



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**NET-CENTRIC CONTROLLED DISTRIBUTED STAND-IN-  
JAMMING USING UAVS—TRANSMISSION LOSSES AND  
RANGE LIMITATIONS DUE TO GEO-LOCALIZATION  
PROBLEM OVER TURKISH GEOGRAPHY**

by

Ali Kaptan

September 2012

Thesis Co-Advisors:

David Jenn  
Edward Fisher

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
<b>1. AGENCY USE ONLY (Leave blank)</b>	<b>2. REPORT DATE</b> September 2012	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE</b> Net-centric Controlled Distributed Stand-in-Jamming using UAVs-Transmission Losses and Range Limitations Due to Geo-localization Problem Over Turkish Geography		<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Ali Kaptan			
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000		<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A		<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited		<b>12b. DISTRIBUTION CODE</b> A	
<b>13. ABSTRACT (maximum 200 words)</b>  Network Centric Warfare (NCW) and swarming have become very important operational terms parallel to the improvements in wireless network technologies. These relatively new concepts are being widely used in many operational applications. The main purpose of this research effort is to examine the metrics of NCW, and the use of unmanned aerial vehicle (UAV) swarms in electronic attack (EA) missions.  UAVs have already been used in many military operations. Swarming a number of small UAVs in a distributed beamforming approach to have the desired operational effect is the current popular research area. Distributed beamforming and swarm behavior of self-synchronized autonomous UAVs are investigated in this study.  Two simulation scenarios were created and implemented to show the effectiveness of EA against radars and wireless communication links. In reality, EA against a single node in a network, such as a radar or communication link, is unlikely to be successful by itself, however simulation results showed that the decision making process of the enemy network and OODA (Observe, Orient, Decide, Act) cycle is directly vulnerable to jamming.			
<b>14. SUBJECT TERMS</b> Distributed Beamforming, UAV, Swarm, Swarming, EA, Electronic Attack, Simulation, Network Centric Warfare, NCW		<b>15. NUMBER OF PAGES</b> 97	
		<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**NET-CENTRIC CONTROLLED DISTRIBUTED STAND-IN-JAMMING USING  
UAVS - TRANSMISSION LOSSES AND RANGE LIMITATIONS DUE TO GEO-  
LOCALIZATION PROBLEM OVER TURKISH GEOGRAPHY**

Ali Kaptan  
1<sup>st</sup> Lieutenant, Turkish Air Force  
B.S., Turkish Air Force Academy, 2006

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN ELECTRONIC WARFARE  
SYSTEMS ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2012**

Author: Ali Kaptan

Approved by: David Jenn  
Thesis Co-Advisor

Edward Fisher  
Thesis Co-Advisor

Dan Boger  
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Network Centric Warfare (NCW) and swarming have become very important operational terms parallel to the improvements in wireless network technologies. These relatively new concepts are being widely used in many operational applications. The main purpose of this research effort is to examine the metrics of NCW, and the use of unmanned aerial vehicle (UAV) swarms in electronic attack (EA) missions.

UAVs have already been used in many military operations. Swarming a number of small UAVs in a distributed beamforming approach to have the desired operational effect is the current popular research area. Distributed beamforming and swarm behavior of self-synchronized autonomous UAVs are investigated in this study.

Two simulation scenarios were created and implemented to show the effectiveness of EA against radars and wireless communication links. In reality, EA against a single node in a network, such as a radar or communication link, is unlikely to be successful by itself, however simulation results showed that the decision making process of the enemy network and OODA (Observe, Orient, Decide, Act) cycle is directly vulnerable to jamming.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>MOTIVATION .....</b>	<b>2</b>
<b>B.</b>	<b>RESEARCH SCOPE AND PREVIOUS WORK.....</b>	<b>2</b>
<b>C.</b>	<b>GENERAL REVIEW .....</b>	<b>3</b>
<b>1.</b>	<b>Background .....</b>	<b>3</b>
<b>2.</b>	<b>Defining the Problem.....</b>	<b>4</b>
<b>3.</b>	<b>Thesis Outline.....</b>	<b>5</b>
<b>II.</b>	<b>ELECTRONIC WARFARE BASICS AND DEVELOPMENT OF UAVS .....</b>	<b>7</b>
<b>A.</b>	<b>ELECTRONIC WARFARE ELEMENTS.....</b>	<b>8</b>
<b>1.</b>	<b>Electronic Attack (EA) .....</b>	<b>9</b>
<b>2.</b>	<b>Electronic Protection (EP) .....</b>	<b>9</b>
<b>3.</b>	<b>Electronic Warfare Support (ES).....</b>	<b>10</b>
<b>B.</b>	<b>DEVELOPMENT OF UAVS.....</b>	<b>10</b>
<b>1.</b>	<b>History of UAV Systems.....</b>	<b>10</b>
<b>2.</b>	<b>Classification of UAVs.....</b>	<b>13</b>
<b>a.</b>	<i>Classification by Weight .....</i>	<i>13</i>
<b>b.</b>	<i>Classification by Endurance and Range.....</i>	<i>14</i>
<b>c.</b>	<i>Classification by Flight Ceiling.....</i>	<i>14</i>
<b>d.</b>	<i>Classification by Wing Loading .....</i>	<i>14</i>
<b>e.</b>	<i>Classification by Engine Type .....</i>	<i>15</i>
<b>III.</b>	<b>NETWORK CENTRIC WARFARE AND SWARM NETWORKS .....</b>	<b>17</b>
<b>A.</b>	<b>SWARM NETWORKS AND DISTRIBUTED BEAMFORMING WITH UAV SWARMS.....</b>	<b>17</b>
<b>1.</b>	<b>Swarm Behavior.....</b>	<b>17</b>
<b>2.</b>	<b>Distributed Beamforming with UAV Swarms .....</b>	<b>17</b>
<b>B.</b>	<b>NETWORK CENTRIC WARFARE .....</b>	<b>21</b>
<b>1.</b>	<b>Origins of Network Centric Warfare.....</b>	<b>22</b>
<b>2.</b>	<b>Fundamentals of Network Centric Warfare .....</b>	<b>26</b>
<b>3.</b>	<b>Network Centric Warfare Metrics.....</b>	<b>27</b>
<b>a.</b>	<i>Connectivity Measure .....</i>	<i>28</i>
<b>b.</b>	<i>Network Reach.....</i>	<i>33</i>
<b>c.</b>	<i>Network Richness.....</i>	<i>33</i>
<b>d.</b>	<i>Characteristic Tempos .....</i>	<i>34</i>
<b>IV.</b>	<b>RADARS AND RANGE EQUATIONS.....</b>	<b>35</b>
<b>A.</b>	<b>BASIC RADAR PRINCIPLES.....</b>	<b>35</b>
<b>1.</b>	<b>Clutter .....</b>	<b>35</b>
<b>2.</b>	<b>Radar Range Equation.....</b>	<b>36</b>
<b>3.</b>	<b>Signal-to-Noise Ratio .....</b>	<b>39</b>
<b>4.</b>	<b>Radar Cross Section (RCS).....</b>	<b>42</b>
<b>B.</b>	<b>RADAR ELECTRONIC COUNTER MEASURES .....</b>	<b>44</b>
<b>1.</b>	<b>Self-Screening Jamming (SSJ).....</b>	<b>46</b>

2.	Stand-off Jamming.....	47
3.	Jammer Burn-through Range .....	47
V.	<b>RADAR AND NETWORK ELECTRONIC COUNTER MEASURES SIMULATION .....</b>	<b>49</b>
A.	<b>SURVEILLANCE RADAR EA SIMULATION .....</b>	<b>49</b>
1.	Scenario.....	49
2.	Parameters and Calculations.....	50
3.	Simulation Results .....	53
B.	<b>INFORMATION NETWORK EA SIMULATION.....</b>	<b>57</b>
1.	<b>3-Node NEADS Simulation .....</b>	<b>58</b>
a.	<i>Simulation Setup</i> .....	59
b.	<i>Simulation Results</i> .....	60
2.	<b>3-Node NEADS with UAV Jammer Swarm Simulation .....</b>	<b>61</b>
a.	<i>Simulation Setup</i> .....	62
b.	<i>Simulation Results</i> .....	63
VI.	<b>CONCLUSIONS AND RECOMMENDATIONS.....</b>	<b>67</b>
A.	<b>SUMMARY .....</b>	<b>67</b>
B.	<b>CONCLUSIONS .....</b>	<b>68</b>
C.	<b>RECOMMENDATIONS FOR FUTURE WORK.....</b>	<b>69</b>
	<b>APPENDIX.....</b>	<b>71</b>
	<b>LIST OF REFERENCES.....</b>	<b>75</b>
	<b>INITIAL DISTRIBUTION LIST .....</b>	<b>79</b>

## LIST OF FIGURES

Figure 1.	Unmanned Aerial Vehicle (UAV) (From [1]).	1
Figure 2.	Electromagnetic Spectrum (From [7]).	7
Figure 3.	Electromagnetic Warfare Elements	8
Figure 4.	(a) Antenna beam formed by a single UAV and (b) Antenna beam formed by a UAV swarm	18
Figure 5.	Synchronization and Relay Nodes	19
Figure 6.	Geometrical Positions and Notations (After [15]).	20
Figure 7.	Platform-Centric Weapon System (After [17]).	24
Figure 8.	Platform-Centric Engagement Envelope (After [17]).	25
Figure 9.	Network-Centric Operations (After [17]).	25
Figure 10.	The OODA Cycle	27
Figure 11.	Connectivity Link Calculations Example with Three Nodes (After [21]).	29
Figure 12.	Realistic Network with Four Nodes and Heterogeneous Links	32
Figure 13.	Corresponding Reference Network for Figure 12	32
Figure 14.	Time Spent in Each Phases of the OODA Cycle (after [24]).	34
Figure 15.	Basic Components of Radar Transmit/Receive Cycle (After [27]).	36
Figure 16.	(a) Bistatic Radar (b) Monostatic Radar	37
Figure 17.	Ideal Band-limited Filter Response (After [28]).	40
Figure 18.	Special Case – Antenna as a Target (After [28]).	43
Figure 19.	Radar Coverage and RECM Scenario – Stand-off (Stand-in) Jamming	45
Figure 20.	SIJ Configuration	49
Figure 21.	Jammer Configuration	52
Figure 22.	RADJAM GUI Inputs	53
Figure 23.	Detection Contour without Jamming	54
Figure 24.	Azimuth Antenna Pattern	55
Figure 25.	Detection Contour with Jamming	55
Figure 26.	SJR versus Detection Range	56
Figure 27.	Target and Jammer Signals versus Range Normalized to Burn-through Range	57
Figure 28.	NEADS Operational Network without Jammer	58
Figure 29.	NEADS Topology without Jammer	59
Figure 30.	NEADS Topology without Jammer Simulation Results	61
Figure 31.	NEADS Operational Network with UAV Jammer	62
Figure 32.	NEADS Topology with UAV Jammer	63
Figure 33.	Trends of Reference Connectivity Measure and Connectivity Measure	65
Figure 34.	Trend of Reference Network Reach	65
Figure 35.	Trends of OODA Cycle Tempos	66

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Important Statistics of V-1 Campaign (After [9]).....	12
Table 2.	Classification of UAVs.....	15
Table 3.	Available Links in Figure 10.....	30
Table 4.	All Possible Routes in Figure 10.....	30
Table 5.	Connectivity Measure Calculations for Figure 10.....	31
Table 6.	Connectivity Measure Calculations for Different $N_T$ Values.....	33
Table 7.	Typical RCS Values of Some Organisms and Objects (After [28]).....	43
Table 8.	Air Surveillance Radar Operating Parameters.....	50
Table 9.	Airborne Target Specifications.....	51
Table 10.	Jammer Operating Parameters.....	53
Table 11.	NEADS Link Connections without Jammer.....	59
Table 12.	NEADS Simulation Setup without Jammer.....	60
Table 13.	NEADS Link Connections with UAV Jammer.....	62
Table 14.	NEADS Simulation Setup with UAV Jammer.....	63
Table 15.	NEADS with UAV Jammer Simulation Results.....	64

THIS PAGE INTENTIONALLY LEFT BLANK

## **LIST OF ACRONYMS AND ABBREVIATIONS**

ADC	Analog to Digital Converter
AOI	Area of Operational Interest
ARM	Anti Radiation Missile
BLOS	Beyond Line of Sight
DBF	Distributed Beamforming
EA	Electronic Attack
EM	Electromagnetic
EMS	Electromagnetic Spectrum
EP	Electronic Protection
ERP	Effective Radiated Power
ES	Electronic Support
EW	Electronic Warfare
GUI	Graphical User Interface
HVAA	High Value Air Asset
MDP	Minimum Detectable Power
NCO	Network Centric Operations
NCW	Network Centric Warfare
NCWC2C	Network Centric Warfare Command and Control Center
NEADS	Netted Enemy Air Defense System
NECM	Network Electronic Counter Measures
OODA	Observe, Orient, Decide, Act
RCS	Radar Cross Section
RECM	Radar Electronic Counter Measures

RMS	Root-Mean-Square
RRE	Radar Range Equation
SAM	Surface-to-air Missile
SEAD	Suppression of Enemy Air Defense
SIGINT	Signal Intelligence
SIJ	Stand-in Jamming
SNR	Signal to Noise Ration
SOJ	Stand-off Jamming
SSJ	Self-screening Jamming
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
WSN	Wireless Sensor Network

## **ACKNOWLEDGMENTS**

I would love to express my deepest respect and appreciations to Turkey and Turkish Air Force for giving me the chance to graduate from Naval Postgraduate School. It was a valuable and wonderful experience for my wife and me.

I would also like to thank to my lovely wife, Esra, for her patience, contributions, love and existence as an illuminator in my life. Thank you for your being my wife and mother of our little daughter, Beril Ela.

Finally, I appreciate the precious efforts of Professor David C. Jenn and Mr. Edward L. Fisher to guide me during this thesis research.

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), looking at the technology from the military perspective, are currently being used for missions in critical environments with intense threats without risk to personnel. While the history of vehicles similar in many respects to modern UAVs goes back to World War II, their use has become common of late due to improvements in electronic and software technologies that make it possible to develop cost efficient and well performing systems.

Beyond the desire for flying an aircraft unmanned, the potential applications of such systems have become an area of interest for many governmental and non-governmental organizations. Because of their “unmanned” feature, UAVs were first met with a large degree of skepticism. This was countered with the reality that separation of a human from the aircraft physically not only eliminated the risk of loss of life, but also led to economic savings on manufacturing and operating costs.

UAVs have been and are currently being used for many military operations, ranging from reconnaissance to intelligence missions and from missile attack to radio relay missions. Electronic Warfare (EW) applications, such as electronic attack using UAVs, are gaining acceptance over time.



Figure 1. Unmanned Aerial Vehicle (UAV) (From [1]).

Every new development in warfare illuminates an idea in the opponents mind about the counter measure to be used against new ideas. Today’s technology and complex

warfare environment requires smaller platforms that are easy and cheap to manufacture, transport, maintain, use, and are survivable. With all of these properties and smaller radar cross-sections, UAVs are playing a crucial role for military operations. Specifically, as the main research area of this thesis, electronic attack (EA) missions using UAVs engaging in swarm tactics within network centric warfare is attractive to many countries around the globe.

## **A. MOTIVATION**

As stated earlier, UAVs are gaining importance for military and non-military applications all over the world. Parallel to the improvement in UAV capabilities, the Turkish Armed Forces updates its own tactical and strategic requirements. Commensurate with this, the aviation industry works to develop national UAV prototypes designed for the needs of the Turkish Military. It is obvious that the engineering, design and manufacturing processes of such advanced systems are complicated and cannot be developed in isolation from real world experiences.

This project will try to put forward some basic fundamentals of electronic warfare, limitations associated with the electromagnetic spectrum and geographical properties of the Turkish terrain. Of course this is not a unique or complete supplement for the decision makers, but most probably will provide a fresh perspective on EW.

## **B. RESEARCH SCOPE AND PREVIOUS WORK**

One previous NPS master's thesis undertaken by Kocaman [2] stimulated the main idea of this research. He asked the question "How can distributed beamforming and opportunistic array concepts be applied to UAV swarms?" and tried to find possible solutions to the main challenges in realizing wireless beamforming in a swarm UAV network and several military applications [2]. At the end of the research, he outlined some key challenges related to the scope of using UAVs in electronic warfare.

Another NPS master's thesis written by Erdemli [3] constructed a broad guide to UAS employment for EW purposes, as stated in the declaration of thesis scope. Certainly, it is not a new idea to use UAVs for EW missions. When examined from the swarm UAV

perspective, EW missions are very prone to some limitations that confine the capabilities of current systems. These limitations provided the basic motivation for this thesis.

The required data links and wireless networks used to conduct any net-centric controlled distributed electronic warfare missions have some limitations. One of the most important limitations is transmission losses due to range and geo-localization problems. Although transmission losses are a general problem for communications systems in any domain, they are more severe for wireless communications. These limitations can easily be addressed to the local position of the UAV inside the battlefield. In other words, geographic position of the area defines the capability of the data link, and mission effectiveness of a single or a swarm of UAVs.

Unmanned aerial vehicles are increasingly important in today's electronic warfare environment. There is a considerable trend toward research on operations of net-centric controlled distributed electronic warfare using UAVs and other low cost lower performance platforms.

UAVs and their subsystems, used for both civilian and military applications are a very wide area of research. In this thesis, the scope is confined to the effectiveness and performance of UAVs in a net-centric controlled distributed environment, given transmission losses and geographical limitations due to geo-localization problems within Turkish terrain. Radiated power requirements, range limitations and associated transmission losses, and the geo-localization problem will be analyzed and an optimal solution will be proposed at the end of the research.

## **C. GENERAL REVIEW**

### **1. Background**

In today's information age, every step taken to destroy or weaken enemy forces motivates a counter measure to reduce or completely eliminate the effectiveness of the associated attack. In the past, human actions occupied the center of all measures, and conceptually affected the warfare environment. But, modern warfare conceptually seeks optimal solutions to conduct missions with smaller, cheaper, and in many cases now, unmanned systems. UAVs have proven their success through the increase in war-fighting

capabilities of armies in real operations. Because of their contributions, many nations and militaries around the world have re-configured their military aviation branch. The Turkish Air Force is one of the more active users of UAVs and there are many ongoing national and international projects associated with this relatively new Unmanned Aerial System (UAS) concept.

Finally, as stated in the scope of this research, advantages of UAVs can be examined with these limitations in mind and an optimal solution can be achieved and modeled for stand-in jamming missions. Stand-in jamming is very similar to stand-off jamming. However, stand-in jammers require less effective radiated power, with the major difference being the position of the jammers. Stand-in jammers conduct missions much closer to the target than the stand-off jammers can. This helps the electronic attack mission by shortening the burn through range. Burn through range can be explained as the range at which the enemy radar overcomes the jamming effect.

## **2. Defining the Problem**

As one of the main elements in today's modern battlefield, many articles, papers and reports have been published on UAVs. Parallel to this, a significant amount of development has been achieved on the capabilities of UAVs. As stated earlier, this research will mainly focus on electronic warfare applications of these low-cost unmanned combat systems. Using UAVs in electronic warfare has a lot of associated advantages. Some of these are:

- They require low power.
- Their observability is relatively low.
- They have a reduced risk.
- They may be more cost-efficient.
- Their mission sustainability is higher.
- They can be less vulnerable to enemy weapons.

The employment of UAVs in various battle scenarios, both for training purposes and real war-fighting missions, stimulated the idea to deploy teams of multiple UAVs in a cooperative or competitive manner [4]. Teams of multiple UAVs can be thought of as a

swarm. Swarm characteristics can be seen among the collaborative insects and other animals within nature. These groups of insects, such as ants and bees, create a “swarm intelligence” as a result of their workload feedback. In another NPS thesis, Frantz [5] explained the intelligence created by the swarm. According to Frantz, the self-organization of the group into ordered patterns is an intelligent characteristic. For a swarm to form ordered patterns, it needs to ‘analyze’ patterns while finding the optimal method [5]. This is exactly the workload feedback, mentioned as the source for emergence of swarm intelligence. The interactions among the autonomous individuals within the swarm rely on mutual local sensing.

We can easily talk about a communication requirement for the swarm. In a general sense, this is a wireless communication medium. Wireless communication is much more vulnerable to external effects. These effects can be due to geo-localization problems or to other intruders sharing the same battlefield, as in the case of an enemy. As well as enemy ground EW emissions, the threat can also be an aerial aggressor. The other main source of trouble can be addressed as range limitations due to the localization problem. This research will help to understand limitations due to range and geographical conditions over an operational area of interest, specified as Turkish terrain. Transmission characteristics in this specific geography and associated limitations will help the Turkish Air Force decide how to optimally use or develop current and future systems.

### **3. Thesis Outline**

Before investigating new electronic warfare applications of UAVs, a proper background for the research starts with a literature review and historical milestones. This research effort will start with a review of current electronic warfare elements and subdivisions. By the end of the review, the use of unmanned aerial vehicles and systems in EW applications will be thoroughly discussed in Chapter II. By doing so, we will attempt to answer some basic questions:

- What is the historical background of electronic warfare?
- What are the elements of electronic warfare?
- What are the electronic attack techniques?

- What is stand-in jamming and how can UAVs be used for electronic attack?

After this literature review, the net-centric controlled distributed operations and will be discussed to address the following questions in Chapter III:

- What is network-centric distributed warfare?
- What is the radar range in a jamming environment?

The previous review will help in the study of radar range equation in the network environment, data link limitations and propagation losses due to range, presented in Chapter IV. The geo-localization problem over Turkish terrain will also be examined in this chapter:

- What are the radar equations?
- What are the data link limitations and propagation losses due to range?

Chapter V will concentrate on optimizing and modeling stand-in techniques with a single UAV. Essentially, a single typical (small) UAV is often not capable of conducting such missions without any being engaged in a collective effort. Because of their relatively small size compared to manned aircraft, UAVs have some limitations in payload capacity and power generated that directly affect provided jammer power. But, taken as a collective whole, the individual abilities of single UAVs inside the swarm can easily make up the required parameters. Likewise, addressing another common concern with modern net centric warfare, transmission limitations and vulnerabilities for a UAV swarm can be eliminated with one or more radio relay UAVs incorporated as elements of the swarm and network.

Finally, Chapter IV will include conclusions and recommendations for future research.

## II. ELECTRONIC WARFARE BASICS AND DEVELOPMENT OF UAVS

According to Schleher's definition, electronic warfare (EW) is a military action whose objective is to control the electromagnetic (EM) spectrum [6]. Of course, the EM spectrum is not typically considered as solely an operational area of military organizations. As well as military usage, the spectrum is used heavily for civilian purposes. We limit the discussion to military use of the spectrum, and thus the very first definition implies the military use of EM and directed energy. The success of EW can largely be measured by the successful control of the EM spectrum.

The electromagnetic spectrum (EMS) is a construct of the range and allocations of frequencies from zero to infinity by which EM radiation through free space (versus wired) is defined. In other words, we can state the EMS as the band designations of EM radiation. Figure 2 shows the EMS [7].

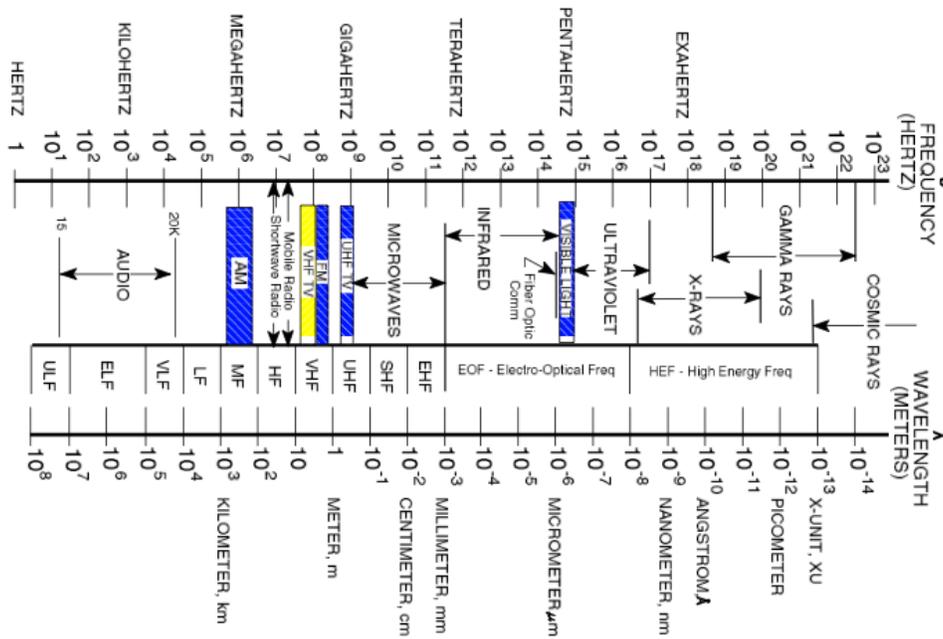


Figure 2. Electromagnetic Spectrum (From [7])

The EMS can also be defined as the carrier domain for the required information before, during, and after military operations. As well as denying the usage of the EMS by the enemy, EW also tries to maintain safe and reliable information sharing between friendly assets. Looking from this perspective, EW can easily be placed as a component under Information Warfare (IW).

### A. ELECTRONIC WARFARE ELEMENTS

Electronic Warfare is one of the crucial elements of war fighting in the modern battle management concept. The definition of EW addresses any military action involving the use of electromagnetic and directed energy to control the critical information within the battle environment or to attack the enemy. According to U.S. and other nation doctrines, the three main subdivisions within electronic warfare are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). These are modern definitions of EW elements, which are revised from previous military terminology. The corresponding names for former definitions are respectively electromagnetic countermeasures (ECM), electromagnetic counter-countermeasures (ECCM), and electronic warfare support measures (ESM) [6]. These earlier terms are still in common use within the industry.

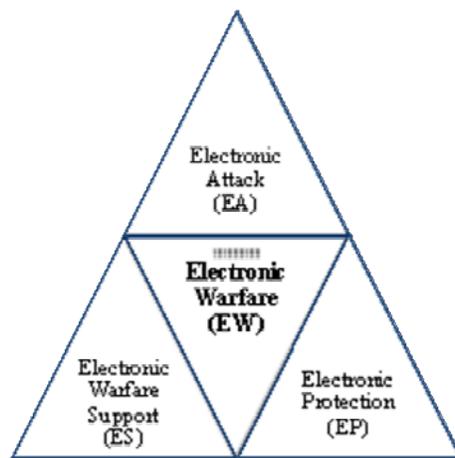


Figure 3. Electromagnetic Warfare Elements

We should have a quick look at the definition of IW before going further. Again, Schleher [6] defines IW as a broad military concept, whose objective is to control the management and use of information to provide military advantage. IW operations are two sided, which corresponds to both attacking the enemy to prevent critical information from being used by the opponent and ensuring one's own information systems are protected against an enemy's IW measures.

### **1. Electronic Attack (EA)**

The EA subdivision of EW involves the use of electromagnetic or directed energy to attack personnel, facilities or equipment with the intent of degrading, neutralizing or destroying enemy combat capability [6]. EA was previously known as Electronic Counter Measures (ECM). EA has two different means of taking offensive action to interrupt or attack the enemy use of the EMS. Non-destructive EA ("soft kill") prevents or reduces the use of enemy weapon systems. Electronic jamming and deception are two typical types of non-destructive EA. Non-destructive EA, as understood from the name, does not intend to destroy enemy weapons physically. Conversely, destructive EA ("hard kill") uses Anti-Radiation Missiles (ARMs) and directed energy to attack and potentially destroy enemy capabilities.

### **2. Electronic Protection (EP)**

Electronic Protection (EP), formerly known as Electronic Counter Counter Measures (ECCM), defines all active and passive measures taken to protect one's own assets including personnel, facilities and equipment against an aggressor's use of electromagnetic or directed energy. The word "aggressor" is used because the effective EA could either be employed by friendly sources or by an enemy. Because of the cause and effect relationship between EA and EP, Schleher [6] called it "a battle of resources," with the advantage going to the side that invests the most resources. A few examples of EP are electronic masking, the use of wartime reserve modes (WARM), electronic hardening, emission control (EMCON), and the integration of EW systems into overall spectrum management [6].

### **3. Electronic Warfare Support (ES)**

It is obvious that the electromagnetic spectrum is also, intentionally or unintentionally, used by the enemy. We need adequate real time information about enemy EMS activities. The ES subdivision of EW includes intercepting, identifying, analyzing, and locating enemy radiation activities. We can generalize these activities as the parameters of enemy radiation. ES includes actions tasked by, or under direct control of an operational commander [7]. The data collected by ES means can help to produce signal intelligence (SIGINT). It is a very common mistake to confuse these two overlapping disciplines. The nuance between these two are defined in [8] as:

The distinction between intelligence and ES is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. ES is achieved by assets tasked or controlled by an operational commander. The purpose of ES tasking is immediate threat recognition, targeting, planning and conduct of future operations, and other tactical actions such as threat avoidance and homing. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements.

In this research, we deal with EW and its subdivisions. Intelligence and related subdivisions are out of the scope of this thesis.

## **B. DEVELOPMENT OF UAVS**

### **1. History of UAV Systems**

The importance of UAVs for both military operations and civilian purposes is growing at a rate equal to their widened scope of employment. UAVs have certain unprecedented advantages. Some of the most important ones are:

- They are smaller and cheaper compared to manned aerial vehicles, therefore they are affordable for many purposes.
- Their capacity is not limited by human factors, especially physical human capabilities, making them easier to develop and maintain.
- They typically have a somewhat smaller radar cross section (RCS), which makes their observability relatively low.

- They can get closer to the operational area of interest or the target, increasing the capability of tactical and operational forces to beyond line of sight (BLOS).

Looking from a historical perspective, early thoughts on unmanned flying objects can be dated back to the early days of aviation itself. The desire to see what is happening beyond natural obstacles was not new at the time, even when the first aircraft was invented. On the other hand, sending weapons or bombs to distant targets was always a technological objective. In the following paragraphs, we look at the early history of UAVs, to see the emerging idea and early development period.

In comparison, the emergence of modern UAVs is fairly recent. At the beginning of the 1900s, UAVs were used experimentally for research. The pre-World War I (WWI) period witnessed a few unsuccessful research projects to employ UAS for military use. The United States, Britain and Germany all tried to develop unmanned attack systems during the war. Even though none of these experimental designs proved to be operationally effective, these efforts led to the development of the first missiles; the guidance system requirement remained largely unsolved until the interwar years. These projects were commonly called flying bombs during this experimental period. Although they were not conventional UAVs by the modern definition, their radio guidance systems developed the fundamentals of controlling the UAVs. At the end of this period, the very first successful radio-controlled unmanned target aircraft “Fairey Queen” entered the British Armed Forces service [9].

Confined by economic conditions and treaty restrictions, German engineers started to think about the war fighting potential of the new unmanned vehicles. After an unproductive period due to decreased funding, a very important step toward the development of modern UAVs was taken by the Germans when they developed the V-1 as the first successful cruise missile. The Germans regarded this new weapon as a good response against the superior air threat posed by the Allies. Although it lacked accuracy compared to modern systems, the resulting weapon was an unpredictable threat to the Allies. Especially notable was its capability to penetrate through to underground targets

due to its free fall kinetic energy. Its economic and psychological effects can be summarized statistically, as seen in Table 1 [9].

Ratio of economic loss (Germans / Allies)	<b>1:4</b>
Total V-1s Launched	<b>10,492</b>
Ground / Air Launched	<b>8,892/1,600</b>
Reaching to Target	<b>2,419</b>
Shoot Downs	<b>By fighters 1847</b> <b>By guns 1878</b> <b>By balloons 232</b>
Civilians Injured / Killed	<b>17,981 / 6,184</b>
Cost to Germans	<b>£12,600,000</b>
Cost to Allies	<b>£47,635,000</b>

Table 1. Important Statistics of V-1 Campaign (After [9])

The V-1 was limited by the technology available at that time. After WWII, UAV technologies underwent a set of improvements, primarily to design and develop unmanned weapons systems. The two superpowers of the Cold War era, the U.S. and the USSR, were both aware of the deficiencies associated with the technology used in the V-1s. This period witnessed a competition between these two superpowers. In the early days of this cold war period, the results were less impressive than expected. There was an apparent halt on projects until more sophisticated surface-to-surface cruise missiles were developed with high levels of reliability and lethality. The Snark and Navaho programs are examples of these development projects; however, the programs proved to be unreliable and were later cancelled.

One of the areas explored by the superpowers was that of airborne decoys. Airborne decoys were first introduced to simulate the RCS of currently employed

manned aircraft. In the early 1950s, the United States worked on three airborne drone projects. The third drone, called Quail, was designed to simulate the B-52 bomber and first flew successfully in 1956. During the same period, the Soviet Union produced a few medium range cruise missiles. Cruise missile projects were followed in parallel by ballistic system projects, and first Sputnik satellite launch in 1957 [9].

From a historical perspective, we can summarize the use of UAVs in operations into five main military or political eras of UAV development and employment. The very first successful large-scale operational use of UAVs was by Germany during WWII with the V-1, used as a weapon against civilian targets. The second era begins with WWII and continues through the Korean War, where UAVs were used against point targets such as ships, buildings, and railroads. Third, UAVs had been used in situations where there was no military intervention, like North Vietnam and China (1960s and 1970s). Although United States had no military encounter with these governments at that time, logistic routes to Vietnam were closely watched during this period. The fourth era is marked by usage of UAVs within military operations with political constraints, as seen in the Vietnam War. The present era we are now in has culminated with the modern concept of UAV operations within warfare, beginning with Israeli operations against Syrian forces inside Lebanon in the 1980s. This contemporary concept accepts and employs UAV capabilities during all phases of war ([9] pp.78 and 115).

Having examined the technological and conceptual development of UAV systems we now discuss the classification of UAVs.

## **2. Classification of UAVs**

There are quite a few different types of UAV classification schemes found in the literature. Therefore it is very hard to make a definite classification and use it as a reference. But, in general, many researchers have tried to classify UAVs by weight, range, maximum altitude, wing span, engine type, etc.

### ***a. Classification by Weight***

- Super Heavy Weight UAVs: Over 2000 kg.

- Heavy Weight UAVs: Between 200 kg and 2000 kg.
- Medium Weight UAVs: Between 50 kg and 200 kg.
- Light Weight UAVs: Between 5 kg and 50 kg.
- Micro UAVs: Under 5 kg [10].

***b. Classification by Endurance and Range***

Endurance of an aircraft system is defined by the total amount of time that the aircraft can stay airborne once employed. This property directly affects the maximum operational range.

- Long Endurance UAVs: Endurance time more than 24 hours, and operational range between 1,500 km and 22,000 km.
- Medium Endurance UAVs: Endurance between 5 hours and 24 hours, and operational range between 100 km and 1500 km.
- Low Endurance UAVs: Endurance time less than 5 hours, and operational range less than 100 km [10].

***c. Classification by Flight Ceiling***

One of the most important critical technical parameters for military aircraft systems is the maximum operational altitude measurement. Altitude directly affects the survivability, lethality, endurance and operational range of the system.

- High Altitude UAVs: Ceiling over 10,000 m.
- Medium Altitude UAVs: Ceiling between 1,000 m and 10,000 m.
- Low Altitude UAVs: Ceiling up to 1,000 m [10].

***d. Classification by Wing Loading***

Wing loading is a technical parameter calculated by dividing total weight of the UAV by wing area.

- High Loading UAVs: More than 100 kg/ m<sup>2</sup>.
- Medium Loading UAVs: Between 50 kg/m<sup>2</sup> and 100 kg/ m<sup>2</sup>.
- Low Loading UAVs: Less than 50 kg/m<sup>2</sup> [10].

e. *Classification by Engine Type*

Another classification is done by engine type. Of course, the engine type is related to the physical dimension of UAV. Major types of engines used for UAVs are fuel rotary, turbofan, two-stroke, piston, propeller, turboprop, electric, and push and pull.

<b>Classification by Weight</b>		<b>Classification by Endurance and Range</b>	
Super Heavy	> 2000 kg	Long Endurance	> 24 hours
Heavy	200-2000 kg		1500-22000km
Medium	50-200 kg	Medium Endurance	5-24 hours
Light	5-50 kg		100-1500km
Micro	< 5 kg	Low Endurance	< 5 hours
<b>Classification by Engine Type</b>			< 100 km
Fuel Rotary		<b>Classification by Ceiling</b>	
Turbofan		High Altitude	> 10000 m
Two-stroke		Medium Altitude	1000-10000 m
Piston		Low Altitude	< 1000 m
Electric		<b>Classification by Wing Loading</b>	
Propeller		High Loading	> 100 kg/ m <sup>2</sup>
Turboprop		Medium Loading	50-100 kg/ m <sup>2</sup>
Push and Pull		Low Loading	< 50 kg/ m <sup>2</sup>

Table 2. Classification of UAVs

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. NETWORK CENTRIC WARFARE AND SWARM NETWORKS**

#### **A. SWARM NETWORKS AND DISTRIBUTED BEAMFORMING WITH UAV SWARMS**

Many technological inventions and concepts are motivated by the natural behavior of animals. A few decades ago, people started to think about the collective behavior of animal colonies, such as a flock of birds, a school of fish, and a colony of bees. After some observations, it was obvious that the colony had a learning intelligence, and an emergent behavior arose from this dynamic process. For example, in a series of experiments on a colony of ants with a choice between two unequal length paths leading to a source of food, biologists have observed that ants tended to use the shortest route [11]. This mutual behavior is called “swarm behavior.”

##### **1. Swarm Behavior**

Keeping the ant colony example in mind, we can make a general definition for swarming. In [12], swarming is defined as a collection of autonomous individuals relying on local sensing and reactive behaviors interacting such that a global behavior emerges from the interactions.

Small contributions of autonomous elements are regarded as reactive behaviors, because they do not require a plan. Emerging global behavior in the swarm develops after a period of time. We shall simply call it locally motivated behavior and it directly depends on local sensing. In other words, local sensing motivates the instant reactive behavior of individual elements. Of course biological swarms are not within the scope of this research. But, it is very important to know some basic properties of swarms to understand distributed beamforming using UAVs in a swarm.

##### **2. Distributed Beamforming with UAV Swarms**

In today’s modern warfare concept, smaller assets with cheaper manufacturing/maintenance costs and lower fatal risks are gaining in importance. Cooperative efforts of these relatively small assets, collected together inside a network,

can result in the same capabilities as with traditional larger platforms. The focus of this thesis is on the application where we use a swarm of UAVs distributed over a given terrain, all with limited capabilities of radiated power, and reach the required Signal-to-Noise Ratio (SNR) to effectively conduct EA. In other words, instead of using a traditional jammer antenna array, an adequate number of UAVs in a swarm can collectively form the same jammer power and achieve the total required SNR, as illustrated in Figure 4.

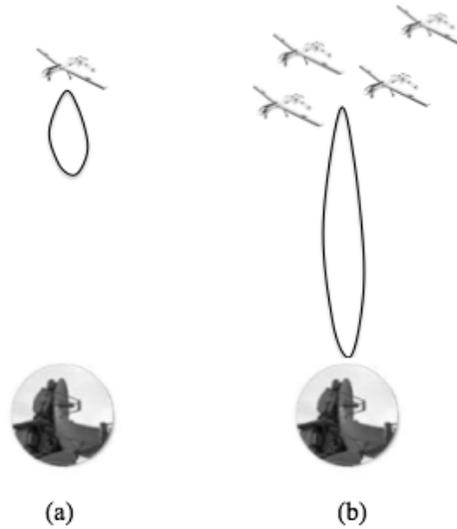


Figure 4. (a) Antenna beam formed by a single UAV and  
(b) Antenna beam formed by a UAV swarm

Using a UAV swarm for Distributed Beamforming (DBF) requires understanding the wireless sensor network architecture. This will be helpful to propose a possible solution for a distributed jamming attack and some transmission and communication problems, especially over the Turkish geography as being in the scope of this research. Swarm behavior in the previous discussion is concerned with local sensing inside the swarm. In a UAV swarm network, individual elements, each which will be called nodes from now on, are also controlled in a similar way. As proposed in [13] and [14], network nodes are required to self-synchronize to a common time and frequency reference, thus the relative locations, and phase offsets of all the nodes are known by the central source or synchronizer as well as the nodes themselves.

For complex geographies like the terrain of Turkey, the central source for appropriate time and frequency synchronization can also be a solution to overcome transmission losses and range limitations due to the geo-localization problem. Let us think about an area of operational interest (AOI), which is beyond line of sight (BLOS) of the UAV base station. In the absence of satellite communication links, a synchronization node can act as a relay station between the operational UAV swarm and the base station. In such a mission, DBF can be modeled as a relay channel, where the base station is the source and the synchronization channel is the relay node. The synchronization node can contain a single UAV, or it can be another UAV swarm, depending on the required SNR value in the warfare environment. Figure 5 is a brief illustration of this concept.

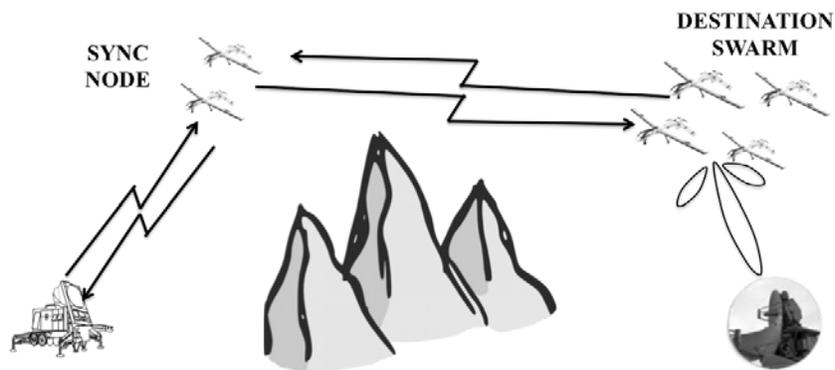


Figure 5. Synchronization and Relay Nodes

When taking the synchronization node into account, the generic analysis of performance is related to ideal weight magnitudes, available channel state information, and the number of cooperating elements [14]. In this analysis, there is a very important property of aerial vehicles that can be regarded as an associated drawback. The location of the relay elements, relative to base station, to the destination operational swarm, and to each other inside the synchronization node is very hard to estimate. But, rapid advances in computer technologies and positioning systems allow each element know their own relative position and share this information with others in timely manner. GPS trackers can be successfully employed and combined with the increased transmission capabilities of each element, and a very accurate synchronization to a reference in time and frequency

can be achieved. It will be helpful to make the complex weight calculations easier, because the sensors within the SYNC node are no longer fixed.

If we consider the synchronization node as a Wireless Sensor Network (WSN) and destination UAV swarm as a single destination node, we can argue that the spatial distribution of sensor nodes in WSN is Gaussian [15], [16]. Let there be  $N$  UAVs all located on the  $(x-y)$  plane, as shown in Figure 6 [15].

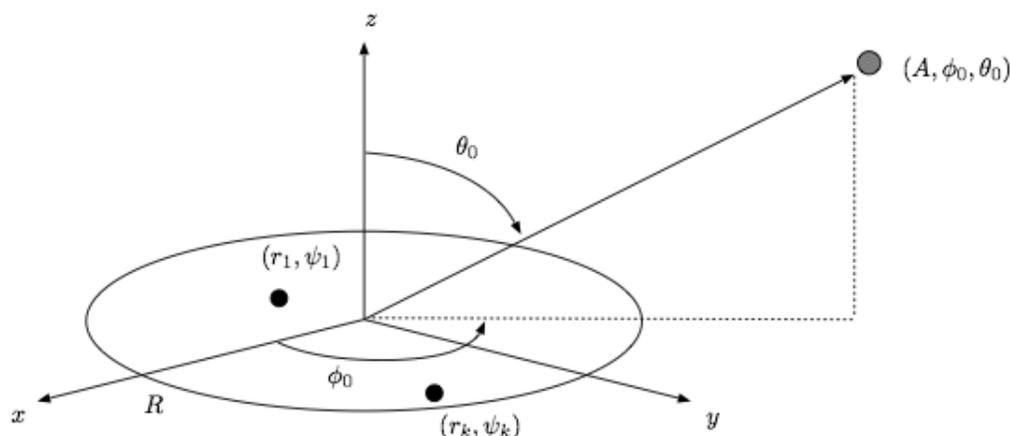


Figure 6. Geometrical Positions and Notations (After [15])

Polar coordinates of  $k$ th UAV are noted as  $(r_k, \psi_k)$ , where  $k = 1, \dots, N$ , and  $\psi_k$  is the initial phase of node  $k$ . The destination node is located at  $(A, \phi_0, \theta_0)$  spherical coordinates. Angles  $\theta \in [0, \pi]$  and  $\phi \in [-\pi, \pi]$  represent elevation direction and azimuth direction, respectively. To make the analysis more simple, the location of each UAV is chosen randomly with uniform distribution. Let the destination node, in our case the destination UAV swarm, be located in spherical coordinates  $(A, \phi, \theta)$ , and  $d_k(\phi, \theta)$  denote the Euclidean distance from  $k$ th UAV to the destination node. If  $A \gg r_k$  in the far-field region, this distance can be written as:

$$d_k(\phi, \theta) = \sqrt{A^2 + r_k^2 - 2r_k A \sin(\theta) \cos(\phi - \psi_k)} \quad (1)$$

Node locations are positioned as  $(r_k, \psi_k)$  in Figure 6, where  $r = [r_1, r_2, \dots, r_N] \in [0, R]^N$  and  $\psi = [\psi_1, \psi_2, \dots, \psi_N] \in [-\pi, \pi]^N$ . Array factors of each node can be written as:

$$F(\phi, \theta | r, \psi) = \frac{1}{N} \sum_{k=1}^N e^{j\psi_k} e^{j\frac{2\pi}{\lambda} d_k(\phi, \theta)} = \frac{1}{N} \sum_{k=1}^N e^{j\frac{2\pi}{\lambda} [d_k(\phi, \theta) - d_k(\phi_0, \theta_0)]} \quad (2)$$

where initial phase of node  $k$  is  $\psi_k = -\frac{2\pi}{\lambda} d_k(\phi_0, \theta_0)$ , and  $\lambda$  is the carrier wavelength.

Coupling effects among all nodes are assumed to be negligible. In the far-field  $A \gg r_k$ , and (1) can be approximated as:

$$d_k(\phi, \theta) \approx A - r_k \sin \theta \cos(\phi - \psi_k) \quad (3)$$

Thus, far-field beam pattern is approximated by

$$F(\phi, \theta | r, \psi) = \frac{1}{N} \sum_{k=1}^N e^{j\frac{2\pi}{\lambda} r_k [\sin(\theta_0) \cos(\phi_0 - \psi_k) - \sin(\theta) \cos(\phi - \psi_k)]} \quad (4)$$

As stated earlier, distributed beamforming using the above equations depends highly on the accurate knowledge of all nodes. Furthermore, synchronization of all nodes relative to  $\lambda$  is very important. Next section will deal with basics of Network Centric Warfare (NCW).

## B. NETWORK CENTRIC WARFARE

The early history of the network centric warfare (NCW) concept goes back to the beginning of the information age, when economic foundations started to realize the importance of dynamic change. Technological improvements let the organizations share and create centralized mutual information, and then experience its potential power. This new condition showed that no economic organization could survive without changing. Being aware of this new challenge, organizations started to create new relationships with others, and share both human and organizational behaviors. Looking at this from the military perspective, this was a very robust idea to link the warfighting capabilities of

geographically scattered assets within the battlefield. With its three key steps, the NCW concept helped to create a mutual situational awareness and understanding of operational needs [17]:

- First of all, the location of the organizations or warfighting assets is very important in NCW. In the past, geographical dispersion from other units was a deadly drawback, because these military assets were very subject to attacks and other threats. But in the NCW concept, warfighting assets are free from geographical constraints. This means that the geographical location of any individual node, source of information, or force asset is no longer perceived as a disadvantage.
- A second key feature in NCW is that all of the economic organizations or military units must be knowledgeable. All the nodes inside the network are linked to each other, thus a shared situational awareness arises from this collective information exchange. By self-synchronizing to a central source of information, every single unit understands the needs of the whole structure. In military terms, every unit knows and understands the needs of commanders. This feature also makes the autonomous operations of the assets more effective, given the proper real-time central information. In this step, central knowledge is converted into battlefield knowledge at the operational level.
- Finally, a proficient and effective linkage among organizations or assets within the battlefield is a key feature. By ensuring this, geographically separated units will create a synergy. This can be achieved with a reliable and powerful information infrastructure that makes mission and responsibility reassignments easier and timely.

### **1. Origins of Network Centric Warfare**

When this NCW concept was first announced in [18] in 1998, the origins of NCW were analogous to the fundamental changes in business, both in the USA and around the world. The transition and adoption of NCW by the military can be seen as the natural

response of the military to the needs of its age. Although the NCW concept is still not accepted universally, it is largely accepted as an ongoing transformation in military affairs parallel to economic changes.

By the beginning of the 21st Century, economic organizations and firms concentrated on larger and more dynamic learning systems that can easily adopt changes within the ecosystem they operate. Firms started to realize that their old competitors can be their new partners, and this relationship and the necessary information sharing among them can yield a powerful knowledge of the economic system. This meant a major shift from a platform focus to a well-designed and powerful network that permits adoption of network centric operations. Partners in this new business model were no longer independent from each other; on the contrary, they were all members of a dynamic economic system. This flexible system helped the firms to make true choices with regard to market research and investments, resulting in more prosperity.

These essential changes in technology, business and daily life opened a new perspective in the military's perception of warfare concepts and tactics. Commanders and headquarters started to notice the importance of networking, and the NCW concept was slowly adapted and adopted, largely as a result of the migration of new technologies into the military command structure. High-speed network links and sensor interactions enabled military units to improve their operational effectiveness. Geographically separated and dispersed, but well informed, units contributed more to the warfighting capability of the entire force [18].

Timely information transfers amongst the nodes inside the network through linkages create a very powerful effect and a potential warfighting capability. In traditional platform-centric warfare, where sensing and engagement phases take place under the same system as seen in Figure 7, weapons platforms follows five steps to successfully intercept the target [17]:

- Search and detect the target.
- Interrogate and identify the target.
- Decide on engagement.

- Give an appropriate order to the weapon associated with engagement decision.
- Fire the weapon.

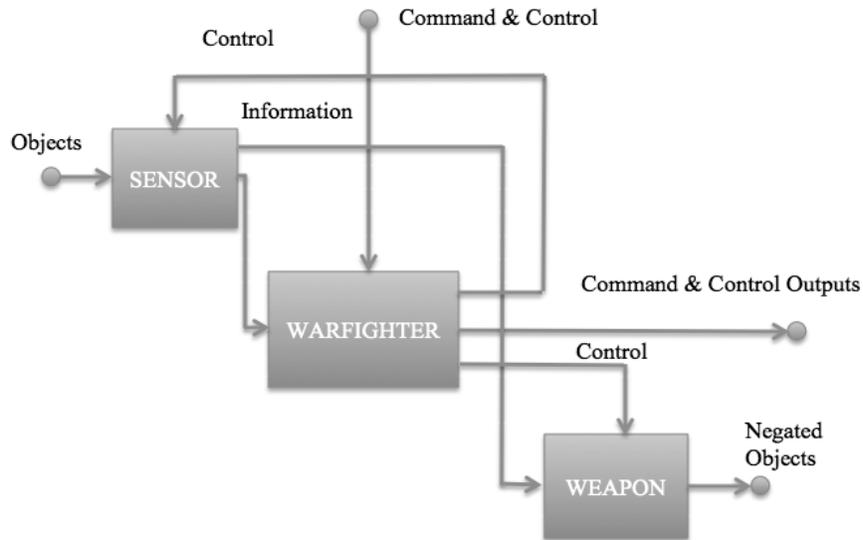


Figure 7. Platform-Centric Weapon System (After [17])

In platform-centric warfare, operational effectiveness is directly related to the onboard sensor's ability to detect, and the radius of weapon's maximum affective range. Generally, onboard sensors have longer detection ranges than the weapon's effective range as illustrated in Figure 8. This effective range is called effective engagement envelope, and reflects the platform's individual combat power. Conversely, in NCW individual capabilities of nodes are digitally linked. Real time accurate information exchange between the nodes supports the warfighters situational awareness [17]. It is no longer necessary for a weapons platform to use organic sensors with a range greater than that of its weapons, as the information that would cue the weapons may now come from other sensors on other platforms that are a part of the network.



Figure 8. Platform-Centric Engagement Envelope (After [17])

Tactical data links are the most indispensable part of network-centric operations that ensures the five required steps for a successful engagement can be conducted in a timely manner. The NCW structure is shown in Figure 9.

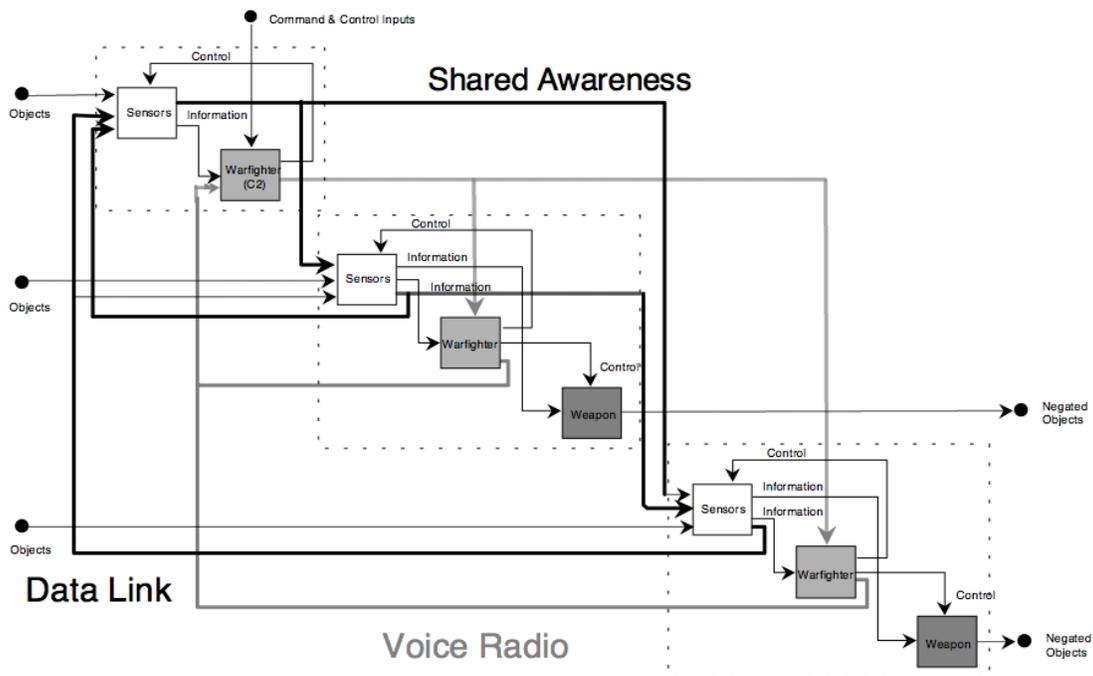


Figure 9. Network-Centric Operations (After [17])

The similarities between the NCW concept and swarm behavior is clearly seen in this brief summary and explanation of NCW. Especially notable is the need for a high-

speed network and link capability, sensor-grid structure, and self-synchronization, all key futures for both. Moreover, distributed beamforming using swarms requires the emergent global behavior of small and limited capacity UAVs that are scattered, or dispersed, over a geographical region. In this model, every individual UAV is analogous to an organization in business ecosystem. They are all self-synchronized and adoptive to the changes within the network and swarm. Next we continue with the fundamentals of NCW.

## **2. Fundamentals of Network Centric Warfare**

To understand the fundamentals of NCW, we examine the three domains of the information environment. These are the physical domain, information domain, and cognitive domain. NCW is the powerful, reliable, fast, timely, responsive, and flexible networking in and among these three domains [19]:

- **Physical Domain:** This is the domain where all the military physical actions are taken, such as attack and defensive maneuvers. It is clear from the name that all of the physical platforms and tactical network links exist in this domain. Since it accommodates the physical assets, operational effectiveness, operational suitability, and combat power are evaluated in this domain.
- **Information Domain:** This is the domain where information itself is created, managed, and communicated among the forces. In this way, warfighters know and understand the commander's aims. The information domain is the place where communication resides. Since it is very vulnerable and open to hostile attacks, it must be well protected.
- **Cognitive Domain:** This is the domain where all the brain-storming takes place. Since it represents the minds of thinkers, decision-makers or commanders, the outcomes of the wars are shaped in this domain. Human factors stand in the center of the cognitive domain, and the information goes through the individual perspectives of the participants.

The NCW architecture is comprised of three grids, which are the global information grid, the sensor grid, and the shooter grid [20], [21].

- The global information grid is the general background for the sensor nodes and shooters, where the information is created and shared continuously. The physical limits of the global information grid extend from the infinity of space to the limit of sea depths, including earth's atmosphere and surface. Sensor and shooter nodes are linked in a network topology.
- The sensor grid is represented by the sensor network, which has sensor nodes such as radar systems. These sensor nodes create emergent sensed information linked to the shooter grid.
- Finally, the shooter grid is occupied by the operational systems, such as weapons and jammers. Since every mission is a unique one, and needs a different tactic in a specified place and time, the shooter grid is re-configurable [21].

### 3. Network Centric Warfare Metrics

Before touching upon the NCW metrics, the OODA concept should be clarified first. The OODA acronym is formed by the first capital letters of Observe, Orient, Decide, and Act, which was first introduced by John R. Boyd in his set of briefings on competitive strategy ([21], [23–25]). In a networked environment, the assets of military power follow the cycle shown in Figure 10.

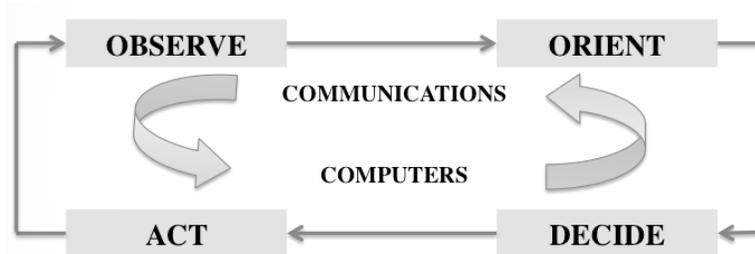


Figure 10. The OODA Cycle

Military activities are confined between two opposing OODA cycles in a warfare environment. In other words, two opposing military powers have similar OODA loops, and make their own individual decisions that are not known by the adversary. On the other hand, some military activities of each side are open for observation and known by the opponent. The speed of the OODA cycle iteration period determines the success of network centric operations.

The information network topology is formed by a set of nodes (or warfighting assets) interconnected with each other. NCW combines technology, organizational structure, command and control, and human factors all together. Network centric operations (NCO) are conducted by interconnecting network-space and battle-space. These two operational planes are connected to each other and to the OODA loop by internal metrics. These measures are listed as [24]:

- Connectivity
- Reach
- Richness
- Characteristic tempos

*a. Connectivity Measure*

Military network structure is defined in [24] as being very similar to the INTERNET network structure. Two very important assumptions are made to analyze a military network. These include:

- The number of nodes within the network is large.
- There are no differences between the nodes in terms of capabilities and roles. The network has a homogenous structure.

To express the connectivity measure of a network with  $N_T$  nodes and  $\frac{1}{2}N_T(N_T-1)$  links, we should first explain the definitions. Firstly, a *link* is a communication means between two nodes. Secondly, *routes* are all possible communication directions between two nodes, and each route has at least one link. Finally, the *connectivity measure* of a network can be expressed as [24]:

$$C_M(t) = \sum_{\mu=1}^{N_T} K_{\mu}(t) \sum_{\nu=1}^{N_{\mu}} \sum_{\gamma=1}^{N_{\mu\nu}} L_{\gamma}^{\mu\nu}(d, t) \quad (5)$$

In the equation,  $N_{\mu}$  is the total number of nodes connected to node  $\mu$ .  $N_{\mu\nu}$  is the total number of routes that are possible between  $\mu$  and  $\nu$  node pair.  $K_{\mu}(t)$  is the *value* of the node  $\mu$ , which represents the capability.  $L_{\gamma}^{\mu\nu}(d, t)$  is the *information flow* parameter of the route  $\gamma$  connecting nodes  $\mu$  and  $\nu$ . Information flow is the function of the length  $d$  of the route, and time  $t$ . Ranges for capability and information flow parameters are  $0.0 \leq K_{\mu}(t)$  and  $L_{\gamma}^{\mu\nu}(d, t) \geq 1.0$ .

We will make these definitions clear with an example, using a normalized value for route length  $d = 1$ . Figure 11 shows nodes, links, routes and capability values of the nodes. Note that each route contains one or more links. Links between the node pairs and possible routes are shown in Table 3 and Table 4 [21].

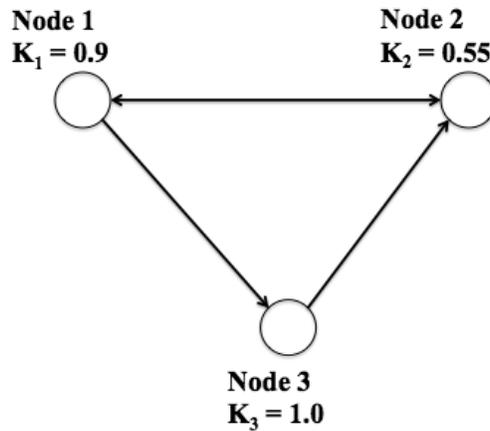


Figure 11. Connectivity Link Calculations Example with Three Nodes (After [21])

LINKS	
FROM	TO
1	2
1	3
2	1
3	2

Table 3. Available Links in Figure 10

START NODE	END NODE	ROUTE
1	2	1 → 2
1	3	1 → 3
2	1	2 → 1
2	3	2 → 1 → 3
3	1	3 → 2 → 1
3	2	3 → 2

Table 4. All Possible Routes in Figure 10

The information flow parameter  $L_\gamma^{\mu\nu}(d, t)$ , which depends on length of route  $d$  and time  $t$ , can be made easier by splitting it into two parts, a time-independent value component part  $L^{\mu\nu}$  and a time-dependent flow coefficient part  $F_\gamma^{\mu\nu}$ , respectively. *Time-dependent flow coefficient*  $F_\gamma^{\mu\nu}$  is scaled by the route length  $d$  raised to the power  $\xi$ , and ranges between 0 and 1. Then the *connectivity measure*  $C_M$  becomes [24]:

$$C_M(t) = \sum_{\mu=1}^{N_T} K_\mu(t) \sum_{\nu=1}^{N_\mu} L^{\mu\nu} \sum_{\gamma=1}^{N_{\mu\nu}} \frac{F_\gamma^{\mu\nu}(t)}{(d_\gamma)^\xi} \quad (6)$$

To clarify these ideas, the connectivity of the network is assumed to be time-independent, with a *time-dependent flow coefficient* is  $F_\gamma^{\mu\nu} = 0$  or 1 showing that two nodes are either connected or not, and a *scaling exponent* of  $d_\gamma$  is to be  $\xi=1$  [24]. After all these assumptions, Table 5 shows the results of connectivity measure calculations for Figure 10.

ROUTE	$K_\mu$	$d_\gamma$	$C_M$ Weight
1 → 2	0.9	1	0.9
1 → 3	0.9	1	0.9
2 → 1	0.55	1	0.55
2 → 1 → 3	0.55	2	0.275
3 → 2 → 1	1	2	0.5
3 → 2	1	1	1
			$C_M = 5.125$

Table 5. Connectivity Measure Calculations for Figure 10

Now, think about a reference network where all nodes are fully connected and identical. In this homogenous structure, all capability values are equal to 1 ( $K = K_\mu = 1$  and  $F = F_\gamma^{\mu\nu}$ ). The *reference connectivity measure* can be calculated as [24]:

$$C_M^R(t) = N_T(N_T - 1) \times \left[ 1 + \frac{(N_T - 2)}{2} + \frac{(N_T - 2)(N_T - 3)}{3} + \dots + \frac{(N_T - 2)(N_T - 3) \dots 2 \cdot 1}{N_T - 1} \right] \quad (7)$$

It is clearly seen from Equation (7) that the only variable that effects the *reference connectivity measure* value is the total number of nodes  $N_T$  [26]. The numerator in each term inside the square brackets is the number of possible routes of the length given in the denominator. Compared to other networks with the same number of nodes, the reference network has the highest connectivity measure.

An example from [21] is used to illustrate the reference network concept. A realistic network with four nodes is shown in Figure 12. The nodes have different capability values ( $K_\mu$ ). In this network, there are two bidirectional and two unidirectional links between the nodes. Unidirectional links are from node 2 to node 4 and from node 3 to node 2. Bidirectional links are between node 1 and node 2, and node 3 and node 4. In Figure 13, the reference network, which corresponds to the network in Figure 12, is shown. Note that all links are bidirectional, homogenous, and have full capability values ( $K = K_\mu = 1$  and  $F = F_\gamma^{\mu\nu}$ ).

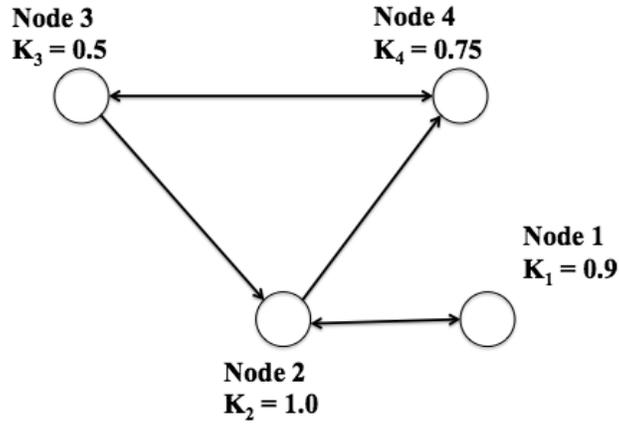


Figure 12. Realistic Network with Four Nodes and Heterogeneous Links

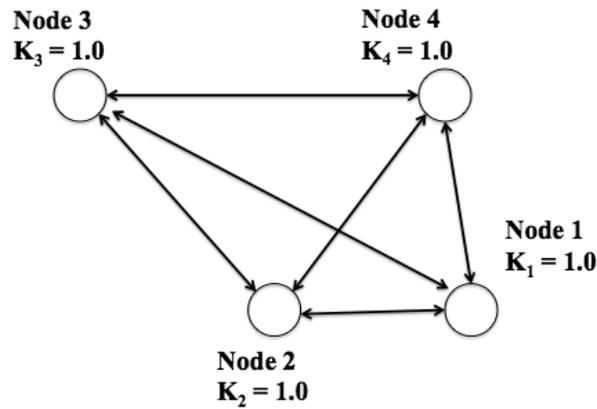


Figure 13. Corresponding Reference Network for Figure 12

For the example network in Figure 12, the total number of node is  $N_T = 4$ , where reference connectivity measure can be calculated as:

$$C_M^R(t) = 4(3) \left[ 1 + \frac{2}{2} + \frac{2(1)}{3} \right] = 32$$

Reference connectivity measures are calculated for a number of different nodes as shown in Table 6:

Total Number of Nodes ( $N_T$ )	Reference Connectivity Measure
3	9
4	32
5	120
6	534
7	2905
8	18976

Table 6. Connectivity Measure Calculations for Different  $N_T$  Values

**b. Network Reach**

A reference network with the highest connectivity measure helps to normalize this connectivity measure. A normalized connectivity measure is named as *network reach* and becomes [24]:

$$I_R \equiv C_N = \frac{1}{C_M^R} \sum_{\mu=1}^{N_T} K_{\mu} \sum_{\nu=1}^{N_{\mu}} L^{\mu\nu} \sum_{\gamma=1}^{N_{\mu\nu}} \frac{F_{\gamma}^{\mu\nu}}{d_{\gamma}} = \frac{C_M}{C_M^R} \quad (8)$$

*Network reach* is a dimensionless value, which is a normalized re-statement of connectivity measure.

**c. Network Richness**

The information-processing rate of each node is important for the calculation of *network richness* ( $R_Q$ ).  $\lambda_{\mu}^{\min}$  is the minimum information processing rate (1/time) for node  $\mu$  to convert information to knowledge according to Shannon Information Entropy. The average rate at which knowledge is measured through the network is defined as network richness, and shown in Equation (9).  $\lambda_{\mu}$  is the rate at which node  $\mu$  processes information at time  $t$ . Taking (9) into account, no knowledge is created if the information-processing rate is less than  $\lambda_{\mu}^{\min}$ . Conversely, if the information-processing rate is 2.72 times faster than  $\lambda_{\mu}^{\min}$ , very little knowledge is generated [24] as evident from the equation.

$$R_Q = \frac{1}{N_T} \sum_{\mu=1}^{N_T} \lambda_{\mu} Q(\lambda_{\mu}) \quad (9)$$

**d. Characteristic Tempos**

Due to technological limitations and telecommunication boundaries, every network has a limited maximum information-processing rate. As proposed in [24], every network has a characteristic time scale or tempo  $\lambda_T$ . The *characteristic tempo* of a network topology is directly affected by the applied information and communications technologies. It is generated by the product of *network reach (dimensionless)* and *network richness (1/time)*, and can be thought of as information exchange frequency:

$$\lambda_T = I_R R_Q (\text{Hz}) \quad (10)$$

We can define a characteristic decision making speed  $\lambda_{C2}$  for every C2 system. The last two phases in the OODA Cycle in Figure 14 depend on network capability and the limitation of physical actions. Physical actions can be sorted as deployment speed, synchronization of weapon systems and platforms, and engagement.  $\eta_1$  and  $\eta_2$  represents the decide-to-act and act-to-observe action tempos, respectively. Finally, we have  $\Delta\tau_3 \geq 1/\lambda_T + 1/\eta_1$  and  $\Delta\tau_4 \geq 1/\lambda_T + 1/\eta_2$ . After stating these parameters, the maximum operation tempo of the network can be concluded as [24]:

$$\Lambda_{OODA} \leq \frac{\lambda_{C2}}{1 + \left( \frac{1}{\eta_1} + \frac{1}{\eta_2} \right) \lambda_{C2} + \frac{3\lambda_{C2}}{\lambda_T}} \quad (11)$$

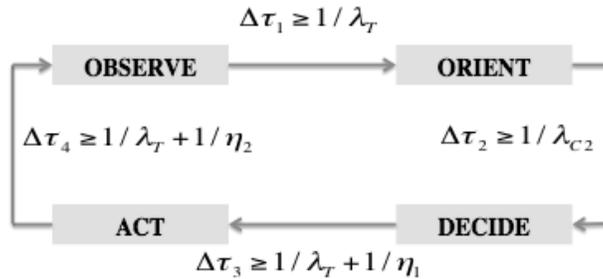


Figure 14. Time Spent in Each Phases of the OODA Cycle (after [24])

## IV. RADARS AND RANGE EQUATIONS

This section will serve as an introduction to radar systems and data links. Since this research aims to examine the electronic attack missions with UAV swarms, it is vital to closely review the basics of these technology areas. In a network centric environment, radars could be a part of the sensor system, or could be the target. In either case, the capabilities and parameters of the radar systems of interest are important.

### A. BASIC RADAR PRINCIPLES

The working principle of a radar system can be explained as the emission of electromagnetic (EM) waves from the transmitter and detection of these waves reflected from the target by the receiver. In this way, the radar system detects and locates the target.

Basic components of the radar transmit/receive cycle are shown in Figure 15. In this cycle, the receive antenna collects the reflected amount of EM energy that is very small compared to originally transmitted energy, and processes it in the receiver circuits. The mixer, amplifiers, detectors and analog-to-digital converter (ADC) amplify and convert these analog signals into digital signals. Finally, these digital signals are processed through a signal processor and the results are displayed. For the detected range  $R$  of the target, we can derive an equation using basic physics. Let  $\Delta T$  represent the total round-trip time of the EM waves from the transmit antenna to the target, and from the target to the receive antenna. Since the EM waves travel a distance of  $2R$  in  $\Delta T$  seconds, the range to the target becomes ([27] pp.4):

$$R = \frac{c\Delta T}{2} \quad (12)$$

#### 1. Clutter

The received EM waves that reach the receiver are not always necessarily reflected back from only the target. There may be some clutter and unwanted reflections from other materials. These environmental and natural obstacles are called clutter, and

can be mistaken as a target. In such a condition, the clutter return will create an equivalent radar cross section (RCS), which will cause a false detection. The RCS of the clutter is very important for the radar calculations. The signal-to-clutter ratio (SCR) is used for adding the effects of clutter on radar detection and ranging equations. The SCR is simply calculated by dividing target RCS ( $\sigma$ ) with clutter RCS ( $\sigma_c$ ) ([27] pp.76):

$$SCR = \frac{\sigma}{\sigma_c} \quad (13)$$

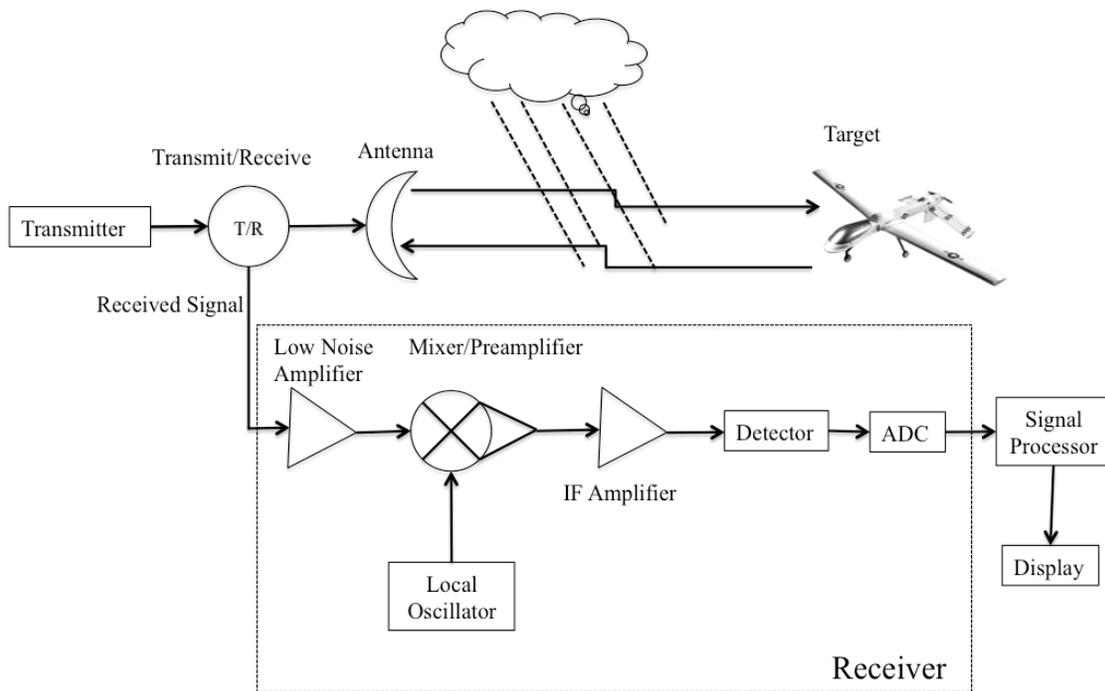


Figure 15. Basic Components of Radar Transmit/Receive Cycle (After [27])

## 2. Radar Range Equation

In the very beginning of this chapter, the basic principle of radar is explained briefly. We can extend this main principle into three basic roles, which are to search and detect, to track detected contacts and in some applications to create an image of the contact [27].

The capability of a radar with given parameters is measured with the radar range equation. With regard to the position of the transmit and receive antennas relative to each other in a radar system, we can group the radars into three main categories. If the transmit and receive antennas are very close to each other or they use the same antenna, this type of radar is *monostatic*. In the case of a slight separation between two antennas that is undetectable by the target, this type of radar is called *quasi monostatic*. In the calculations and derivations, monostatic and quasi monostatic radars can be regarded as the same. Finally, if the transmit and receive antennas are located in different positions, the radar is *bistatic* [28].

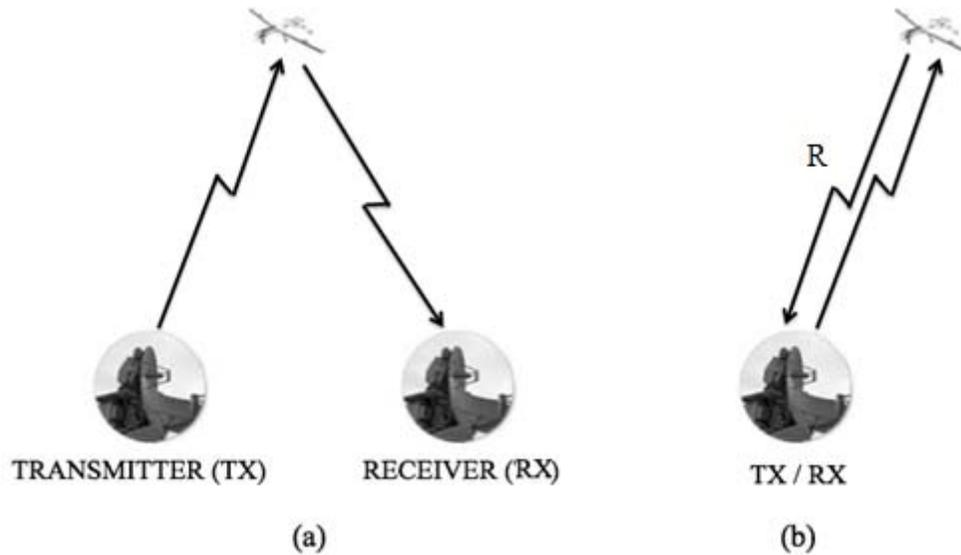


Figure 16. (a) Bistatic Radar (b) Monostatic Radar

If we think about a monostatic radar with a single antenna used for both transmitting and receiving EM waves, the range between the radar and target ( $R$ ) determines the power density incident on the target. If  $P_t$  is the radar transmitter power and  $G_t$  is the antenna gain, the power density ( $W_i$ ) at range  $R$  becomes [28]:

$$W_i = \frac{P_t G_t}{4\pi R^2} \quad (14)$$

When the target is illuminated by the transmitted power coming from a distance  $R$ , a portion of the energy that is proportional to the RCS of the target reflects back to the

receiver. The RCS  $\sigma$  of a target is dependent on the surface area of the target, appearance and architecture of the target, and the substance used for building and painting the target. After the reflection, the power density inbound to the radar receiver becomes ([27] pp.62):

$$P_{refl} = W_i \sigma = \frac{P_t G_t \sigma}{4\pi R^2} \quad (15)$$

Reflected power that is reradiated from the target travels the same distance  $R$  back to the receiver. After this second propagation, scattered power density back at the radar becomes [28][29]:

$$W_s = \frac{P_t G_t}{4\pi R^2} \cdot \frac{\sigma}{4\pi R^2} = \frac{P_t G_t \sigma}{(4\pi R^2)^2} \quad (16)$$

Scattered EM waves are collected by the receive antenna, which has a finite effective area. This is called the effective aperture of the receive antenna ( $A_{er}$ ). This can be expressed as the physical area of the antenna  $A$  multiplied by an efficiency  $e$  [28]

$$A_{er} = Ae \quad (17)$$

Applying the aperture equation, received power at the radar becomes [28][30]:

$$P_r = W_s A_{er} = \frac{P_t G_t}{4\pi R^2} \times \frac{\sigma}{4\pi R^2} A_{er} = \frac{P_t G_t \sigma A_{er}}{(4\pi)^2 R^4} \quad (18)$$

As stated earlier, the portion of the scattered power back at the receive antenna is the product of scattered power density and effective aperture area. Effective area can be expected in terms of gain as in (19), where wavelength  $\lambda = c / f$  ( $c$  = speed of light,  $f$  = frequency) [31]:

$$A_{er} = \frac{G_r \lambda^2}{4\pi} \quad (19)$$

After a final revision by substituting (19) into (18), received power becomes:

$$P_r = \frac{P_t G_t G_r \sigma \lambda^2}{(4\pi)^3 R^4} \quad (20)$$

Equation (20) is the most basic form of the radar range equation (RRE) and derived disregarding many other effects. For more precise calculations, some other performance parameters should be included in the RRE. These parameters can be listed

as radar system internal and path losses ( $L$ ), internal noise, clutter, signal processing gains ( $G_p$ ), and moving target Doppler effect. If we note that  $L \geq 1$  and  $G_p \geq 1$ , the RRE becomes [28]:

$$P_r = \frac{P_t G_t G_r \sigma \lambda^2 G_p}{(4\pi)^3 R^4 L} \quad (21)$$

For *monostatic* radars where transmission and reception are done through the same single antenna, we can use a single gain such as  $G_r \equiv G_t \equiv G$ , and then  $G_r G_t \equiv G^2$ . On the other hand, *bistatic* radars have two physically separated antennas used to transmit and receive the EM energy. In this condition, we have possibly two different ranges. One is from the transmit antenna to the target ( $R_t$ ), and the other is from the target to the receive antenna ( $R_r$ ). As a result, the denominator  $R^4$  term in Equations (20) and (21) becomes  $R_t^2 R_r^2$ .

### 3. Signal-to-Noise Ratio

In Section A1, we discussed clutter, which is caused by environmental objects that reflect the EM energy. In addition to these undesired reflections, other EM activity in the vicinity also affects the radar performance. The activities of other radars, communication links, radio stations or emitters that intend to jam the radar system are called *interference* [28]. In addition, we also discussed internal *noise*, which Blake [32] explained as the existence of voltage fluctuations in every circuit due to thermal excitation of electrons.

When observing the received signal power in a radar system very close to the noise level, it is hard to decide whether the receiver output voltage is caused by detected valid target or by random or intentional noise [32]. Signal processing techniques are not an entirely adequate solution to this problem, since the same process is applied to both the target-reflected RF energy and to the received noise. We can talk about a minimum detectable power (MDP)  $P_{r(min)}$  which is the smallest received power level that can overcome the noise [28]. Similarly, if we talk about a minimum detectable signal-to-noise power ratio  $(S/N)_{min}$ , MDP becomes [32]:

$$P_{r(\min)} = (S/N)_{\min} P_n \quad (22)$$

where  $P_n$  is the system noise power.

According to Nyquist (1928) (cited in [32]), the root-mean-square (RMS) voltage (in Volts) produced in a conductor with resistance  $R$  and effective temperature  $T_e$  is:

$$E_{n(rms)} = \sqrt{4kT_eRB} \quad (23)$$

where  $k$  is the Boltzman's constant ( $k = 1.38 \times 10^{-23}$  J/K), and  $B$  is the noise frequency bandwidth in which the voltage is measured.

If we assume an ideal filter where the “filter response is perfectly uniform within the bandwidth” [32], as seen in Figure 17 [28], we can say that the filter response is a step function:

$$H(f) = \begin{cases} 1, & f_1 \leq f \leq f_2 \\ 0, & f < f_1, f > f_2 \end{cases}$$

In Figure 17, bandwidth is  $B = f_2 - f_1$  and center frequency is  $f_c = \frac{f_2 - f_1}{2}$ .

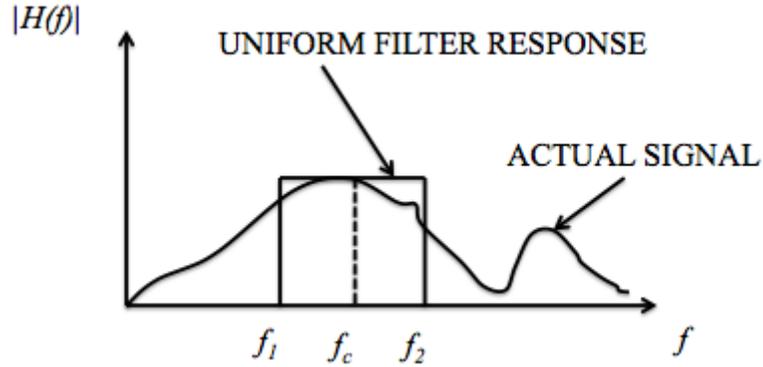


Figure 17. Ideal Band-limited Filter Response (After [28])

If we think of RMS the voltage across the conductor as applied to a matched load, where  $R = R_{load}$ , the voltage divider rule will ensure that the voltage and delivered power across the load will be:

$$E_{n(load)} = \frac{\sqrt{4kT_eRB}}{2R} R = \sqrt{kT_eRB} \quad (24)$$

and

$$P_n = \frac{E_{n(load)}^2}{R} = kT_eB \quad (25)$$

As stated earlier,  $T_e$  is the effective thermal temperature generated by the receiver circuits due to movements of free electrons in the system. In addition to the effective internal temperature of the system, there are some other external non-thermal sources that can produce heat and be detected by the antenna. This is called *antenna noise temperature* [28]  $T_A$ , and forms *system noise temperature* combined with *receiver effective temperature*:

$$T_s = T_e + T_A \quad (26)$$

If we rewrite Equation (22), MDP becomes:

$$P_{r(min)} = (S/N)_{min} kT_s B_n \quad (27)$$

Combining Equation (21) and Equation (27) together, we can state the minimum SNR for target detection as:

$$SNR_{min} = \frac{P_{r(min)}}{kT_s B_n} = \frac{P_t G_t G_r \sigma \lambda^2 G_p}{(4\pi)^3 R^4 kT_s B_n L} \quad (28)$$

For modern radar systems, the minimum SNR values are generally between linear 10 and 100 [28], or 10 to 20 dB using the simple logarithmic conversion:

$$SNR_{min}(dB) = 10 \log_{10}(SNR_{min(LINEAR)}) \quad (29)$$

After the derivation of minimum SNR required to detect a target, we can solve Equation (28) to find maximum detection range associated with the minimum SNR [28]:

$$R_{\max} = \left[ \frac{P_t G_t G_r \sigma \lambda^2 G_p}{(4\pi)^3 R^4 k T_s B_n \text{SNR}_{\min} L} \right]^{1/4} \quad (30)$$

#### 4. Radar Cross Section (RCS)

In the previous section, we derived maximum range by Equation (30). As is true for other parameters in the equation, the accurate value of the RCS ( $\sigma$ ) is of vital importance for the precise determination of maximum range. The RCS of real targets is a complicated function of many variables and is greatly influenced by the complexity of the target's shape. These variables can be addressed as operating frequency, target aspect angle, and EM wave polarization. For an ideal case, we can assume frequency and EM wave polarization constant, but the aspect angle will be a time dependent variable for moving targets or radar. This variation will cause the RCS to vary as well [32].

The evaluation of RCS is basically accomplished by calculating the scattered electric field from a radar target. In words, RCS is represented by [28]:

$$\frac{\text{Power Reflected to Receiver per Unit Solid Angle}}{\text{Incident Power Density}/4\pi}$$

or more mathematically

$$\sigma = \lim_{R \rightarrow \infty} 4\pi R^2 \frac{\left| \vec{E}_s \right|^2}{\left| \vec{E}_i \right|^2} \quad (31)$$

where  $\vec{E}_s$  and  $\vec{E}_i$  are scattered and incident electric field intensities, respectively. The incident field is assumed to be a plane wave.

RCS is generally measured in dB, and calculated by the same conversion shown in Equation (29). Depending on the size of the target, RCS ranges from 10,000 m<sup>2</sup> (40 dBm<sup>2</sup>) to 0.0001 m<sup>2</sup> (-40 dBm<sup>2</sup>). The Table 7 shows some typical RCS values [28].

Objects	RCS (m <sup>2</sup> )	RCS (dBm <sup>2</sup> )
---------	-----------------------	-------------------------

Insects	0.0001	- 40
Birds	0.01	-20
Creeping and Travelling Waves	1	0
Fighter Aircraft	100	20
Bomber Aircraft	1,000	30
Ships	10,000	40

Table 7. Typical RCS Values of Some Organisms and Objects (After [28])

To better understand the behavior of RCS, we will use Jenn's [28] special case, where an antenna is used as the target (illustrated in Figure 18). We assume that the radar and target antennas are pointed at each other. In other words, they are pointed as main beam on main beam. The gain and effective area of the target antenna is given by  $G_a$  and  $A_{ea}$ , respectively. We also assume that there is no loss at the terminal, which means incident and radiated power are the same. As a result, we can say that target antenna acts like an emitter with a transmitted power  $P_c$  where:

$$P_c = \frac{P_t G_t A_{ea}}{4\pi R^2} \quad (32)$$

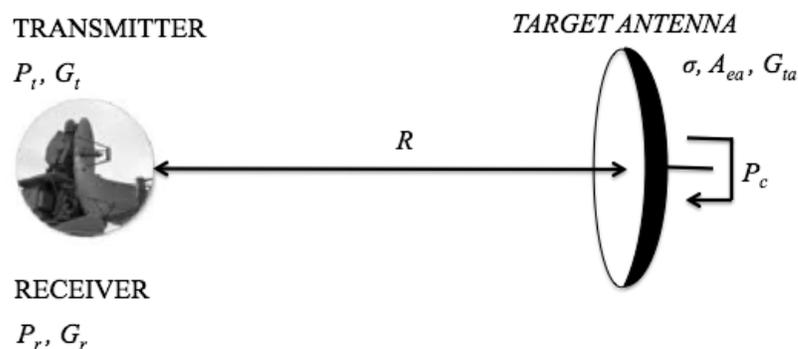


Figure 18. Special Case – Antenna as a Target (After [28])

Thus, power density and received power back at the radar antenna become [28]

$$W_r = \frac{P_c G_a}{4\pi R^2} \quad (33)$$

and

$$P_r = \frac{P_t A_{ea}^2 G_t G_r}{(4\pi R^2)^2} \quad (34)$$

When compared to Equation (20) and Equation (34), since both equations calculate received power, a relationship between  $\sigma$  and  $A_{ea}$  can be seen as [28]

$$A_{ea}^2 = \frac{\lambda^2 \sigma}{4\pi} \quad (35)$$

$$\sigma = \frac{4\pi A_{ea}^2}{\lambda^2} \quad (36)$$

Since wavelength is in the denominator in Equation (36) and it decreases with higher frequencies ( $\lambda = c/f$ ), the RCS of a constant surface area increases with frequency.

## B. RADAR ELECTRONIC COUNTER MEASURES

The main function of a radar network is to surveil all aspects of a ground asset in a given terrain, such that no airborne aggressor can penetrate through this coverage without using radar electronic counter measures (RECM). Figure 19 shows the general concept of radar coverage with regard to a RECM scenario. The main goal of RECM can be one or a combination of any of the following [33]:

- Deny accurate target detection by an enemy radar system
- Confuse enemy radar operators
- Cause delays in detection and tracking
- Generate false targets displayed on the radar system
- Overload the radar computer system with false targets
- Force false target ranging and positioning

We combine the RECM methods into two basic groups [28]

1. *Low observability or “stealth.”* This method includes manipulating the RCS of the target, using radio frequency absorbing materials and shaping.
2. *Electronic Counter Measures (ECM):* ECM includes passive techniques such as chaff and radar decoys, or active techniques like radar jamming.

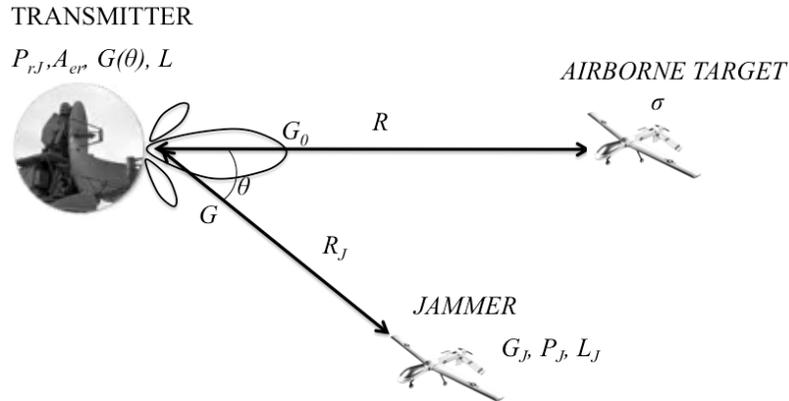


Figure 19. Radar Coverage and RECM Scenario – Stand-off (Stand-in) Jamming

In this research, we will mainly focus on RECM with regard to jamming. Jammers have some characteristic system parameters that identify their capability of the jammers. These include the jammer operating bandwidth  $B_J$  and effective radiated power (ERP). ERP is directly proportional to jammer transmitter power [33]

$$ERP = \frac{P_J G_J}{L_J} \quad (37)$$

where  $L_J$  is the total jammer losses and  $G_J$  is the jammer antenna gain.

In the following discussion we will basically focus on stand-in jamming (SIJ) applications with UAVs accomplished via UAV swarms. Supporting this, we will briefly examine Self-Screening Jamming (SSJ) in the next section. We will also take a brief look at stand-off jamming (SOJ), since SIJ is very much like SOJ, except for the position and range of the jammer to the radar system.

## 1. Self-Screening Jamming (SSJ)

In SSJ, the airborne target itself conducts radar jamming, using onboard ECM systems. This is also commonly referred to as self-protection jamming. If the jammer and the target are different vehicles and they are very close such that they appear as a single target to the radar system (i.e. they are in the same resolution cell), then this configuration can also be treated as SSJ. Since target and jammer are contained within the same platform, then target and jammer distances are equal,  $R = R_J$ , relative to the target. On the other hand, receive angles for reflected waves from the target and the jammer signals will also be the same, ensuring that the jammer uses main beam gain  $G_0$ . If we say the radar has a wavelength  $\lambda$ , effective aperture  $A_{er}$ , bandwidth  $B_r$ , receiver losses  $L$ , transmit power  $P_t$ , and tries to detect a target with RCS  $\sigma$  at a distance  $R$ , then received power at the radar becomes [33]

$$S = \frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 R^4 L} \quad (38)$$

Similarly,  $P_J$  is the jammer peak power,  $G_J$  is the jammer antenna gain,  $B_J$  is the jammer operating bandwidth which is usually larger than  $B_r$ , and  $L_J$  is the total jammer losses. The jamming power received at the radar is [33], assuming the jammer is in the radar mainbeam

$$J = \frac{P_J G_J}{4\pi R^2} \frac{A_{er}}{L_J} = \frac{P_J G_J}{4\pi R^2} \frac{\lambda^2 G}{4\pi} \frac{1}{L_J} = ERP \frac{\lambda^2 G}{4\pi R^2} \quad (39)$$

Now, we need to derive S/J ratio for SSJ. If we combine Equation (38) and Equation (39), and account for different bandwidths of the jammer and radar, S/J becomes [33]

$$\frac{S}{J} = \frac{P_t \tau G \sigma B_J}{(ERP) 4\pi R^2 L} \quad (40)$$

where  $B_r \approx 1/\tau$  has been assumed.

## 2. Stand-off Jamming

Stand off jammers typically use very high ERP, since they operate farther out from the radar's lethal targeting area. SOJ creates a safe region for the friendly penetrator or penetrators beyond their path. In a SOJ environment as seen in Figure 19, power received at the radar from the SOJ becomes [33]

$$J = \frac{P_J G_J}{4\pi R_J^2} \frac{\lambda^2 G}{4\pi} \frac{1}{B_J L_J} = \frac{ERP}{4\pi R_J^2} \frac{\lambda^2 G}{4\pi} \frac{1}{B_J} \quad (41)$$

and SJR becomes

$$SJR = \frac{S}{J} = \frac{P_t \tau G R_J^2 \sigma B_J}{(ERP) 4\pi R^4 L} \quad (42)$$

We will use the same equations for SIJ.

## 3. Jammer Burn-through Range

We will now use the SOJ scenario in Figure 19 to derive jammer burn-through range. Assume that the radar antenna main beam has the gain  $G_0$  and directly incident on the target with RCS  $\sigma$ . Also consider that the jammer has a transmitted power  $P_J$  and a gain  $G_J$ . The radar antenna has gain  $G(\theta)$  in the direction of the jammer. Then the jammer power incident on the radar antenna is [28]

$$P_{rJ} = W_i A_{er} = \left( \frac{P_J G_J}{4\pi R_J^2} \right) \left( \frac{\lambda^2 G(\theta)}{4\pi} \right) = \frac{P_J G_J \lambda^2 G(\theta)}{(4\pi R_J)^2} \quad (43)$$

Similarly, if we assume no loss and processing gain in the system, the power received at the radar from the target is given by Equation (20). Now, we need to find the ratio of the target received signal power to jammer power incident on radar antenna,

which is called *signal-to-jam ratio (SJR)*. If we also assume a monostatic radar antenna where  $G_t = G_r = G_0$  with no thermal noise, SJR becomes [28]

$$SJR = \frac{S}{J} = \frac{P_r}{P_{r,j}} = \left( \frac{P_t G_0}{P_j G_j} \right) \left( \frac{R_j^2}{R^4} \right) \left( \frac{\sigma}{4\pi} \right) \left( \frac{G_o}{G(\theta)} \right) \quad (44)$$

assuming  $B_j = B_r$ .

Moreover, if we include Gaussian noise to the jamming, we should also include noise to our calculations [33]:

$$SJR = \frac{S}{J+N} = \frac{\left( \frac{P_t G_0 \sigma A_{er} \tau}{(4\pi)^2 R^4 L} \right)}{\left( \frac{(ERP) A_{er}}{4\pi R^2 B_j} + kT_s \right)} \quad (45)$$

Remember that  $k$  is Boltzman's constant and  $T_s$  is the receiver effective noise temperature.

Jammer *burn-through range* is at  $SJR = 1$  ( $S = J$ ) [28] and is given by [33]

$$R_{BT} = \sqrt{\left( \frac{(ERP) A_{er}}{8\pi B_j k T_s} \right)^2 + \left( \frac{P_t G_0 \sigma A_{er} \tau}{(4\pi)^2 L \frac{S}{J+N} k T_s} \right)^2} - \frac{(ERP) A_{er}}{8\pi B_j k T_s} \quad (46)$$

We will simulate a EA on a surveillance radar system in Section 5.

## V. RADAR AND NETWORK ELECTRONIC COUNTER MEASURES SIMULATION

### A. SURVEILLANCE RADAR EA SIMULATION

In this section, we simulate a typical RECM application using MATLAB<sup>®</sup>. We use *RADJAM* (version 2.2) simulation toolbox [34], *burn\_thru.m* and *sir.m* files [33] to examine burn-through range, detection contours and jamming effects.

#### 1. Scenario

We simulate a stand-in jamming profile using a single small UAV. As stated earlier, it is infeasible to conduct this mission with such a small platform, since it has some size, weight, and power (SWAP) limitations compared to those of conventional manned jamming aircraft. We will assume that a single UAV is capable of radiating the required jamming power in the given configuration. In other words, we will assume that a single UAV has the required power level that can be produced with multiple UAVs in a UAV swarm as an emergent behavior. The SIJ configuration used in the simulation is shown in Figure 20. In this configuration, both the target and the jammer are assumed to be in the radar main beam. Since the radar main beam and the jamming main beam are in alignment with each other, and that the target is aligned on the same axis, then the radar, target and jammer height are equal. For simplicity, we will assume they are zero while not concerning ourselves with Fresnel Zone effects that would be present at or near ground elevations.

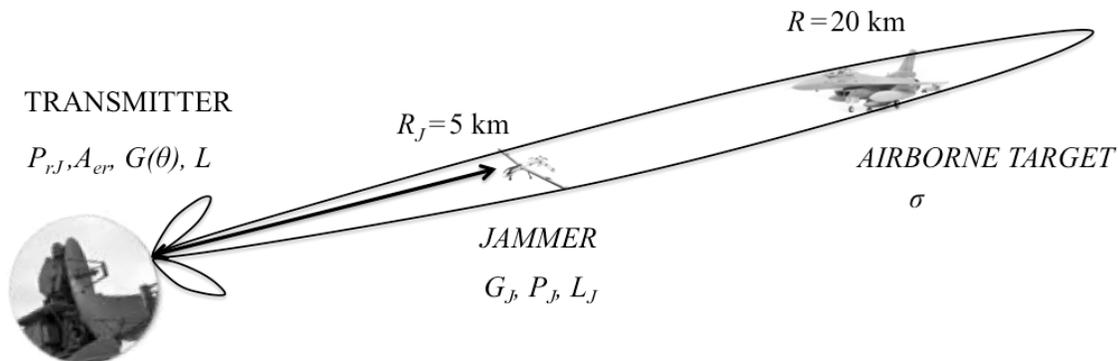


Figure 20. SIJ Configuration

## 2. Parameters and Calculations

We use air surveillance radar operating configurations shown in Table 8. These specifications are very realistic and chosen to be similar to the AN/SPS-49 shipboard surveillance radar system [35].

Peak Transmitter Power	360 kW
Antenna Azimuth Length (m)	7.3
Antenna Elevation Length (m)	4.3
Antenna Height (m)	0
Antenna Gain	29 dB
Radar Processing Gain	10 dB
Frequency	900 MHz
Pulse Width	1 $\mu$ s
Noise Bandwidth	1 Mhz
Antenna Noise Temperature	80 K
Receiver Noise Temperature	2800 K
Minimum SNR	15 dB
Radar Antenna Efficiency	0.9
Side Lobe Level	-35 dB
Back Lobe Level	-60 dB

Table 8. Air Surveillance Radar Operating Parameters

Before we establish the jammer configuration, we can make some preliminary calculations based on our radar parameter performance. First of all, thermal noise power from Equation (25) and Equation (26) becomes

$$T_s = T_e + T_A = 2800 + 80 = 2880\text{K}$$

$$P_n = kT_s B = (1.38 \times 10^{-23})(2880)(10^6) = 3.97 \times 10^{-14} \text{ Watts}$$

$$P_n(\text{dBW}) = 10 \log(3.97 \times 10^{-14} \text{ Watts}) = -134\text{dBW}$$

Similarly, we can convert the SNR from dB to linear and calculate MDP using Equation (28)

$$SNR_{\min} = \frac{P_{r(\min)}}{kT_s B_n} = \frac{P_{r(\min)}}{P_n} = 10^{15/10} = 31.62$$

and

$$P_{r(\min)} = SNR_{\min} P_n = 1.26 \times 10^{-12} W = -119 \text{dBW}$$

Effective radiated power of the radar antenna:

$$ERP = P_t G_t = (360 \times 10^3)(10^{29/10}) = 285.96 \text{MW}$$

Effective area of the radar antenna using Equation (19):

$$A_{er} = \frac{G_r \lambda^2}{4\pi} = \frac{(794.33)(0.333)^2}{4\pi} = 7.02 \text{m}^2$$

Using MDP in Equation (21) with 5 dB atmospheric losses ahead of the receiver, we calculate the maximum range for the target given in Table 9.

Target RCS (m <sup>2</sup> )	10
Target Height	0

Table 9. Airborne Target Specifications

Proceeding with the calculation of maximum range, since

$$P_r = \frac{P_t G_t G_r \sigma \lambda^2 G_p}{(4\pi)^3 R^4 L}$$

then

$$R_{\max} = 231.47 \text{km}$$

Note that the calculated maximum range does not include aperture efficiency and maximum gain of the radar antenna. RADJAM results return the maximum range calculated with these included.

Jammer operating parameters are shown in Table 10. For SIJ, we assume that the UAV jammer position is fixed. This is impossible in reality. However, if we use two UAVs orbiting at a given coordinate as seen in Figure 21 and neglect the length of the flight path inbound to the radar antenna, we can assume a fixed stand-in jammer. In this orbit configuration, two UAVs synchronize with each other and one of them is always inbound to the radar antenna with jamming on while the other is outbound with no jamming radiated towards the target radar.

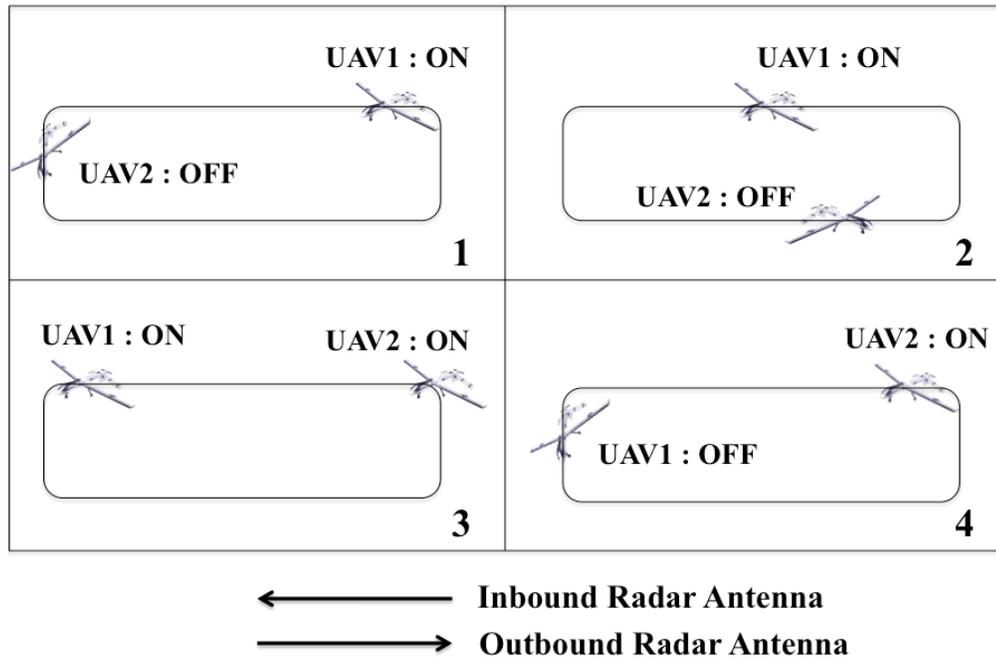


Figure 21. Jammer Configuration

We calculate the SJR for the given parameters and ranges in our scenario using Equation (45)

$$SJR = \frac{S}{J+N} = \frac{\left( \frac{P_t G_0 \sigma A_{er} \tau}{(4\pi)^2 R^4} \right)}{\left( \frac{(ERP) A_{er} + kT_s}{4\pi R^2 B_j} \right)} = 56.22 \times 10^{-4} = -22.5\text{dB}$$

Jammer Height (m)	0
Jammer Range (m)	5000
Azimuth (Deg)	0
Jammer Gain (dB)	5
Jammer Power (W)	20
Jammer Bandwidth (MHz)	10

Table 10. Jammer Operating Parameters

### 3. Simulation Results

Radar, jammer, and target parameters are entered into the RADJAM graphical user interface (GUI) as seen in Figure 22.

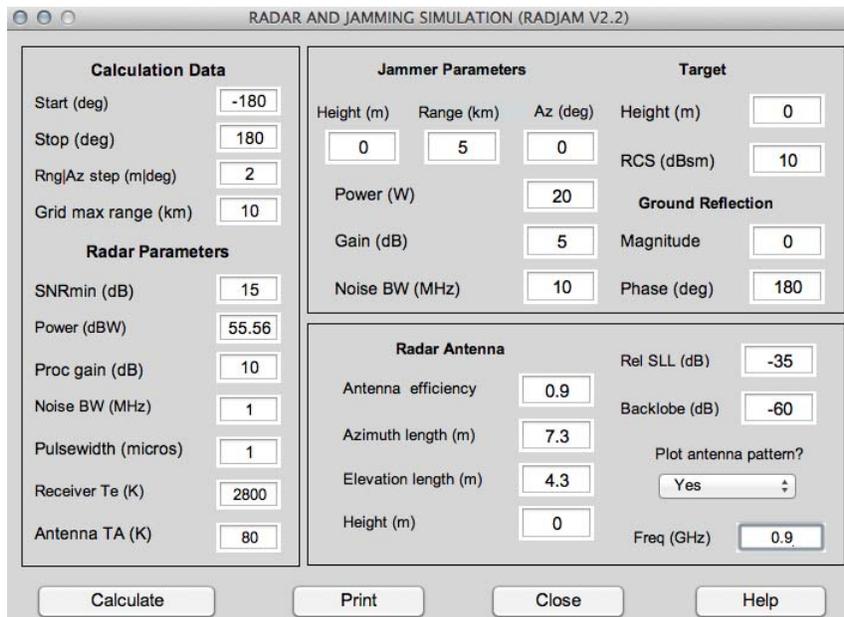


Figure 22. RADJAM GUI Inputs

Since we assumed that the radar main beam, the target and the jammer are all on the same plane, we can easily examine the azimuth tracking of the radar system. The detection contour of the radar is plotted and shown in Figure 23. Without jamming, the maximum detection range is 357.65 km and represented by a circle on the detection contour plot.

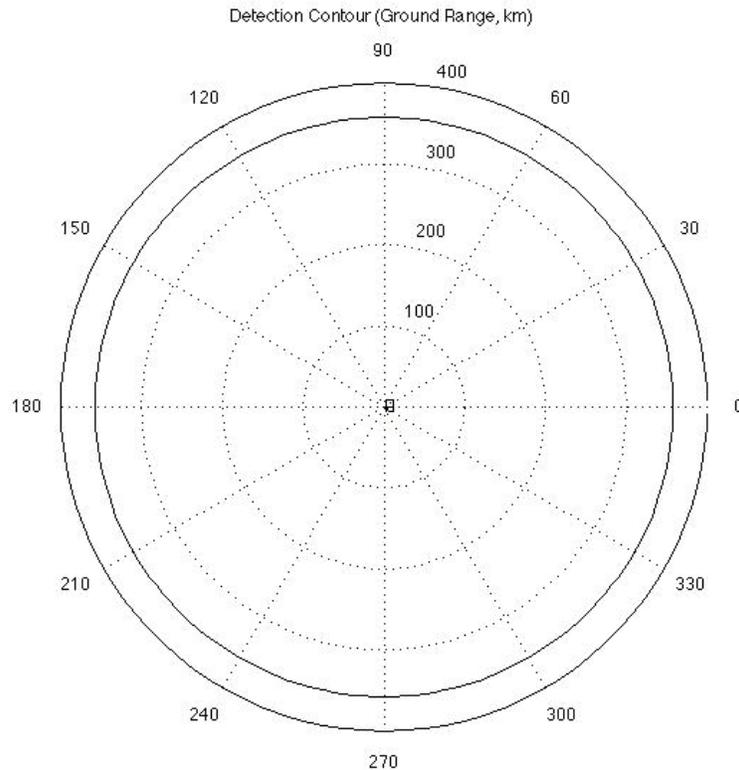


Figure 23. Detection Contour without Jamming

The radar antenna is located at the center of the plot and shown by R, and the jammer position is represented by symbol J. Since the radar system simulates a surveillance radar, it has relatively long range coverage compared to smaller surface search radars. As a result, the R and J symbols are very close to each other due to the close SIJ range. The polar antenna pattern is plotted and shown in Figure 24. The antenna pattern plot includes antenna efficiency and computed antenna dimensions. When the jammer is active and in the main beam, the resulting detection contour with jammer is shown in Figure 25.

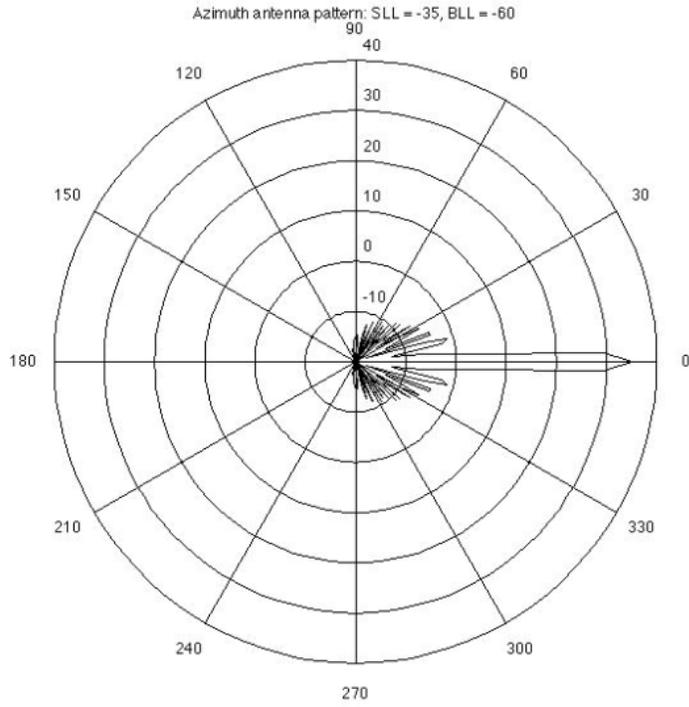


Figure 24. Azimuth Antenna Pattern

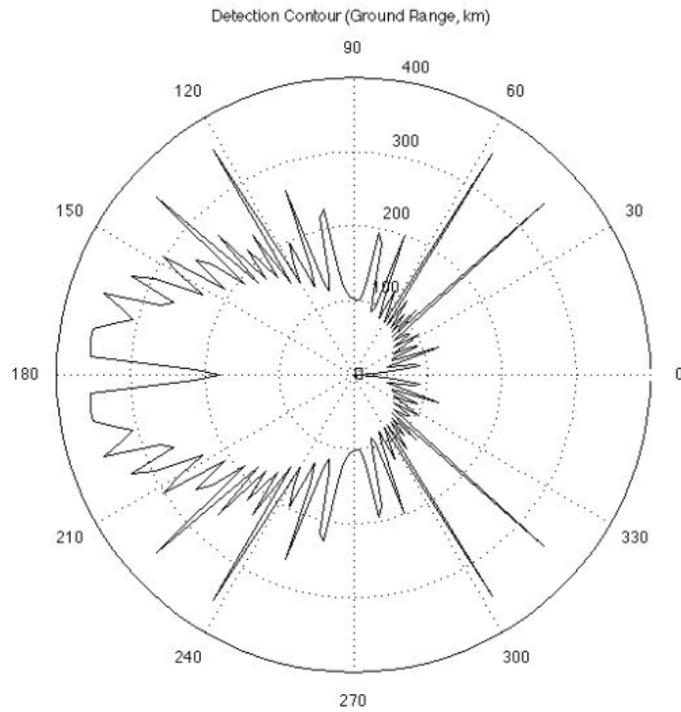


Figure 25. Detection Contour with Jamming

The MATLAB<sup>®</sup> function “esraberilela.m,” given in Appendix A, calculates SJR and burn-through range using Equation (45) and Equation (46). To show the SJR versus detection range, the UAV is assumed to be performing SSJ. In other words, jammer and target assumed to be the same aircraft. Keeping the ERP of the jammer constant, SJR and detection range are plotted in Figure 26. The burn-through range is calculated for our SIJ scenario by the MATLAB<sup>®</sup> function and returned to be -22.5012 dB. This is the same result as calculated in Section 5C.

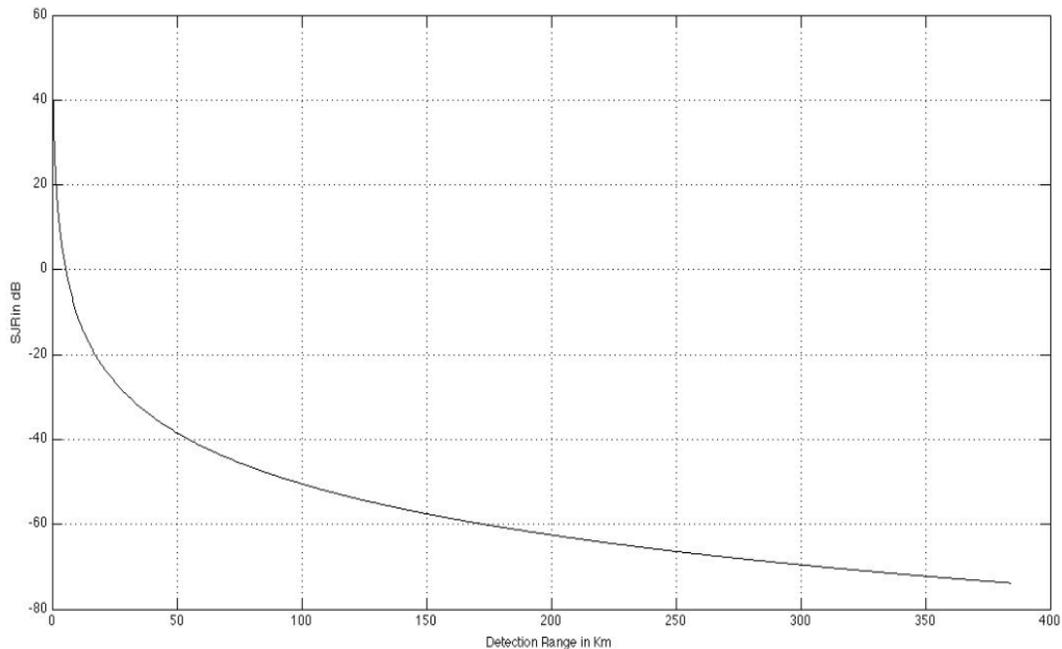


Figure 26. SJR versus Detection Range

We know that the burn-through range occurs when  $SJR=1$ . This happens when signal power is equal to jammer plus noise power. Since they are equal, division of equal values in Equation (45) gives unity. Figure 27 shows the relative signal and jamming amplitude (dB) versus range normalized to burn-through range. When we examine Equation (44) closely, we can infer a few fundamental characteristics [28]:

- Being located at a different and closer position to the radar, the jammer can utilize the range advantage,  $(R_j)^2$  versus  $(R)^4$ .

- Typically radar antennas have higher gain compared to jammer antenna gain,  $G$  versus  $G(\theta)$ . This generally goes against the effectiveness of the jammer. If the jammer is in the main beam as in our scenario, it is not a disadvantage anymore.
- Sidelobe cancellation methods decrease the effectiveness of the jammer.
- When assumed to be stationary at a given geometry, the jammer can only control the ERP.
- Radar operators can easily detect jamming and can locate the jammer using other techniques.

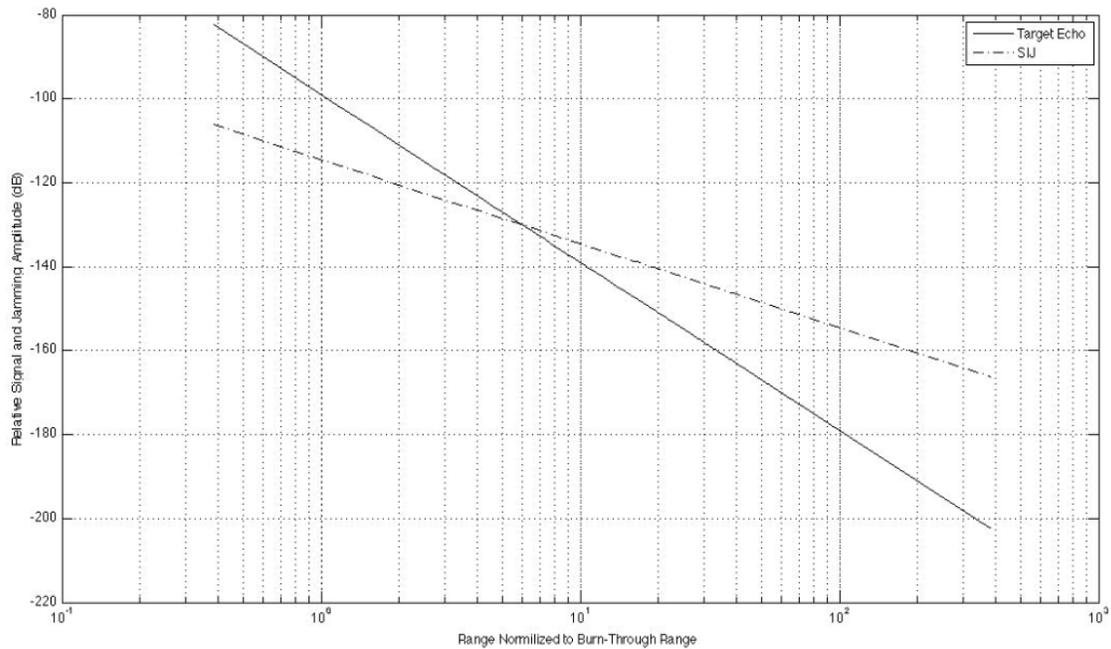


Figure 27. Target and Jammer Signals versus Range Normalized to Burn-through Range

## B. INFORMATION NETWORK EA SIMULATION

In this section, we simulate network electronic counter measures (NECM) application using LPISimNet, developed by Pace and Chen [21, 36]. We will see the affects of a very basic EA attack mission using UAVs against a netted enemy integrated air defense system (NEADS). In today's warfare environment with improved

technologies, EA against a radar does not insure the suppression of enemy air defenses (SEAD). EA against a radar system within a NEADS can be compensated for by other enemy systems connected with data links. However, EA missions against such point targets can harm, weaken, deceive, and delay enemy decision-making and lengthen the OODA cycle. To show the EA effects on a NEADS, we use the operational NCW parameters established in Chapter IIIB to simulate two different warfare topologies. The first one will show a 3-node NEADS topology without a jammer. The second simulation will show a 4-node warfare topology, involving a UAV jammer swarm. In contrast to common usage, the enemy forces and NEADS are labeled “blue forces,” and the UAV jammer swarm is labeled as “red forces” in this simulation.

### 1. 3-Node NEADS Simulation

In the first simulation, we model a NEADS operational network with three nodes connected with data links, shown in Figure 28 and in Table 11. These three nodes are a surveillance radar site, a surface-to-air missile (SAM) site, and an F-16 air-to-air interceptor wing. Simulation results will show the calculations based on NCW metrics introduced in Chapter IIIB.

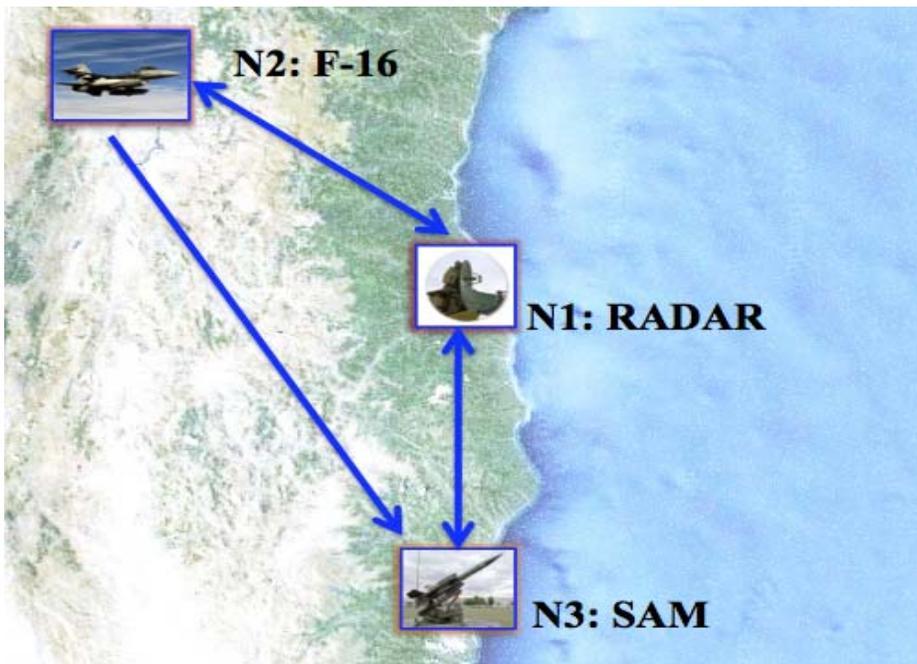


Figure 28. NEADS Operational Network without Jammer

Link Connections			
FROM \ TO	1	2	3
1		Yes	Yes
2	Yes		Yes
3	Yes	No	

Table 11. NEADS Link Connections without Jammer

*a. Simulation Setup*

The simulation setup and NEADS topology are shown in Figure 29. The scenario setup is shown in Table 12. In this NEADS configuration, the surveillance radar site is considered to be an operational NCW command and control center (NCWC2C) with an information capability of 1. There is no link connection from the SAM site to the F-16 fighter aircraft, shown by the decreased information capability of the SAM site with a value of 0.4.

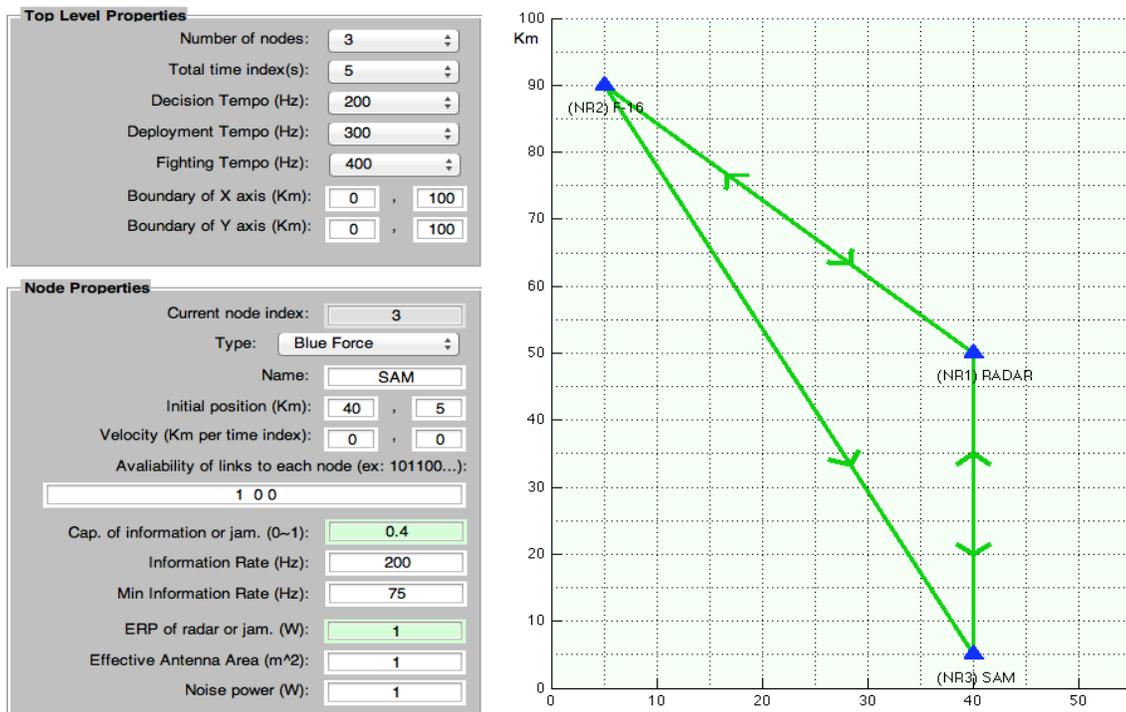


Figure 29. NEADS Topology without Jammer

Number of Nodes	3			
Decision Tempo (Hz)	200			
Deployment Tempo (Hz)	300			
Fighting Tempo (Hz)	400			
		<b>Information</b>		
<b>Node Index</b>	<b>Asset Name</b>	<b>Capability</b>	<b>Rate (Hz)</b>	<b>Min. Rate (Hz)</b>
1	Radar	1	300	100
2	F-16	0.8	200	100
3	SAM	0.4	200	75

Table 12. NEADS Simulation Setup without Jammer

***b. Simulation Results***

After running the simulation, network parameters are calculated for the 3-node NEADS as seen in Figure 30. Detailed MATLAB<sup>®</sup> calculations are shown below.

```

-----
Analysis of Reference Connectivity Measure
-----
Number_of_Node   Reference_Connectivity_Measure
3                9
-----

Analysis of Connectivity Measure at Time index = 1-5
-----
Route           Bottleneck_Node      Contribution_to
                  Connectivity_Measure
-1-2             1                      1
-1-3             1                      1
-1-2-3          2                      0.4
-2-1             2                      0.8
-2-3-1          3                      0.2
-2-3             2                      0.8
-2-1-3          2                      0.4
-3-1             3                      0.4
-3-1-2          3                      0.2
Connectivity Measure= 5.2
-----

```

# Analysis of Network Richness

-----  
**Network Richness = 111.5984**

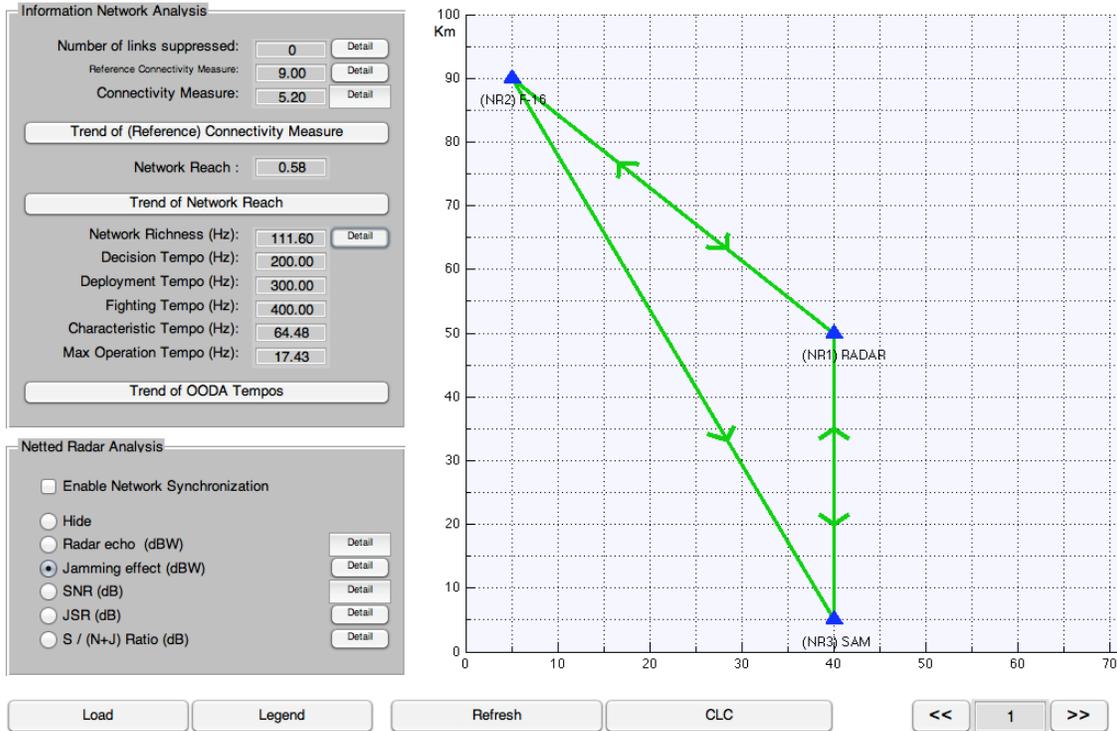


Figure 30. NEADS Topology without Jammer Simulation Results

## 2. 3-Node NEADS with UAV Jammer Swarm Simulation

In the second simulation, we model a NEADS operational network with three nodes connected with data links and attacked by a UAV jammer swarm, shown in Figure 31 and in Table 13.

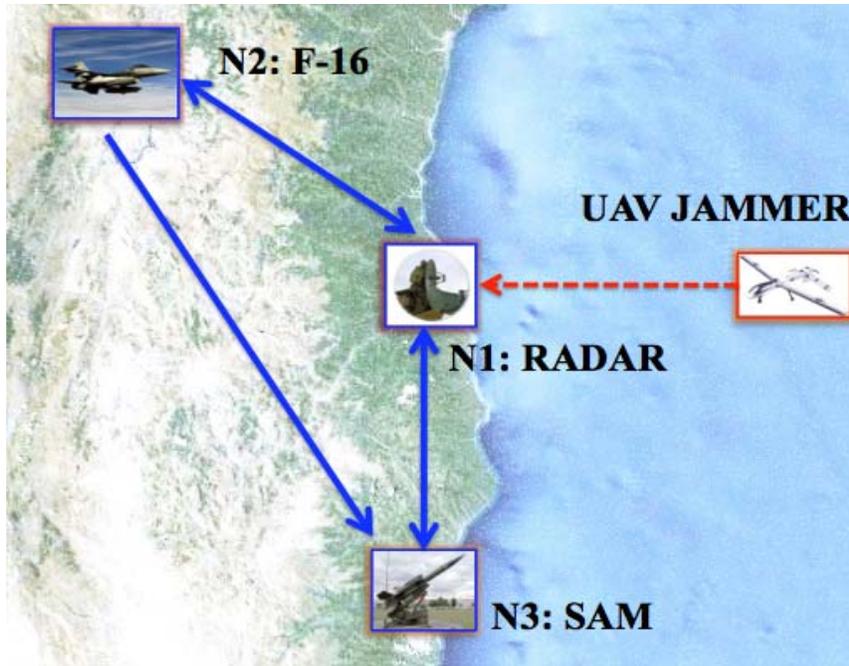


Figure 31. NEADS Operational Network with UAV Jammer

Link Connections				
FROM \ TO	1	2	3	4
1		Yes	Yes	No
2	Yes		Yes	No
3	Yes	No		No
4	Yes	No	No	

Table 13. NEADS Link Connections with UAV Jammer

*a. Simulation Setup*

The simulation setup and NEADS topology is shown in Figure 32. The scenario setup is shown in Table 14. In this NEADS configuration, a UAV jammer swarm applies EA against the radar site. Since the UAV jammer has a moving capability, we added 5 time indexes to our simulation. We assume that the F-16 air-to-air fighter aircraft orbits at a given location which can be thought of as stationary. However, the UAV jammer swarm moves at a given velocity, 8 km per time index toward the radar in this simulation.

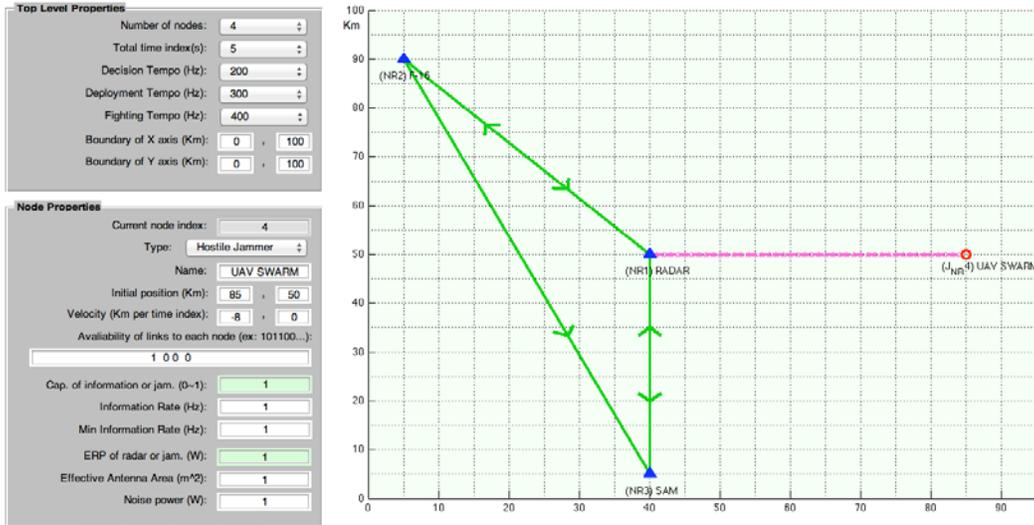


Figure 32. NEADS Topology with UAV Jammer

Number of Nodes	4			
Number of Time Indexes	5			
Decision Tempo	200			
Deployment Tempo	300			
Fighting Tempo	400			
		<b>Information</b>		
<b>Node Index</b>	<b>Asset Name</b>	<b>Capability</b>	<b>Rate (Hz)</b>	<b>Min. Rate (Hz)</b>
1	Radar	1	300	100
2	F-16	0.8	200	100
3	SAM	0.4	200	75
4	UAV SWARM	0.4		

Table 14. NEADS Simulation Setup with UAV Jammer

**b. Simulation Results**

The simulation results for 5 time indexes are shown in Table 15. As seen from the results, EA against the NEADS links harms the enemy OODA cycle. In this specific simulation setup, the NEADS lost two link connections. The information link connection from the SAM to the radar was jammed in time index 1. In time index 2, the information link from the F-16 to the radar was jammed by the UAV swarm. Without any

link connection from its weapon systems, it is impossible for a NCWC2C to maintain situational awareness during any type of mission.

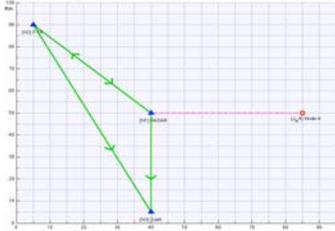
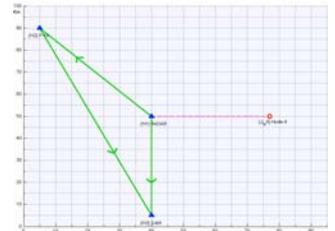
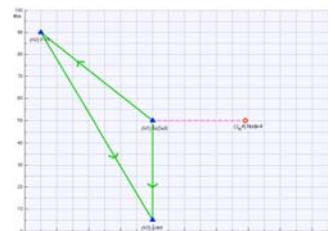
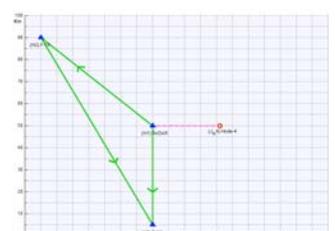
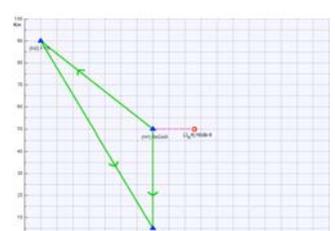
Time Index	Metrics	Result	Map	Links Suppressed
1	$C_M^R$	9		SAM to Radar Suppressed
	$C_M$	4.4		
	$I_R$	0.49		
	$R_Q$	221.46		
	$\lambda_T$	108.27		
	$\Lambda_{OODA}$	25.95		
2	$C_M^R$	9		SAM to Radar and F-16 to Radar Suppressed
	$C_M$	3.2		
	$I_R$	0.36		
	$R_Q$	221.46		
	$\lambda_T$	78.74		
	$\Lambda_{OODA}$	20.44		
3	$C_M^R$	9		SAM to Radar and F-16 to Radar Suppressed -No New-
	$C_M$	3.2		
	$I_R$	0.36		
	$R_Q$	221.46		
	$\lambda_T$	78.74		
	$\Lambda_{OODA}$	20.44		
4	$C_M^R$	9		SAM to Radar and F-16 to Radar Suppressed -No New-
	$C_M$	3.2		
	$I_R$	0.36		
	$R_Q$	221.46		
	$\lambda_T$	78.74		
	$\Lambda_{OODA}$	20.44		
5	$C_M^R$	9		SAM to Radar and F-16 to Radar Suppressed -No New-
	$C_M$	3.2		
	$I_R$	0.36		
	$R_Q$	221.46		
	$\lambda_T$	78.74		
	$\Lambda_{OODA}$	20.44		

Table 15. NEADS with UAV Jammer Simulation Results

The simulation results and EA effects against the NEADS can also be examined directly looking at the trends of NCW. Trend graphics of reference connectivity measure, connectivity measure, network reach, and OODA cycle tempos are given in Figures 33, 34 and 35. A negative slope in the trends of connectivity measure, network reach, and characteristic tempo in time index 1 and time index 2 shows the effects of EA against the NEADS.

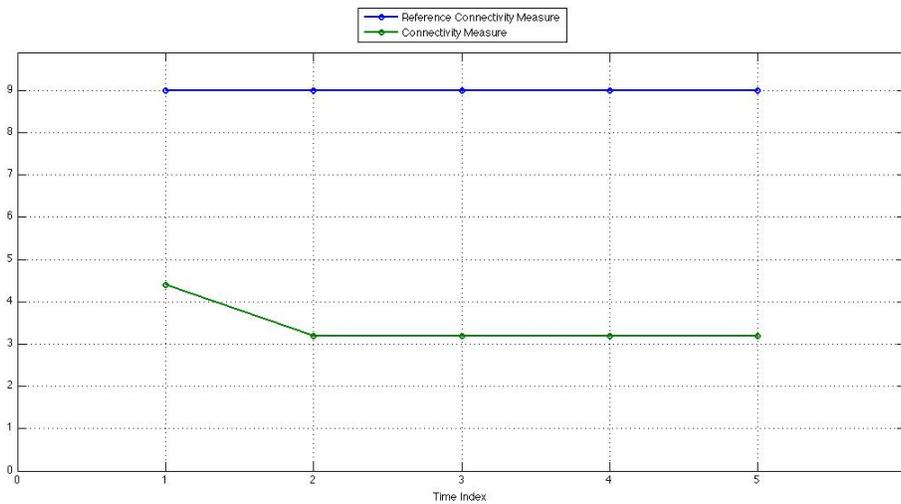


Figure 33. Trends of Reference Connectivity Measure and Connectivity Measure

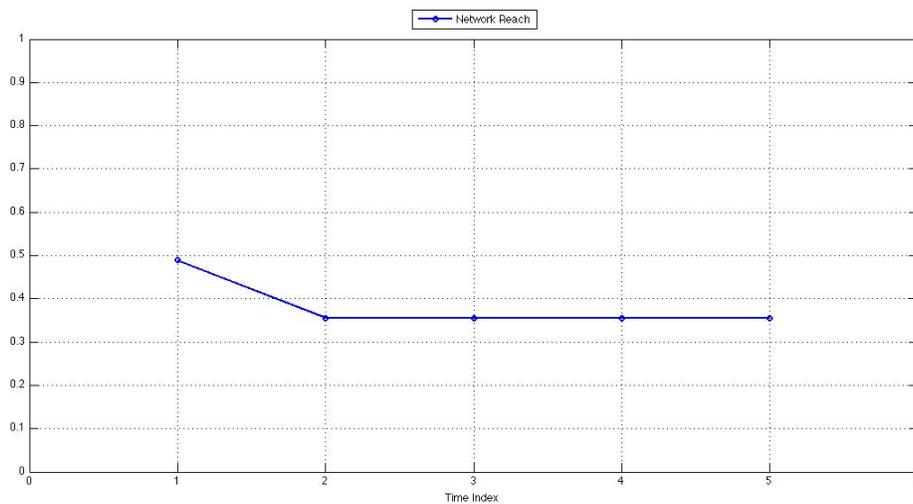


Figure 34. Trend of Reference Network Reach

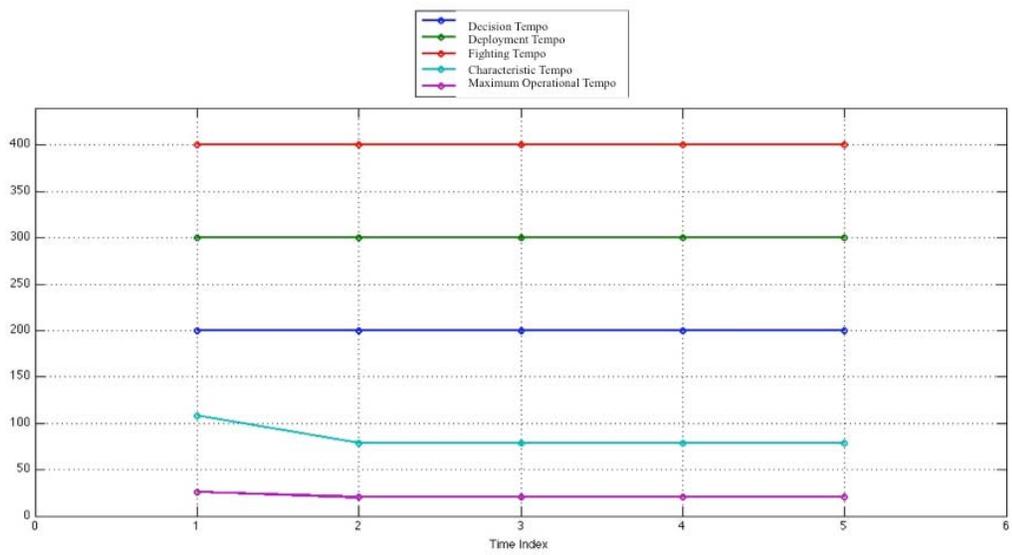


Figure 35. Trends of OODA Cycle Tempos

## VI. CONCLUSIONS AND RECOMMENDATIONS

### A. SUMMARY

The main purpose of this research was to examine stand-in-jamming missions against radars and information links using UAV swarms. Swarming technologies have undergone dramatic improvements parallel to improvements in the network-centric operations (NCO) concept. NCO emerged as a business model at the beginning of 21st Century. The idea was to create and share information within a network of different companies operating in the same environment. This new idea was adopted as a military concept, network-centric warfare (NCW). NCW depends on netted warfighting assets that share and relay information using data links. To show the effectiveness of networks and measure the networking capabilities, we examined the NCW metrics thoroughly.

UAVs are being used for very diverse military applications. Using UAVs for EA missions is not a new idea; however, to swarm a number of small UAVs to create the same emergent capability compared to that of traditional jamming aircraft is relatively new. Although UAVs have some inherent drawbacks regarding their payload and power capacity, the swarm behavior can collectively overcome these disadvantages. Moreover, the smaller RCS that UAVs possess is a very important advantage in airborne EA missions. Smaller body structures and RCSs makes it possible to use UAV swarms positioned closer to the enemy integrated air defense systems, making SIJ using UAV swarms possible.

To examine UAV swarm EA missions, we examined the distributed beamforming and wireless communication networks. UAV swarms and distributed beamforming are proposed as an economic solution to overcome transmission losses and conduct EA closer to the target receivers. We regarded UAV swarms as a warfighting asset in the NCW environment. The swarm itself is a network of autonomous individuals synchronized to a reference node within the swarm. Self-synchronization is a very important requirement for distributed beamforming and swarming behavior.

Finally, we modeled and simulated EA missions against a typical air surveillance radar and a three-node information network. Since they still apply to any platform being detected or aiming to jam the receiver, we examined the radar range equations prior to comparing them to the simulation results.

## **B. CONCLUSIONS**

In a NCW environment, information sharing among the assets in a timely manner is critical. In times of heightened tensions or war, both friendly and enemy forces operate in their own network and make decisions using their own OODA cycle. Since NCW consists of multiple information nodes within the network, loss of one to a few individual link connections can be easily tolerated, depending on the robust nature of the network design. For example, a radar system can be jammed by a hostile jammer and totally lose individual situational awareness. However, other information nodes and receivers in the same network provide accurate information about the jamming and jammer position to the IADS. In other words, the incapacitated state of the victim radar can be tolerated within the network. Real time information transfer using data links results in a very powerful warfighting capability.

In the first part of the simulation, the RADJAM simulation toolbox helped to illustrate the jamming effect on an air surveillance radar. The detection contour shows how the energy of the radar is countered by the SIJ. The radar undergoing a SIJ attack was unable to detect the target and the jammer without having any netted connection from other information sources. Although the direction of the jammer can be easily concluded from the detection contour, it is still problematic to detect the targets. This means that the radar will have no accurate information about the jammer and target, regarding their number, range, altitude, and heading.

On the other hand, this research and the simulation results showed that an EA mission against radar systems and data links affects the decision-making capability of the adversary. This is very important in today's wars, especially for time-critical missions. The EA against data links simulation with LPISimNet in Chapter V showed that the connectivity measure ( $C_M$ ), network reach ( $I_R$ ), information exchange frequency ( $\lambda_T$ ),

and operation tempo ( $\Lambda_{OODA}$ ) decreased considerably in the first two time indexes where the jammer successfully jammed two data links. Moreover, the victim node in the simulation was the NCW headquarters that makes the jamming more advantageous against NEADS OODA cycle.

### **C. RECOMMENDATIONS FOR FUTURE WORK**

Although we introduce a brief explanation of swarming, we assumed that a single UAV has the required parameters for EA that can, in reality, be achieved by swarm behavior of multiple UAVs. Emergent behavior of self-synchronized autonomous UAVs can result in the same ERP of a conventional jammer aircraft. A UAV swarm is a network of autonomous nodes connected by wireless communication links. Distributed beamforming is a result of swarm behavior of these nodes. As stated earlier in this research, all the nodes in the swarm network should self-synchronized to a common node. Self-synchronization and emergent ERP production of a UAV swarm may be examined in detail in a future work.

UAV swarm networks use wireless links to share the information for intra-swarm and inter-swarm communications. Wireless networks have some hereditary drawbacks. They are open and vulnerable to jamming as is every wireless communication. The effectiveness and results of an EA against UAV swarms may be investigated in a future study.

Since the UAV are considered as communication and sensor nodes in the swarm, NCW metrics and calculations apply for the UAV network. As a result, the loss of a single or multiple UAV in the swarm decrease the NCW parameters and change the effectiveness of swarming. On the other hand, a few losses can be tolerated without considerably changing the operational power of the swarm. NCW metrics within the UAV swarms may be a good research for a future study.

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX

```
%File Name      :esraberilela.m
%Author         :Ali Kaptan
%Date          :18 July 2012
%
%Function       :Calculates and plots detection range
%              :versus SJR and relative
%              :signal and jamming ratio vs range
%              :normalized to burn-through range.
%
%Courtesy      :Original idea of these calculations
%              :and plots cited from
%              :Mahafza and Elsherbeni (2000) [32].
%              :However, the codes
%              :are re-written according to the
%              :simulation needs.

clear all
clc
rad=pi/180;

% RADAR PARAMETERS
*****
Pt = 360e3;      % Radar trasmitter power
TA = 80;        % Antenna temperature
Te = 2800;      % Effective temperature of radar receiver
Ts = TA+Te;     % Radar system noise temperature
er = 0.9;       % Radar antenna efficiency
freq = 0.9e9;   % Frequency
c = 3e8;        % Velocity of light
tau = 1e-6;    % Pulsewidth
wave = c/freq;  % Wavelength
k = 2*pi/wave;  % Wave number (propagation constant)
ta = 1e-6;     % Radar pulse width
boltz = 1.38e-23; % Boltzman's constant
Gantdb = 29;   % Antenna gain

% TARGET PARAMETERS
*****
rcsdb = 10;     % Target rcs
Rtar = 20000;   % Target Range

% JAMMER PARAMETERS
*****
Gjdb = 5;       % Jammer gain in direction of radar (in
db)
hj = 0;        % Jammer altitude
Bj = 10e6;     % Jammer bandwidth
```

```

Pj = 20;           % Jammer transmitter power
Rj = 5000;        % Jammer range fixed

% Max detection range with no jamming (From RADJAM Results)
RRmax=384000;

%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%Basic Calculations and Conversions
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Gj = 10^(Gjdb/10);
rcs = 10^(rcsdb/10);
Gant = 10^(Gantdb/10);
ERPr = Pt*Gant;   %Radar ERP
ERPj = Pj*Gj;    %Jammer ERP
Aer = Gant*wave^2/(4*pi); %Effective Area
demoJN = ((ERPj*(Aer)/(4*pi*Rj^2*Bj)))+(boltz*Ts); % J + N

%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%Calculate Detection Range (km) vs SJR (dB)
%%[(45)]
%%No loss
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Rinc = linspace(0, RRmax, 1000);
SJR = Rinc;

for i=1:1000
demoS = ERPr*rcs*(Aer)*tau/(4^2*pi^2*Rinc(i)^4);
demoSJR = demoS / demoJN;
SJR(i) = 10*log10(demoSJR);
end

Rinc = Rinc./1000;
figure(1)
plot(Rinc, SJR, 'k');
xlabel('Detection Range in Km');
ylabel('SJR in dB');
grid;

Star = ERPr*rcs*(Aer)*tau/(4^2*pi^2*Rtar^4);
SJRtar = 10*log10(Star / demoJN);
disp(['Signal-to-Jammer Ratio for the target at ',...
num2str(Rtar/1000), ' km = ', num2str(SJRtar), 'dB. ']);

%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%Show Burn-Through Range for SSJ
%%S=J+N from [(45)]
%%No loss

```

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
S_ss_j_demo = Pt*Gant*racs*Aer*tau/(4^2*pi^2);
JN_ss_j_demo = ERPj*Aer/(4*pi*Bj);
S_ss_j = 1:1:1000;
JN_ss_j = 1:1:1000;

for j = 1:1000
    S_ss_j(j) = 10*log10(S_ss_j_demo/(Rinc(j)*1000)^4);
    JN_ss_j(j) =
10*log10((JN_ss_j_demo/(Rinc(j)*1000)^2)+boltz*Ts);
end

figure(2)
semilogx(Rinc, S_ss_j, 'k', Rinc, JN_ss_j, 'k-');
xlabel('Range Normalized to Burn-Through Range');
ylabel('Relative Signal and Jamming Amplitude (dB)');
legend('Target Echo', 'SIJ');
grid;

```

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- [1] TAI. (2012, Aug.15), [Online], Available: <http://www.tai.com.tr/tr/basin-bultenleri/anka-ucus-testlerine-basariyla-devam-ediliyor>
- [2] I. Kocaman, “Distributed beamforming in a swarm UAV network,” M.S. thesis, Naval Postgraduate School, 2008.
- [3] M. G. Erdemli, “General use of UAS in EW environment—EW concepts and tactics for single or multiple UAS over the net-centric battlefield,” M.S. thesis, Naval Postgraduate School, 2009.
- [4] M. Pavone, K. Savla, and E. Frazzoli, “Sharing the load: Mobile robotic networks in dynamic environments,” *IEEE Robotics and Automation Magazine*, vol. 16, no. 5,2, pp. 52–61, Jun. 2009.
- [5] N. R. Frantz, “Swarm intelligence for autonomous UAV control,” M.S.thesis, Naval Postgraduate School, 2005.
- [6] D.C. Schleher, *Electronic Warfare in the Information Age*. Norwood, MA: Artech House, 1999.
- [7] Avionics Department AIR-4.5. “Electronic warfare and radar systems engineering handbook,” Washington, DC: Naval Air Systems Command, 1999.
- [8] Joint Publication 3-13.1, “Joint doctrine for electronic warfare,” Washington, DC: Joint Staff, 2007.
- [9] M. Armitage, *Unmanned Aircraft*, 1st ed. London: Brassey's Defence Publisher Ltd, 1988.
- [10] M. Arjomandi, *Classification of Unmanned Aerial Vehicles*. Adelaide, Australia: The University of Adelaide, 2007.
- [11] A.Grag, P. Gill, P. Rathi, Amardeep, and K. K. Garg, “An insight into swarm intelligence,” *International Journal of Recent Trends in Engineering*, vol.2, no.8, pp. 42–44, Nov. 2009.
- [12] B. T. Clough, *UAV Swarming? So What are those Swarms, What Are the Implications, and How do we Handle Them?* Wright-Patterson AFB, OH: Air Force Research Laboratory, 2002.
- [13] D. C. Jenn, “Transmission equation for multiple cooperative transmitters and collective beamforming,” *IEEE Antennas and Wireless Propagation Letters*, vol. 7, pp. 606–608, 2008.

- [14] J. Uher, A. Wysocki, and B. J. Wysocki, "Review of distributed beamforming," *Journal of Telecommunications and Information Technologies*, vol. 1, pp. 78–88, 2011.
- [15] H. Ochiai, P. Mitran, H. V. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *IEEE Transactions on Signal Processing*, vol. 53, no. 11, pp. 4110–4124, 2005.
- [16] M. F. Ahmed, and S. A. Vorobyov, "Collaborative beamforming for wireless sensor networks with Gaussian distributed sensor nodes," *IEEE Transactions on Signal Processing*, vol. 8, no. 2, pp. 638–643, 2009.
- [17] D. S. Alberts, J. J. Gartska, and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd revised ed. Washington, DC: CCRP Publication Series, pp. 87–103, 2000.
- [18] A. K. Cebrowski, and J. J. Garstka, "Network-centric warfare: Its origins and future," *Proceeding of the Naval Institute*, vol. 124, no. 1, pp. 28–35, 1998.
- [19] Department of Defense, Section 3, In *Network centric warfare report to congress*, pp. 3-1–3-20, 2001.
- [20] A. K. Cebrowski, *Implementation of Network-centric Warfare*. Washington, DC: Office of Force Transformation, 2004.
- [21] P. E. Pace, *Detecting and Classifying Low Probability of Intercept Radar*, 2nd ed. Norwood, MA: Artech House, 2009.
- [22] J. R. Boyds, "A discourse on winning and loosing," One of Boyd's briefing titles on competitive strategy, 1987.
- [23] T. Moon, E. Kruzins, and G. Calbert, "Analyzing the OODA cycle," *Phalanx*, vol. 35, no. 2, pp. 9–13, 34, 2002.
- [24] M. F. Ling, T. Moon, and E. Kruzins, "Proposed network centric warfare metrics: From connectivity to the OODA cycle," *Military Operations Research*, vol. 10, no. 1, pp. 5–13, 2005.
- [25] Y. Q. Chen, and P. E. Pace, "Simulation of information metrics to assess the value of networking in a general battlespace topology," *Proc. of the IEEE International Conf. on System of Systems Engineering*, 2008.
- [26] M. Magalhaes, T. E. Smith, and P. E. Pace, "Adaptive node capability to assess the characteristic tempo in a wireless communication network," *IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks*, pp. 3040–3045, 2012.

- [27] M. A. Richards, J. A. Scheer, and W. A. Holm, *Principles of Modern Radar—Basic Principles*, Raleigh, NC: Scitech Publishing Inc, 2012.
- [28] D. C. Jenn, “Radar cross section,” In *Radar and Cross Section Engineering*, 2nd ed. Reston, VA: American Institute of Aeronautics and Astronautics Inc., pp. 1–37, 2005.
- [29] M. I. Skolnik, *Introduction to Radar Systems*, New York, NY: McGraw-Hill Companies, pp. 30–103, 2001.
- [30] M. Skolnik, *Radar Handbook*, New York, NY: McGraw-Hill Companies, pp. 1.10–1.13, 2008.
- [31] D. P. Meyer, and H. A. Meyer, “Review of the radar range equation,” in *Radar Target Detection - Handbook of Theory and Practice*. New York, NY: Academic Press, Inc., pp. 1–3, 1973.
- [32] L. V. Blake, *Radar Range-performance Analysis*. Lexington, MA: Lexington Books, 1980.
- [33] B. R. Mahafza, and A. Z. Elsherbeni, *Matlab Simulations for Radar Systems Design*. Boca Raton, FL: Chapman & Hall/CRC Press, 2000.
- [34] D. C. Jenn. (2012, July 14), *RADJAM MATLAB<sup>®</sup> toolbox(version 2.2)* [Online], Available: <http://www.dcjenn.com/>
- [35] P. E. Law, *Shipboard Antennas*. 2nd ed. Dedham, MA: Artech House, 1986.
- [36] Y. Chen, “Simulation of network-enabled electronic warfare metrics to access the value of networking in a general information and radar topology,” M.S. thesis, Naval Postgraduate School, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dan Boger  
Department of Information Sciences  
Monterey, California
4. David C. Jenn  
Department of Electrical & Computer Engineering  
Monterey, California
5. Edward L. Fisher  
Department of Information Sciences  
Monterey, California
6. 1<sup>st</sup> Lt. Ali Kaptan  
Turkish Air force  
Ankara, Turkey
7. Hava Kuvvetleri Komutanligi Kutuphanesi  
Hava Kuvvetleri Komutanligi  
Ankara, Turkey
8. Kara Harp Okulu Kutuphanesi  
Kara Harp Okulu  
Bakanliklar, Ankara, Turkey
9. Deniz Harp Okulu Kutuphanesi  
Deniz Harp Okulu  
Tuzla, Istanbul, Turkey
10. Hava Harp Okulu Kutuphanesi  
Hava Harp Okulu  
Yesilyurt, Istanbul, Turkey