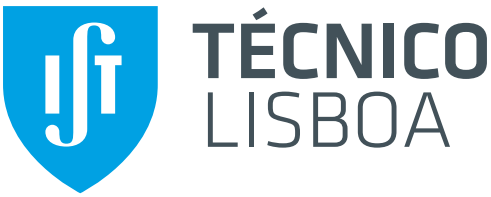


Electronic Warfare Aeronautical Systems

Research Report

Pedro Afonso	João Manito	Daniel de Schiffart
66277	73096	81479

Integrated Avionics Systems

Integrated Masters in Aerospace Engineering

Instituto Superior Técnico

December 2018

Abstract

In this research report we will present a general discussion on the topic of electric and electronic aeronautical systems and their presence within the context of war and warfare, beginning with an historical overview of the presence of these systems in aeronautics, their growth and expansion, the detection and exploitation of their vulnerabilities and subsequent and ongoing battle between exploitation and protection of these systems. Following it will be a presentation of some of the currently used systems for aerial electronic warfare, as well as a simple explanation of their functionality and inner workings.

Contents

1 Introduction

Electronic Warfare is defined as a set of measures and actions performed by the conflicting sides to detect and electronically attack enemy electronic systems for the control of forces and weapons, including high precision weapons, as well as to electronically defend one's own electronic systems and other targets from technical intelligence (electronic intelligence, ELINT), *jamming* and non deliberate interference. Electronic attack can be achieved by:

- Jamming (active, passive, false targets);
- Reduction of radar and thermal detectability;
- Changing the electrical properties of the environment (conditions for the propagation of electromagnetic waves).

Typically, EW methods of operation can be either offensive or defensive in nature. When we speak of offensive operations, first and foremost we have in mind operations conducted using *jamming* or

employing weapon systems that automatically home in on radiation sources. Both of these offensive operation methods are used not only to attack (or destroy) electronic systems for the control of forces and weapons, but also to defend one's own electronic systems against ELINT and *jamming*.

In the first instance, the *jamming* targets are the receivers of radar, communications, and radio navigation systems. In the second case, the jamming targets are ELINT receivers that form a part of active jamming and ELINT stations, as well as of reconnaissance and strike systems.

Typical defensive EW operations involve protecting the respective systems from *jamming* and ELINT by increasing their equivalent specific energy potential, modifying their time, frequency, space and other characteristics, or by making them more secure (masking, deception).

As a rule, the most effective solution to the problem of protecting against *jamming* is achieved by combining both purely defensive and offensive operations. More precisely, this is achieved by destroying the jammer or by electronically jamming ELINT systems and active jammers. Thus, it may be said that jamming and ELINT, taken together, by and large comprise the basis of EW.

When viewing radar and other electronic devices as targets of E\x! (*jamming*), we should keep in mind that jamming signals directly affect radio receivers. A priori, as a rule, the jammer or other electronic attack system does not have full information about the target of the attack. In order to eliminate the element of chance for the victim receiver, it should be attempted to orient oneself by assuming that the victim system uses optimum or quasi-optimum processing methods for the signals received and within a certain standard (conditional) electronic environment. Depending on how the radar or other electronic device operates, differing variants of processing optimization may occur, thus resulting in various mathematical models.

Part I

History

The nature of warfare and the history of the development of any warfare technology is to develop and implement superior tools of war and deny the opponent the same privilege. With that in mind, the story of the development of electronic warfare can best be described by Newton's third law, which states

> *For every action, there is an equal and opposite reaction.*

The growth of the technologies of war can not only be described by the advances made by either side of a war, but also by the progress made by the opposing sides in denying said advance. Such is the story of the dichotomy of electronic warfare, both in the offensive (attacking) and defensive (protecting) fronts of development.

2 Early Beginnings

2.1 First known instance

The story of electronic warfare can have different begins based on what the actual definition of the term entails and is considered to be, regarding both halves of the term. The *electronic* part, where a definition of what constitutes a useful application of electricity and electronic components, and the *warfare* side of the term, where ambiguity can be found on what could be actually considered as deliberate attacking action and protection thereof within the electronic realm.

Ambiguities aside, a good starting point can be traced all the way back to the time of the civil war of the United States of America, where the early developments of the telegraph by Samuel Morse and their uses in the war gave their users (in this case, the Union forces) clear advantage in long distance communication[1]. To counteract this advantage, the Confederate forces rerouted telegraph wires, forged fake communications, or straight up cut the communication channels. This can be traced all the way back to the start of the civil war in 1861 as the first recorded example of signal jamming, and therefore, the **first known instance of electronic warfare**.

2.2 Beginning of *modern* electronic warfare

With the emergence of radio technology, demonstrated by Heinrich Hertz in 1888, the transmission of Morse code became less restricted to physically mounted transmission lines and could be used for long-range communications with much more facility than ever before. Quickly these systems became commonplace, first with a focus on civilian use and not much later for military use.

With these developments, the interest in disrupting these *wireless* communications became bigger. Approaching the more modern definition of electronic warfare, the objective was set at intercepting or blocking these communications entirely. The first recorded instance of radio *jamming*, as the procedure quickly came to be known as, occurred in 1901 in the United States of America, in a civilian yacht race.

> *The first recorded instance of deliberate radio jamming took place in September 1901, in the U.S. Interestingly, it was aimed at securing commercial gain rather than military advantage. As now, there was considerable public interest in the America's Cup yacht races, and the newspaper first to reach the stands carrying each result stood to reap a large profit. In that year, Marconi obtained a contract from Associated Press [...] Another company, [...] Wireless Telegraph Company of America, secured a contract [...] A third company, the American Wireless Telephone and Telegraph Co., [...] failed to get a sponsor but decided to exploit the situation (and)[...] used a transmitter more powerful than its competitors, and one of its engineers, John Pickard, worked out a method which allowed him to jam signals from the other companies while at the same time reporting on the progress of the race from his boat [...] thus only AWT&T was able to pass accurate reports on the races. [7]*

[1] As mentioned in Kucukozyigit [7]. Most of this section was written using references Evans [3] and Price [13] as well as the aforementioned reference.

This event effectively marked **the first occasion of offensive *jamming*** and therefore the **first occurrence of modern electronic warfare**. Although the event didn't accumulate much military attention, radio *jamming* was becoming widely implemented and experimented with in military exercises, first by the British Navy in 1902 and by the U.S. Navy in 1903. This set precedents for western countries and their respective military forces to counteract the ever-increasing use of radio.

In the eastern warfronts, the appearance of *jamming* came by the Russians in the 1904-1905 Russo-Japanese war, which marked the first known war in which both sides used radio communications.

2.3 Growth and expansion of radio

In a period of relative peace and quick scientific progress, this new-found technology was developing rapidly. The beginning of the 20th century saw radio technology improve its transmission ranges, and more channels were being introduced by the narrowing of channel bandwidths. Not only that, but the transmitter and receiver technologies were being continually improved, and as a result, interference was lowering and communications became clearer.

Portability of radio systems was improving as well, which made the pairing with the emergent aeronautical field an obvious choice. Soon enough, aeroplanes were being fitted with radio communications.

3 World War 1

The spark of the first major World War, *the war to end all wars*, made the first real testing scenario for a lot of emerging warfare technology in all fields, from weapons to transportation to information to communication, and at the forefront of this last topic lied the radio.

By this point, most countries involved in the war had implemented and exercised with some form of signal *jamming*, with the remaining countries quickly catching up. But the functionality and importance of this technology and of radio communications wasn't fully understood by their users, and most mid-battle signal *jamming* occurred between friendly forces, when too many radio communications were being attempted within a small space.

Towards the end of World War 1, the use of radio communications was so widespread that its presence could be exploited by either side of the war. A notable example was the detection of German U-boats in the Mediterranean, which started as a major threat to Allied forces in the battle for the sea, but whose detection and persecution became trivialised by the implementation of primitive direction finders that worked based on the communications performed by these underwater vessels.

4 War Aftermath and Further Developments

World War 1 was, up to that point, the biggest stage for military use of radio and the then-emerging field of electronic equipment and technology in the military, and the potential was present. With the desire of a lasting peace, the countries involved in the war agreed to organise and prevent similar

events from happening again, but the mistrust created meant that while peace looked possible, all the parties involved were preparing themselves should the need arise again.

With the aforementioned potential, this meant that research was going to develop quickly, specially without the pressure of short-term war. In the period after the war, radio-transmitting equipment had its weight and size reduced, its reliability and performance improved, and its implementation for various uses widespread, which raised overall population education with the technology. This meant that communication between land, sea, and air was continually improving.

4.1 RADAR

A major breakthrough happened in this period with the appearance of **RADAR**[2] in the early 1930s, which came as a consequence of the developments listed previously. This technology allowed for the detection of incoming traffic and enemy forces from very long distances with a similar technology as radio, and soon enough radar would be implemented in military forces worldwide. By the end of the 1930s, radar technology would develop from detecting aircraft at 30 kilometres to detecting them at 160 kilometres, with the major obstacle becoming the radius of the Earth.

This quickly prompted the emergence of countering technology. With radars being so widespread, a way to approach enemy bases undetected would be a major warfare advantage, so development gained expedience in methods to avoid detection or disabling radars from afar by *jamming* them in much the same way as it is done with radio communications. Around this time, the first tests with this purpose in mind were done in London using continuous wave transmitters directed at the radar.

Quickly enough, radar *jamming* became commonplace.

5 World War 2

If World War 1 was a showcase of the potential of electronics in the battlefield, World War 2 would meet a much more mature field of the exploitation of the electromagnetic spectrum in tools of war. With the development highlighted in section 4, radio communication and navigation and radar would give significant advantages to their respective users. A key in disrupting communication and flow of intelligence in either side would be the effective development and use of methods of *jamming* and interception, effective tools of electronic warfare.

5.1 *Battle Of The Beams*

A notable example of electronic warfare in World War 2 occurred in the beginning of the war, a period in which the Axis forces (namely German forces) increased the use of radar and used the technology for *blind* bombing in the United Kingdom [4].

Using diverse radio navigation systems, the Germans had accurate bombing ranges of up to 200 nautical miles from their fronts while completely in visual nighttime darkness.

[2] **RA**dio **D**etection **A**nd **R**anging.

The British forces were forced to implement counter-measures to the German radars by *jamming* their signals accordingly. However, the technology used was unknown by the British, so they were forced to adapt depending on what intelligence could be gathered.

5.1.1 The *Knickebein*

The first used radar technology, *Knickebein*, relied on the German-developed Lorentz [8]. This radar, used for approach and landing procedures in German soil, used two radio beams transmitting Morse dots and dashes respectively, to allow for a pilot to centre their trajectory with the two emitters by measuring the proportion of either signal, as seen in figure 1.

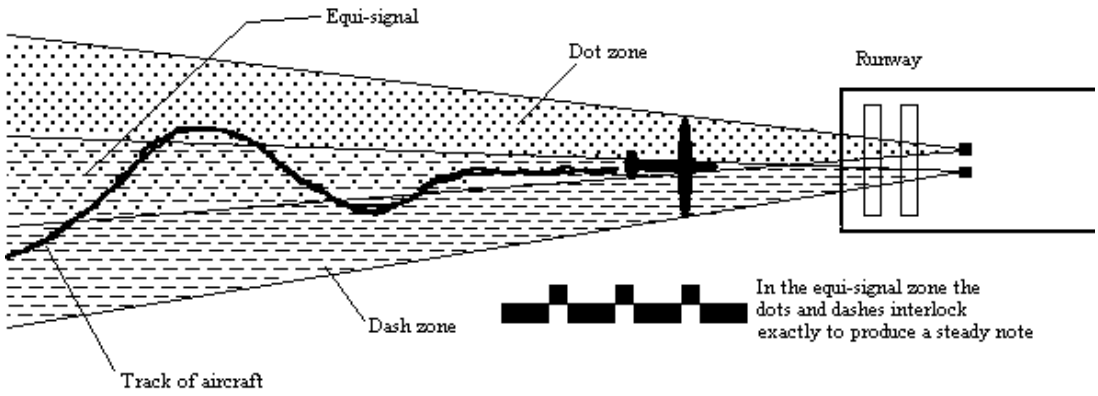


FIGURE 1: *The functioning of the German Lorenz radar.*

This radar was adapted to orient the bombers towards targets in the United Kingdom by separating the beams far from each other to define the latitude and longitude of the dropping point, as can be seen in figure 2. This allowed the pilots to fly blind and accurately find the bombing point in a pre-radio navigation era.

The technology was countered by mimicking the signals sent by German forces to the pilots to force them to drop bombs in safe areas and land wherever the signals guided them to do. Some German pilots even end up landing in British bases believing they were in Germany, as visual darkness prevented them from distinguishing one from the other.

5.1.2 German counter-countering

The Germans countered this by implementing different technologies, named *X-Gerät* and later *Y-Gerät*, unknown to the British, which meant new counter-measures had to be found. These technologies were effectively shut down when the Allied forces found intelligence within crashed bombers that allowed them to jam the correct German-used frequencies.

The titled *Battle Of The Beams* period ended when the German air force *Luftwaffe* attention diverted to the Soviet Union front. But this period highlighted the **measure-counter-measure nature of electronic warfare** in the World War 2, an element of electronic warfare which persists to this day.

FIGURE 2: *Map of the German Knickebein radar beams used for the night bombings of the Battle Of The Beams.*

5.2 Further War Development

The British had learned lessons within the field and moved on from defence to offence, by beginning to implement aircraft-detection *jammers*, namely the airborne *Mandrel* [7]. The *Mandrel* swamped the return echo of the enemy radars, distoring reception sizes and ranges and difficuling accurate detection.

Later on, both sides of the war would see widespread use of *chaff*, called *window* by the British and *düppel* by the Germans, which consisted of materials dispersed in the air to create false radar positives to conceal real threats.

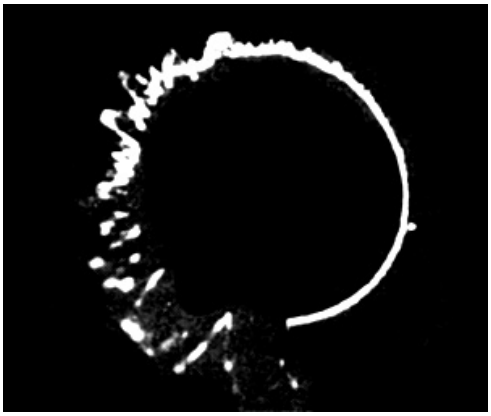


FIGURE 3: *Effect of chaff in a radar display. On the right, the display is clear and a target is visible, while on the left the chaff scattered around distorts the input signal.*

Massive use of passive *jammers* by English bombers started on June 24, 1943 during the nighttime bombing raid on Hamburg and continued systematically in subsequent raids. The *jamming* targets were *Wiirzburg* gunlaying radar stations, which had an emitted signal wavelength of about 50 cm. In this case, the passive jamming consisted of manually launched tinfoil strips (dipoles) of the order of

25 cm in length (i.e., equal to approximately half the radar wavelength). As a result of this jamming, bomber losses decreased by about half for several months. This use of *jamming* was preceded by lengthy reconnaissance of the *jamming* targets. The decision to employ *jamming* was made after losses reached the maximum permissible level.

To a large extent, this *jamming* was so highly effective due to the wavelength selected for the *Wiirzburg* radar. The absence in it of circuits to protect against passive *jamming*, which appeared only at the end of the war; and the absence of the possibility to change wavelength. In October 1943, U.S. bombers began employing active jamming against *Wiirzburg* radar using carpet-type *jammers*, which turned out to be highly effective because it was not possible to alter the carrier frequency.

In the pacific front, *jamming* saw widespread use, but little to no development.

6 Post-War Development and Other Trials

The biggest stage for electronic warfare had just passed and with it came several advancements in relevant warfare technology, in which numerous resources and man-hours were invested due to the urgency and necessity for these technologies in the middle of all-out war between many developed countries. The arrival of peace allowed for more experimentation with the advancements of wartime, but warfare trials for any developed tools would not arrive in the same scale as the one that just passed. Still, the years that followed World War 2 would still see scattered warfare with numerous chances for implementation of new technology.

With the standardisation of electronic warfare, other aspects of each armed forces were starting to take notes. Air tactics now had to consider heavily the presence of enemy radars and develop manoeuvres and procedures to avoid detection, and the emergence of **stealth** technology meant a whole new field of engineering which would see a lot of investment. This period would also see the first appointment of Electronic Warfare Officers.

It is possible to distinguish approximately four basic phases of significant change in the structure and algorithms of both radar and electronic warfare systems. The period of the 1950s corresponds to the development of non-coherent radar with rapid alteration of the carrier frequency and anti-*jamming* devices built using pulse-to-pulse cancellation. In *jammers*, electronic frequency alteration was introduced. Special devices for the launching of chaff were developed.

This period also saw the invention of the first functional surface-to-air missile system, which saw the deployment of radar-guided missiles controlled from the ground to meet and annihilate airborne targets. This soon prompted the beginning of development of counter-*jamming* of these systems.

7 Two Global Superpowers

The Cold War that covered most of the second half of the 20th century was heavily reliant on intelligence and the protection thereof, as both sides of the war, the U.S.A. and the ever-growing U.S.S.R., wanted to develop as many tools of war as possible while hiding their information from the opponent. Thus

gathering opposing force intelligence was, at the time, of major importance, but was also a major risk, as both parties were not officially at war with each other, and either side being caught stealing technology from the other could risk starting war, or *setting off the keg*, as was commonly referred.

This meant that electronic warfare came to the forefront of intelligence gathering missions. Aircraft were being developed with more complex and advanced electronic warfare devices on-board, such as *jammers*, radio, and computers. These aircraft were being steadily employed by the United States on Electronic Intelligence missions, now commonly referred to as **ELINT missions**.

At the time, the *Lockheed U-2* was at the forefront of these developments. The aircraft was often used in these ELINT missions for gathering visuals of Soviet military and industrial installations and intelligence on Soviet radars and signals with the technology it carried on-board. With the widespread use of radar by both parties of the war, the aircraft was designed to gather a number of data from the enemy, including (but not limited to):

- The rate of scanning of a radar beam, including direction and speed;
- Time width of radar pulses;
- Rate of radar pulses;
- Frequency of opponent emitters;
- Signals and emitter locations.

FIGURE 4: *The Lockheed U-2 aircraft, used by the United States of America for ELINT missions during the Cold War.*

While remaining on *friendly* terms with the Soviet Union, the United States performed several reconnaissance missions with this and several similar aircraft, until some were shot down by advancing anti-aircraft and anti-*jamming* technology.

8 The Vietnam War

The late 50s and early 60s saw the United States joining the war in Vietnam. Fighting a war on foreign soil meant several problems for the joining forces, as they were entering the enemy's battlefield and

would have to face the enemy's setup as opposed to preparing their own ground. Early in the war, the invading forces suffered numerous airborne casualties due to Vietnamese radars, surface-to-air missile systems and anti-aircraft units installed on their grounds, which could detect and intercept invading aircraft.

This saw the development of counter-measures to fight this type of tracking and detection, and new models of codenamed *Wild Weasel* aircraft were shipping out equipped with Radar Homing and Warning systems, developed to shut down the aforementioned threats. These aircraft carried numbers of radar-seeking missiles, which would hone in on radar signals emitted by enemy forces to destroy them and provide cover for more ground-oriented bombers and other aircraft.

FIGURE 5: *An F-16 Wild Weasel aircraft.*

This greatly facilitated the invasion and made the attack of heavily fortified areas possible without heavy casualties using a coordination of ground, sea, and air forces, but also reconnaissance and intelligence, as the anti-aircraft weaponry relied greatly on radar detection to remove airborne threats.

The Vietnam War very much highlighted the importance of correct knowledge and use of electronic warfare in the modern war landscape and its position as a key factor in the outcome of modern warfare.

9 The First Gulf War – Operation Desert Storm and The Beginning of The Modern Age

The first Gulf War at the beginning of the 1990s once again put the current status of electronic warfare and its importance to the test. Both sides and their arsenal were put to the test, and as proven time and time again, intelligence would play a major role in the final outcome.

FIGURE 6: *A Lockheed F-117 Nighthawk aircraft taking off during Operation Desert Storm, one of the first aircraft to be designed with stealth technology in mind.*

The Iraqi military were setting up with massive amounts of anti-aircraft artillery and surface-to-air missile systems to contain the invasion of the coalition forces, and an imposing airborne arsenal comprised of a mix of old and new Soviet-developed aircraft.

Unlike previous war, despite the Iraqi communication, transportation, military and power infrastructure being well-run and providing their forces with the necessary power for battle, the coalition forces aimed for disabling their command and control system to turn the outcome of the airborne warfare in their favour.

This meant that the coalition would favour targets such as command posts, communication systems, anti-aircraft radars and electrical generation networks to debilitate the electronic warfare capabilities of the Iraqi forces.

A combination of radar decoys, *jamming* aircraft and land-attack missiles were used to swiftly destroy air command and communications centres. Following these eliminations, technology developed from the radar-seeking missiles used in the Vietnam War was used to eliminate the Iraqi's radar-powered anti-aircraft capabilities. Decoys simulating larger aircraft were escorted by bombers to disperse Iraqi attention and distract them from the real targets, while providing cover for those bombers to infiltrate and reach advantageous positions for attack.

A host of targets in Iraq were also destroyed by stealth aircraft, which possess a very low radar signature and could fly in surveyed areas relatively undetected as long as it remained out of visual and audible detection. This meant that the overall airborne casualty count remained very low for the dimension of the battles fought.

Combined with a host of other technology unavailable to the Iraqi forces meant that the war quickly and swiftly swung in favour of the coalition forces. The first Gulf War marked the turning point of modern warfare, with electronic warfare securing its central position as deciding factor in the outcome of modern warfare.

Part II

Electronic Attack

10 Introduction

Electronic attack can be implemented by jamming, changing the electrical and magnetic characteristics of the environment, or by reducing the radar and thermal detectability of aircraft. At the present time, the basic means of electronic attack in the radio frequency band is the use of various jamming signals that directly affect electronic systems. These signals are deliberate electromagnetic emissions with the appropriate amplitude, frequency, phase, polarization, space and time characteristics. Practically speaking, jamming signals are·produced by jammers (electronic attack systems).

In a given electronic environment, jammers are used in particular ways depending on the specifics of the targets being jammed and the capabilities of the jammers.

In the general case, electronic attack systems comprise an information support and control system, a subsystem for producing jamming signals, high-frequency amplifiers and generators with modulators, and antenna devices. *ELINT* systems, knowledge bases and computer data that enter into the *EW* complex serve as the basis for the information support and control system. The *ELINT* subsystem seeks out, receives and processes radio signals from jamming targets. By comparing signals coming in from *ELINT* and a priori information contained in the knowledge base and computer data:

- The electronic environment is evaluated;
- The jamming target is determined, as well as the type and parameters of the jamming signal needed;
- A means of attacking the jamming target is selected and executed.

Jamming methods are determined by the characteristics of the jamming targets and the abilities of jammers to cause information damage to the victim, given specific conditions of the operational and tactical environment.

Information damage means the quantity of information that the attacked side loses during a specific time interval as a result of the effect of jamming or other *EW* measures.

Thus, jamming signals, as well as systems and techniques of jamming, can be considered to be the basic elements of electronic attack.

Three types of jamming signals have been defined to date: destructive, masking and deception. They also occur in combinations. As a rule, masking and deception jamming signals are additive.

The basic targets for jamming using airplane and helicopter based jamming systems are *AAD - Army Air Defense* - radar systems of various types (for control of *AAD* forces and weapons etc...). Besides these jammers, passive jamming is widely used, as well as optoelectronic jamming systems.

The determining element in a modern airborne jamming system is automatic active jammers with an information support system permitting the control both of active and passive jamming systems and

optoelectronic jamming systems in the dynamics of *EW*.

A block diagram for an automatic jammer is given by the figure 7, which is the logical result of the analysis of a smoothed radar environment, occurring at the current time in the dynamics of *EEW*. The structure of a jammer permits the formation of jamming signals both for the jamming of radar systems for control of *AAD* forces and weapons. The information support system of the jammer and the jamming system as a whole are represented as an *ELINT* station, with its processor, knowledge and databases, a receiver, and the processor of the jammer itself. Besides this, the information support system also contains onboard information systems: the central onboard computer with its knowledge- and databases, the onboard radar system, the onboard optoelectronic intelligence system, the navigation and data interchange (radio communications) systems, and, possibly, an automated control system for EW systems.

A stream of signals from radar stations, which are the operations targets, arrive at the receiving antennas of the *ELINT* devices and jammers.

As a rule, while transmitting, *ELINT* receivers are not able to detect signals from a radar irradiating the aircraft in the corresponding frequency band.

After the radar signal has been detected, an analysis of the electronic environment is conducted and the operations target identified. Then, a jamming signal is generated. Depending on its type, either direct radiofrequency (RF) jamming (direct noise interference) is generated or jamming modulation of RF radiation is performed. Jamming signals are emitted in the appropriate direction by the jammer transmitter antennas.

We can include methods of concealing airplanes (helicopters) and other targets from stationary areas, figure 8, using jamming; methods of screening helicopter or airplanes in battle formation, figure 9, using jamming; the mutual screening of airplanes using electronic jamming systems; the self-screening of airplanes (helicopters) using electronic jamming systems; and the combination of electronic jamming with the destruction of electronic targets using firepower.

10.1 Destructive Jamming

Destructive jamming signals are implemented using deliberate high-energy electromagnetic radiation. The effect of destructive jamming signals is to cause irreversible damage to input components in the receivers of the targets being jammed. This damage remains even after the jamming operation has finished. In order to restore the receiver or other device, it is necessary to replace (or repair) the damaged component.

Destructive jamming effects, independent of the frequency band of radio emissions, can be implemented using radiation sources of sufficiently high-energy. In the optical band of emissions, destructive effects can be attained with the assistance of high-energy lasers. The direct target of such radiation is the semiconductor devices comprising the input components of receivers (mixers, detectors, parametric amplifiers). The heat effect or the rupturing of the field of a p-n junction results in irreversible changes in the electrical properties of the input components, due to which mixers, envelope detectors and

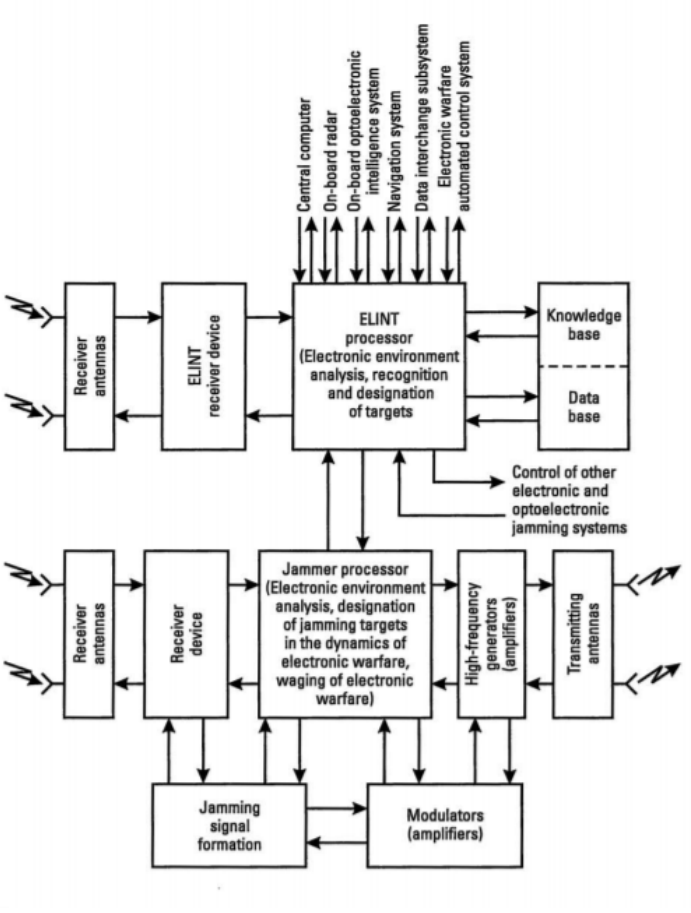


FIGURE 7: *Block diagram for an automatic jammer*

other modern electronic equipment can no longer function. We consider these radiation sources to be electronic destruction systems and not jamming systems. For this reason, sometimes we do not speak of the destruction effect, but of functional destruction.

In order to evaluate the required effective radiated power for a source of destructive jamming signals in the radio band, it is necessary to determine the power of the jamming emission P_{rec} that is acting on the semiconductor component and compare it with its threshold value P_{thresh}. Assuming that the radiation is moving in free space and the maximums for the antenna radiation patterns of the target and the jamming system correspond, we obtain:

$$P_{rec} = \frac{P_j G_j}{4\pi D_j^2} A_{rec} \gamma_j \eta_j$$

$P_j G_j$ is the effective radiated power of the jamming system; P_j is its power and G_j is the gain of the antenna; A_{rec} is the effective area of the receiving antenna of the target being jammed; γ_j is a coefficient allowing for the difference in polarization of the antennas of the target and the jamming system; and η_j is the attenuation coefficient for the jamming emission in the waveguide transmission line. This number also takes into consideration the attenuation in safeguard devices against destructive effects; D_j is the distance from the source of destructive radiation to the target being jammed.

By the other side, jamming actions that cause reversible destructive effects and result basically from

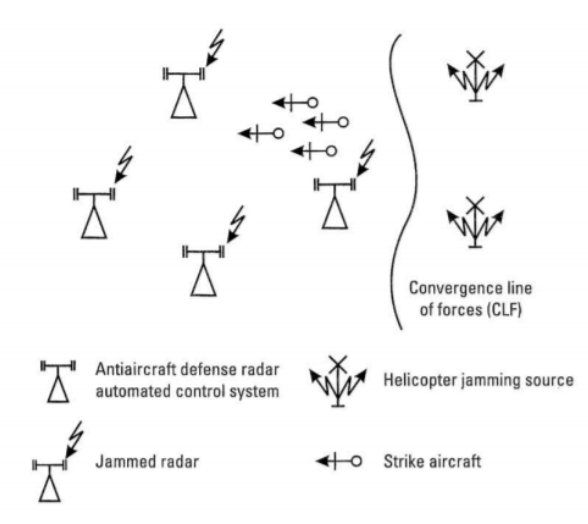


FIGURE 8: *Methods of concealing airplanes (helicopters) and other targets from fixed areas using jamming.*

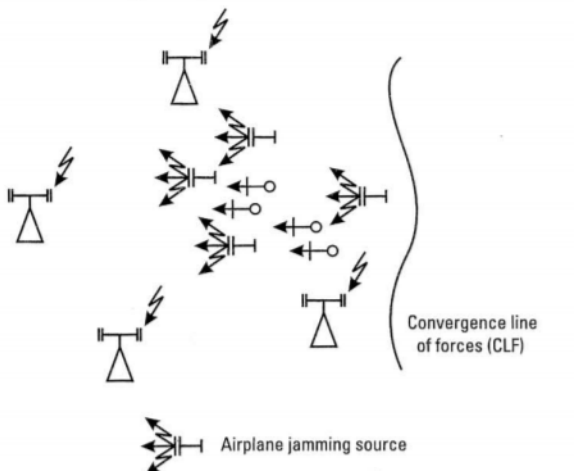


FIGURE 9: *Methods of screening airplanes in battle formation using jamming.*

the limited dynamic range of receivers K_{drr}. The latter may be defined as the ratio of the maximum and minimum values of the input signal powers, where information losses in the receiver during processing do not exceed a certain permissible value:

$$K_{drr} = \frac{P_{recmax}}{P_{recmin}}$$

Depending on the sensitivity limit P_{recmin}, the dynamic range of the receiver K_{drr} and the distance D_j from the jammer to the target being jammed, the value of the required effective radiated power causing a dynamic overload in the receiver varies over a wide range of values. When the sensitivity of the receiver is degraded, the minimum effective radiated power increases accordingly.

Passive jamming is understood to be signals formed at the input to the victim receivers as a result of the scattering of electromagnetic waves by objects employed in significant quantities. As a rule, the electromagnetic waves scattered are those emitted by victim antennas. Normally jamming is generated by scatterers such as chaff that is employed on a massive scale. However, as a rule, the chaff cloud does not change the electrical properties of the environment, since the distance between the chaff dipoles in the cloud is many tens or hundreds of times greater than the wavelength. Therefore, the effect of passive jamming is to form a masking background analogous to noise jamming. At the present time passive jamming is generated basically with anti radar chaff, dispersed in large quantities in the atmosphere. Chaff is made from paper, glass fiber, or kapron, covered with a conductive layer.

10.1.1 Masking Jamming

Masking jamming signals, acting on the receiver in combination with the useful signal, exclude or, to a significant extent, hinder the decision about detection and recognition (classification) of useful signals at the input to the receiver. In this case, the effects of jamming are reversible. After jamming operations

end, the properties of the receiver are restored.

One of the special features of attack using masking and deception jamming is its increased sensitivity when compared to other types of armed warfare and to countermeasures by the target being jammed. The latter is due to the fact that the jamming radiation being considered does not cause irreversible destructive effects in the jamming target. This permits the latter to take defensive countermeasures directly during the period of the jamming action, attenuating it or totally removing it.

What has been said justifies the necessity of developing mathematical models of jamming techniques reflecting the conflict aspect of the problem and permitting us to find the optimum course of action, taking into consideration countermeasures by the jamming target.

At the present time, such problems are being analyzed in the theory of games and statistical solutions.

10.1.2 Deception jamming signals

The basic parameters of deception jamming signals are intentionally made to appear like the signal parameters of the targets being simulated, which can result, for example, in the victim systems for control of forces and weapons being redirected from the real targets to false ones. Just as with masking jamming, deception jamming signals do not directly cause irreversible changes in the targets being jammed. The latter circumstance permits the side being jammed to exclude or attenuate the jamming effect by using the differences between the jamming and useful signals that result from specific circuits in the jamming devices generating them, and also the way they are used in the dynamics of *EW*.

11 Tactical level - Jamming

On a tactical level, the definition of jamming as a battle element can be substantiated using the example of airforce subdivisions conducting military operations against antiaircraft defense missile systems on the front line. When aircraft battle formations are screened using jamming, they can strike antiaircraft positions without suffering significant losses. In this case, airborne jamming systems represent an essential battle element. They directly participate in the delivery of material damage, having beforehand caused information damage to the electronic antiaircraft control systems. By information damage, we mean the size of the coverage area eliminated from the region where the attacked electronic system was acquiring information while working in normal operating mode during the dynamics of EW. Therefore, jamming is a weapon and not merely a means of support.

12 Operations level-Jamming

On the operations level, the thesis we have mentioned about jamming is borne out by the example of military actions taken during a defensive operation to fend off strikes by an enemy who is conducting offensive air and ground operations. In this case, jamming systems may be given the task

of thwarting a massive strike using high-precision weapons. By delivering information damage to synthetic aperture radar, *ELINT* stations within intelligence and strike systems, and high-precision radio navigation systems, jamming significantly decreases the probability that groups of aircraft and missiles, *AAD* systems, and other targets belonging to the defending side will be hit. Thus, their average combat life becomes significantly longer. In this instance, jamming prevents potential material damage by delivering information damage to the enemy's electronic systems for control of forces and weapons, thereby creating conditions for a counter-strike.

Part III

Electronic Protection

13 Introduction

As previously seen, jamming and other Electronic Attack methods are incredibly useful tools in the modern battlefield, especially in the air theatre. However, these methods present a significant drawback: the adversary might also possess sophisticated jamming systems, which can render radar, communications and weapons completely useless in the battlefield. As such, even on the early days of Electronic Warfare, special attention is given to systems and methods that are designed to counter jamming, so that one side can have an advantage over the enemy. These systems and methods are collectively called Electronic Protection (EP) measures (or by their old acronym Electronic Counter Counter-Measures, ECCM).

Throughout the years, several Electronic Protection methods where devised and implemented. There are also surely several EP methods currently in use that we aren't aware, due to military secrets. For the present report, we shall only focus on methods that are currently in active use. Of those we will explore a few:

- Pulse compression using linear frequency modulation;
- Frequency hopping;
- Sidelobe blanking;
- Polarization;
- Chaff;
- Radiation homing.

14 Pulse compression using linear frequency modulation

As a practical example of application of pulse compression, let us examine a pulse radar system. This system is based around the concept of transmitting a signal, listening to it's reflection and measure

the time delay to obtain a range. For such a radar, and assuming a simple sinusoidal pulse, we have a signal-to-noise ratio given by

$$SNR = \frac{K^2 A^2 T}{\sigma^2}$$

where K is the received signal attenuation factor, A is the amplitude of the pulse, T the pulse duration and σ is the standard deviation of the noise. As we can see, if we increase the pulse duration we can directly increase the SNR of the received signal, which is useful in defeating radar jamming. However, this also increases the transmitted signal power, while also reducing the range resolution of the radar, which is given by

$$\Delta R = \frac{1}{2} c \Delta T$$

One method to avoid these problems and increase SNR at the radar receiver is by modulating the pulse using linear frequency modulation, also called chirping. By modulating the transmitted signal linearly across a frequency band Δf centered on the carrier frequency, we obtain a signal whose correlation between transmitted and received signal is centered at $t = 0$, which behaves as a *sinc* function at that point. The -3dB temporal width of that function gives us the pulse duration of the modulation signal, which is

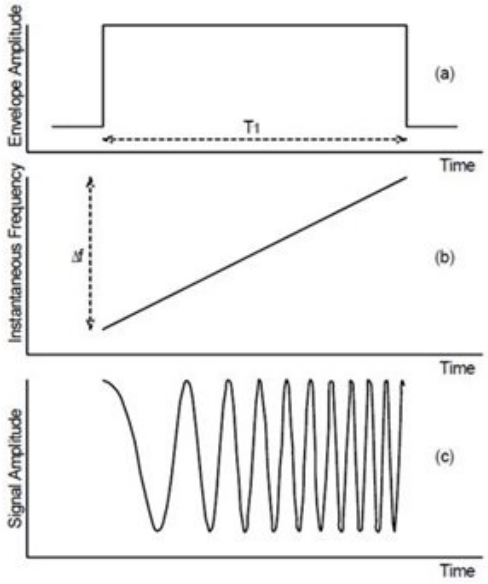


FIGURE 10: *Modulation of the transmitted pulse*

$$T' = \frac{1}{\Delta f}$$

By using suitable values of Δf, we can obtain a value of T' that is smaller than the unmodulated pulse duration T, hence the name pulse compression.

Comparing two signals, one unmodulated and the other "chirped", and considering that the energy of the signal does not change during the modulation, the relationship between the power of the

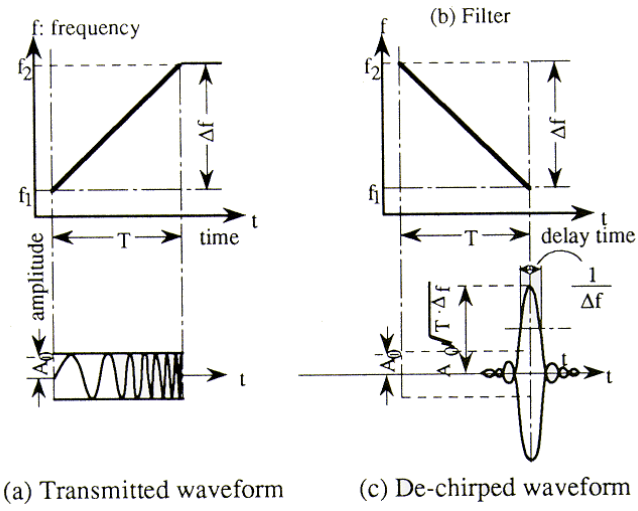


FIGURE 11: *Demodulated echo signal*

unmodulated signal (P) and the modulated signal (P') is

$$P' = P \times \frac{T}{T'}$$

Since T' is smaller than T, we have an increase in the received signal power after the modulation, without increasing the transmitted wave's energy and also increasing the range resolution of the radar.

15 Frequency hopping

In aerial warfare, transmitter-receiver links are of paramount importance; as such, it is natural that a great deal of research is done to both jam and prevent jamming those links. One way to mitigate the effects of jamming on those systems is based on the concept of frequency hopping.

Let us have a transmitter-receiver pair, operating on a fixed frequency. If a high-power jamming system is present on the theater of operations and operating on the same frequency, the pair is innoperable. However, if both systems change their frequency mid-operation, the jamming system would be rendered ineffective. This is the concept behind frequency hopping: by varying the transmitter-receiver operating frequency during operation, jamming on a specific frequency can be avoided. This is possible by using a previously coordinated set of frequencies, generated by a pseudorandom code.

Since the transmission is spread over a wider frequency range, the jamming source must spread it's jamming over a wider range of frequencies, reducing the effective noise on each specific frequency and making it easier to reconstruct the transmitted message.

16 Sidelobe blanking

A directional antenna always has sidelobes, sections of its radiation pattern that are not aligned with the antenna direction that have lower, but nonzero, gain than the main lobe. For a receiving antenna,

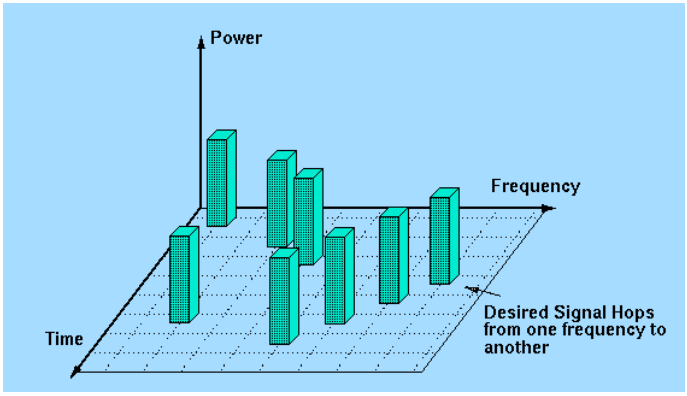


FIGURE 12: *Example of frequency hopping*

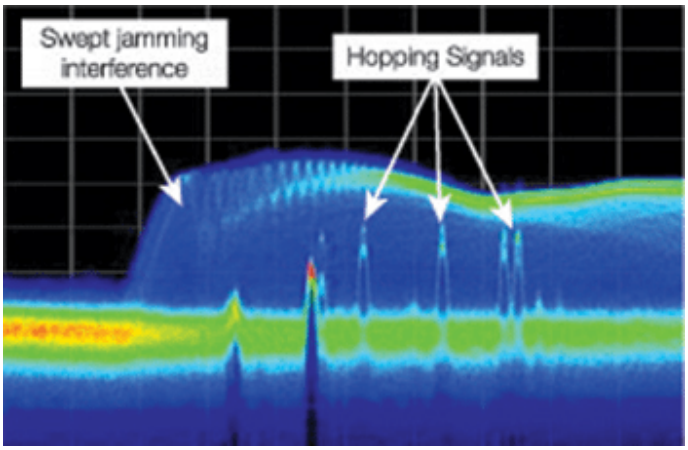


FIGURE 13: *Spectrum of a frequency hopping signal, in the presence of a jamming source*

this allows it to receive signals not in it's primary direction. Such a phenomenon is easily exploitable by jamming signals, which, with enough transmitting power, can be detected by an antenna's sidelobe and overload any wanted signals.

To prevent jamming of such a receiving antenna, we can use a technique called Sidelobe Blanking (SLB). This technique is used in the presence of pulsed interference, and consists in using an auxiliary omnidirectional antenna in tandem with the directional antenna. Having an omnidirectional receiver whose gain is adjusted to be above the gain of the sidelobes, we can compare the received signals on both receivers. Whenever the output of the auxiliary antenna is greater than the output of the main antenna, we are in a sidelobe reception state, and we can then ignore the received signal as unwanted noise, for example jamming. An example of the sidelobe suppression method working can be seen in Figure 16, where we see two radar indicator examples, one without sidelobe suppression showing several artifacts and another with sidelobe suppression, showing only a single line in the radar indicator.

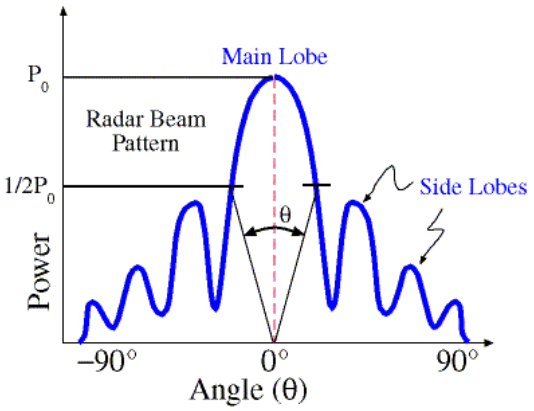


FIGURE 14: *Beam pattern of a radar antenna*

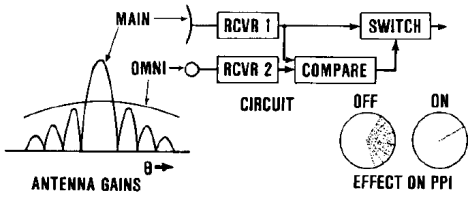


FIGURE 15: *Sidelobe suppression system functional diagram*

17 Polarization

When transmitted, an electromagnetic signal presents some kind of polarization. For an antenna system to receive a signal, such signal must have a polarization equal to that of the receiving antenna. In the case of a jamming system where only one polarization is present, the simplest method of Electronic Protection consists in the usage of two antennas with different polarizations. In the presence of jamming, only one of the antennas will have a significant received signal from the jamming transmitter, allowing the receiver to discriminate the received signals and reject the jammer.

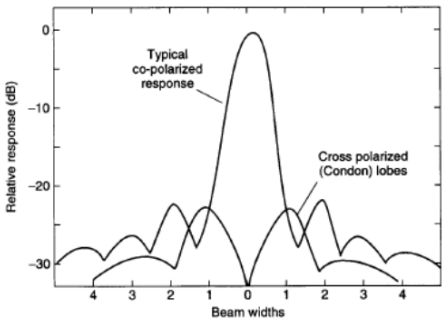
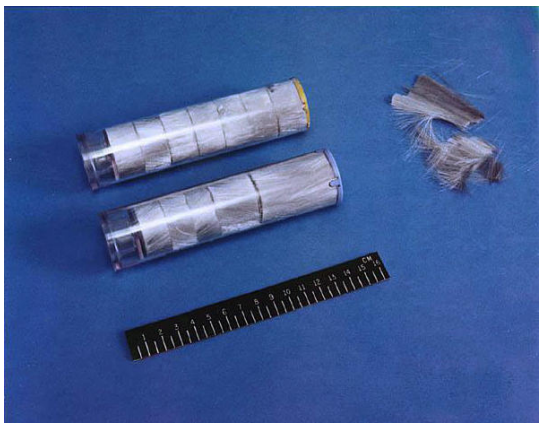


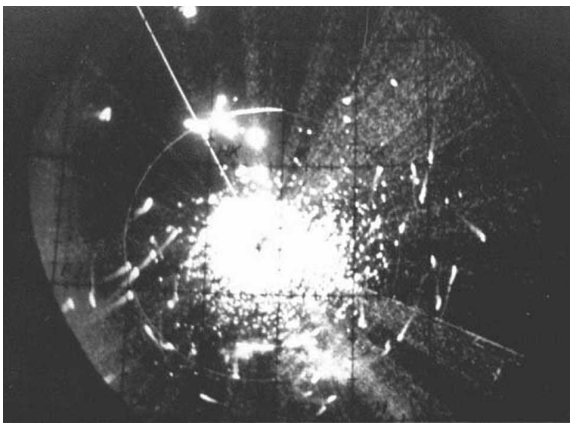
FIGURE 16: *Polarization response of a parabolic antenna*

18 Chaff

One of the earliest airborne methods of radar countermeasures, chaff is a radar countermeasure that consists in the spreading of a large number of small, thin pieces of metal or metalized material, as seen on Figure 17a. These pieces of metal are cut to sizes that are equal to half the wavelength of the signal that is intended to counter, creating a cloud of half-dipole antennas. These tunned half-dipole antennas resonate with the radar signals, creating a cloud of radar echoes designed to mask the presence of the aircraft, diverting radar-guided missiles. When used in large clouds, they can also suppress the radar of ground-based anti-air artillery and render radar detection from enemy aircraft useless for a short time. Examples of the usage of chaff can be seen in Figures 3 and 17b.



(A) *Modern chaff, in use with the United States Navy*



(B) *Radar echoes of a chaff cloud*

FIGURE 17: *Overview of radar chaff.*

19 Radiation homing

While most of this section is dedicated to negate the effects of jamming, there are cases where the desire is not to reject jamming but to focus on it. One such case is radiation homing, where we use the jamming signal to detect the location of a jammer and use it to direct a weapon, usually a missile. These weapons are usually called Anti-Radiation Missiles (ARM). One such missile is presented in Figure 18.

There are several ways to implement such a weapon. However, one of them makes use of one unintended characteristic of the sidelobe suppression method previously mentioned. By using this system to focus on the reception of the jamming signal and suppression of other signals, the jamming signal's angle of arrival can be determined and, subsequently, the jammer locked on and destroyed by the missile.

FIGURE 18: *AGM-88 HARM Anti-Radiation Missile*

Part IV

Electronic Warfare Support

One of the main functions of communication electronic warfare (EW) systems is determining the location of an emmitting target. It is useful to know the location of targets by three different reasons:

- knowing the location of targets indicates the disposition of forces;
- precision location of targets allows for use of global positioning system (GPS)-enabled fire-and-forget munitions for negation of the target;
- can give an indication of the type of entity at a particular location by clustering different types of emmiters.

A frequently used parameter for point fixed computation is the azimuth angle of arrival (*AOA*) of a signal, or its line of bearing (*LOB*). Two or more *LOBs*, assumed to be measured from sensors at known locations on the same target at more or less the same time, may intersect as in figure 19. The technique name is triangulation and it is used for point fix determination. Noise, measurement errors, and multipath reflections typically limit the point fix accuracy.

Triangulation can be implemented on all varieties of platforms, including aircraft, ships and ground vehicles. Triangulation requires an array of antennas, if signal phase is used as the parameter for computing the *LOBs* with a baseline shorter than half a wavelength to avoid ambiguities in phase angle measurement. Impinging on the antenna array at an intercept site provide us several methods to estimate the azimuth angle of arrival of signals, based on measuring the time difference of arrival or phase difference of the signals at two antennas that are spaced half a wavelength or less apart. Relative amplitude and other parameters, can also be used as the angle indicator. Most methods require the antenna array.

Available algorithms for optimum point fixed calculation are based on the least-square error *(LSE)* estimation technique.

Considering just two dimensions, there are two sensors, S_1 and S_2, separated by distance d and a single target, illustrated in figure 20. Instead of using two sensors it could be used the same sensor moved distance d. Each of the sensors computes an *LOB* relative to some reference, which is the same for both sensors. Using trigonometry:

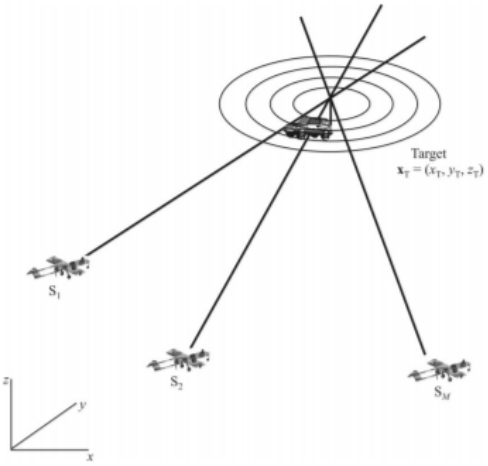


FIGURE 19: *Intersection of measured LOBs*

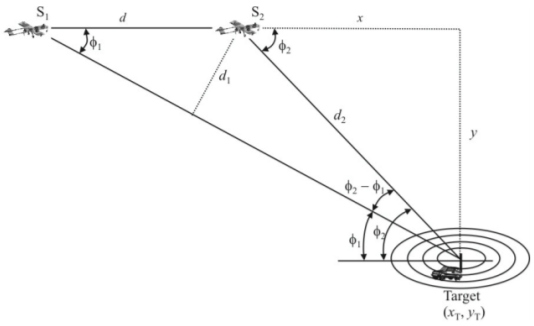


FIGURE 20: *Geometric relationships for Point Fixed by triangulation*

$$\sin\phi_1 = \frac{d_1}{d} \Rightarrow d_1 = d\sin\phi_1$$

$$\sin\phi_2 - \phi_1 = \frac{d_1}{d_2} \Rightarrow d_2 = \frac{d_1}{\sin\phi_2 - \phi_1} \Rightarrow d_2 = \frac{d\sin\phi_1}{\sin\phi_2 - \phi_1}$$

The distances to the target from S_2, x and y, can be computed as:

$$x = d_2\cos\phi_2$$

$$y = d_2\sin\phi_2$$

These principles can be extended to three dimensions and to the use of more than two sensors. The resulting coordinates can be averaged taking two sensors at a time and computing the coordinates of the target.

Plotting the measured *LOBs* and see where they cross is another technique for triangulation. The sensors could be one moving, as shown in figure 21, or three stationary, and the same results would apply.

In general, the *LOBs* are corrupted with measurement error and noise. Zero mean additive white Gaussian *AWGN* frequently characterises the noise. The *LOBs* would all cross at a single point in the absence of errors in the measurement process.

However, the result on the Point Fixed computation is to cause the *LOBs* to move away from crossing at a single point. As illustrated in figure 22, if the noise is random, the measured *LOB* could be larger than or smaller than the actual *LOB* resulting in an error ellipse.

> *The sensors could also exhibit biases, which many parameter estimators do. Biases can be caused by being an inherent property of the algorithm to compute the Point Fixed or they can be due to systematic errors in the parameter measurement device.*

[11]

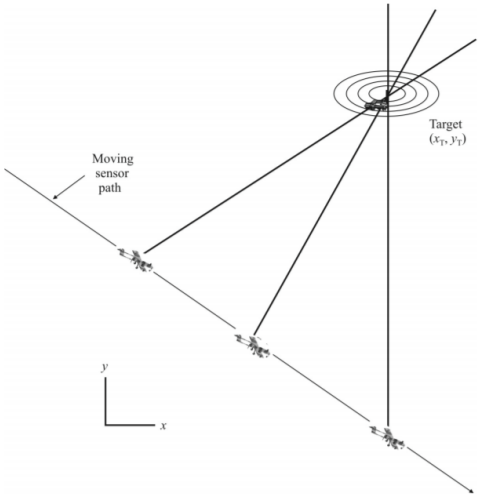


FIGURE 21: *Triangulation*

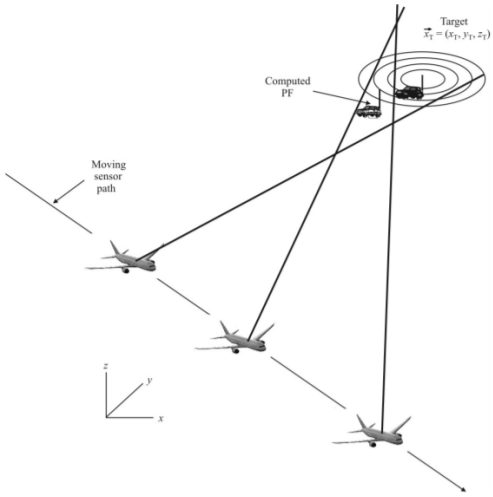


FIGURE 22: *Random error effects on computing the PF*

With three *LOBs* available, a triangle is formed closed to the actual location of the target, figure 21. Three nonstatistical methods are shown here to estimate the location of the target given the triangle, figure 23. All these techniques are used for estimating the centroid of the area of the triangle.

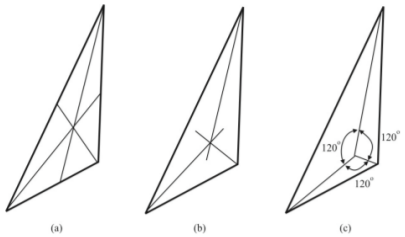


FIGURE 23: *Nonstatistical Point Fixed calculations with only three LOBs: (a) intersection of medians, (b) intersection of angle bisectors, and (c) Steiner point (defined by the point where the angles between the lines from the corners are all 120º). They are all methods for estimating the centroid of the triangle.*

The sides are connected with the opposite angle by its median, figure 23a). The angles are bisected and the Point Fixed is chosen through the point where the bisectors intersect, illustrated inf figure 23 b). At last, the Point Fixed is chosen by the intersection of lines drawn from each angle to the point in the triangle where the lines form 120° angles, figure 23 c).

Can be taken three *LOBs* at time, figure 24 (b-e), if there are more than three *LOBs* in the calculation, as shown in figure 24 a). For final fix determination, the coordinates of the resultant centroids can be averaged, white circle illustrated in figure 25. Averaging the intersections of bearings may lead to biased results.

Some optimisation methods that rely on finding an estimate, based on minimizing the error between the estimate and the actual value of the Point Fixed are enumerated here. It was decided to dodge the

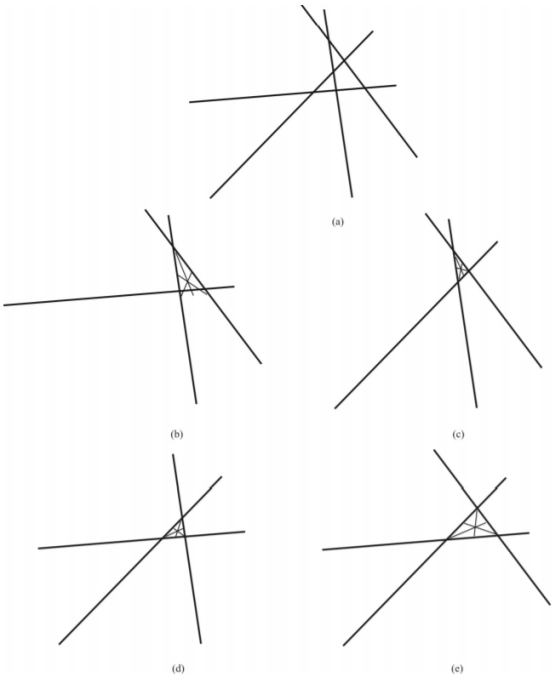


FIGURE 24: *(a-e) Calculating the Point Fixed when there are more than three LOBs. PFs are computed using three LOBs at a time. After that, the results are combined.*

calculus behind these methods because of their big extension and complexity. We only mention some of them, remembering that are generalisations of Least Square Estimation Algorithm:

Total Least-Squares Estimation Allows for the existence of noise in not only the measurements but also for errors in the observation matrix;

Weighted Least-Squares Estimation Weighting Matrix $\mathbf{W_k} \neq I$;

Brown's Least-Squares Triangulation Algorithm Is based on minimising the square of the miss distance of the Point Fixed from the measured *LOBs*, figure 29 from page 32;

Hemispheric Least-Squares Error Estimation Algorithm The measured bearing from a sensor, ϕ_i , projected onto the surface of the Earth in the northern hemisphere (the other hemisphere will work as well with appropriate change of variables), illustrated in figure 30 from page 32;

$$\cos\phi_i = \frac{y_t - y_i}{\sqrt{(y_T - y_i)^2 + (x_T - x_i)^2}}$$

x_i is the longitude of the sensor during the ith observation interval; y_i is the latitude of the sensor during the ith observation interval; x_T is the actual longitude of the target emitter; y_T is the actual latitude of the target emitter; η is the heading of the sensor relative to north; ϕ_i is the ith measured bearing; $\Delta\phi_i$ is the error in the ith measured bearing; x_i is the error in the calculation of the longitude in the ith observation interval; Δy_i is the error in the calculation of the latitude in the ith observation interval;

Pages-Zamora Least-Squares LSE algorithm based on the cellular phone requirements imposed by the Federal Communications Committee in the United States. Illustrated in figure 31 from page 33.

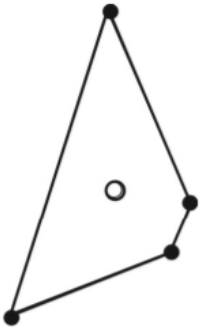


FIGURE 25: *The centroid of the polygon formed by connecting the centroids of the triangles formed with three LOBs yields the final fix.*

$$\vec{d_0} = d_{oi} \vec{+} d_i \vec{v_i}$$

$$x_T = x_i + d_{oi} \cos \phi_i$$

$$y_T = y_i + d_{oi} \sin \phi_i$$

Total least-squares estimation *(TLSE)* method Starts with squaring the equantion from *Hemispheric Least-Squares Error Estimation Algorithm*:

$$\cos \phi_i{}^2 = \frac{(x_t - x_i)^2}{(y_T - y_i)^2 + (x_T - x_i)^2}$$

Measuring the time of arrival of the signal is another possibility at several dispersed sensors located substantially more than a wavelength apart. Typically the time of arrival are transferred to a central site where are computed between the sensors, two at a time but the time of arrival can also be used to compute the point fix, where the isocontours are circles.

Computing the range differences between the sensors and the target is closely related to the method using time of arrivals. The range differences are related to the time of arrivals by the speed of propagation in the medium through which the signal propagates. Normally assumed to be the speed of light in the air, if the signal is an audio signal then in the air it is the speed of propagation of sound through the air, which can be influenced by humidity and other parameters in the air. The speed of propagation is the sound through water, if the signal is an audio signal underwater.

Measuring the differential Doppler is another form of quadratic processing. Such measurements generate target location isochrones upon which the target is estimated to lie. Large errors can occur when trying to measure Doppler differences if the target is moving. Otherwise, errors can occur in the point fix calculations. These errors can be mitigated if the target's motion is detected. It is required to estimate the time delay between the sensors to determine the line of position.

Using reflections off the Earth's ionosphere, high frequency signals can propagate for considerable distances. Variations in the electron and ion density in the ionosphere causes the bending of the signal.

Knowing the azimuth angle of arrival of the signal, as well as its elevation angle, combined with an estimate of the equivalent height of the ionosphere where the signals are reflected allows estimation of the point fix of a target with a single sensor. Such point fix techniques are known as single-site location (SSL)... ... Perhaps the most used form of AOA estimation is amplitude comparison since that is the popular technique used in aircraft survivability equipment (ASE), in particular, in radar warning receivers (RWRs). Every combat aircraft in the Air Force and Navy has this equipment employed on it. The downfall of the method is that it is fairly inaccurate. [11]

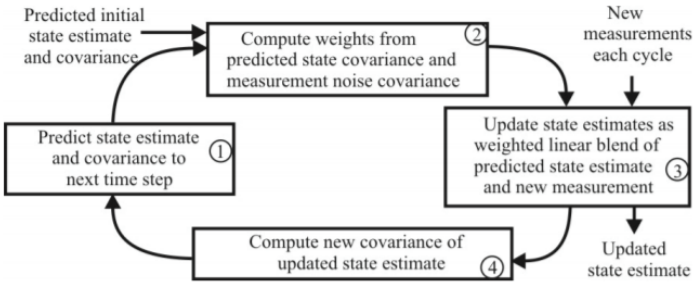


FIGURE 26: *The standard Kalman Filter algorithm*

To the point fix estimation problem The Kalman filter can be applied in a variety of ways. In the case of the standard Kalman filter, the results are optimum in the least mean-squares error sense. A flowchart for the standard Kalman filter is illustrated in figure 26.

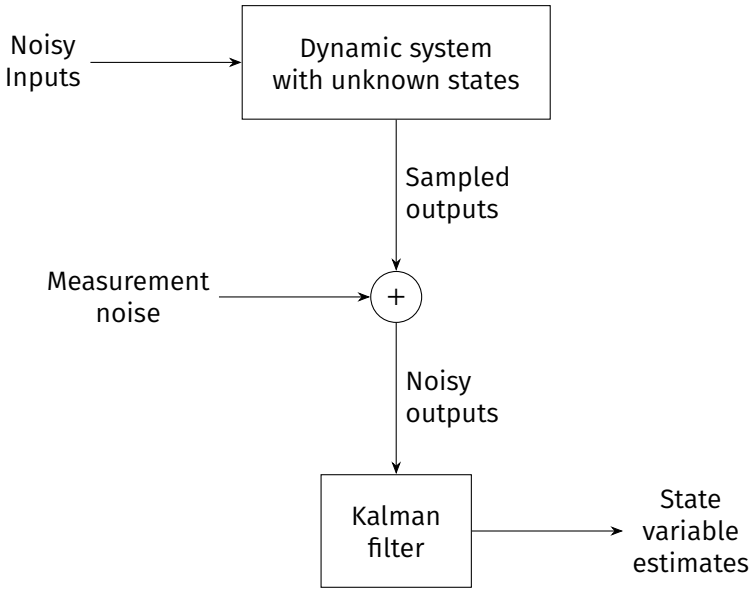


FIGURE 27: *Kalman filter application.*

In some cases, knowing only the PF of a target is inadequate. Examples of this include subsurface oceanographic targets that are tracked with active sonar and surface and airborne targets that are tracked by active radar. Thus, methods were devised to accommodate such

tracking. Kalman filtering is one of those methods, although Kalman filters have much broader applications than tracking targets. Kalman filtering is based on the principles of MMSE [...] Kalman filter estimation uses a form of feedback control: the filter estimates the process state at some time and then obtains feedback in the form of noisy measurements. The behavior of a dynamic system can be described by the time evolution of the state variables. As indicated previously, the state variables of a dynamic system cannot be determined exactly by direct measurements; instead, the measurements available are functions of the state variables corrupted by random noise. It is then necessary to estimate the state variables from the noisy observations. The measurement and estimation process is illustrated in Figure 27. The purpose of the Kalman filter is to optimally estimate the state variables in the dynamical system. Optimum in this sense means that the mean squared estimation error is minimised [...]

The Kalman filter fall into two groups: time update equations and measurement update equations. The time update equations are responsible for projecting forward in time the current state and error covariance estimates to obtain the estimates for the next a priori time step. The measurement update equations are responsible for the feedback, that is, for incorporating a new measurement into the a priori estimate to obtain an improved a posteriori estimate. [11]

Applying the standard Kalman filter used in the linear systems to nonlinear systems with Additive White Gaussian Noise by linearizing the nonlinearity with Taylor series expansion, ignoring the terms of second order and higher is called Extended Kalman Filter.

There is one problem in the convergence to a reasonable estimate. It may not be obtained if the initial guess is poor or if the noise is so large that the linearization is inadequate to describe the system. *EKF* can have instability problems caused by the linearization approximation. Example of *EKF* apllication is given by figure 28.

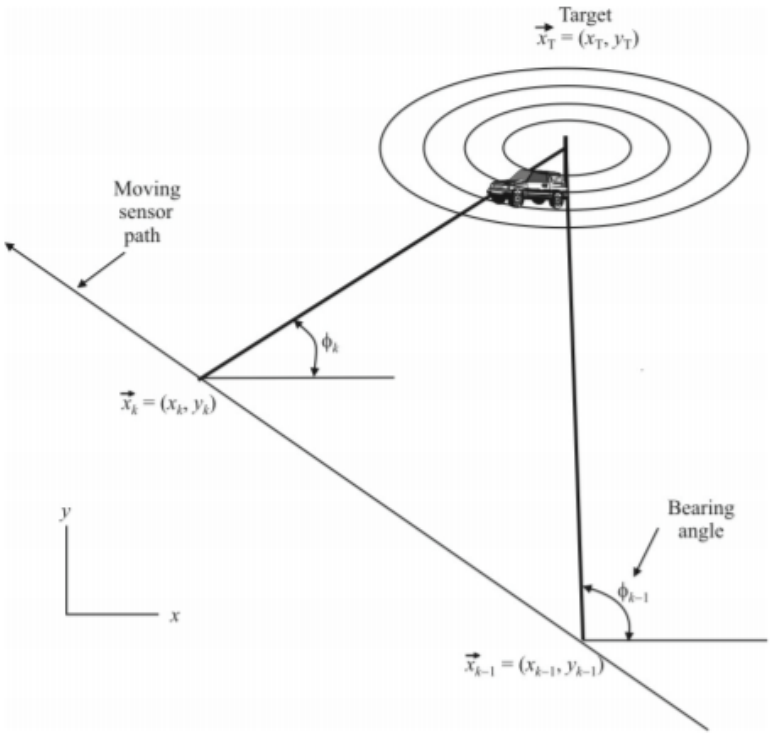


FIGURE 28: *Geometry for Extended Kalman Filter Point Fixed analysis*

A Auxiliary Images

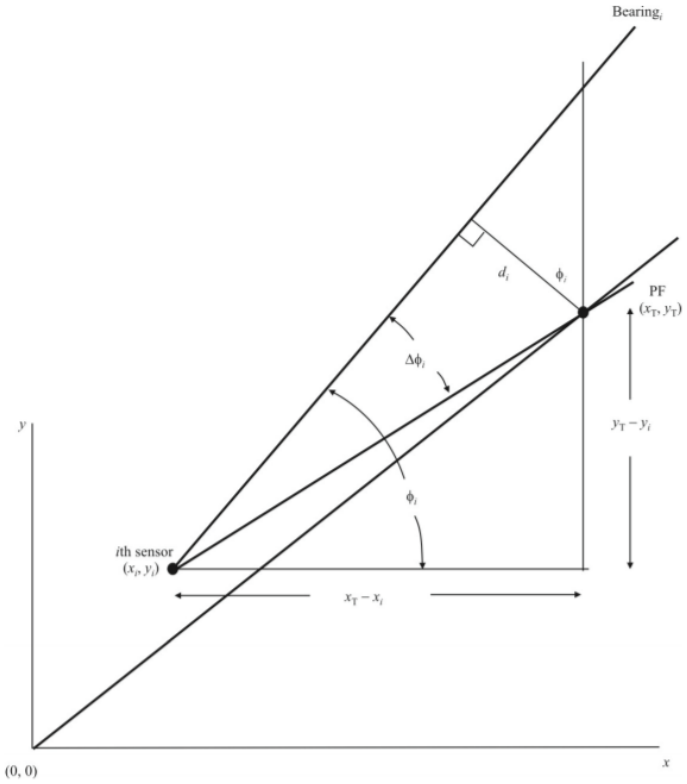


FIGURE 29: *Definitions of the terms for derivation of Brown's mean-squares distance algorithm.*

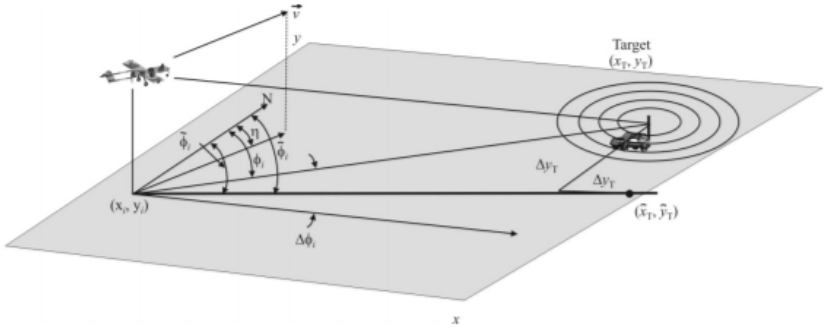


FIGURE 30: *Geometry for hemispheric least-squared.*

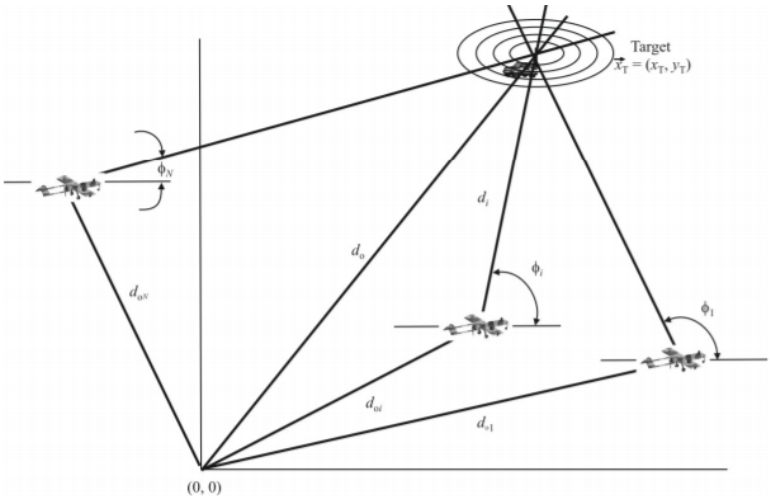


FIGURE 31: *Geometry describing the algorithm developed by Pages-Zamora.*

References

[1] David Adamy. *EW 101: A first course in electronic warfare*. Vol. 101. Artech House, 2001.

[2] *Electronic Warfare Aircraft*. URL: https://www.militaryfactory.com/aircraft/electronic-warfare-aircraft.asp (visited on 12/11/2018).

[3] Gareth Evans. *The evolution of electronic warfare: a timeline*. Army Technology. June 7, 2018. URL: https://www.army-technology.com/features/evolution-electronic-warfare-timeline/ (visited on 12/14/2018).

[4] Greg Goebel. *The Wizard War: WW2 & The Origins Of Radar*. Nov. 1, 2018. URL: http://vc.airvectors.net/ttwiz_07.html (visited on 12/15/2018).

[5] August Golden Jr. "Radar electronic warfare". In: *Washington, DC, American Institute of Aeronautics and Astronautics, Inc., 1987, 347 p.* (1987).

[6] Adrian Graham. *Communications, Radar and Electronic Warfare*. John Wiley & Sons, 2011.

[7] Ali Can Kucukozyigit. "Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO) – Considerations for Turkey". Naval Postgraduate School, Sept. 2006. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a457350.pdf (visited on 12/14/2018).

[8] *Night Level-Bombing Navigation Tactics. Knickebein (crooked leg)*. Arsenal of Dictatorship. URL: http://www.oocities.org/pentagon/2833/general/tactics/knickebein/knickebein.html (visited on 12/16/2018).

[9] Richard Poisel. *Electronic warfare target location methods*. Artech House, 2012.

[10] Richard Poisel. *Introduction to Communication Electronic Warfare Systems*. Artech House Information Warfare Library. Artech House, 2002. ISBN: 1580533442.

[11] Richard A. Poisel. *Electronic Warfare, Target Location Methods*. 2nd ed. Artech House. ISBN: 9781608075232.

[12] Richard A Poisel. *Information warfare and electronic warfare systems*. Artech House, 2013.

[13] Alfred Price. *Instruments of Darkness: The History of Electronic Warfare*. Macdonald and Jane's, 1977.

[14] James Bao-Yen Tsui. *Microwave receivers with electronic warfare applications*. SciTech Publishing, Inc., 2005. ISBN: 1-891121-40-5.

[15] Sergei A Vakin, Lev N Shustov, and Robert H Dunwell. "Fundamentals of electronic warfare". In: *IEEE Aerospace and Electronic Systems Magazine* 16.10 (2001), pp. 13–14.