University of Cape Town
Introduction to Electronic Defence EEE5106F

P.F. Potgieter and J.D. Vlok

2 April 2012

Contents

1 Introduction

Electronic Defence (ED) is a military action whose ultimate aim is to control the electromagnetic spectrum (EMS). The objective is to exploit, reduce or prevent hostile use of the electromagnetic spectrum while still retaining friendly use thereof. Electronic Defence (ED) comprises of three main disciplines, which have found numerous electromagnetic (radio frequency (RF), optical etc.) as well as acoustic civilian and military applications.

1. Electronic Support (ES), previously known as Electronic Support Measures (ESM).
2. Electronic Attack (EA), previously known as Electronic Countermeasures (ECM).
3. Electronic Protection (EP), previously known as Electronic Counter-Countermeasures (ECCM).

These disciplines are shown in Figure 1 and are described in detail in subsequent study themes.

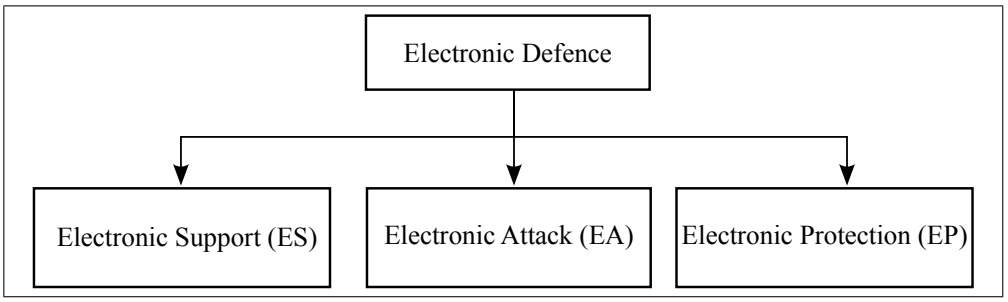

Figure 1: Breakdown of the main Electronic Defence disciplines.

2 Lecturer Information

Lecturer:	Mr. P.F. Potgieter
Office:	Building 44, Room B408
	CSIR Scienta Campus
	Brummeria, Pretoria
Telephone:	012 841-3151
Fax number:	012 841-2455
E-mail address:	pfpotgieter@csir.co.za
Consulting hours:	By appointment.
	The preferred method of contact is via e-mail.
Secretary:	Mrs. Mathabo Hlongwane
Telephone:	012 841-2822
Fax number:	012 841-2455
E-mail address:	mhlongwane@csir.co.za

3 Course Objectives and Study Themes

The course aims to introduce the student to Electronic Defence. A good prior knowledge on the topics of digital signal processing, electromagnetics, mathematics and statistics is highly recommended for this course. A relatively good knowledge of radar and a moderate knowledge of communications would be very beneficial to students. Students should be competent in using scientific programming languages such as Matlab or Octave.

Students have to master fundamental concepts in Electronic Defence on a high-level (identification of tactics and applications) as well as on a detail level (the design of a suitable detector to required specifications). Students are required to link theoretical concepts in Electronic Defence to typical applications and to solve problems of an engineering nature.

3.1 Theme 1: The History of Electronic Defence

Ever since long distance radio transmission was invented by Guglielmo Marconi, the potential to communicate and sense influenced the way militaries and societies function. Alongside this work, Heinrich Hertz showed that radio waves reflected off metallic objects, but it wasn't until the early 1930's when many nations independently developed their own versions of radar. Radar presented nations with a great tactical advantage and the countering thereof gave rise to what is now referred to as Electronic Defence.

Theme objective: To review how the developments in radar gave rise to Electronic Defence and how critical conflicts such as World War II, the Six-Day war and the first Gulf war shaped this kind of defence.

Study material: Lecture material as well as literature supplements and historical internet references.

Theme outcome: The student is required to identify the approach, techniques and mechanisms developed at each point in history that counteracted the capabilities of radar.

3.2 Theme 2: Overview of Electronic Defence

Since the early days, Electronic Defence has developed into such a critical capability that it has become a subject of study on its own. It has found applications in many domains such as communications, optronics, acoustics and cyber. The key to successful Electronic Defence is an intimate knowledge of the *target*, whether it be radar or infra-red (IR) missile seekers.

Theme objective: Given the historical developments of advanced sensors, the student will be exposed to the formal definition of Electronic Defence and the three main disciplines thereof. After a brief review of relevant radar and communication concepts, students will learn about the application of Electronic Defence.

Study material: The prescribed textbook, lecture material as well as literature supplements.

Theme outcome: The student is required to recognise and apply any of the main Electronic Defence principles to case studies. Case studies are typically formulated in a setting where radar and/or communications are exploited for a given objective.

3.3 Theme 3: Electronic Support

Practically every Electronic Defence operation starts by performing Electronic Support (ES). It provides the necessary information, description and intelligence to enable (or support) effective ED. Electronic Support is defined as *the search for, the interception, the location and the classification of sources of intentional and unintentional radiated EM energy.* The detection of low probability of intercept (LPI) emissions is very valuable. In turn the accurate estimation of emitter parameters would enable successful exploitation (via EA) or avoidance (via EP) thereof

Theme objective: The student will learn about the various approaches to ES against radar and communications systems. Here, the technical details and capabilities are presented that make each approach unique. LPI radar will be a case study and search, detection, location and classification principles are applied.

Theme material: The prescribed textbook, lecture material as well literature supplements.

Theme outcomes: The student is required to have an understanding of ES and be able to analyse emitter detectability and design (in concept) a suitable ES solution for a given scenario.

3.4 Theme 4: Electronic Attack

Electronic Attack (EA) deals with the deliberate actions taken to radiate or reflect EM energy in order to disable or degrade the EM spectrum to enemy capabilities. EA comprises of impairing, disrupting and deceiving enemy sensors (or assets) to gain control in a given scenario. A typical EA case would be an aircraft having to create phase front distortion towards a tracking radar in order to break it's track. There many different methods in EA are referred to as jamming, spoofing and deception jamming. EA may be categorised further into, active radiation of EM energy, passive EA (for example, chaff and passive decoys) and the reduction of radar observations of targets.

Theme objective: The student will learn about the various EA techniques and the radar or communications components that are targeted. Here, the technical details of EA are presented. Both radar and communication jamming will be cases of study.

Theme material: The prescribed textbook, lecture material as well as literature supplements.

Theme outcomes: The student is required to have an understanding of EA and be able to analyse jamming effectiveness and design (in concept) a suitable EA solution in a given scenario.

3.5 Theme 5: Electronic Protection

Actions taken to protect facilities and equipment from any effects of friendly or enemy EA is commonly referred to as Electronic Protection (EP). Many designers of radar and communication systems regularly make use of EP. The following strategies are regarded as *protecting* facilities against EA:

1. Overpowering of jammers.
2. Intelligent signal design to reduce jamming effectiveness.

3. Preventing receiver overload.
4. Radar versus jamming signal discrimination.
5. Avoiding jamming signals altogether.

Examples of EP are emissions control and communication security. By controlling where, when, how often and on which frequency you are transmitting the would-be jammer will find it difficult to meet all the conditions for effective EA. Furthermore, securing transmitted data using encryption protects the content of data even if it is intercepted.

Theme objective: The student will learn about the various aspects of EP. Here, the technical details of EP are presented.

Theme material: The prescribed textbook, lecture material as well as literature supplements.

Theme outcome: The student is required to have an understanding of EP and its relevance in radar and communication system design.

4 Prescribed Text and Relevant Material

Electronic Defence with all its components cover a broad scope of multiple topics, which make a single definitive text on it rather impossible. The prescribed text book will be used as a guideline, with reference to many other sources during the course. The prescribed book for this course and a short description thereof follows,

D. Curtis Schleher, *Electronic Warfare in the Information Age*, Artech House, 1999, ISBN 9780890065266.

This book is an advanced guide to the concepts and threats associated with modern Electronic Warfare (EW). It identifies and explains relevant radar and communications threats, and provides EW and radar engineers, managers, and technical professionals with practical, "how-to" information on designing and implementing EA and EP systems.

4.1 Relevant Material

The following text provides useful reference information that would supplement the content presented during lectures as well as the prescribed textbook. An electronic copy of this book will be made available on the course website.

Naval Air Systems Command, 1999, *Electronic Warfare and Radar Systems Engineering Handbook*.

5 Recommended Approach

It is strongly advised to interact and participate during the lecture week, as it provides the only opportunity for face-to-face contact time. The study material, assignments and the exam will be communicated during that week. Any interaction after the lecture week will be dealt with via e-mail. All the themes (and their respective assignments) are introduced and discussed before the next theme is considered.

6 Assessment

6.1 Grading Policy

This course is worth **15** credits toward the degree requirements for the Radar Masters Programme. The final mark for EEE5106F will consist of a combined assignment mark (50%) and an examination mark (50%).

6.2 Marking Guidelines

As a general guideline, each assessment component (assignments or exam) will be evaluated based on a the following levels (or corresponding marks) of grading:

- **0–Severely Deficient** (Essentially no attempt was made). There was nothing useful to evaluate and no marks could therefore be awarded.
- **1–Poor** (An attempt was made but mostly incorrect). Methodology, answers, results and/or implementations are mostly incorrect, superficial and have critical errors or problems. The answer shows little or no understanding and depth of the material. Presentation has fundamental problems in terms of structure, number of errors and technical quality.
- **2–Fair** (An attempt was made but contains many errors, with a minimal level of description). Methodology, answers, results and/or implementations are basically correct but have major errors or problems, or have limited depth. The answer shows a basic understanding of the material but limited depth. Presentation meets minimum standards but has significant problems in terms of structure, errors and technical quality.
- **3–Average** (A basic attempt was made with some errors, and a basic level of description). Methodology, answers, results and/or implementations are mainly correct but have moderate errors and detail, or are not optimal. The answer shows moderate depth and understanding of the material. Presentation is generally good but has minor problems in terms of structure, errors and technical quality.
- **4–Good** (A complete and correct attempt together with sufficient level of description). Methodology, answers, results and/or implementations are mainly correct and detailed but have minor errors, or are not optimal. The answer shows a very good depth and understanding of the material. Presentation is mostly well-structured and error free, and of good technical quality.
- **5–Excellent** (A comprehensive and detailed submission). Answers and results are correct and detailed, as is the working and methodology used to obtain them. The answer shows an excellent, deep and synthesised understanding of the material. A degree of critical analysis is evident and alternatives have been explored. Additional research has been done (as appropriate) and references have been provided. The implementations are flexible and modular facilitating application on new problems. The material is well-structured, error free and of high technical quality.

6.3 Assignments

There are three (3) assignments scheduled for this course. Each assignment will test the student's ability to apply the concepts learned during each study theme. Each assignment will be introduced during the lecture week and are due at 13:00 on the day specified in the course schedule. Assignments must be submitted electronically and must be self contained in a single document, unless specified otherwise. The combined score for all assignments will count 50% towards the final mark.

6.3.1 Late Assignments

Any assignment submitted late will be penalised as follows;

- A maximum mark of 65% can be obtained for assignments up to one (1) day late.
- A maximum mark of 50% can be obtained for assignments up to two (2) days late.
- A maximum mark of 40% can be obtained for assignments up to three (3) days late.
- Any assignment handed in later than three (3) days after the deadline will not be accepted for marking.

6.3.2 Declaration of Originality

Plagiarism is considered a serious offence by the University of Cape Town. Whenever you do written work you must differentiate between your own ideas and those, which you did not think of yourself, but which you have read elsewhere. You must distinguish what you have written from what you are quoting and your own work. The University of Cape Town requires that all material submitted, including assignment answers to be accompanied by a signed Declaration of Originality. The first page of any submitted material must be a title-page. The second page must be the signed declaration. A template of the declaration provided in Appendix A. **NOTE: No assignments will be accepted for marking without a signed declaration**.

Students may choose their own convention of attribution and acknowledgement in written work. The preferred style of referencing for engineers is that of the Institute of Electrical and Electronics Engineers (IEEE), for more information students may consult the IEEE Style Manual.

For more information on plagiarism and the University's policy, students are encouraged to familiarise themselves with guidelines to avoiding plagiarism at the following link. The **Library Staff**, the **Writing Centre** and the **Centre for Information Literacy** are willing to assist students, by providing details of referencing conventions, and help in using them.

6.4 Exam

The exam will test the student on every study theme in the course. It is a three (3) hour closed-book written exam and will comprise of both theory and problems. The total exam score will count 50% towards the final mark.

7 Course Schedule 2012

Date	Event
7 to 11 May	Thematic lectures and contact time
21 May	Assignment 1: History and introductory concepts
25 May	Assignment 2: Electronic Support
1 June	Assignment 3: Electronic Attack and Protection
12 June	Exam (on all study themes)

Lectures will be held in the L6 Seminar Room, Level 6, George Menzies building, Library Road, Upper Campus. Practical sseions will be held in the Blue Lab.

7.1 Lecture Programme

Time	Monday 7 May	Tuesday 8 May	Wednesday 9 May	Thursday 10 May	Friday 11 May
08h00	Welcome and Course Overview	Theme 3: ES Introduction	ED in Communications	Theme 4: EA Introduction	Theme 5: EP Introduction
09h00	Theme 1: History of ED	Emitter Search and Detection	ED in Communications	Expendables and Decoys	Sidelobe Blanking and Cancellation
10h00	History of ED	Emitter Location and Classification	ED in Communications	EA Techniques	RCS Reduction and Stealth
11h00	**Tea**				
11h30	Theme 2: ED Overview	Signal Deinterleaving and LPI Intercept	Communications ED Practical	Cross-eye Jamming and Directed Energy	EP for Search and Tracking radar
12h00	Overview of ED	Receiver Architectures	Wrap-up of Theme 3 and Assignment 2	EA System Architectures	Wrap-up of Theme 5 and Assignment 3
12h30	**Lunch**				
13h30	ED Fundamentals	ES Practical	Excursion	EA Practical	Course Conclusion and Exam Briefing
14h30	ED Fundamentals	ES Practical	Excursion	EA Practical	
15h30	**Tea**		Excursion	**Tea**	
16h00	Wrap-up of Theme 1 - 2 and Assignment 1	ES Practical	Excursion	Wrap-up of Theme 4	
17h00	**Close**				

The excursion will be a visit to The Institute for Maritime Technology at 14h00. IMT performs defence research to satisfy South African Ministry of Defence strategic needs for techno-military support, products and services and to establish applicable technology and systems to further the interest of the South African National Defence Force (SANDF).

A Declaration of Originality Template

DECLARATION OF ORIGINALITY

UNIVERSITY OF CAPE TOWN

INTRODUCTION TO ELECTRONIC DEFENCE
EEE5106F

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use anothers work and pretend that it is ones own.
2. I have used the _____ convention for citation and referencing. Each contribution to, and quotation in, this assignment/report/_____ from the work(s) of other people has been attributed, and has been cited and referenced.
3. This assignment/report/_____ is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.
5. I acknowledge that copying someone elses assignment or essay, or part of it, is wrong, and declare that this is my own work.

Student Name: _____

Signature: _____

Date: _____