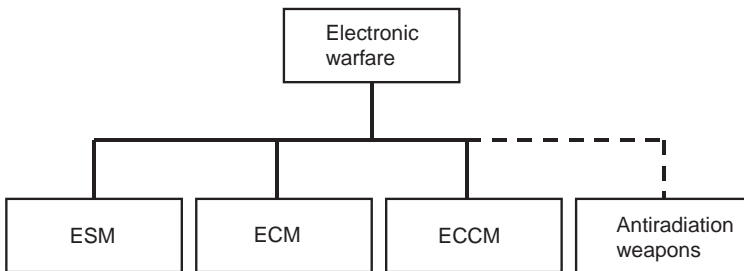


Figure 1.1 Electronic warfare has classically been divided into ESM, ECM, and ECCM. Antiradiation weapons were not part of EW.

Antiradiation weapons and directed energy weapons were not considered part of EW, even though it is well understood that they are closely allied with EW. They are differentiated as weapons.

In the last few years, the subdivisions of the EW field have been redefined as shown in Figure 1.2 in many (but not all) countries. Now the accepted definitions (in NATO) are:

- Electronic warfare support (ES)—which is the old ESM.
- Electronic attack (EA)—which includes the old ECM (jamming, chaff, and flares) but also includes antiradiation weapons and directed-energy weapons.
- Electronic protection (EP)—which is the old ECCM.

ESM (or ES) is differentiated from signal intelligence (SIGINT) [(which comprises communications intelligence (COMINT) and electronic intelligence (ELINT)], even though all of these fields involve the receiving of enemy transmissions. The differences, which are becoming increasingly vague as the complexity of signals increases, are in the purposes for which transmissions are received.

- COMINT receives enemy communications signals for the purpose of extracting intelligence from the information carried by those signals.
- ELINT receives enemy noncommunication signals for the purpose of determining the details of the enemy's electromagnetic systems so we

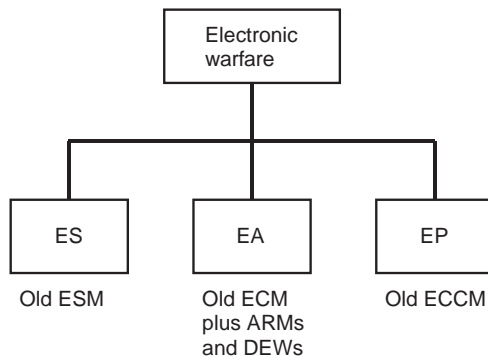


Figure 1.2 Current NATO electronic warfare definitions divide EW into ES, EA, and EP. EA now includes antiradiation and directed-energy weapons.

can develop countermeasures. Thus, ELINT systems normally collect lots of data over a long period of time to support detailed analysis.

- ESM/ES, on the other hand, collects enemy signals (either communication or noncommunication) with the object of immediately doing something about the signals or the weapons associated with those signals. The received signal might be jammed or its information handed off to a lethal response capability. The received signals can also be used for situation awareness, that is, identifying the types and location of the enemy's forces, weapons, or electronic capability. ESM/ES typically gathers lots of signal data to support less extensive processing with a high throughput rate. ESM/ES typically determines only *which* of the known emitter types is present and where they are located.

1.2 Information Warfare

A significant change that has occurred since the publication of *EW 101*, is the association of EW with information warfare (IW). EW is considered an integral part of information warfare—the action part. Information warfare includes actions taken to preserve the integrity of one's own information system from exploitation, corruption, or disruption, while at the same time exploiting, corrupting, or destroying an adversary's information system, as well as the process of achieving an information advantage in the application of force.

Figure 1.3 shows the so-called pillars of IW: psychological operations (PSYOPS), deception, electronic warfare, physical destruction, and operational security (OPSEC). These elements interfere with the enemy's ability to effectively use their military as shown in Figure 1.4. The OODA (observe, orient, decide, act) loop, shown in Figure 1.5 is the process required to take effective

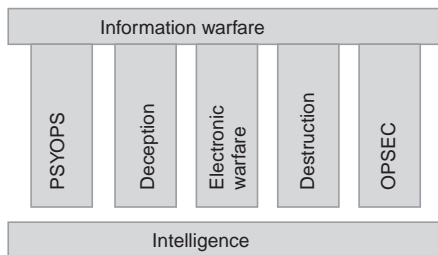


Figure 1.3 The pillars of information warfare are PSYOPS, deception, EW, destruction, and OPSEC, all supported by intelligence.

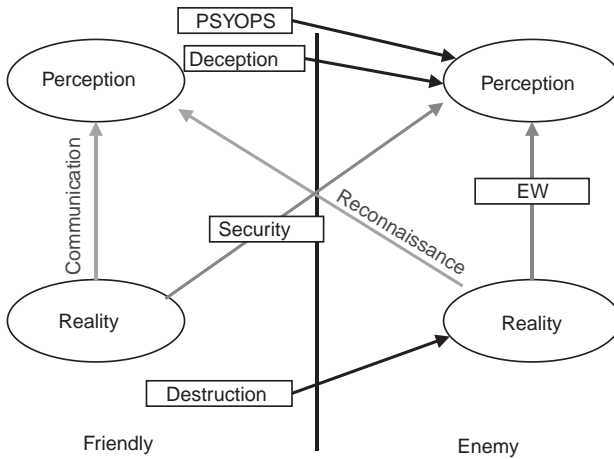


Figure 1.4 The elements of information warfare deal with friendly and enemy reality, and perception of reality.

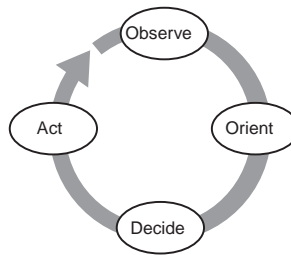


Figure 1.5 The OODA loop is the process involved in taking military action. IW interferes with the first three elements in the enemy's process.

military action. IW interferes with the first three steps in the OODA loop—with electronic warfare as the “action” element. This book focuses on EW, so we will not discuss IW further here, but it is important to understand the relationship between EW and IW in order to use EW techniques effectively in the current military environment.

1.3 How to Understand Electronic Warfare

It is the contention of the author that the key to understanding EW principles (particularly the RF part) is to have a really good understanding of radio

propagation theory. If you understand how radio signals propagate, there is a logical progression to understanding how they are intercepted, jammed, or protected. Without that understanding, it seems (to the author) that it is almost impossible to really get your arms around EW.

Once you know a few simple formulas, like the one-way link equation and the radar range equation in their dB forms—you will most likely be able to run EW problems in your head (to 1-dB accuracy). If you get to that point, you can quickly cut to the chase when facing an EW problem. You can quickly and easily check to see if someone is trying to break the laws of physics. (OK, a piece of scratch paper is allowed as long as it is crudely torn from a pad—your colleagues will still class you as an EW expert when you get them out of trouble.)

2

Threats

Electronic warfare is, by its nature, reactive to threats. EW receivers are designed to detect, identify, and locate threats, and EW countermeasures are designed to reduce the effectiveness of those threats. In this chapter, we look at threats in general: the classes of threats, the platforms they threaten, the signals associated with them, and the classes of countermeasures used against them.

2.1 Some Definitions

Like most fields, electronic warfare is practiced by professionals who use their own special language. Unfortunately, this language is often a variance with proper usage in the native tongue of the land. To avoid confusion in later discussions, here are some important definitions associated with EW threats.

2.1.1 Threats Versus Threat Signals

Threats are the actual destructive devices and systems. In EW, we normally deal with the signals associated with the threat systems, so we often define a “threat” as a signal associated with the actual threat. While this can be confusing, it is the way people in our profession express themselves—a grammatical “sin” we have been committing for many years—and will continue to commit throughout this book.

2.1.2 Radars Versus Communication

We often divide threat signals into radar and communications classifications. The differentiation is that radar signals are used to measure location, distance, and velocity—while communication signals carry information from one point to another. While they have totally different functions, the two types of signals can have similar parameters. Radar signals can be either pulsed or continuous wave while communication signals are, by their nature, continuous (except for rare special cases). Radar signals are typically in the microwave frequency range, but can be as low as high VHF and extend up into the millimeter range. Communications signals can carry voice or data. They are typically considered to be in the HF, VHF or UHF frequency range. However, they can be found from VLF to millimeter wave. (There will be more about frequency ranges a little later.)

2.1.3 Types of Threats

Figure 2.1 is an overview of the types of threats to assets protected by various electronic warfare techniques. Note that this chart is somewhat controversial since some new threats cross the normal classification divisions. The purpose of this chart is to show the normally expected threat applications. As shown, radar-guided weapons are primary threats to aircraft and ships. The primary threats to ground mobile and fixed sites are weapons that home on laser-designated targets. Heat-seeking missiles are a primary threat to aircraft. Lethal communication is described in Section 2.1.7. It is a primary threat to aircraft and fixed site assets—enabling a variety of types of weapons.

Lethal communication is described in Section 2.1.7. It is a primary threat to aircraft and fixed site assets—enabling a variety of types of weapons.

Type of Threat	Platform Threatened			
	Aircraft	Ships	Ground Mobile	Fixed Sites
Radar-Guided Weapons	●	●	◐	○
Laser-Guided Weapons	○	◐	●	●
Heat-Seeking Weapons	●	○	◐	○
Lethal Communications	●	◐	◐	●

● Primary Threat ◐ Secondary Threat ○ Not Normally

Figure 2.1 The various types of threats are normally threatening to these types of assets that are protected by EW systems.

2.1.4 Radar-Guided Weapons

As shown in Figure 2.2, radar is used to locate targets and to predict their paths of travel. A missile is guided to intercept the target. Note that the missile can be a rocket or a projectile (or many projectiles) from a radar-controlled gun. There are four basic guidance schemes that can be applied to radar-controlled weapons. Each has a different radar (or passive sensor) configuration and has strengths and weaknesses associated with the types of targets for which it is appropriate.

Ships are most commonly attacked by radar-controlled weapons. An aircraft (or other platform) locates a ship and identifies it as a target. Then, a missile is launched against the ship. Usually, the platform from which the missile is launched then leaves the engagement. When the missile gets close enough to the target to acquire it by radar, the missile homes on the ship, tracking its movement. The missile either attacks the target ship at the water line or makes a last minute vertical motion to strike it straight down through the deck.

2.1.5 Laser-Guided Weapons

Figure 2.3 shows an attack on a ground mobile target. The same technique can be used to attack a fixed asset, for example the pier of a bridge (the part most difficult to repair). In this type of attack, the laser must track the target so that a missile (which is typically fired by another platform) homes on the scintillation of the laser from the target. The designating platform can be either a manned or unmanned aircraft. It must remain within line of sight of the target during the whole attack.

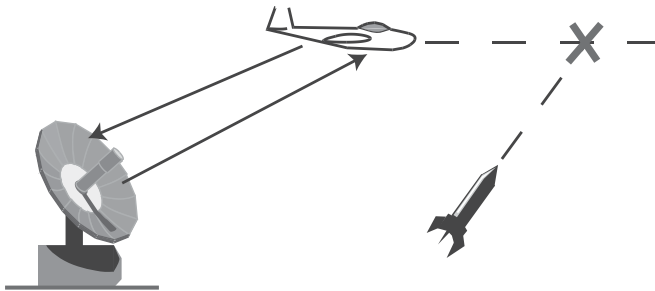


Figure 2.2 A radar-guided anti-air threat determines the location and motion vector of a target aircraft to predict its flight path and cause a missile to intercept that flight path using one of several guidance approaches.

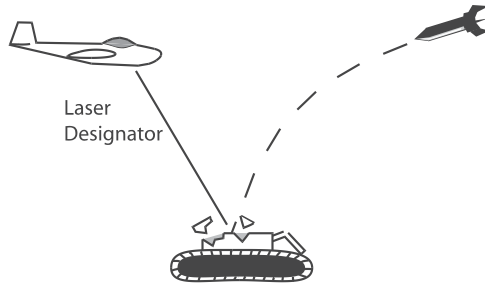


Figure 2.3 A laser-guided threat homes on the scintillation of a laser designator from a fixed or mobile target.

2.1.6 Infrared Energy: Guided Weapons

Everything emits some level of infrared energy (IR); the hotter the object, the more energy it emits. Since a jet aircraft engine is very hot, it provides a lucrative target for heat-seeking missiles. Early missiles attacked from behind the aircraft and homed on this high-heat target. Note that small, handheld weapons firing infrared missiles can be lethal to low-flying aircraft. IR missiles are used in air-to-air, ground-to-air, and air-to-ground attacks. Modern missile sensors can detect and home on the IR energy from targets at considerably lower temperature than that of a jet engine.

2.1.7 Lethal Communications

Lethal communications sounds like a contradiction in terms, since communication is merely the transfer of information. However, in almost all weapons above individual firearms, the information about the target's location and the ability to guide a weapon to the target are in different places. Thus, the sensor must transfer its information to some type of attack coordination center and that center must transfer acquisition and/or guidance commands to the actual weapon. The communication that transfers that information is extremely lethal.

Consider a simple example of lethal communication as shown in Figure 2.4. Artillery has killed more soldiers than any other type of weapon, and cannot typically engage targets without communication. The guns apply nonline-of-sight fire in response to calculated elevation, windage, and powder charge commands from a fire-control center. The fire-control center modifies its commands to the guns in response to communicated inputs from a forward observer who can see the target and the strikes of the rounds fired. Both communication paths are extremely lethal.

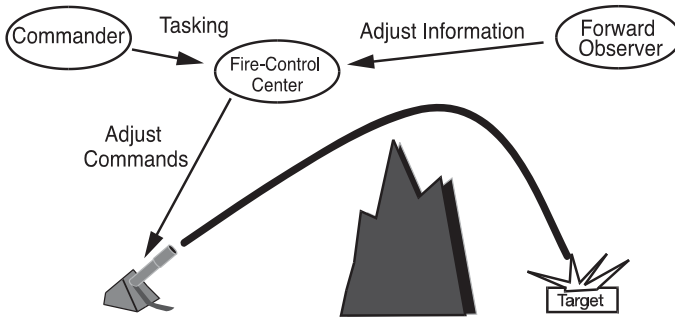


Figure 2.4 Artillery fire is adjusted to the target through lethal communication between a forward observer and a fire-control center and between the fire-control center and the guns.

2.1.8 Radar Resolution Cell

The resolution cell of a radar is the geometrical volume in which it cannot distinguish multiple targets. If there are multiple targets within the resolution cell, the radar will assume that only one target is present—at the weighted centroid of the individual target locations.

2.2 Frequency Ranges

Figure 2.5 shows the common names for frequency bands in the important threat range of 1 MHz to 100 GHz. This figure has three different columns, showing the three most common ways that frequency ranges are described. The left-hand column shows the common scientific notation. You will note that these bands divide at multiples of three. This is because each covers an order of magnitude of wavelength. For example, VHF is from 30 to 300 MHz—which corresponds to wavelengths from 1m to 10m.

The relationship of frequency to wavelength is given by the formula: $f\lambda = c$, where f is the frequency in hertz, λ is the wavelength in meters, and c is the speed of light (3×10^8 m/s).

The right-hand column shows the electronic warfare bands. The frequencies of threat radars are normally described in terms of these band designations. For example, D-band covers 1 to 2 GHz.

The middle column shows the official radar bands. Note that components (antennas, amplifiers, receivers, oscillators) are designated in catalogs in terms of these bands. It is also common to describe communications in terms of these bands. For example, satellite television broadcasting is done in C- or Ku-bands.