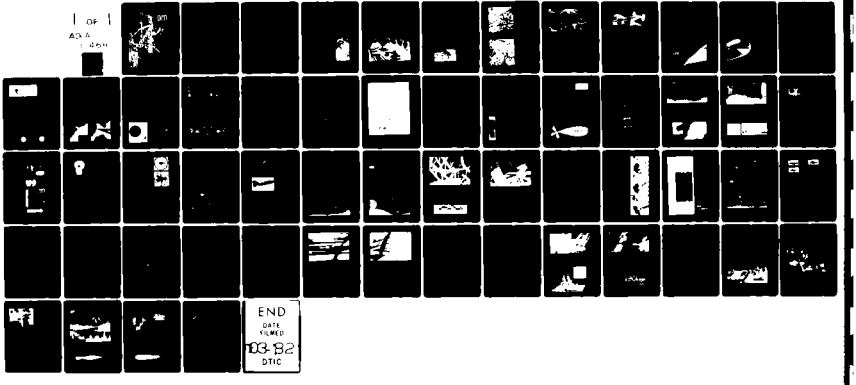
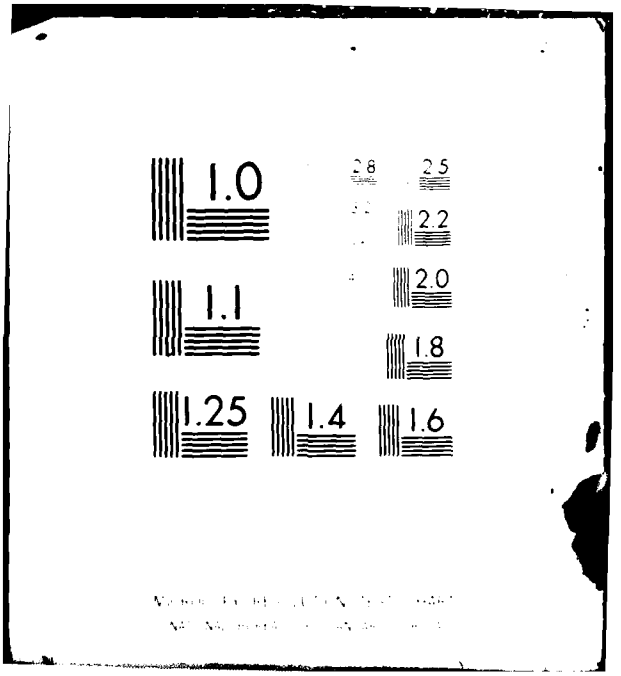
AD-A111 468 RESEARCH INST OF NATIONAL DEFENCE STOCKHOLM (SWEDEN) F/G 17/4
FOA INFORMATION FROM THE RESEARCH INSTITUTE OF SWEDISH NATIONAL--ETC(U)
1967 M FEHRM

UNCLASSIFIED NL




1.0
2.8
2.5
2.2
1.1
2.0
1.8
1.25
1.4
1.6

FOA orienterar om

Special issue
in English

FOA orienterar OM

Information from the Research Institute of Swedish National Defence on

ELEC TRONIC WARFARE

Ansvarig utgivare:

Martin Fehrm

Editor:

Birger Gripstad

Drawings: Alf Björklund and Lars-Owe Bernhager.

Print: Wiking Tryckeri AB, Södertälje, Sweden 1967.

This publication is a special issue of one number of a popularized documentary series dealing with research fields of special interest to the Swedish defence. It can be ordered from

FÖRSVARETS FORSKNINGSANSTALT
Information
Stockholm 80, Sweden

Price: Sw.kr. 10

Director General Martin Fehrm:

FOA Informing on . . .

Defence research in Sweden is organized on lines compatible with the alliance-free policy of the country. The research must be broadly based, and many problems have to be tackled from the bottom before they can be brought to a practicable solution. In many aspects defence research cannot be regarded as an isolated matter, and therefore it has to be coordinated with civil scientific research. Among the many university, industrial and military organisations which in Sweden are involved in defence research, the central organization is the Research Institute of Swedish National Defence, *i.e.* FOA.

A few figures may be of interest. For the fiscal year 1967 68 FOA has been granted 69 million Swedish Kronor (about 14 million dollars); the number of its employees is about 1500. In addition, a large number of scientists contribute to the work of FOA on a consultative basis.

The activities of FOA are divided mainly into four scientific departments. FOA 1 works with problems in chemistry and medicine, FOA 2 with physics, FOA 3 with electronics and telecommunication, FOA 4 with nuclear physics and nuclear chemistry. In addition to these four departments, FOA has a division for Research Planning and Operations Research, FOA P, a Materials Research Division, FOA M, and a special Military Electronics Laboratory, FTL, for type testing and standardization of electronic components and equipment. And finally an administrative department, FOA A.

One of the main problems in scientific research is how to get an effective internal and external information service. In the matter of defence research there are special problems associated with military secrecy. Much attention has been paid to information problems at FOA. In the sphere of external information about the activities of FOA several series of reports, journals and information booklets are now available. Most of these publications are written in Swedish, but some of them are available also in English. The most important of these publications are:

Research Institute of Swedish National Defence, a short publication on FOA and its activities.

FOA Reports, a series of original research reports distributed to libraries and research organizations all over the world.

FOA Reprints, a series of scientific papers which FOA scientists have published in international journals and other publications outside FOA.

The first issue of the series *FOA orienterar OM . . . (FOA Informing on . . .)* to become available also in English was "FTL—The Swedish Military Electronics Laboratory", describing the activities of FTL in the fields of reliability research, standardization, and type testing.

The purpose of the series *FOA orienterar OM . . .*, of which this is the second English issue, is to present easily and broadly understandable surveys in advanced research domains. The various publications are written by specialists from the research staff of FOA, but—as in the case of this issue, "Electronic Warfare" —they do not necessarily concern Swedish conditions. On the other hand the *OM* publications always deal with fields in which FOA is in some way involved.

From the secrecy point of view this *OM* issue, "Electronic Warfare", has been extremely difficult to write. In the way it has been published, "Electronic Warfare" may be looked upon more as a basic textbook than as a statement of the work of FOA and the conditions of Swedish defence in this field.

Contents

The publication may be divided into two main parts, the first of which deals with the historical, scientific and technical foundations of electronic warfare (up to page 33). The second part is made up of three examples of electronic warfare situations.

The foundations of electronic warfare may be regarded as already available in international papers and other sources, and consequently the value of the FOA publication is in this respect the way in which the information has been summarized and displayed. As in other *OM* publications the illustrative material is considered to give the best information. This is also true of the three examples of electronic warfare situations, which are rather particularized. It may be stated that these examples are to be looked upon as purely imaginary situations. They do not allude to specific Swedish conditions. Similarities between the examples and Swedish defence systems relate only to principle, and they do not imply evaluations or estimates of existing systems.

It is believed that this publication, "Electronic Warfare", is rather unique and that few unclassified publications have presented such a detailed and complete view of the subject. It is also hoped that "Electronic Warfare" will give some idea of the level of Swedish military electronics.

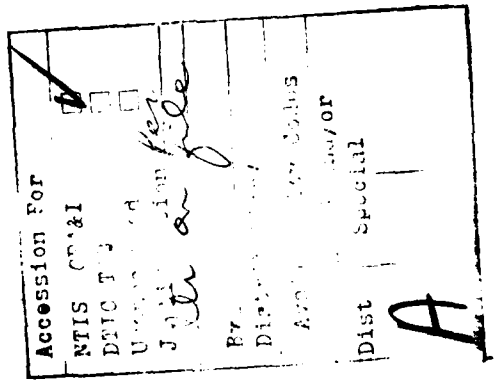
Nils-Henrik Lundquist, Head of Electronics Department, FOA 3

On Electronic Warfare

Nuclear weapons and biological and chemical agents are modern weapons in the arsenal of the great powers, which in the course of time have become more or less familiar to the general public. Through technical reports, comments and discussions in various publicity organs their characteristics and effects, and to some extent their consequences for military strategy and policy, have come to the knowledge of the circle of readers interested in military technology.

Another highly important field of military technology which has not become so widely known is that of *electronic countermeasures* (ECM) and *electronic warfare*. To give a summary definition of these terms one may say that electronic countermeasures are technical instruments for international interference with the enemy's radio communications, radar, radio navigation systems etc. in order to put them out of action as links in the total military machine. Electronic warfare is the entire strategic and tactical game that can be played —with electronic or other countermeasures—around these extremely important links in a modern military system, in order to maintain them in action or to eliminate them, depending on the side on which the game is played.

Publicity has not been altogether lacking in questions concerned with electronic warfare, but the material is both difficult of access, since it has been published almost exclusively in technical journals, and is incomplete, insofar as it deals particularly with purely technological principles and equipment design problems, while very little



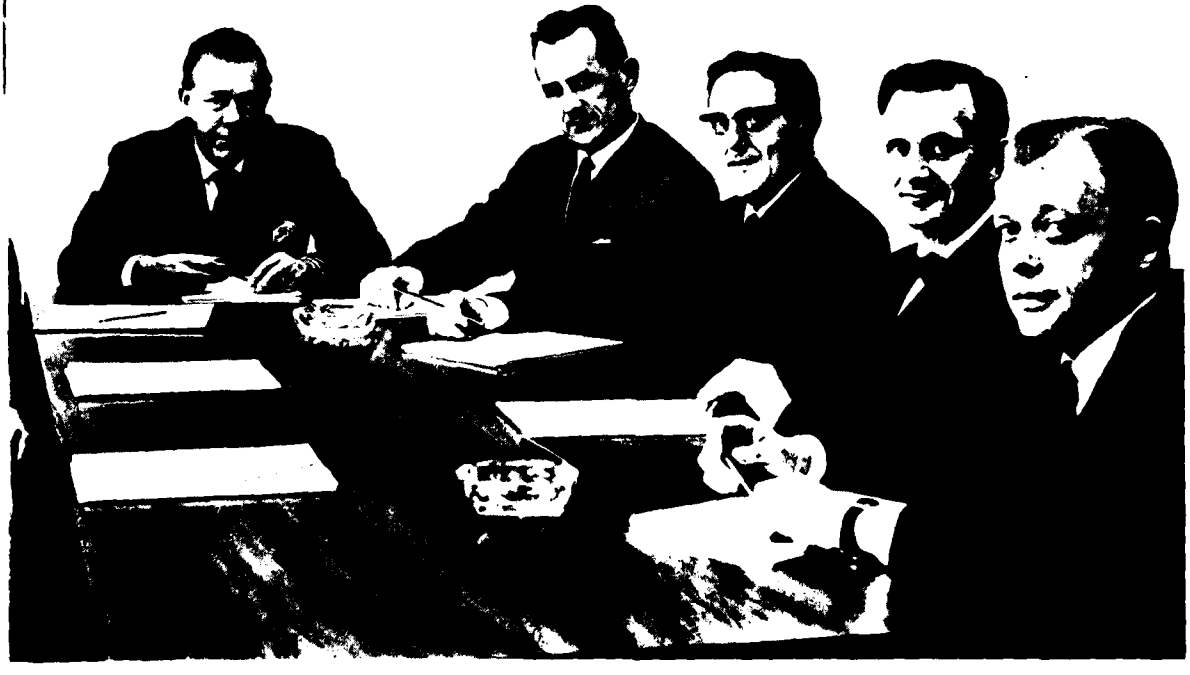
This publication is the result of teamwork by members of FOA 3, who are presented in the adjoining photograph. (From left) Alf Lindgren, Rolf Gezelius, Sven Sundius, Nils-Henrik Lundquist, Gösta Levin, Ingmar Persson, Sven Hasselrot and Torsten Linell.

has been written about the role of the equipment in operative contexts. This is due to the strict secrecy in all countries which are in any way active in this field; the reasons for this secrecy will be considered in the next section.

But even if there are grounds for secrecy in certain respects, there are also strong reasons for imparting general information about the existence and significance of electronic warfare. In this publication, therefore, the Research Institute of the Swedish National Defence (FOA)— in consultation with the Defence Staff—has wished to present the problems of electronic warfare in such a way as to enable the general reader with an interest in military matters to assess the role that this form of warfare may assume, both in general and in relation to our own defence problems.

Within FOA the Electronics Department (FOA 3) is responsible for technological and scientific research and investigations on questions of electronic warfare. In a way one may say that it is the main job of the Department. It conducts studies of communication, navigation, and radar techniques, and of countermeasures against them. These studies cannot be conducted separately, however, but must be coordinated: an idea for a new radar solution brings up the question of countermeasures, just as a new countermeasure against a navigation system brings up the question of electronic counter-countermeasures (ECCM). This continous internal technical duel within the Department is a small scale model of what is happening on the international military scene, and it is intended to provide the Swedish Defence with a basis for optimal balance in equipment procurement. This goal has found practical expression in the preparation of this publication, in that the members of the team of authors have their daily work in widely different parts of the Department's organization.

These remarks must suffice as presentation of FOA 3's engagement in questions of electronic warfare. For reasons of secrecy no concrete exemplification will be given of specific assignments at FOA, nor a technical account of equipment or projects which concern the various branches of defence. I hope nevertheless that this will not make the publication uninteresting, but that it will fulfil its informational purpose as indicated above.



History of Electronic Warfare

The course of the second world war was characterized to a large extent by two great innovations, the large-scale use of armoured vehicles and bombing aircraft, and the methods of defence against them, antitank weapons and air defence. A third new technical feature was the use of electronics for new functions and on a wider scale, without which, in fact, the expanded tasks of air warfare, both offensive and defensive, would have been impossible.

At that time the first modern radio navigation systems came into use to guide the bombing aircraft to their targets in darkness and poor visibility. But at the same time the first radar systems were developed, both ground-based to give early warning of air attack, and fire-control and airborne intercept radar to help the active air defence weapons in their task. Radar proximity fuzes were introduced for exploding anti-aircraft shells, radio methods were developed for guiding bombs into their path of descent, radar and radio navigation found marine applications as well, to name only a few examples.

But these developments were also a challenge to try to jam the enemy's radar and radio equipment, and the "Electronic War" was thus an established fact. It was a silent war, without front-line reports or other publicity, but it often had a great significance for the course of the war as a whole, and it was full of dramatic situations.

During the bombing of Britain in the winter of 1940-41 the Germans employed a system with the code name "Knickebein" to guide the planes to the bomb-release point. The British had the great ingenuity to detect and analyse this system, based on a number of directional radio transmitters, before it came into operational use. They constructed a countermeasure consisting of a large transmitter, the signals from which were mixed with the control signals so that, without knowing it, the bomber was led to a false bomb-release point. The same thing happened with other systems which were employed later, and it is calculated that as a result of jamming only one fifth of the total bomb load reached the target areas.

At midnight on February 27, 1942, a small group of parachutists landed on a coastal plateau at Bruneval just north of Le Havre. They quickly overcame the local defence and held it in check while a group of technicians examined and dismantled a peculiar installation on the edge of the cliff; the group then made its way down to the beach where it was picked up by units of the British navy. This was the first military raid made against the German-occupied French coast, its aim being to procure information about what was—rightly—suspected to be a new German fire-control radar. This information and the captured items of equipment were later invaluable for the protection of the allied armadas against the German anti-aircraft defences.

One such protective method was "Window", i.e. strips of metal-coated paper, which were scattered in large numbers from bombers and, through their reflections, produced innumerable deceptive and masking echoes on the anti-aircraft, fighter and air surveillance radar screens. The idea had actually been conceived before the war, but its use in practice was delayed partly on account of doubt as to its effect, partly from a fear that the enemy could use it with greater result. In the summer of 1943, however, it was decided to use the method in the large-scale attacks on Hamburg, and the result in the form of confusion of the air defence surpassed all expections. It is part of the irony of history that the same technique had been developed in

This photograph, taken by a British reconnaissance aircraft, gave the first indication of the German fire control radar "Würzburg" and led to the Bruneval raid, well-known in the annals of the technical intelligence service.

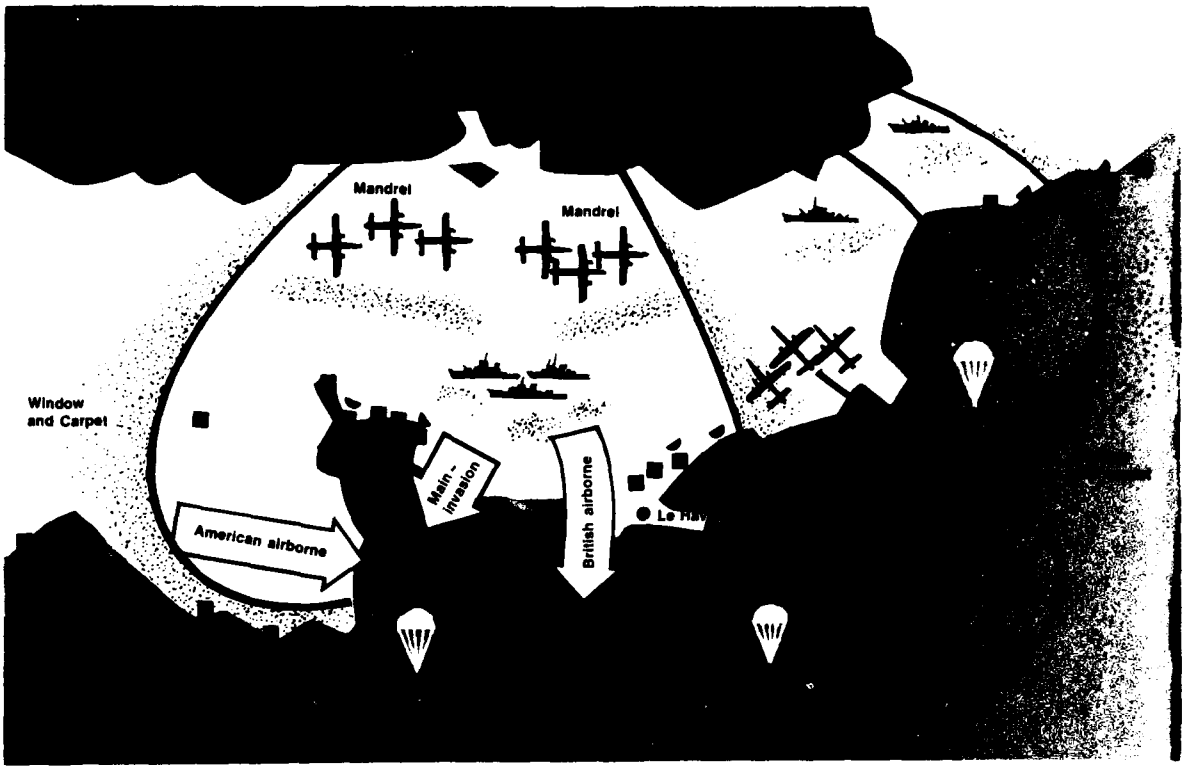
(Above) A radar picture of the centre of Hamburg with Lakes Aussen-Alster and Binnen-Alster; between them Lombard Bridge. (Below) The same area after radar camouflaging: Binnen-Alster is covered by a street-network-like reflector pattern, and a simulated Lombard Bridge cuts off the inner portion of Aussen-Alster.

Germany, and Göring had been informed about it in 1942. His main concern was the consequences for the German air defence if the allies got wind of the method, and he therefore forbade all further work on it and had all the documentation confiscated, one result being that the radar personnel in the Hamburg area were entirely unprepared for the forms of interference employed in the giant attacks on that city.

In general, however, the Germans were by no means lacking in appreciation of the possibilities of countering the allies' electronic measures. From the winter of 1943-44 and onwards the allies used airborne radar on their bombers for navigation and bombing; the black areas representing lakes, mouths of rivers etc. on the radar indicator were features of navigational importance. This was realized by the Germans and a widely used—and largely effective—countermeasure was the camouflaging of open water with rafts carrying a set of radar reflectors.

The high-point of electronic warfare during the second world war, however, was in conjunction with the invasion of Normandy in 1944. There it formed part of an overall plan, the aim of which was to deceive the defenders concerning the point at which the main thrust of the invasion would come. Innumerable means were used to this end: mock concentrations of troops and tonnage, deceptive radio communication, spreading of rumours, false agents' reports etc., all designed to create the impression that the main effort would be across the Straits of Dover. The role of electronic warfare was in broad outline as follows.

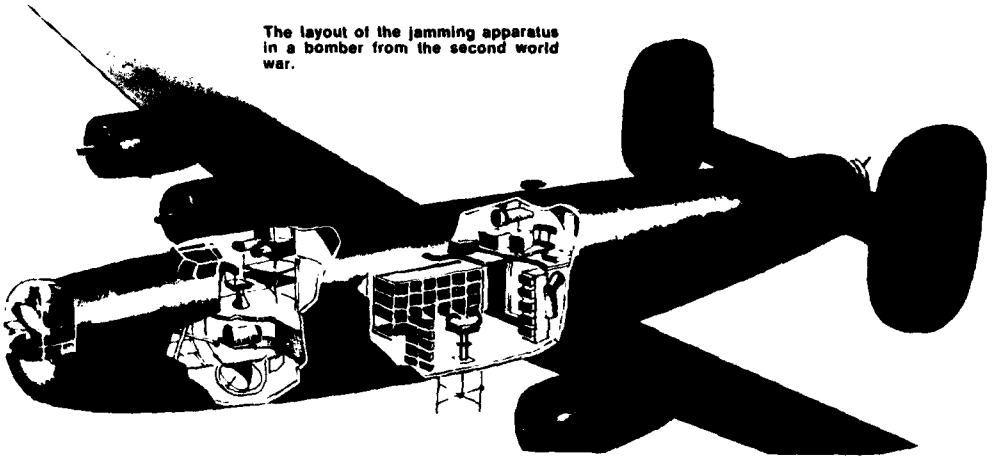
On the days before the invasion the radar stations were subjected to heavy bombardment which, however, left a number of stations intact on the simulated invasion coast but only a few



on the intended site of the real invasion. At the time of the actual invasion the remaining stations were subjected to jamming which, however, was less intense in the Calais sector. There, instead, aircraft were sent out which slowly circled forwards at low altitude, releasing window in order to simulate a large invasion fleet on the move. As is known, this entire deceptive operation succeeded in its strategic intention: the setting-in of the strategic reserve to reinforce the defence in the critical sector was delayed so long that the invasion forces gained a firm foothold. One single authentic observation of the actual invasion force was reported to headquarters from a radar station near Caen, but it disappeared in the welter of false, contradictory or irrelevant reports.

As the examples show, the use of new electronic systems and new countermeasures to them was due to the desire to obtain *surprise* in conjunction with an important operation, and this necessitated very strict *secrecy* around the systems that were being developed. A similar secrecy has been customary also during the period since the war. This, perhaps, does not apply so much to new electronic measures —radar stations, navigation systems, guided missile systems —the essential data of which cannot be kept secret in practice after they have come into use for training, exercises and operational service, but it does apply to a very great extent to the electronic countermeasures, as regards their operative status, functions and practical performance.

The reasons for this secrecy, however, are no longer the same. One cannot now expect to achieve any major strategic surprise at the outbreak of a conflict by means of a new type of countermeasure—the technical possibilities are all too well known for that; nor is there reason to plan a series of successive tactical surprises when the prospect of a rapid and devastating outcome based on nuclear weapons is the alternative to which the main attention must be paid. No, the difference is, quite simply, that there has been peace btween the great military powers since 1945. This does not mean that each individual nation does not make the military preparations needed for armed conflict. The tactical succession of new measures and countermeasures during actual war has given



The layout of the jamming apparatus in a bomber from the second world war.

way to a similar, peacetime, succession of equipments and doctrines in respect of measures and countermeasures introduced in the armed forces as technology has developed and intelligence concerning the opponent's technical dispositions has become available. Viewed in this light, the electronic armaments race does not differ in principle from that in other technological fields. The reason for secrecy is, quite simply, the desire to create an *uncertainty* in other powers as to how far one has come, an uncertainty which may be presumed to have a deterrent effect on aggression.

From these points of view it may seem as though the general secrecy surrounding electronic countermeasures is unnecessarily strict. This may be so, but there are some special reasons for it. One is that electronic equipment is fairly flexible in use and that its technical data can often be quite easily modified. If it is known that the opponent has a jamming equipment which is operative within a given frequency range and at a given power level, it can often be quite easily parried, for example by detuning or change of tubes. Another, perhaps more profound, reason is that the effect of jamming of, for example, a radar system is so difficult to assess that certain forms of interference may—even if they are known in principle—have a more or less overwhelming surprise effect in the opening stage of a conflict.

Under these conditions, therefore, a kind of *drawing-board war* has been waged between the designers of electronic measures and countermeasures during the last 20 years without any actual confrontation taking place. The Korea War was not of a character which required advanced electronic weapons; nor the Cuba crisis either, even if it gave rise to technologically qualified reconnaissance tasks. In conjunction with the repeated Berlin crisis the use of window has sometimes been reported as a risk for civil aviation; but it appears as if the psychological warfare element involved therein, and in the publicity surrounding it, has been the most important factor. On the other hand, the Vietnam conflict does seem to involve some trial of strength in the electronics field.

It is known that electronically controlled anti-aircraft missiles of Soviet type have been used in North Vietnam; it is also known that the losses they have caused to attacking American aircraft have been very slight. What this may be due to—poor quality of weapons, inexperienced operating staff or effective countermeasures—cannot at present be decided; but the American military and electronics press has reported that specially equipped planes accompany the bombers in order to locate the missile bases and to take countermeasures consisting both of jamming of the missile radar and of evasive action by the attacking aircraft. It is also stated that the U.S. Navy has used "Shrike" missiles, which are designed to home on and destroy radar stations, but that the result has hitherto been comparatively modest.

It is hardly likely, however, that the most advanced electronic methods would be used in a conflict of this kind. One may expect that there are other electronic weapons kept in reserve, in the event of a direct confrontation between the great powers.

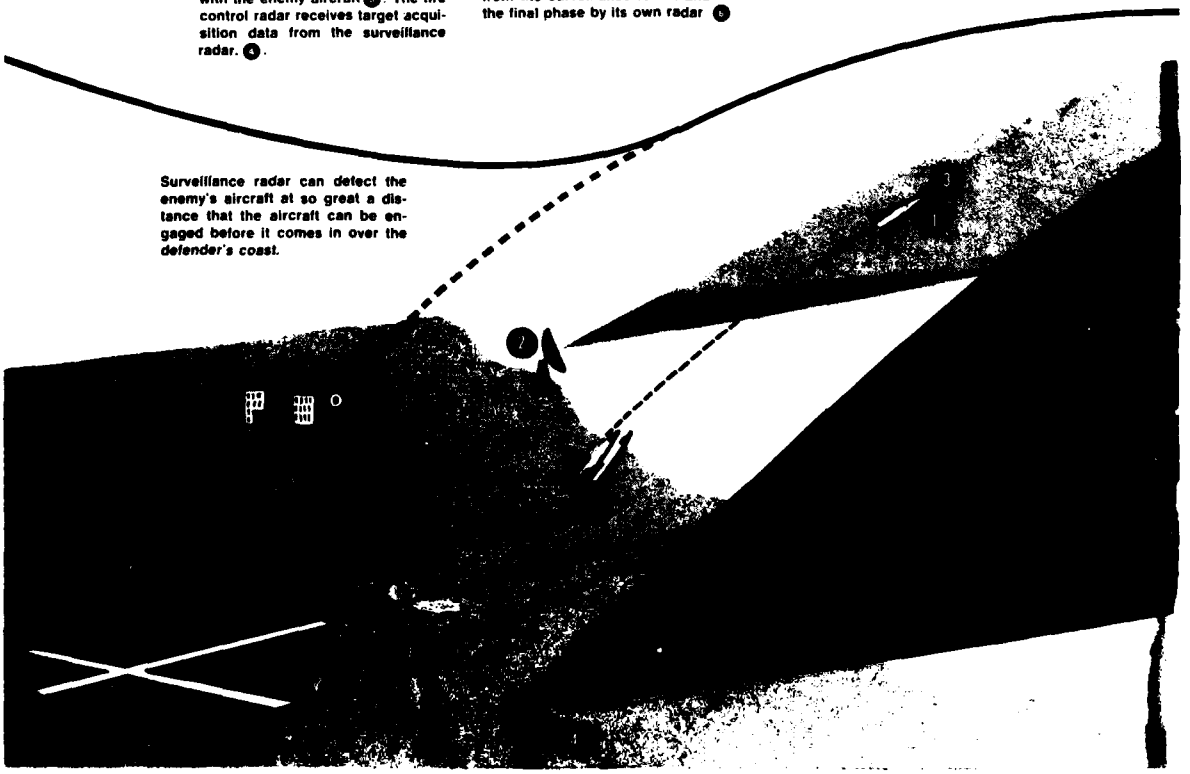
The Role of Electronics in the Weapon Systems of Today

In order to understand the background and the conditions for the achievement of combat economy through the use of electronic weapons, it is necessary to analyse the function of electronics in modern weapon systems.

One finds that such military engineering branches as weapons technology, aeronautics etc. have developed an increasingly high degree of efficiency, speed, range, altitude, coverage, etc. This had led to correspondingly stricter requirements of *surveillance, coordination and control* of the combat systems in order that technically and tactically effective results may be attained. In the majority of cases these requirements can be met only through the use of electronics, chiefly because of the *range, speed, capacity, independence of weather, and precision* that are thereby attained. Electronic methods and equipments have therefore become indispensable *components* in many military systems, without which the other advances in weapon systems cannot be effectively utilized.

An example is the large radius of action of modern bomber aircraft. This requires a navigational system which, regardless of ground visibility, operates along the entire route of the attacking force and, especially in the final phase, leads the aircraft exactly to their target. Apart from the inertial navigation methods, all long range and high precision navigation systems are based on the use of radio waves. The precision of inertial navigation, moreover, diminishes rapidly with increasing distance unless very advanced equipment is employed.

Likewise the condition for defence against bombing attacks is that the aircraft can be detected at so great a distance that fight-



ers and/or anti-aircraft (A.A.) missiles can engage the enemy aircraft before they reach their target. This is possible only by using radio waves, e.g. in a surveillance radar.

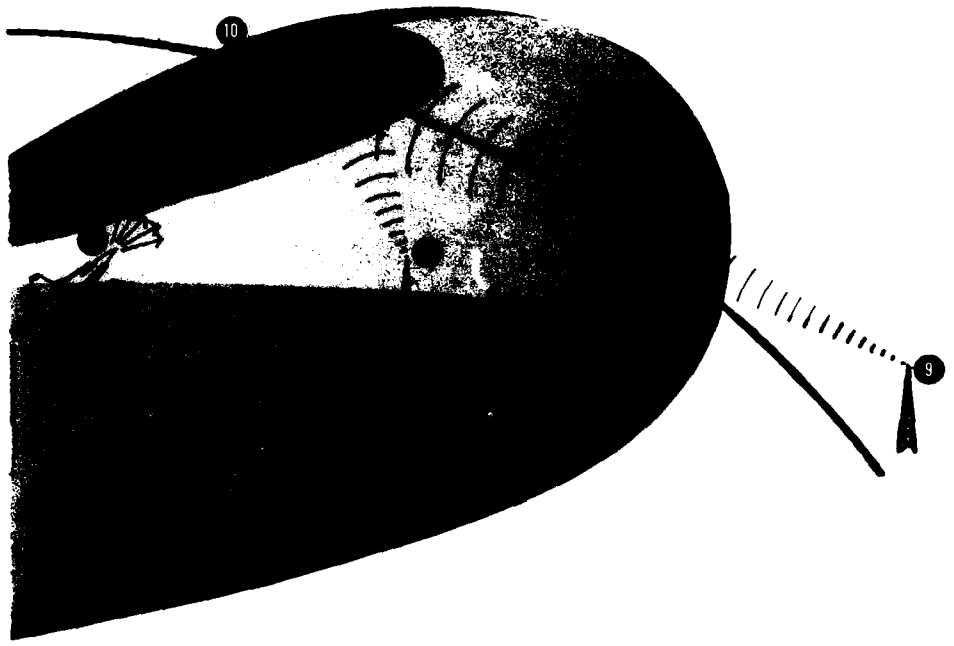
Fighter aircraft and A.A. missiles must be *directed* or *guided* to their target. The long distances and the extremely short times available require a very great range and precision in the fighter aircraft or A.A. missile.

The increased requirements of *surveillance* and *coordination* of the operations may be exemplified by the increased need in nuclear warfare to operate with many small dispersed forces which, however, must be capable of quick concentration for decisive efforts. This places greater requirements than before on the means of communication, both for the quick and reliable passing of orders to the units concerned and as regards the reliability and speed of the reporting units. Similar requirements of *surveillance* and coordination exist within A.A. defence. When enemy aircraft are detected by a surveillance radar, a decision must be made whether to issue an air raid warning and how to coordinate the means of defence. If the enemy attack comes in waves or at several points, an order of priorities must be decided. This requires an effective display of complicated and quickly changing battle situations.

The best way of using fighter aircraft, A.A. missiles and other means of defence must be quickly calculated and orders must be transmitted over long distances to the combat units. Here, again, it is the electronic methods of data collection, display, processing and transmission that have made it possible to fulfil the functional requirements.

Now that electronics have become essential elements in weapon systems, they have also become *vulnerable points* in these systems. A nuclear weapon can be caused to miss its target by deluding the navigation system of the weapon carrier just as well as by shooting down the carrier, and the air defence can be rendered ineffective by jamming its radar stations just as well as by destroying its air bases or command centres. If it proves cheaper to reduce the effect of the opponent's weapon system by electronic interference than by direct combat, a rationally planning military power will quite certainly choose this alternative. This is the economic basis for the functional role of electronic *counter-measures*.

The enemy aircraft is guided to the target ⑧ by radio navigation ⑨ and its own radar ⑩.



Military Electronics

In the light of what has been said about the role of electronics in modern weapon systems it may be as well to briefly review the most important of the military electronic systems to see what are their jobs, how they function, and what are the scientific and technological conditions for their operation.

In passing, it may be remarked that weapon systems sometimes make use also of aids based on the optical frequency range. Examples are infrared homing devices and laser rangefinders. As a whole, however, the optical field lies outside the scope of this publication.

The chief military assignments for electronics are *reconnaissance, communication, guidance and navigation.*

By means of *reconnaissance* one attempts to define and locate military targets. By *communication* is meant the reporting of the results of reconnaissance or the transmission of orders for action. *Guidance* and *navigation* comprise methods for bringing weapons to or near the military target. It may be added that many military systems, such as the Swedish air defence system Stril 60, must be able to perform all operations of surveillance, communication, navigation and guidance. Another example of how these combined functions are necessary for carrying out a military operation is shown in the illustration on this page.

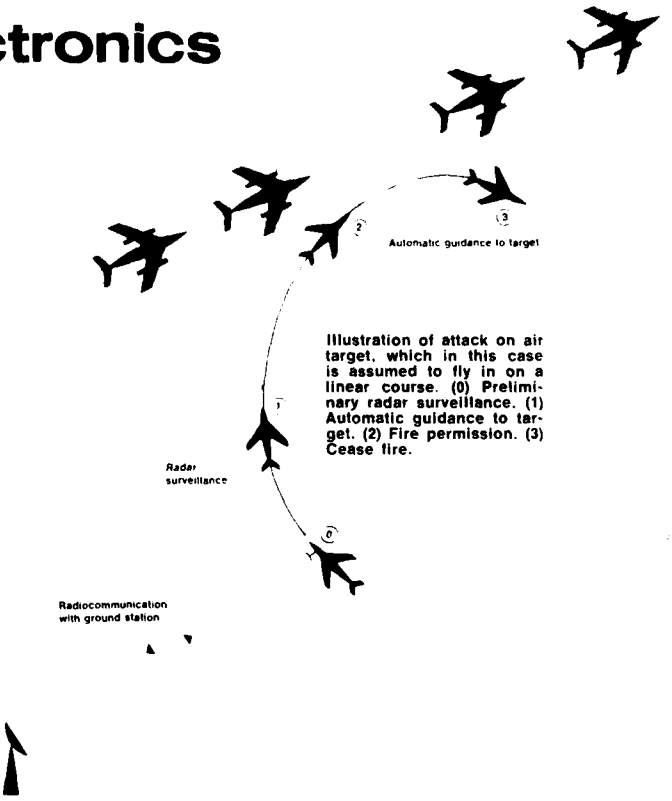


Illustration of attack on air target, which in this case is assumed to fly in on a linear course. (0) Preliminary radar surveillance. (1) Automatic guidance to target. (2) Fire permission. (3) Cease fire.

Technical functions

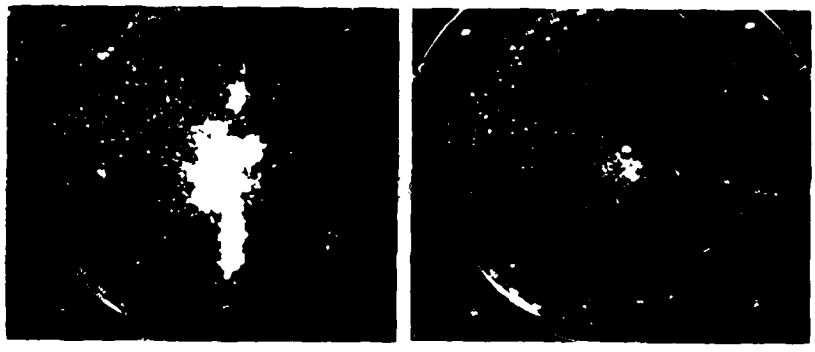
The technical arrangements for performing these military operations may be classified under the headings of *radar, radio communication, navigation* and *missile guidance.*

Radar

Radar, i.e. Radio Detecting and Ranging, is used for surveillance of air, sea and ground targets. The most common form of radar is still the *pulsed radar*, which works with pulsed signals, the distance to the target being determined by measurement of the time of passage of a pulse to a target and back (by reflection). The bearing is determined in principle by rotating the aerial, which must have good directivity, so that the received signal attains maximum. For determining the altitude of the target a height-finder radar can be added to the pulsed surveillance radar.

Radar is now an extensively ramified and refined technique. Radar types may be classified in several ways according to which factor or property is chosen as parameter. The classification may be based on the basic radar principle, e.g. whether the radar works with *amplitude difference* of the echo signal, like ordinary pulsed radar, or *with frequency difference* such as *doppler radar*. Radar may also be classified according to whether it is stationary or mobile, *ground-based* or *airborne radar*, or to its application, *surveillance, fire control* or *navigation* (e.g. in homing missiles). Another method of classification is the frequency band in which the radar works (*L-band, X-band radar* etc.).

Among the more recent and specialized types of radar may be mentioned *three-dimensional radar*, which may be regarded as a combination of surveillance and height-finder radar and which presents a kind of three-



Radar picture without (left) and with MTI.

dimensional picture of the surroundings. The *side-looking radar* is designed for reconnaissance from the air and provides radar maps of cities or landscapes. In supplementation of pulsed radar, use is sometimes made of *MTI* (moving target indicator) which, by means of the doppler principle, suppresses the echo from stationary objects in the neighbourhood, while the moving objects (aircraft or ships) appear all the more clearly on the radar screen.

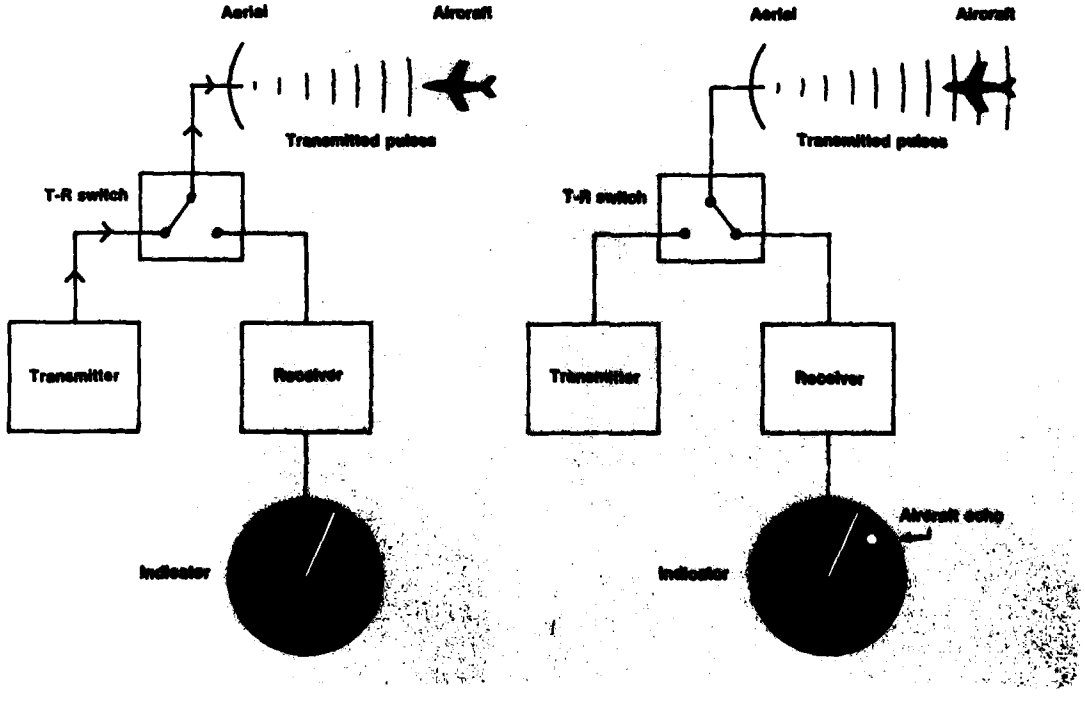
Telecommunications

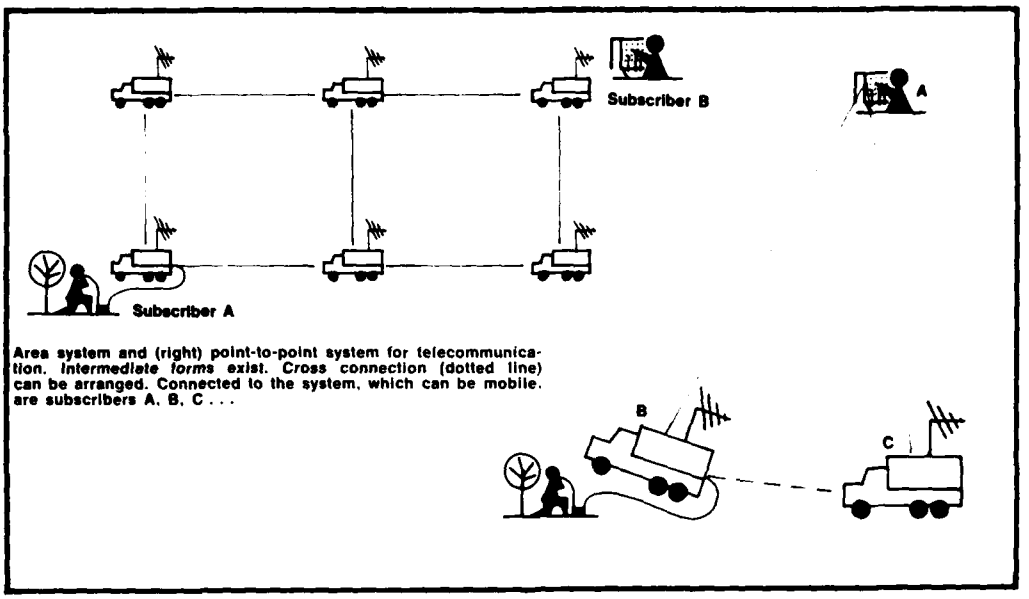
Telecommunications are still the main means of military liaison. In the future, communications technique based also on optical frequencies (laser) may be of some significance. For electronic warfare it is primarily *radiocommunication* that is of interest since *wire communication* can hardly be jammed by electronic measures. In the same way as radar, radio communication equipment can be systematized on different principles, e.g. principle of operation, frequency range, stationary or mobile connections, range, degree of directivity, applications etc.

Within military communications radio is used particularly for *speech* and *telegraphy*, the latter usually in the form of *teletype*. *Data transmission* may be regarded as telegraphy at a much higher than the usual speed of transmission. Data transmission is used, for example, in Stril 60.

PRINCIPLE OF PULSED RADAR
During transmission the transmitter and aerial are coupled together. The aerial, which rotates and is common to transmitter and receiver, transmits pulsed waves into the atmosphere. The sweep of the indicator electron beam moves synchronously with the aerial.

During reception the aerial and the receiver are coupled together. Pulses reflected from a target, e.g. an aircraft, are picked up by the aerial and, via the receiver, reach the indicator, the screen of which lights up in the position corresponding to the position of the aircraft. The T-R switch is a high-speed switch, which protects the receiver during the transmission pulse.





Area system and (right) point-to-point system for telecommunication. *Intermediate forms* exist. *Cross* connection (dotted line) can be arranged. Connected to the system, which can be mobile, are subscribers A, B, C . . .

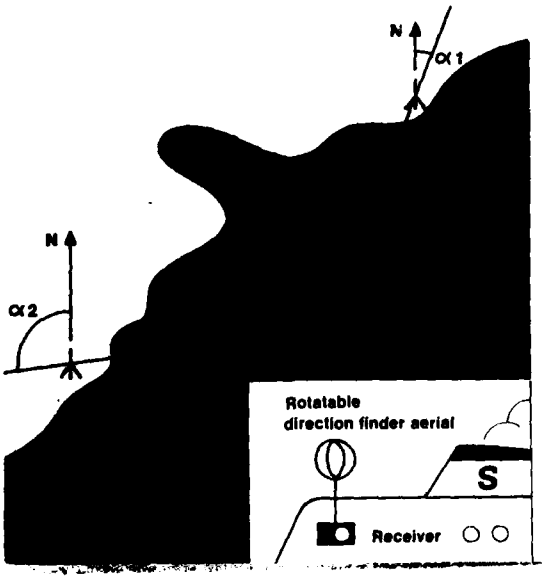
In military communications a distinction is made between two main types of network, namely those based on lines of command *(point-to-point system)* and those which are tied to a given area *(area system)*. With the latter the military units can connect to a number of exchanges interconnected by, for example, radio links. The area systems are expensive and, as yet, are used only in the U.S.A. Intermediate forms of the two main types also exist.

Radio communication can work either with *stationary* or *mobile connections*. By mobile radio communication is meant traffic with or between ships, aircraft, ground vehicles, mobile units or individual soldiers.

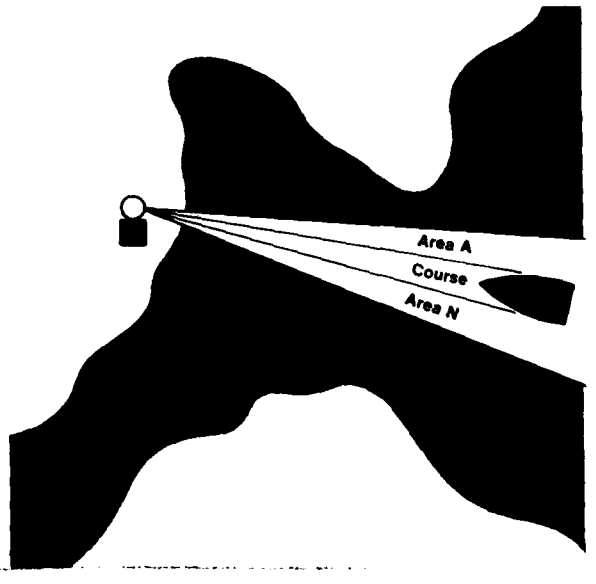
A radio transmitter may be designed either for *omnidirectional or unidirectional transmission*. Large distances can be covered by means of strongly directional microwave radio link connections, sometimes passing through several relay stations (page 54).

The *range* of a radio communication equipment is determined by several factors such as transmitter power, aerial gain, receiver sensitivity, and wave pro-

Cross-bearing position finding against non-*directional* radio beacons with shipborne direction finder.



***Unidirectional* radio beacon, so-called A-N beacon. North of the line of course the beacon sends morse signals for "A" and south of it for "N".**



pagation conditions. These factors are usually greatly dependent on the frequency used.

Radio and radar navigation

Advanced technical methods are often used for military *navigation*, in particular *radio and radar navigation* and *inertial navigation*. The latter, however, is not an electronic method and will not be dealt with in this publication.

For *radio navigation* use is made of the linear propagation of radio waves for determination of direction and of their constant velocity for determination of distance.

If navigation is based solely on rectilinear wave propagation, one gets radial lines of position proceeding either from the vehicle, e.g. in *direction finding*, or from a stationary ground transmitter, *directional beacon navigation*. The accuracy of angle determination depends, among other things, on aerial size and frequency.

Direction finding is based on the rectilinear propagation of radio waves and on the directional effect of the receiver aerial. Land-based *non-directive radio beacons* act as transmitters. In aircraft the direction finding receiver is automatic and is called *radio compass*. Direction finding can also be done from ground-based stations against vessels or aircraft.

Directional beacon navigation is also based on rectilinear wave propagation. The radio beacons are either *unidirectional* or *omnidirectional*. The signal character is in some way related to the bearing. Several different systems exist.

For determination of position by pure range-finding one can either measure the range between the vehicle and a station or the difference in range to two fixed stations. In the former case one gets circular lines of position, *circular system*, in the other hyperbolic lines of position with the transmitters in the focal points, *hyperbolic system*.

Examples of existing radio navigation systems are Consol, Decca, Loran, VOR. These *area coverage systems* are used chiefly for *general navigation* of ships or aircraft. For precision navigation and for *homing and landing navigation* other systems are used, e.g. Instrument Landing System, ILS.

Radar navigation is often used both for ships and aircraft, based on measurement of the range and bearing of the targets. The display is usually in the form of a map on a plan-position indicator, PPI.

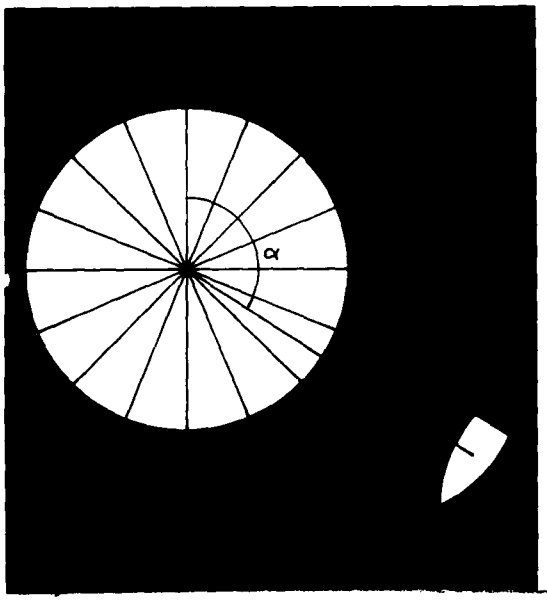
Radio and radar guidance

Guidance systems for missiles are important factors in electronic warfare. By guided missile is meant a controllable unmanned weapon carrier equipped with rocket or jet engine.

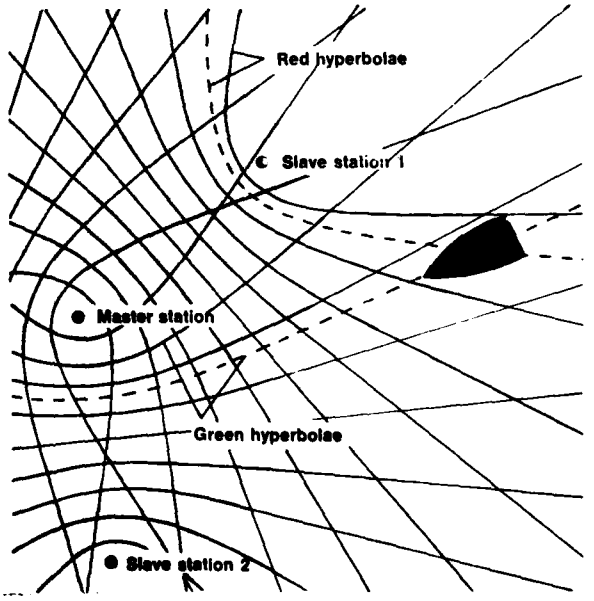
Guidance of the missile implies that its path to the target is corrected for attitude errors, external disturbances, and changes in movement or position of the target. Among the various principles of guidance may be mentioned *radar homing*, *beam riding* and *command guidance*.

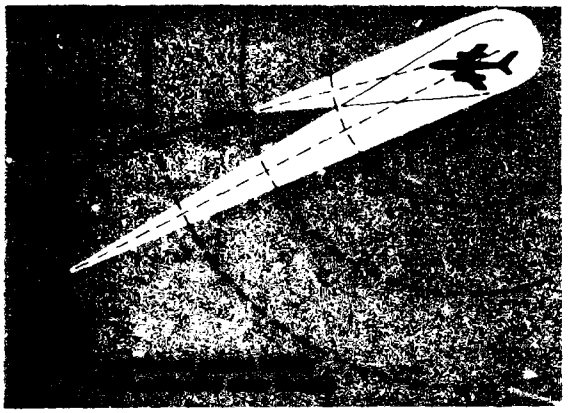
Radar homing may be *active* or *semiactive*. In the former case the missile has both a radar transmitter and a receiver with which it can find the direction to the target and itself home on the target. A semi-active homing de-

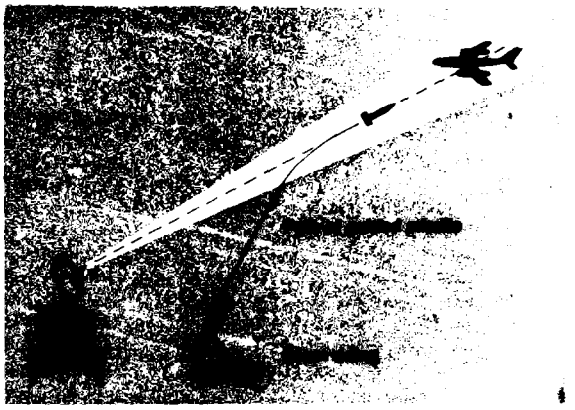
Omnidirectional radio beacon. The signal character is dependent on the bearing α, which can thus be measured with a receiver in the ship or aircraft.



Hyperbolic navigation. The receiver measures the time between signals from two pairs of stations with a common master station. The navigation chart shows a series of "red" and "green" hyperbolae which indicate the position of the vehicle relative to the two pairs of stations.







vice, on the other hand, contains only a radar receiver, while the target is illuminated from a ground transmitter.

Beam riding implies generation by the radar of an electronic guidance line from the firing site to the target and that the missile contains equipment which causes it to follow this line.

Command guidance, finally, implies that the position of the missile relative to the target during homing is determined at the command centre, e.g. by radar. On the basis of the received data a computer calculates the missile control data and they are transmitted to the missile by radio.

Technical and scientific basis

Some technical functions of importance for electronic warfare have been described above. Insofar as they come within the radio engineering field, these functions are dependent on certain radio science factors, the most important of which will be discussed below.

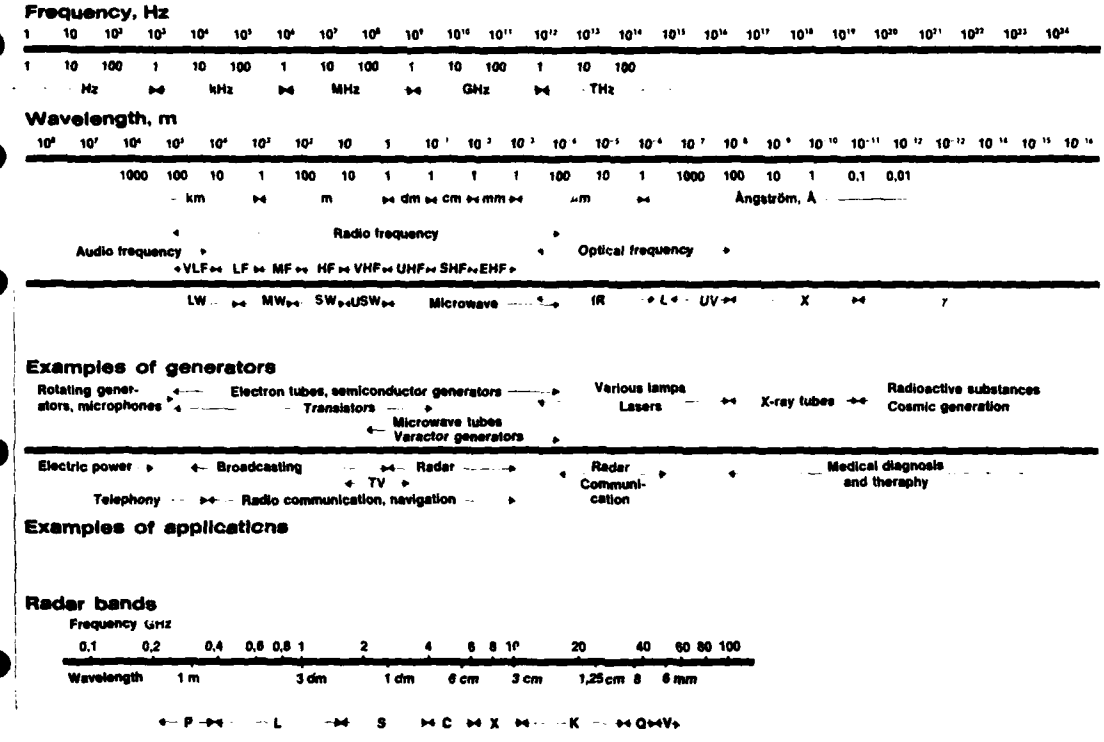
An electronic transmission system in its simplest form may be characterized by the lower part of the illustration below. In a communications system (an example is shown in the upper part of the picture) the input quantity is what the speaker says. By means of a microphone his speech can be modulated on a carrier wave and, by wire or radio, transmitted to the receiver where it is amplified and demodulated, and the listener hears the speech. Radar and navigation systems are based on the same idea, though the working principle is somewhat different.

Attempting to give concrete form to the main parts of this schematic system, one finds the first need to be a *converter* (input device) from acoustical optical etc. to electrical energy, and further a *transmitter*, the main part of which is a *generator* of electrical energy for the radio frequency carrier wave. The *transmission medium* may be *wire*, *the atmosphere* or *space*. In the latter cases *aerials* are required, which are converters of conducted electrical energy to radiation energy and vice versa, one at the transmitter and one at the receiver. After the latter there follows a *converter* (output device) of electrical signal energy to a form of energy intelligible to man. Examples of such converters are *earphones* and *radar indicators*. Alternatively, in large systems, the signals from the receiver can be fed into a computer for further processing.

Some factors of special significance for military electronics will be briefly discussed in conjunction with the various building blocks.

An electronic system is characterized to a large extent by its *operation frequency*. The fre-

(Cont. on p. 18)



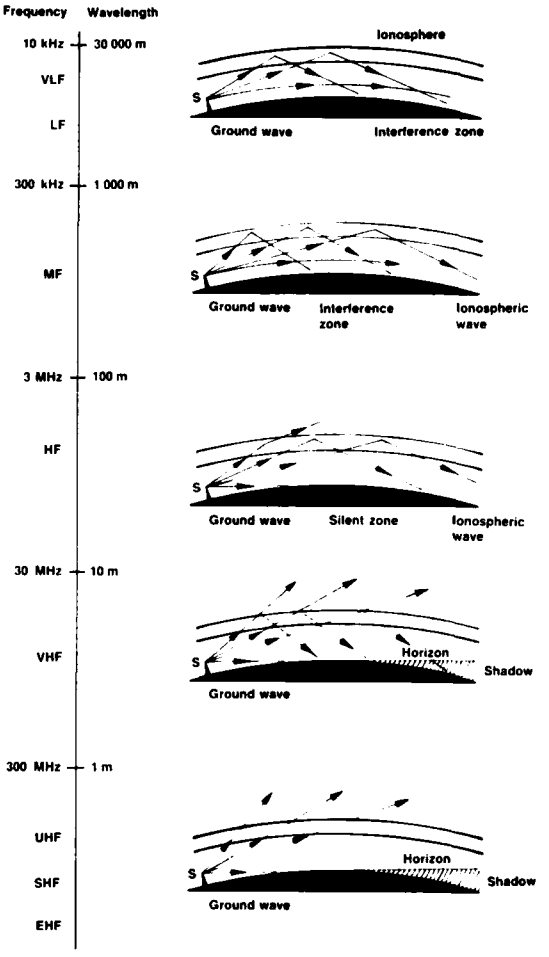
The electromagnetic frequency spectrum

Scales ❶ and ❷ show the relations between frequency and wavelength according to $f \cdot \lambda = c$, where f is the frequency in Hz, λ the wavelength in m, and c the velocity of light $2.988 \cdot 10^8$ m/s. Scale ❸ shows the names of the chief bands within the audio frequency, radio frequency and optical ranges.

VLF	very low frequency	3– 30 kHz
LF	low frequency	30– 300 kHz
MF	medium frequency	0.3– 3 MHz
HF	high frequency	3– 30 MHz
VHF	very high frequency	30– 300 MHz
UHF	ultra high frequency	0.3– 3 GHz
SHF	super high frequency	3– 30 GHz
EHF	extra high frequency	30– 300 GHz
LW	long wave	<100 kHz
MW	medium wave	0.1– 1.5 MHz
SW	short wave	1.5– 30 MHz
USW	ultra short wave	30– 300 MHz
Microwave		0.3–3000 GHz
IR	infrared waves	300– 0.7 µm
L	light waves (visible waves)	0.7– 0.4 µm
UV	ultraviolet waves	4000– 100 A
X	X-rays	100– 0.1 A
γ	γ-rays	<0.1 A

Scale ❹ shows some general examples of generators and of applications within the various frequency ranges, and scale ❺ the accepted, originally American, names of the frequency bands used in radar and military electronics.

***P*-band**	225–390 MHz
L- »	390–1550 MHz
S- »	1.55–3.9 GHz
C- »	3.9–6.2 GHz
X- »	6.2–11.0 GHz
K- »	11.0–36.0 GHz
Q- »	36.0–46.0 GHz
V- »	46.0–56.0 GHz



Ionospheric reflection predominates during night-time. Insignificant attenuation of ground wave.

Ionospheric reflection principally at night-time. Low attenuation at night, high in the day, and lower in winter than in summer. Range of ground wave less than at VLF and LF.

Ionospheric reflection both day and night. The ionospheric wave predominates and gives long range. The conditions vary greatly at different hours of the day and seasons of the year and with the time to sunspot maximum. The ground wave quickly disappears.

Ionospheric reflection only sporadically. Ground wave heavily attenuated. The range is limited largely by the horizon. At 5-10 m wavelength, however, the possibility of interference by an ionospheric wave must be taken into account.

No ionospheric reflection. Range limited by the horizon. Even relatively small objects are large in relation to the wavelength and therefore cause reflections. Good possibility of energy concentration by means of directional aerials. The weather conditions greatly affect the propagation.

Propagation of radio waves of different frequency. (From Elektroteknisk Handbok.)

quency scheme for electromagnetic waves is shown on page 17.

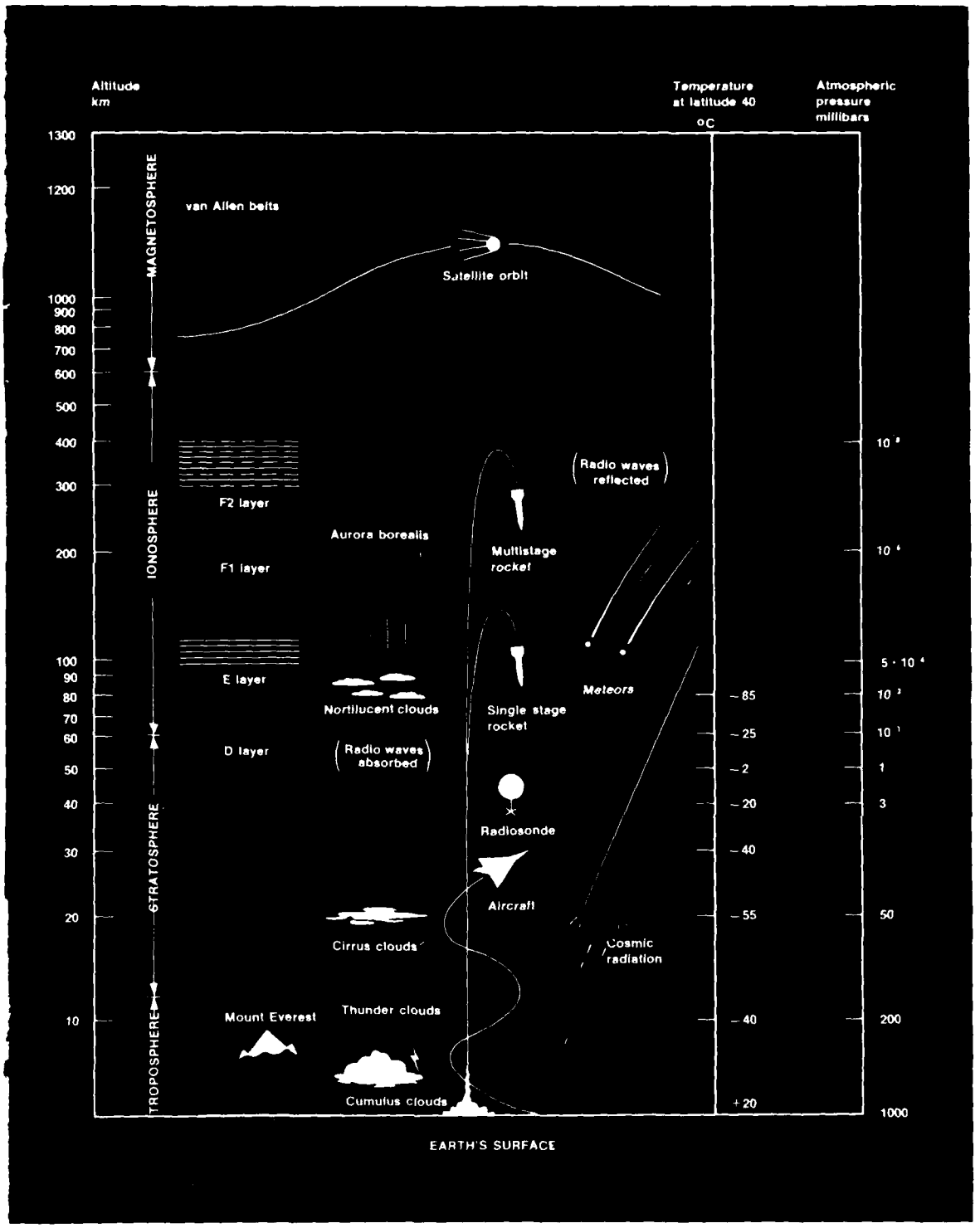
Another important point is the *propagation conditions for the radio waves* over the ground surface and in the atmosphere. The various atmospheric layers are shown in the picture on page 19, which also contains some other particulars of interest for telecommunications.

When the radio waves are propagated in the atmosphere, they are affected by different factors, as are the light waves, namely, refraction, diffraction, absorption, dispersion, interference and reflection. The effect is in all cases more or less dependent on the frequency; and therefore the propagation conditions —and so the attenuation, velocity and direction of propagation of the waves—are usually greatly dependent on the frequency.

At very short wavelengths, for example—about 2 cm and less —the radio waves are attenuated in the atmosphere, especially in bad weather, and their range is reduced.

The amount of attenuation—and equipment factors such as the design and size of the trans-

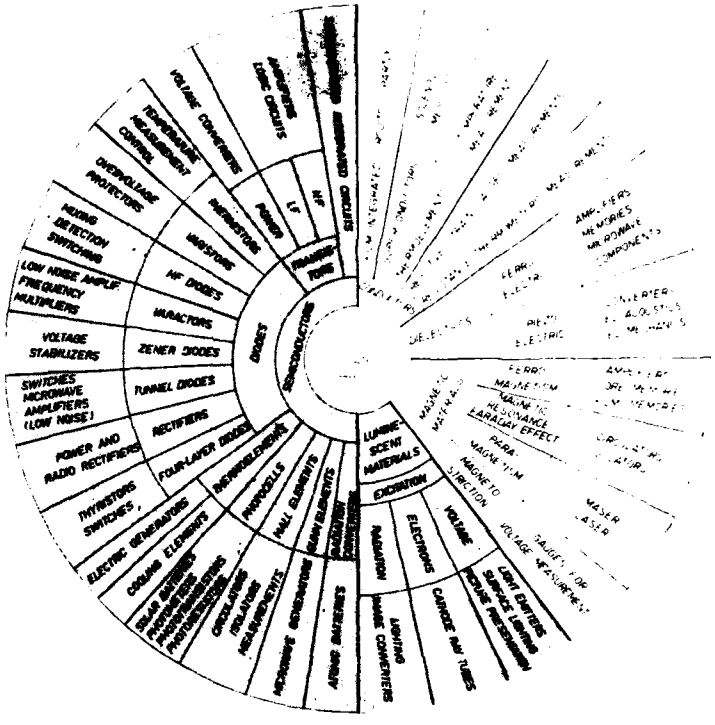
(Cont. on p. 20)



Section through atmosphere with data of interest for telecommunications.

SOLID STATE ELECTRONICS

Attempt at system atization of solid state electronics. The parent science (as for certain other applied sciences) is solid state physics (in centre). The solid state electronics field is divided radially into five groups *of materials—conductors, semi*conductors, dielectrics, magnetic and luminescent materials. On the basis of these materials electronic components have been developed, e.g. transistors and thermo-elements, or the physical or electronic effects are indicated, e.g. radiation luminescence. On the periphery are shown examples of electronic applications.



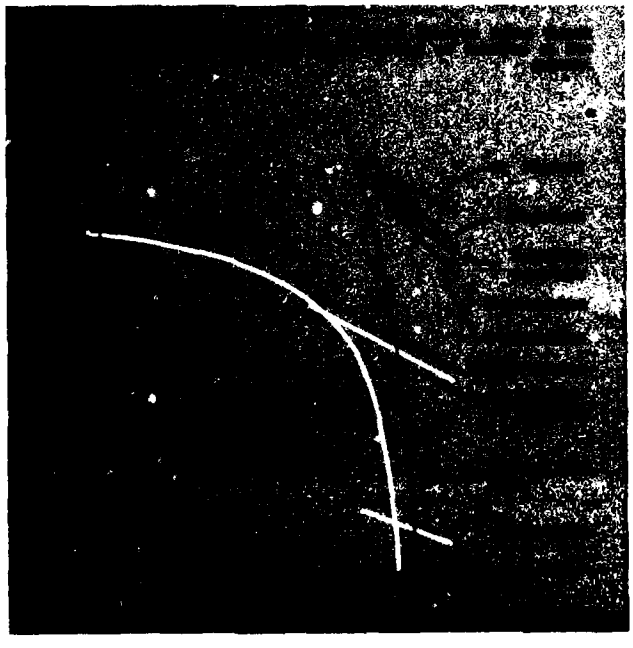
mitter and receiver aerials—are *what decide the range of the* system. The picture on page 18 shows the range within different frequency bands. The propagation conditions differ for *ground waves* and *ionospheric waves*.

The possibility of directing radio wave radiation is of very great importance for many military electronic systems. Radio wave radiation is directed by means of directional aerials, the directionality of which increases with the dimensions of the aerial in relation to the wavelength. Optimal directionality is aimed at in most equipments for radar, communication, navigation and guidance.

The more concrete parts of the electronic systems are made up of different subassemblies or units, e.g. transmitters and receivers, and these in turn are made up of *components*. The term *component* is rather vague, but a distinction is customarily made between *passive components* (e.g. resistors, capacitors) and *active components* (e.g. electron tubes, transistors). As active components in electronic systems the *electron tubes* have in recent years been increasingly replaced by *transistors* and other *solid state electronic* components. Strictly speaking, it is only for the combination of high frequency—high output that no particular prospects can yet be seen for solid state components.

This means that they cannot at present replace the militarily important high power microwave tubes, e.g. radar transmitter and jammer tubes. On the other hand many solid state components can perform circuit functions which electron tubes have never been capable of.

The solid state electronics field is a vague and very heterogeneous concept. An attempt at systematization is shown in the picture above.



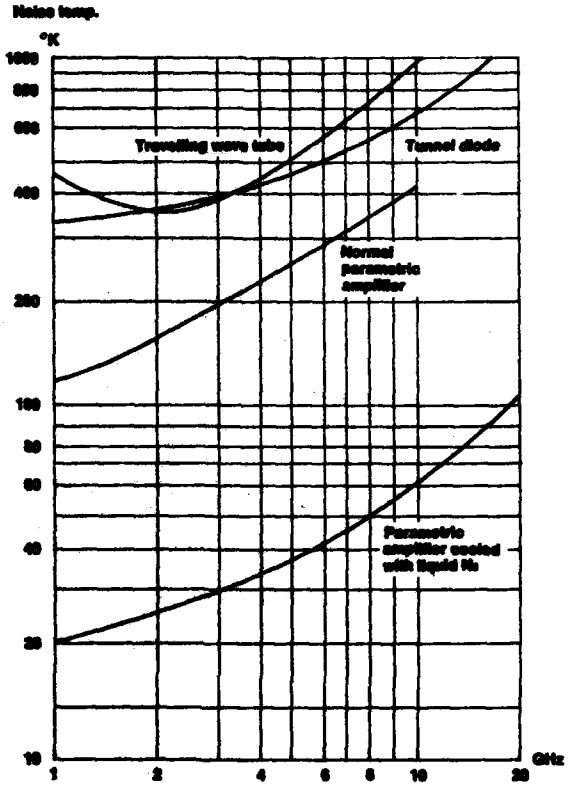
An important section of the solid state field is the *integrated electronic circuit technique* (IEC), which is attracting very great interest within applied electronics.

IEC implies the prefabrication of small encapsuled circuit units containing 10—100 component functions. These units, resembling components in their externals, are then combined into larger circuits and subassemblies. The chief use of IEC so far has been for digital devices, e.g. computers, but efforts are being made to use IEC also for the microwave field, e.g. in radar receivers.

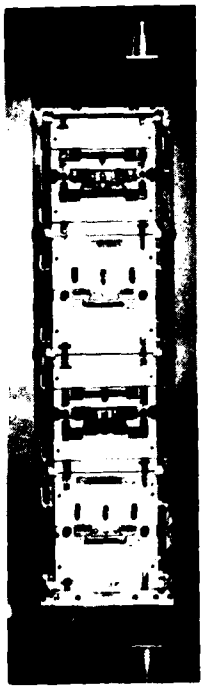
Microwave tubes, a special type of electron tube, are used as *high power generators* in the microwave field. For *radar transmitters* the classical *pulsed magnetron* is cheap, simple and robust, and is still used to a large extent. In new radar equipments increasing use is being made of transmitting tubes with quicker frequency tuning than the conventional pulsed magnetron possesses.

Jamming tubes usually work on a continuous basis and, according to the type of jamming, different types of microwave tubes can be used for this purpose, such as *CW magnetrons*, *M carcinotrons* or *travelling wave tubes*. Approximate outputs at different frequencies are shown in the diagram on the adjoining page. Further particulars concerning jamming tubes will be found in the section on "Technique of electronic countermeasures and counter-counter measures".

For receivers, e.g. *radar receivers*, tubes with a low noise factor are wanted in order to attain maximal sensitivity of the receiver and therefore optimal range of the radar. On the electron tube side the main interest is in *travelling wave tubes* with low noise factor. On the solid state side, however, various devices have been developed, chiefly *tunnel diode amplifiers* and *parametric amplifiers*, which offer alternatives with practically as good characteristics as those of the travelling wave tubes.



Variation of noise characteristics of some microwave amplifiers with the frequency.



A four-stage microwave amplifier for 1-2 GHz with noise factor 3 dB and gain 40 dB, made up of integrated circuits. Its size will be seen by comparison with the coin at the bottom.

Signal Intelligence

Signals within a frequency band are displayed on a screen of the panoramic receiver.

Signal intelligence is practised by many countries. It is aimed at other countries' communications—radio, radio link, data transmission systems—and at their radar, navigation and guidance systems etc. The former type is usually called *communications intelligence* (comint) and the latter *electronic intelligence* (elint).

The object of signal intelligence is to *detect, identify* and *locate* the *radiation sources* and to yield data which can be used in different ways after processing.

Signal intelligence may be strategic or tactical. *Strategic signal intelligence* is the only means of intelligence which, without provocation, reaches far into the territory of a presumptive opponent in peacetime, when, in fact, it has its perhaps greatest significance. *Tactical signal intelligence* is used almost exclusively in war and is very poorly documented in the literature. The following account deals with strategic signal intelligence even if it is applicable to many cases of tactical intelligence.

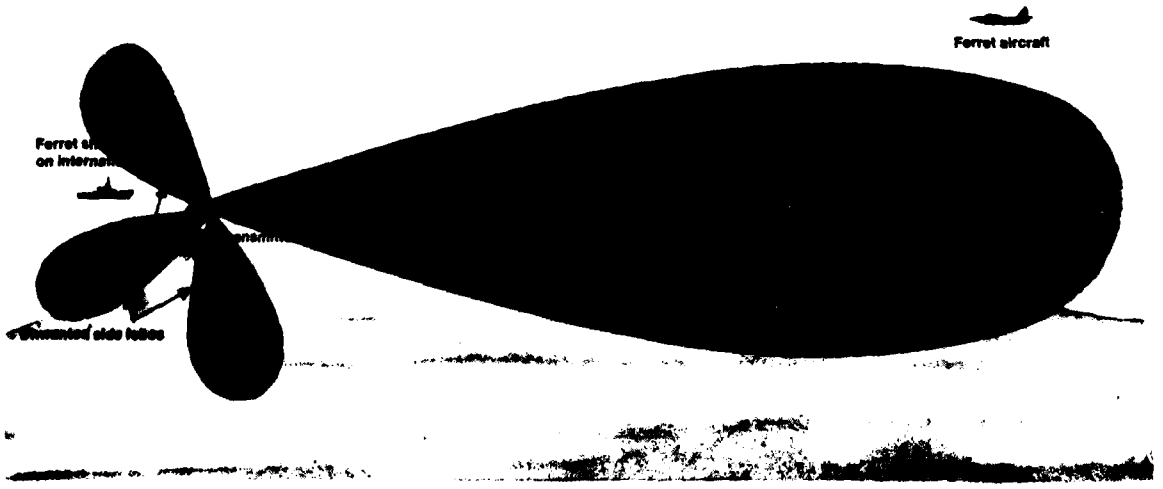
Acquisition

of signal intelligence can be done in several ways: from fixed stations within one's own territory or from shipborne or airborne stations operating on or over international waters. In the case of mobile stations both East and West are reported to use ferret aircraft, and the Soviet Union also to use specially equipped trawlers.

Ground-based intelligence often adequate against short-wave signalling at least for maintenance of contact at distances up to a thousand kilometres or more. The wave propagation, however, is greatly dependent on the frequency, on the time of day, on the season of the year, and on the time within the eleven-year sunspot cycle. On account of the welter of irrelevant short-wave traffic, manually operated receivers are used almost exclusively, naturally in combination with the necessary recording apparatus such as teleprinters etc. *Direction finding* is done from fixed stations of varying type, the bearing being presented visually or in data form after manual setting of the frequency.

Interception of low power *ultra short-wave* or *microwave* communication (radio link and non-directive or directive ultra short-wave) can in principle be effected at a distance roughly equal to the distance to the horizon. A ferret aircraft at an altitude of 7000 m thus has a range against these low-power transmitters of over 300 km. Conversely, ultra short-wave communication from an aircraft at this altitude can be monitored from ground stations at the same distance. In the case of a microwave link it may be necessary, at these distances, to keep in the main lobe of the link—to within, perhaps, ± 10 km—even if some of the side lobes at times may be

Even if the transmission is directed, as in the case of a radio link, some energy leaks out in other directions, at times sufficient for a signal interceptor. In the extension of the line of the link the airborne signal interception can attain satisfactory results.



accessible to interception. Under conditions of wave propagation anomaly (fairly common over the Baltic, for example, in the summer) signals in the ultra short and microwave ranges may during short periods (from minutes to days) reach one ground station from another, even at distances of some hundreds of kilometres.

The reception of ultra short and microwave signals can be done manually or automatically. If it is desired to retain the text of the transmission, manual methods are used, even if a panoramic receiver may be of valuable assistance. The latter scans continuously over the frequency range and displays the signals on a screen with a frequency scale.

Against radar signals one can use either a panoramic receiver which supervises small parts of the frequency band, one after another, with great sensitivity or a wideband receiver, which receives a larger frequency band at a time but has a lower sensitivity. Analysis of a particular signal can be done manually or automatically. Measurements are made of carrier frequency, pulse repetition frequency, pulse length, scanning pattern and other parameters of interest. Often a recording is made on video tape, but when this is not sufficient (e.g. for pulse length measurements—oscilloscope screens are filmed with the signal reproduced on different time scales.

Processing

of the information may in some cases be said to have started at the time of acquisition. Intelligent selection by the operator must not be underestimated. According to open sources, American experience is that data which have been automatically collected during hazardous enterprises cannot be handled owing to their enormous quantity. Sifting by the operator when collecting the data can save many processors! According to this philosophy a ferret aircraft should be a kind of flying laboratory.

Signal intelligence against communications involves traffic processing and text processing. Traffic processing involves the elucidation of network configurations, lines of command, order of battle. Text processing is done from linguistic and cryptological aspects.

The results of electronic intelligence are processed for several purposes, the main aim naturally being to detect new technical devices—gaps in the signal security organization may be greatest during the experimental period—to obtain "fingerprints" of the opponent's

equipment and systems and to provide early advice for planning of countermeasures. Another aim is to obtain directly useful operative data such as positions of ships, degree of air activity etc.

Comparisons are, of course, also made with the results of other sources of intelligence, e.g. photographic and radar reconnaissance.

By recording changes in volume of traffic, radar activity etc., the signal intelligence organization can fulfil an important function as an "alarm clock".

Signal security

Signal intelligence can be countered by *signal security*, which may be on the tactical, signal engineering or cryptological plane. Radio and radar silence is a radical but extremely two-edged weapon. High speed transmission (5–0.1 sec.) on short-wave, whereby the signals are hidden in irrelevant traffic, is a very effective method. Directional transmission affords some signal security. A link transmitter may be difficult to locate since the same "programme" is transmitted at the same frequency by several stations in a chain. Identical or randomly varying values of radar parameters complicate the identification and can make it very difficult to combine the resulting bearings. The use of one-time cipher of blanket type makes cryptological analysis impossible.

It should be added that the aim of signal security is to counter not only signal intelligence but also jamming (for which, however, intelligence is sometimes essential).

In general it may be said that, in this area as well, there is the same well-known interplay between development of measure and countermeasure as in many other fields. Signal intelligence becomes more difficult, but is also more difficult to counter.

Technique of Electronic Countermeasures and Counter-countermeasures

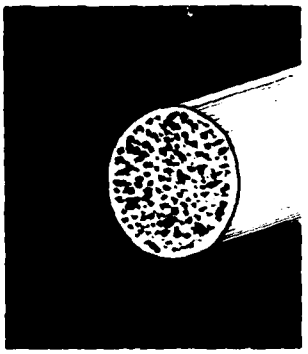
The large variety of military electronic systems, and the various tactical requirements and technical facilities, have given rise to a whole series of methods of jamming. These may be classified in different ways on the following principles:

- *Passive* and *active* methods.
  Passive methods employ only the radiation transmitted from the enemy electronic system.
  Active methods imply that the jammer generates radiation to counteract the enemy electronic system.
- *Masking* and *deceptive* methods.
  Masking ("Barrage") jamming has the aim of concealing the information which the enemy's electronic system is intended to collect or transmit.
  Deceptive jamming introduces false information into the electronic system.

Passive jamming

is used chiefly against radar and homing missiles. Different kinds of reflectors are used for this purpose. In their most elementary form these consist of large quantities of metallic or metallized strips or wires. Their length should preferably be adapted for resonance within the frequency band of the radar or homing device concerned. These small reflectors can be dropped directly from aircraft or guided missiles or from rockets fired from aircraft or ships. Owing to their slow rate of fall their action continues for a fairly long time. Window—as these strips are called—can be dropped both for

A bundle of window (life size) with which an aircraft echo can be simulated on the radar indicator.



Within a corridor of window dropped in advance aircraft can move unseen by the defender's surveillance radar, which gives them surprise in attack.

When the fire control radar has locked on the aircraft during pullout, the aircraft drops window continuously for a few seconds. The radar can then be deceived into ranging on a point in the window behind the aircraft.

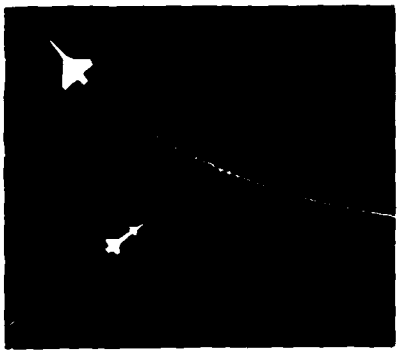
masking and deceptive purposes. A concentrated cloud of some tens of thousands of strips produces a reflection corresponding to that of an aircraft and produces a fictitous target which may confuse a fire control radar or guided missile. Strips fired up by rockets from ships simulate the splash of projectiles and so confuse the fire control. Aircraft can be masked by dropping window in very large quantities in long lines or over a wide area within which the aircraft can move without being detected by the enemy's radar.

Technical developments have favoured this method of jamming. Modern window—metallized nylon or glass wires—can be carried in very large quantities in little space. An "aircraft echo" thus requires only a few c.c. of volume.

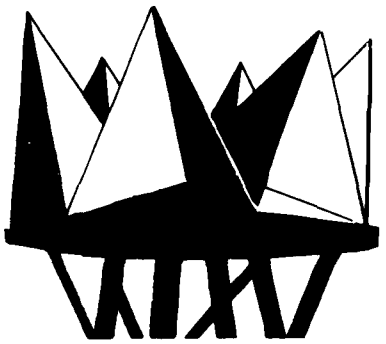
Other types of reflectors which can be used for generating false targets are *corner reflectors* and *Luneberg reflectors*. These both have the property of reflecting incident radiation, within a large solid angle, chiefly back to the source, roughly like a cat's eye or reflex tape.

The *corner reflector* consists in principle of three metal plates perpendicular to one another and joined together so as to form one or more "internal" corners.

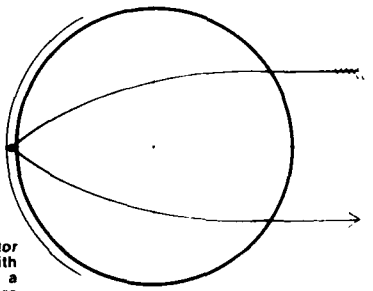
The aircraft drops window under simultaneous evasive action. The attacking missile locks to the window and homes onto it.



The attacked vessel fires window rockets to simulate the splash of projectiles and confuse the enemy's fire control.



The corner reflector is an old and well-tried method of increasing the radar target area.



The Luneberg reflector —a dielectric globe with metallized cap—is a more modern and more efficient echo enhancer.

The *Luneberg reflector* consists of a number of concentric spherical shells of a material of which the refractive index decreases with increasing radius. A corner reflector or a Luneberg reflector in a small boat or missile can simulate a large ship or aircraft for a radar homing device.

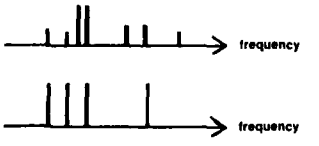
Active jamming

is effected with barrage or deceptive jammers and can be used against the most varying types of electronic measures such as long-wave navigation, short-wave and VHF communication, microwave missile guidance and fire control.

The character of the jamming signal, and therefore of the jamming apparatus, depends on the nature of the object to be jammed and a knowledge of its data, on the technical facilities and on the tactical situation. The most universal jamming signal is white noise, the power of which is uniformly distributed over a very wide frequency band. Even if this method of jamming is *simple in principle*, it is often difficult to achieve owing to the large power requirement and strict specifications as regards certain transmitter components. Usually, therefore, the attempt is made to match the jamming signal to the data of the enemy transmitter, a knowledge of which is acquired both from the intelligence service and by means of receivers which in most cases form part of the jamming apparatus.

If the frequency of the enemy transmitter cannot be determined with sufficient accuracy, if the frequency is often changed or if several transmitters are to be covered simultaneously, it is often advisable to use *wide-band* jamming. Hereby the jamming power is distributed over a wide frequency band, perhaps many MHz on VHF or many hundreds of MHz on microwave. This method is akin to the aforementioned universal method, but owing to limitations in component data and power resources it

Narrow-band jamming



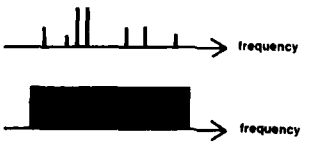
ADVANTAGES

High efficiency.
Small weight and volume.
Easy to avoid jamming of certain frequencies.

DISADVANTAGES

Requires accurate signal analysis and trained operator or complicated automatic equipment.

Wide-band jamming



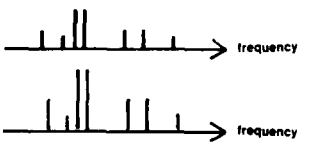
ADVANTAGES

Little signal analysis required.
Simple setting.

DISADVANTAGES

Low efficiency.
Large weight and volume.

Repeater jamming



ADVANTAGES

Little signal analysis required.
Automatic.
High efficiency.
Small weight and volume.

DISADVANTAGES

Easy to block by false transmission.
Technical problems (e.g. insulation between receiver and transmitter aerial).

is often necessary to work with other types of signals than white noise, e.g. a wide-band frequency modulated signal, and to choose particularly suitable tactical situations.

If the frequency of the enemy transmitter is known and is not changed too often, *narrow-band* or more correctly frequency selective jamming can be employed. In this case the attempt is made to concentrate the jamming to the particular channel or channels used by the transmitter. This results in satisfactory power economy but usually requires careful supervision or complicated automatic equipment for parrying changes of frequency of the transmitter.

Wide-band as well as narrow-band jamming are used for masking purposes. A third form which is perhaps used most for deception, at least within the radar and homing fields, is *repeater jamming*. This consists of amplification and retransmission of the transmitter signal, possibly distorted. Repeater apparatus is usually wide-band i.e. it is prepared to respond to any frequency whatsoever within a wide band.

Components

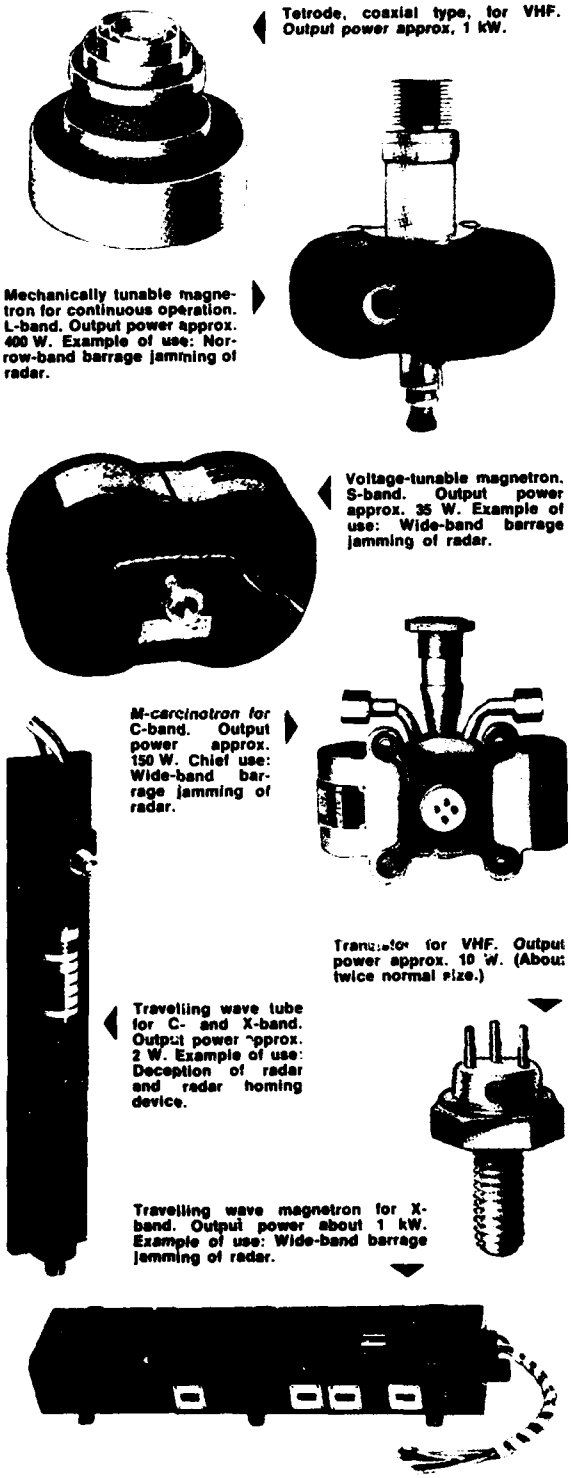
Among the components for jammers the *electron tubes* in particular may be mentioned. At frequency bands below about 1000 MHz use is made of conventional triodes, tetrodes etc., with which output powers as large as the application calls for, or the primary power resources allow, can be obtained.

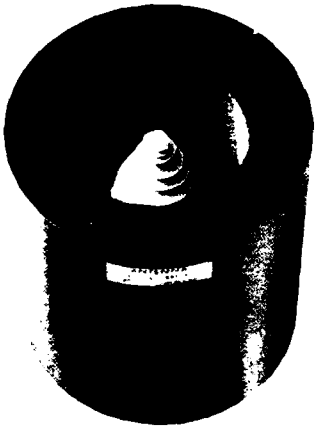
In the microwave region there is an abundance of special purpose tubes; their data often place a limit on the performance of the jammer.

Magnetrons of different types can be used for narrow-band or frequency-modulated wide-band jamming.

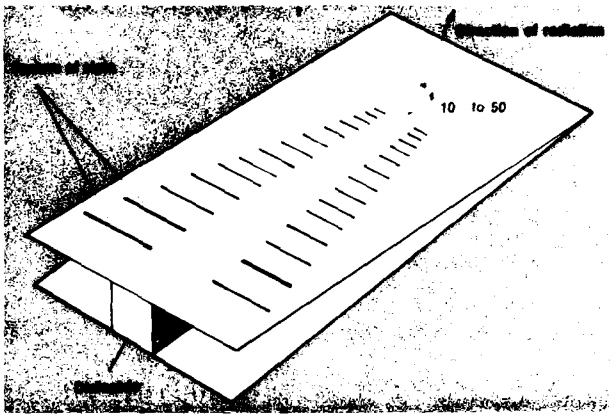
Carcinotrons are used for frequency-modulated wide-band jamming.

COMPONENTS FOR JAMMERS





In many jamming systems one wishes to receive and transmit simultaneously, which requires good insulation between the aerials. This wideband microwave aerial has therefore been surrounded by a wall of radiation-absorbing material.



Jamming transmitter aerials must often have a constant directivity over broad frequency bands and at the same time stand up to a high power. The sketch shows the principle of a log-periodic high power aerial for microwaves.

Travelling wave tubes of different kinds are suited for repeater transmitters or for transmission of wide-band noise.

Intense development work on microwave tubes is being done in many countries, and greatly improved *jammer performance* may be expected in the future.

Semiconductor components and *integrated circuits* are undergoing rapid development and are of great significance for jamming. They will permit fully automatic systems and smaller and lighter jamming apparatus, e.g., for aircraft, missiles, parachutists and saboteurs.

Aerials with suitable characteristics in respect of bandwidth, directivity, polarization etc. are particularly important for jamming.

Jamming of radar and radar homing devices

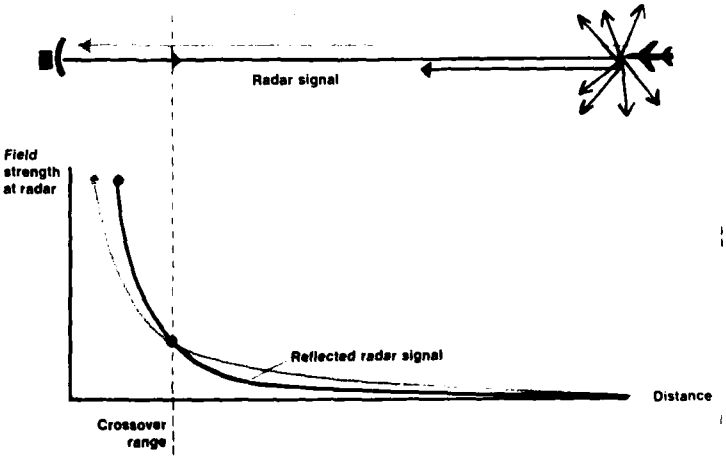
is an important and diversified part of jamming technique and will be considered chiefly from the point of view of the possibilities and limitations of this technique.

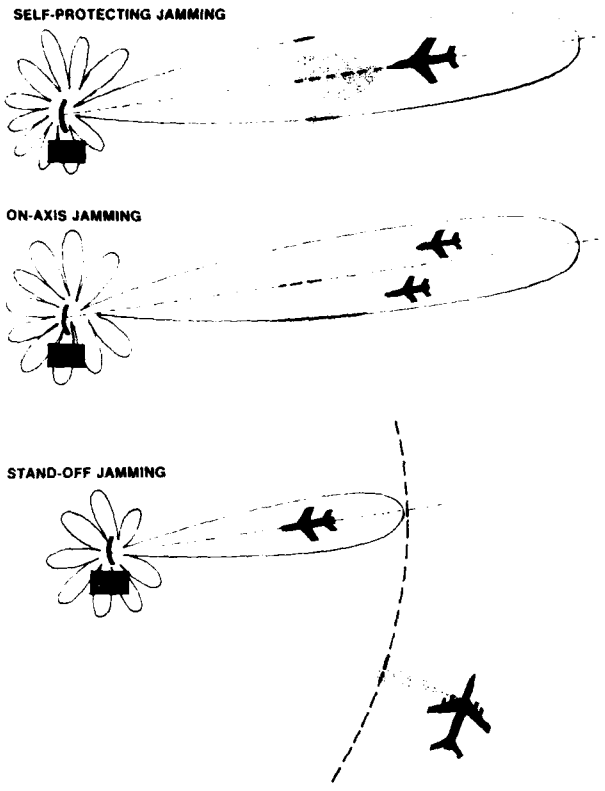
Radar systems work within the microwave or, for certain purposes, the VHF band.

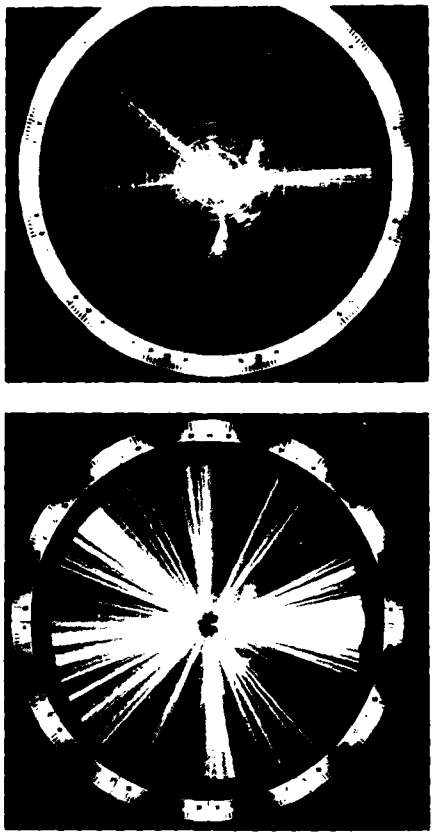
The radar illuminates the target by means of a directional aerial and receives the reflected signal with the same or, in some cases, another aerial. The direction of the aerial and the time of travel of the electromagnetic wave provide the desired target data.

Radar systems must generally have both a high power output and a high receiver sensitivity. This is because the radiated energy must travel from the radar to the target and back, and that much energy is lost in all directions in being reflected from the target, which may also

The radar signal must make the return journey from radar to target, while the jamming signal needs only a "single ticket". This is why a jamming target can be concealed beyond a crossover range but not closer.







PPI pictures from a surveillance radar subjected to weak and strong barrage jamming from a target on bearing "3 o/c".

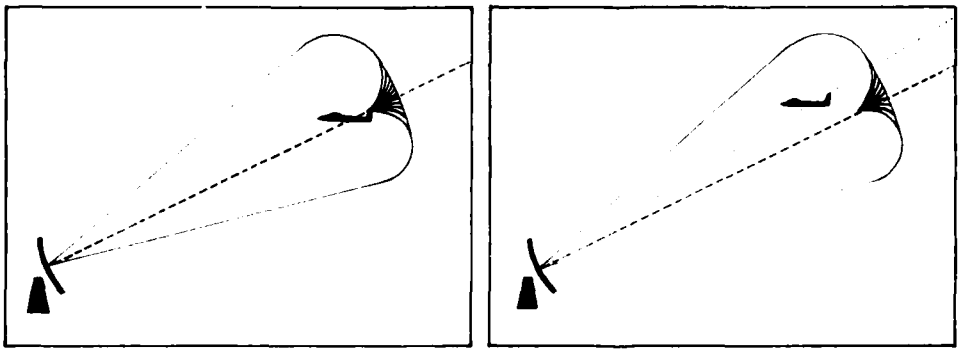
be of small size. The jamming signal, on the other hand, has only the single distance from the jammer to the radar to travel. These circumstances—differences in travel and losses in reflection—make radar jamming particularly favourable from the power aspect. The different dependence of the signals on distance means that less power is required for jamming a radar if it is far from than if it is close to the target: an aircraft approaching the radar and sending barrage signals can be concealed by these signals in to a given "crossover range". Within this range the aircraft echo is seen through the jamming signals on the radar indicator.

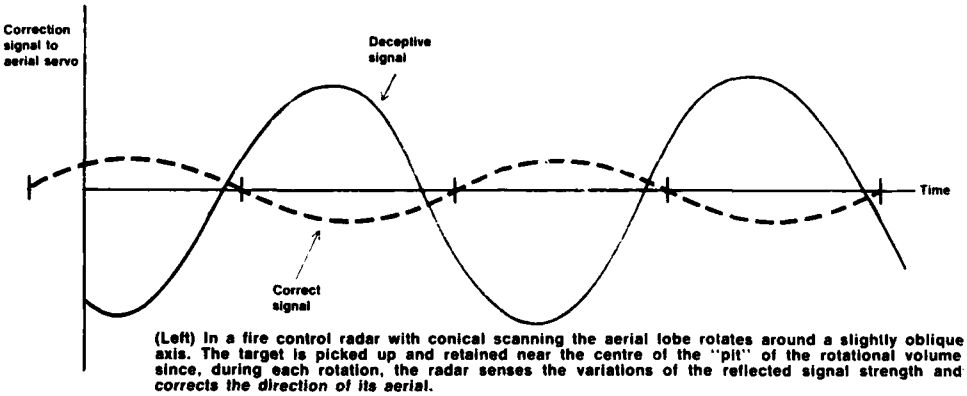
Surveillance radar generally scans all round the horizon with a continuously rotating aerial; its job is to detect and locate relatively distant targets.

With barrage jammers one can reduce the range of the radar, but the latter, in return, can often locate the jammer. The jammer may be in the target (self-protecting jamming) or on the same bearing as the target (on-axis jamming) and in such case makes range-finding in that direction difficult or impossible. This method requires only a small or moderate power output from the jammer. The jammer may also be on another bearing than the target (stand-off jamming). In this case the jamming signal enters the side lobes of the radar aerial and also reduces the range on the target bearing. Both ranging and direction finding are thus prevented; but owing to the unfavourable angle of incidence in relation to the radar aerial the method often requires a high-power jamming signal concentrated on the radar by a good directional aerial. Special jamming aircraft can be assigned for this purpose, circling outside the range of the air defence.

Deceptive jammers can be used to produce false targets, either placed at random on the radar indicator or with a specific position, course and speed. This type of jamming requires little power, and it may be impossible to locate the jammer, at least from the jammed radar.

Fire control radar locks on and follows fairly close targets to provide accurate fire data.

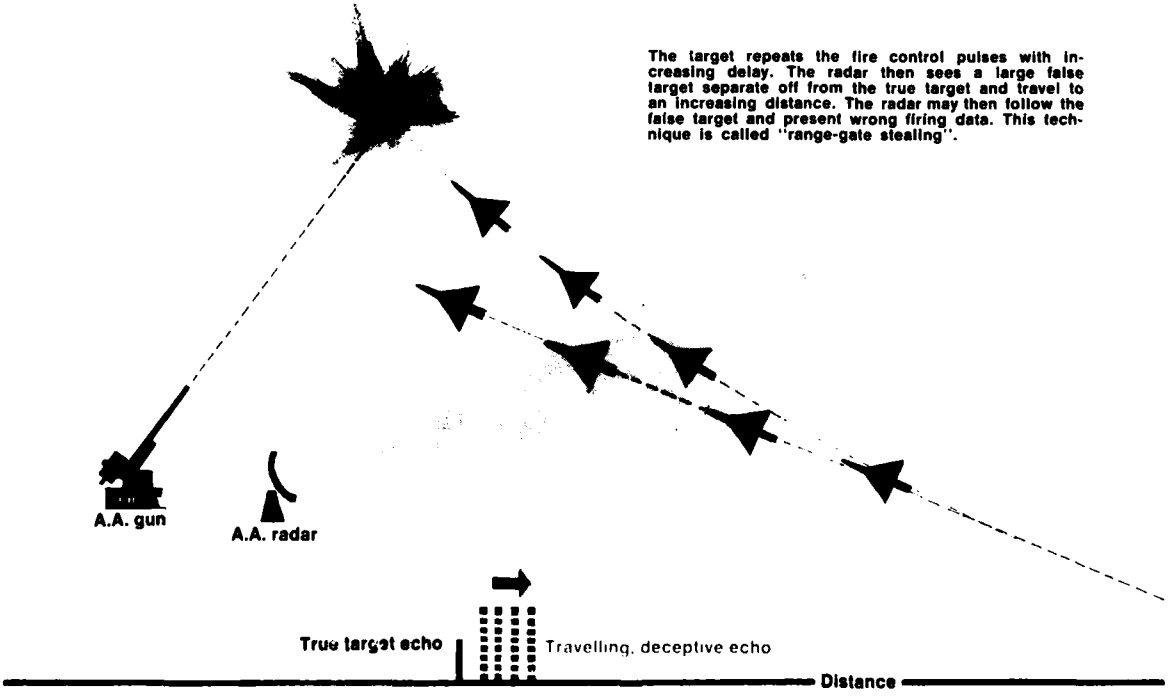


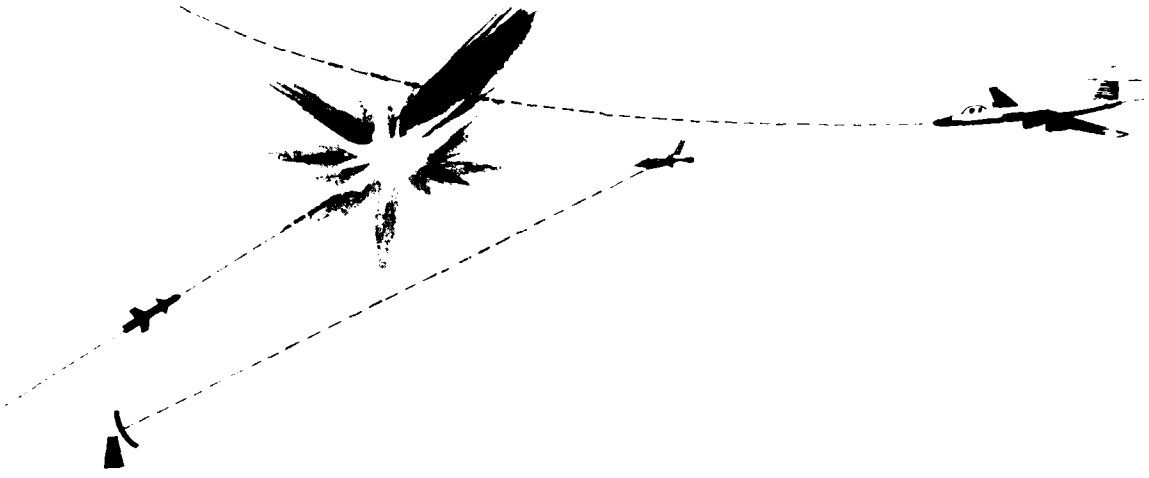


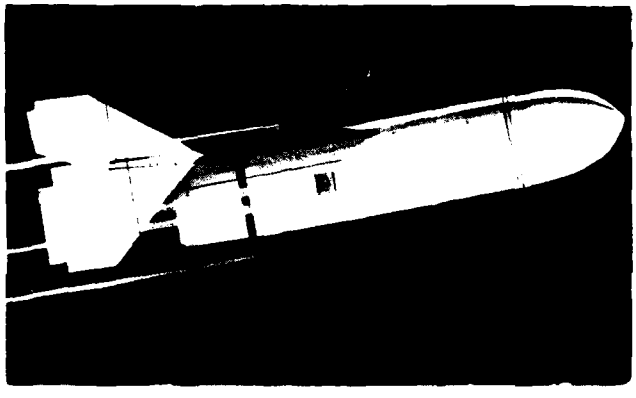
(Left) In a fire control radar with conical scanning the aerial lobe rotates around a slightly oblique axis. The target is picked up and retained near the centre of the "pit" of the rotational volume since, during each rotation, the radar senses the variations of the reflected signal strength and corrects the direction of its aerial.

(Right) The target can deceive the radar into an angular error by repeating the radar signals with reversed strength variations. The radar then miscalculates the position of the target in the "pit" and turns its aerial away from the target. This jamming technique is known as "inverse conical scan repeater".

The target repeats the fire control pulses with increasing delay. The radar then sees a large false target separate off from the true target and travel to an increasing distance. The radar may then follow the false target and present wrong firing data. This technique is called "range-gate stealing".







When the bomber's radar interception receiver indicates that the bomber has been picked up by the illumination radar of the missile system, the bomber fires a missile with echo enhancer (Luneberg reflector or repeater transmitter). The missile attack can then be diverted to this decoy while the bomber completes its mission. The photograph shows an American decoy missile.

Barrage jamming is in this case usually not so advantageous. Owing to the small target distance the method requires high power and must generally be in the form of self-protective jamming. The radar can then not be prevented from taking a bearing on the target and measuring its angular velocity.

Deceptive *jamming* of *fire* control radar can be directed against the radar's angle or range tracking equipment, or against both simultaneously. Using angular deception against, for example, a fire control radar with conical scanning, the radar signals can be retransmitted with distorted amplitude relations by a repeater transmitter. The tracking servo of the radar aerial thus receives false correction signals and turns the radar away from the target. Range deception can also be effected with a repeater transmitter, which repeats the radar signals with suitably varying delay.

Radar homing devices in guided missiles may be either *active* with a complete radar in the missile or *semiactive*, in which case the missile uses the target-reflected radiation deriving from a radar transmitter at another position. It is primarily the angular information that is used for guiding the missile.

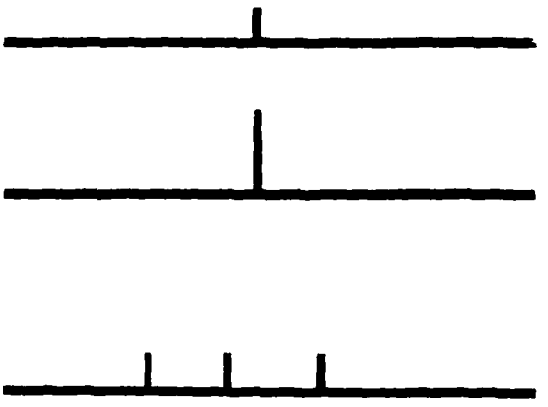
Self-protective barrage jamming may in this case be directly hazardous, since many types of missile have the property of homing on such jammers.

Stand-off barrage jamming is a conceivable measure but one that requires high power. From a point beyond the range of the missile sufficient power must be generated at the correct frequency to act upon the missile even from an unfavourable angle of incidence.

Angular deception can be effected with repeater jammers in the same way as against fire control radar. Decoys containing echo-enhancing repeater transmitters may also be released to attract the missile to them. Decoys for this purpose may also contain reflectors or consist of "bursts of window".

Jamming of radio communication

has naturally certain technical resemblances to radar jamming.



By an increase of power one can sometimes penetrate through the jamming.

An attempt can be made to utilize the weaknesses of the jammer by multifrequency transmission.

but there are essential differences. The radio signal often goes directly from the transmitter to the receiver and not, as with radar, via dissipating reflection from a small target (an exception, however, is transmission by scatter). A large amount of radio communication takes place on short wave and the lower VHF band, on which it is difficult to use effective *directional aerials*. The concepts of self-protective and stand-off jamming etc. have little meaning in this context. The wave propagation and aerial conditions, moreover, mean that the risk of conflict with one's own frequency channels is often greater in the jamming of radiocommunication than of radar. For this reason, and owing to the mobility of radiocommunication in time and frequency, there is often a need for an instantaneous survey of the situation on the frequency band concerned. Some of the problems of communication jamming are further dealt with in the section on Land Warfare (pp. 53).

Jamming of other types of electronic systems

e.g. navigation systems, is often technically possible and tactically suitable. The technique is so varied, however, that general comments can hardly be given.

Electronic countercountermeasures

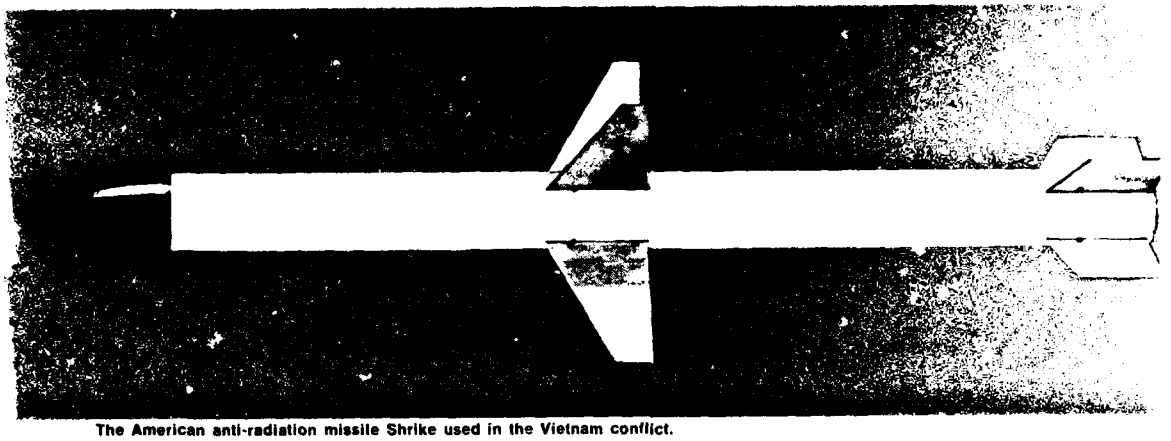
of many kinds can be used to reduce or eliminate the effect of jamming. Some of them are fairly universal, while others are more specific to a given type of electronic system or to a particular type of jamming.

A universal method against active jamming is to use a high-power transmitter with a good aerial in order, quite simply, to "shout down" the jamming signals.

On many frequency bands, particularly microwave and upper VHF, a directional aerial can be used on the receiver; this amplifies the desired signal but suppresses jamming signals from other directions.

Rapid change of frequency or the use of several frequencies

The aircraft can fire its antiradiation missile from a point outside the range of the surveillance radar. For the missile it is a question of "memorizing" the bearing to the radar while, during its rotation, the radar aerial points in another direction.



The American anti-radiation missile Shrike used in the Vietnam conflict.

simultaneously are means of avoiding narrow-band jamming or of making use of the weaknesses of a wide-band jammer (e.g. gaps in its frequency coverage).

The receiver should, if possible, be built so as to accept only the type of signal used by the system it is to counter: for different reasons, such as limitations of electron tubes, the jamming signal often has a different frequency or time function.

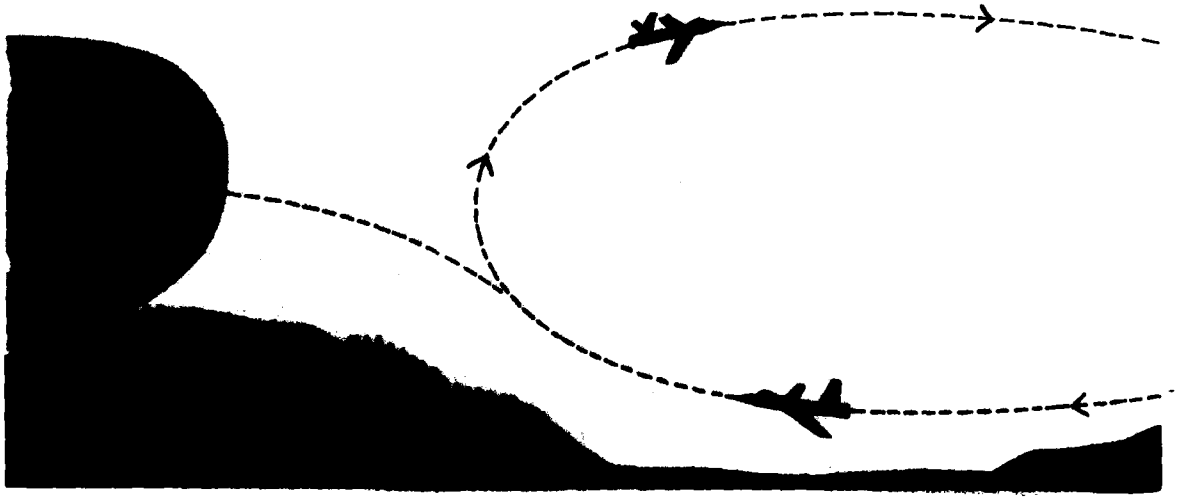
A drastic antijamming measure is to attempt to locate the jammer's position (e.g. by direction finding) and then to destroy it with weapons.

If window is dropped by moving targets, the difference in speed of the targets and of the relatively stationary window can be used to diminish or eliminate the interference. This is done in doppler and MTI radar. A radar with very high angular and range resolution is also able to distinguish targets from window that is fairly sparse and cannot give so strong an echo from the small volume corresponding to the radar's resolution.

Anti-radiation missiles

may be regarded as an electronic countermeasure with directly destructive action. These missiles are equipped with homing devices which can home on radar stations, radio link transmitters or other signal sources which are in operation for long periods. The missile warhead can destroy not only the transmitter but also targets associated with it, such as a ship or staff headquarters. Several such missile projects are known from the U.S.A. Despite certain weak points, it is likely that some type is in operative use.

If an attack by an anti-radiation missile is feared, the transmitter should be shut down or operated for short periods at long intervals so that the missile loses its way. Deception of the missile by means of false transmitters is another conceivable countermeasure.



Situation. *Power B attacks power A. The hostilities start with a stage of combat lasting about a week, during which B engages targets within A's territory in preparation for an invasion by sea. A has mobilized when war breaks out. Use of ABC weapons is not intended. Period 1968. B has the resources of a great power.*

Defender's (A) air defence

A.A. missile batteries

Mobile A.A. missile batteries can be regrouped between the various sectors.

Main data of A.A. missile system:

Max. altitude 18 km.
Range 60 km.
L-band surveillance radar.
X-band semi-active homing system with lobe rotation.

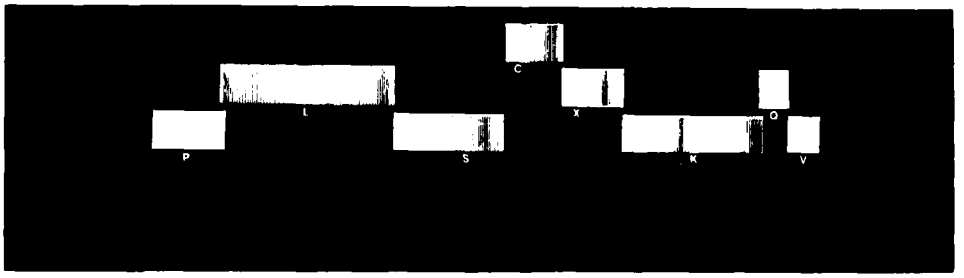
A.A. artillery

The A.A. artillery consists of a large number of batteries, most of which belong (organizationally) to the field army and follow the movements of the army units. Each battery has a C-band surveillance radar (pulsed), X-band fire control radar and 40 mm. A.A. guns.

Fighter defence

The fighter defence consists of interceptor aircraft.

The radar bands. The shaded portions indicate the most commonly used frequencies.



Electronic Warfare against Air Defence (Example)

Main performance data:

Max. speed 1100 km hour.

Armament:

air-to-air radar homing missiles
air-to-air rockets
25 mm. guns.

The Air Defence Control System consists of a well-protected Centre per section with (per sector):

1—2 stationary P-band high-altitude surveillance radar of non-modern type, especially in respect of ECCM.
1—2 stationary L-band high-altitude surveillance radar.
3—4 mobile C-band surveillance radar.
3—4 S-band low-altitude surveillance radar at fixed positions on heights along the coast.

Communication between the Centre and the fighter aircraft is by radio.

Attacker's (B) air forces

Aircraft	Speed km hr	Max. alt. km	Range	Armament	Countermeasures
Bombers, strategic	1000	14	Range sufficient for engaging targets within A's entire territory	6 t bombs	Standard equipment*) 4 jammers 2 window dispensers
Bombers, tactical	1300	12		2 t bombs	Standard equipment*) 2 jammers 1 window dispenser
Strike aircraft	1600	16		1 t bombs or rockets (missiles)	Only in outer pod and at the cost of part of the armament (jammer and or window dispensers)
Strike aircraft	900	12		0.5 t bombs or rockets (missiles)	Ditto

*) More countermeasures can be carried, but at the cost of part of the armament.

The efficiency of a modern air defence of the type assumed in the following example is very greatly dependent on the degree to which the attacker exploits the electronic weak points in the air defence system. The efficiency is thus dependent on the manner of and the extent to which electronic warfare is conducted.

In the situation exemplified electronic warfare will be seen to favour the offensive party: the aggressor has ample alternatives in the choice of strategy.

If the attacker does not exploit the weaknesses of the air defence— its susceptibility to jamming, its susceptibility to attack (owing to its positions being detectable by signal interception and to the fact that, for example, anti-radiation missiles can be used), difficulties of low-altitude coverage etc.—the effect of the air defence would be disastrous, causing a loss (in aircraft per attack) of perhaps 25—50 per cent. The attacker cannot possibly accept such losses but must adopt effective means of electronic warfare. It is likely that his losses would then be greatly reduced.

Weaknesses in the air defence that can be exploited by the attacker

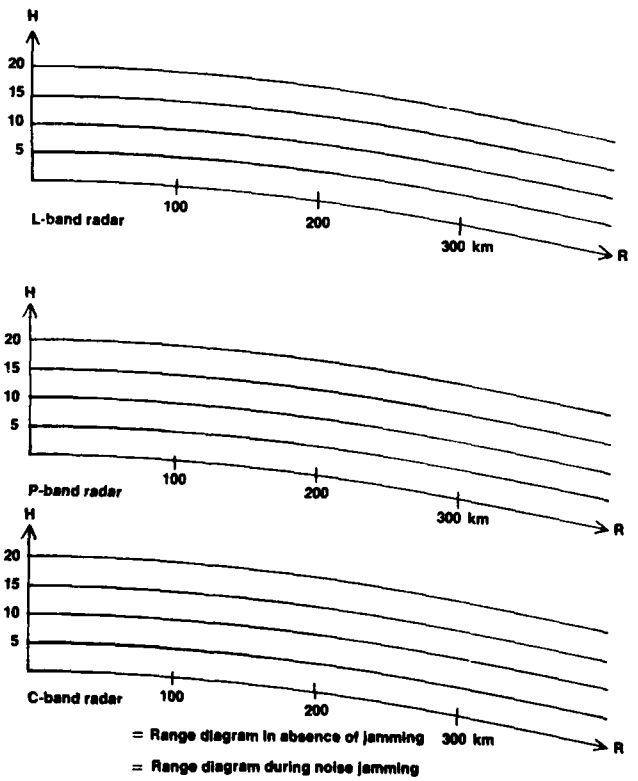
Range and altitude coverage of surveillance radar stations can be reduced by jamming

Noise-modulated jamming on the radar frequency drowns and conceals the echoes of the attacking targets. As the aircraft approaches the radar stations, the aircraft echo grows more quickly than the noise level, so that at sufficiently short distances the aircraft echo may be visible despite the jamming. The result is that the radar's range is correspondingly reduced. The reduction depends, among other factors, on the power of the jammer.

The jammers may either be carried in the attacking aircraft (self-protective jamming) or placed in special jamming aircraft which accompany the formation (on-axis jamming) or patrol outside the range of the defence weapons (stand-off jamming).

The attacker may, for example, adopt self-protective jamming of the L- and C-band stations and stand-off jamming of the P-band stations, which are more sensitive to jamming. The ranges and altitude coverage are then considerably reduced, as

Reduction of range and altitude coverage of surveillance radars by jamming.



shown in the picture, if the jammer performance is on a level with modern achievements. It should be noted especially that, at altitudes above 10 km, approaching targets are detected only by the P-band stations and then only at short ranges.

Surveillance radar stations can be jammed by window

Jamming of surveillance radar by window can be given the form of barrage jamming by dropping the window so densely that a continuous corridor of window is laid. The following aircraft can then fly-in without being detected by surveillance radar.

The bundles of window can also be dropped at larger intervals by a forward line of aircraft. The large number of false echos caused by separate clouds of window naturally delay the detection of the true targets and place difficulties in the way of the command control centre.

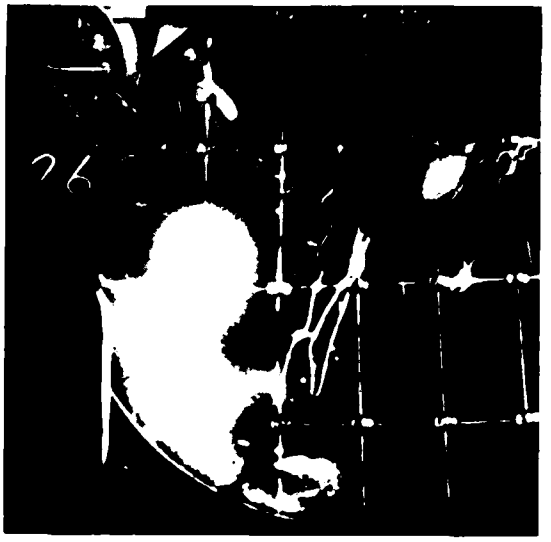
In a situation such as that described, window should not be considered as an alternative to the use of jammers against surveillance radar but as a supplementary measure which greatly adds to the interference effect.

Radar stations can be located by signal interception (direction finding)

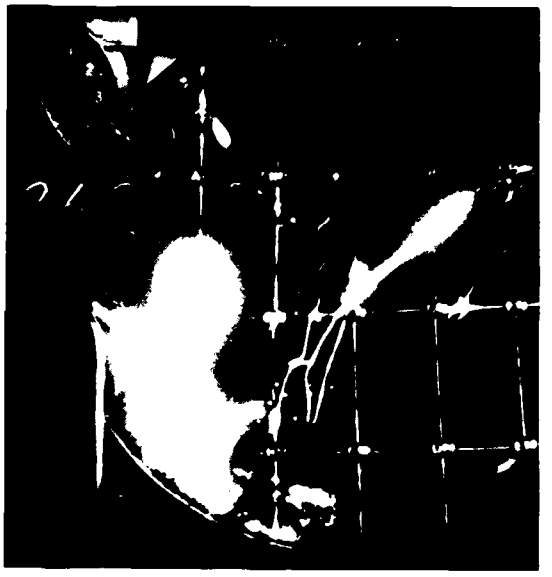
Through electronic intelligence the attacker can obtain data for planning of countermeasures and can identify and locate radar stations and other signal sources. These are then, of course, easier to put out of action.

Typical figures of accuracy in location that the attacker can count on in this case will be seen from the diagram on the next page. The interception is assumed to take place from ferret aircraft 150 km off the coast or from ships 20 km from the coast. Electronic intelligence can be collected in peacetime and normally provides data for the use of other more accurate reconnaissance methods.

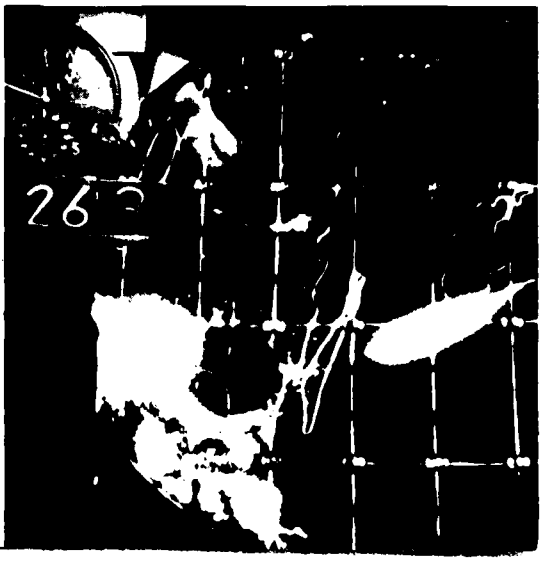
Window jamming of surveillance radar in Swedish trial between islands of Gotland (top right) and Öland. Window observed on radar indicator at STRIL 60. Air Force photographs.



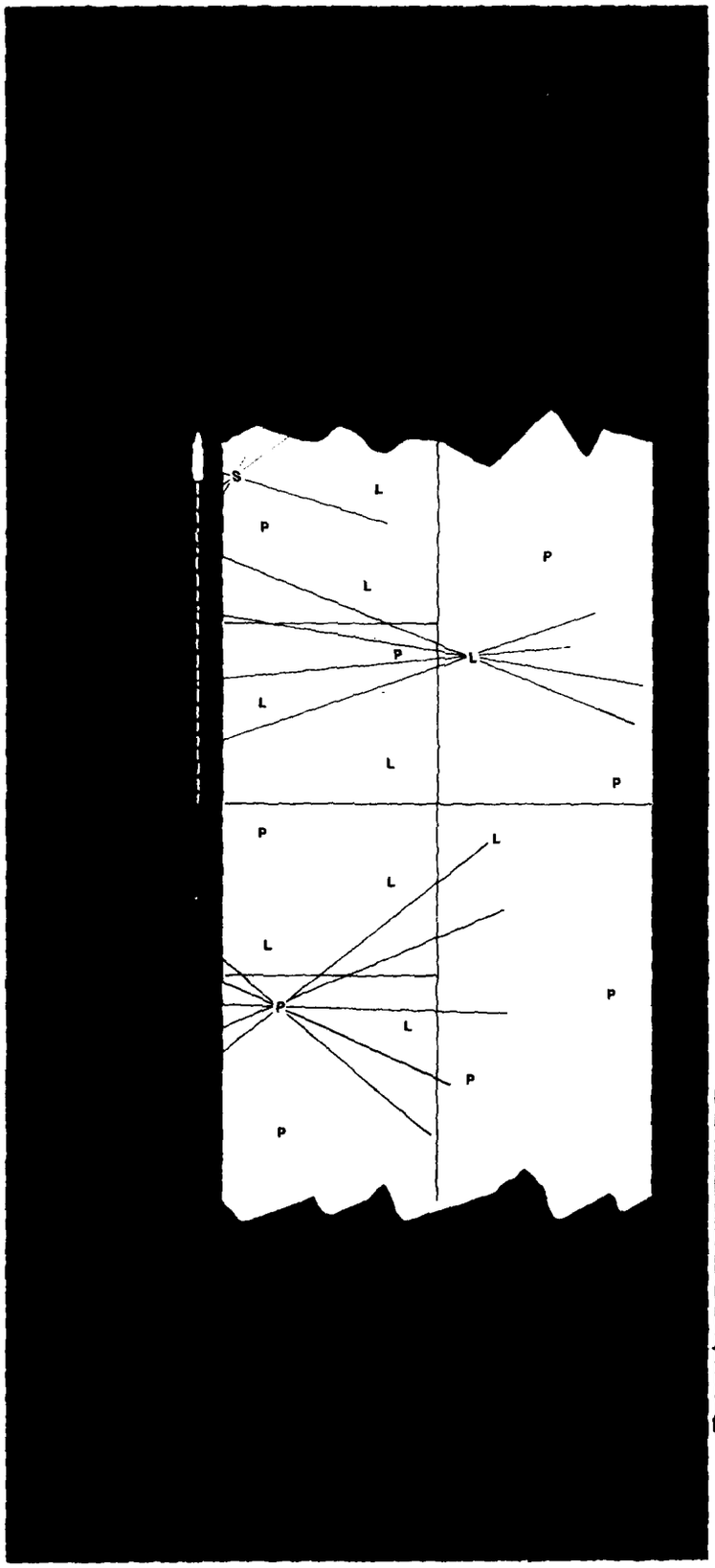
1815 hrs
Start of laying of a corridor of window at high altitude north of Visby.



1825 hrs
Window laid from Visby to Öland (Böda).



1949 hrs
The window is still effective but has drifted with the wind about 30 km southwest.



Radar stations can be destroyed by *anti-radiation missiles*

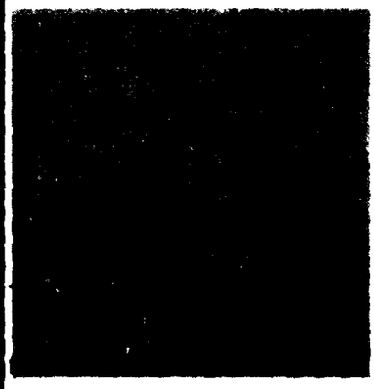
As radar stations send out signals, they are potential targets for anti-radiation missiles, the passive homing device of which guides the missile to the source of the signal during the homing phase.

The attacker is assumed to possess short-range anti-radiation missiles which can be launched from aircraft. An attack with such missiles may proceed as shown in the series of pictures below.

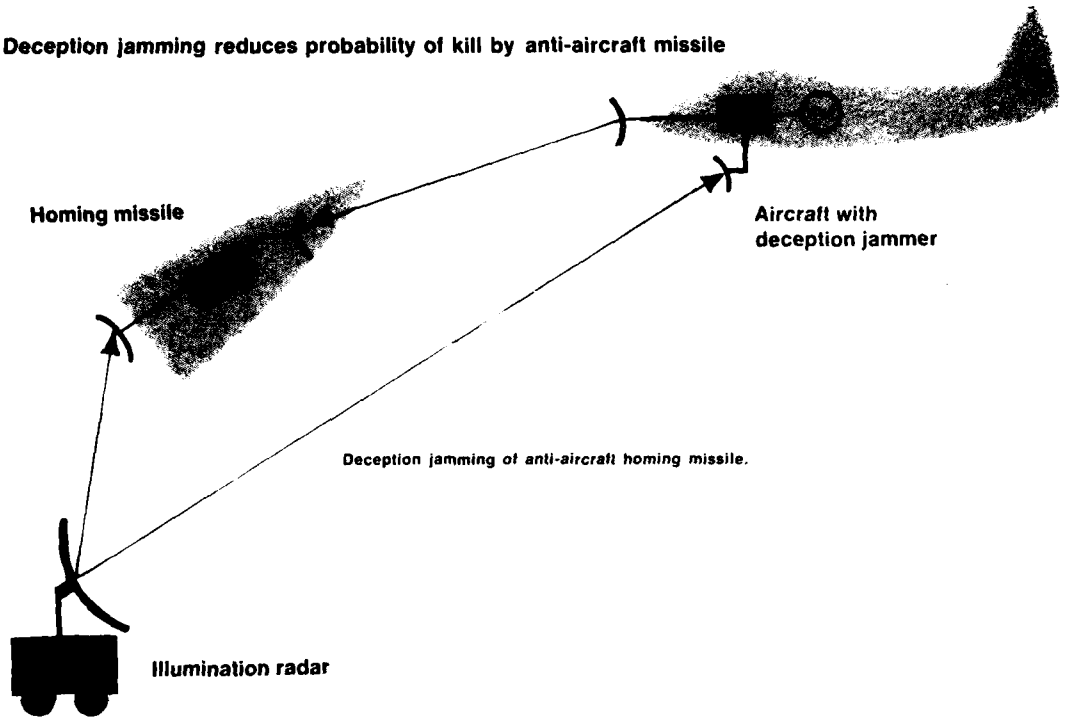
The efficiency of anti-radiation missiles against radar—i.e. the likelihood of destruction of the radar—is very highly dependent on the countermeasures taken, for example the use of decoy transmitters.

If no effective decoys are available for deception of the missile, the probability of destruction of the radar is high unless it is closed down during the attack.

◀ *Example of area of uncertainty.*



Deception jamming reduces probability of kill by anti-aircraft missile



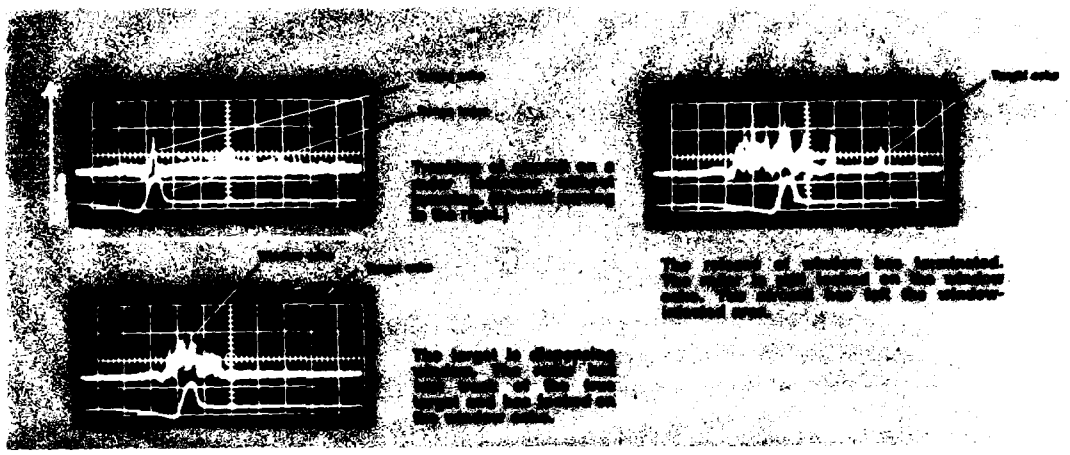
Deception jamming of anti-aircraft homing missile.

The probability of kill by surface-to-air missiles can be reduced by deceptive jamming.

A surface-to-air missile is normally aimed at the point ahead of the target where the hit is intended to take place, while the homing aerial is continually turned so that its radiation lobe rotates round an axis pointing at the target.

If the target sends jamming signals, amplitude-modulated at roughly the same frequency as the frequency of rotation of the homing aerial, this causes an error in the homing device. The homing aerial is deceived into rotating on an axis which no longer points exactly at the target. The lead is therefore wrongly predicted and the missile will miss the target by a more or less wide margin or, in the event of a very high degree of modulation, will entirely deviate from the proper course since the homing device is turned away altogether and can no longer follow the target.

Attack with air-to-ground antiradiation missile against surveillance radar.



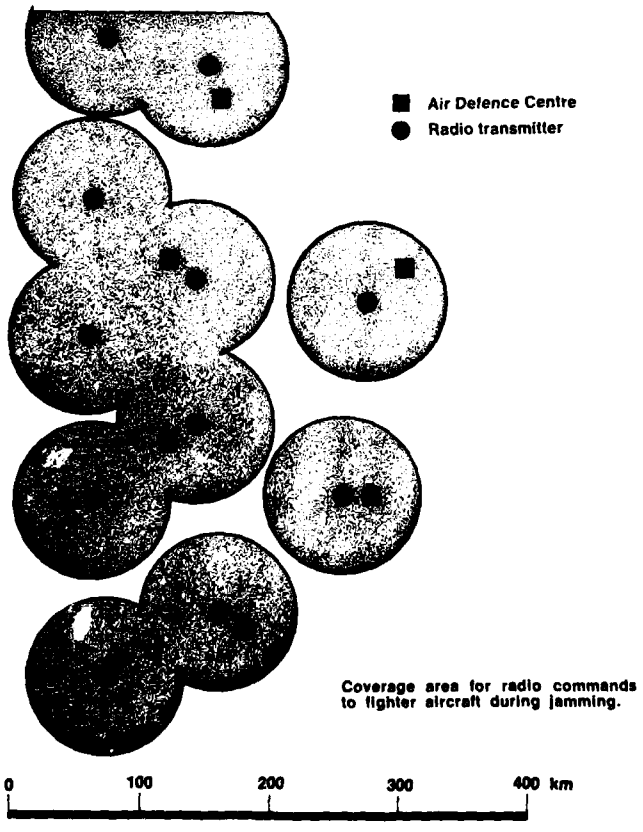
Jamming of strike aircraft fire control radar by window

In the absence of jamming it is easy for the radar to detect the target, lock on the echo and obtain continuous and accurate ranges.

If the target releases window, on the other hand, the radar will lose the target and lock on part of the window-infected area.

The probability of successful jamming depends on the characteristics of the radar, the quantity of window, the course of the target and other factors, but is high on any one occasion.

Jamming of communication between Air Defence Centre and fighter aircraft

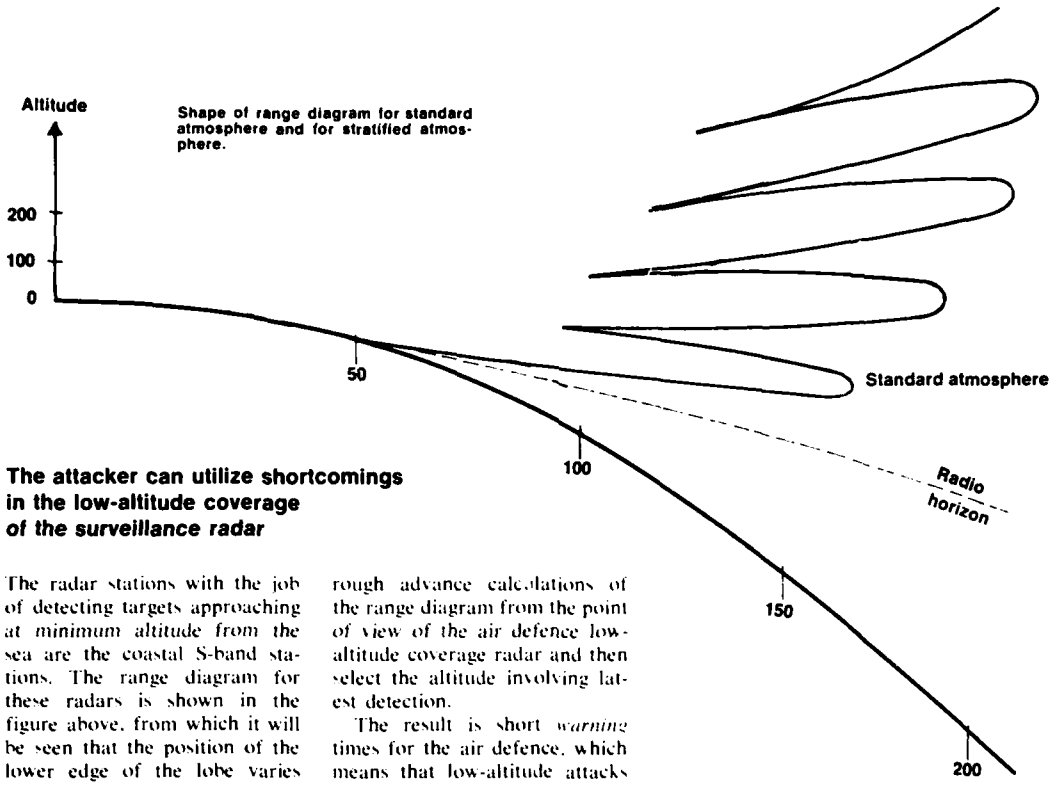


Coverage area for radio commands to fighter aircraft during jamming.

A's fighter aircraft are directed from the ground, by some form of voice communication by radio, to a point so close to the target—the enemy aircraft—that the pilot detects it on his radar or visually. For this purpose there are radio transmitters on the ground, so located as to provide complete coverage of the air space concerned.

If the enemy aircraft jams the radiocommunication, the area where the fighter pilot can receive orders from the command centre—and in which he can effectively engage the enemy—is reduced to the more or less immediate vicinity of the command radio transmitters.

In the illustration (left) the shaded areas are those within which the fighter pilot can distinctly hear radio commands. There is incomplete overlap and corridors exist where the attacker can fly-in without encountering fighter aircraft under control from the ground. These corridors are widened if any command radio transmitter is out of action.



Shape of range diagram for standard atmosphere and for stratified atmosphere.

The attacker can utilize shortcomings in the low-altitude coverage of the surveillance radar

The radar stations with the job of detecting targets approaching at *minimum altitude* from the sea are the coastal S-band stations. The range diagram for these radars is shown in the figure above, from which it will be seen that the position of the lower edge of the lobe varies greatly with the atmospheric situation.

In a *standard atmosphere*, as will be seen, the radar lobe does not follow the curvature of the earth. This means that targets approaching at an altitude of 100 m cannot be detected until they come within a range of about 75 km.

In a stratified atmosphere, which is fairly common in the summer months, the radio waves at a small angle of elevation are reflected back to the earth's surface and follow a duct. In these conditions targets approaching at minimum altitude can be detected at very long ranges. Above the duct, however, there is a very large "gap" in the radar lobe, which means that targets approaching at an altitude of 100 m cannot be detected until they come within a range of about 40 km.

With the aid of meteorological observations and, possibly, airborne refractometer measurements the attacker can make rough advance calculations of the range diagram from the point of view of the air defence low-altitude coverage radar and then select the altitude involving latest detection.

The result is short *warning* times for the air defence, which means that low-altitude attacks against targets in coastal areas cannot be intercepted.

The attacker can utilize the difficulties of fighter aircraft to pick up and track low-altitude targets on their radar

The defence fighter aircraft are here assumed to be equipped with fire control radar of ordinary pulsed type. This makes it difficult for them to engage targets employing low-altitude tactics.

If a fighter aircraft heads on a target flying at low altitude, the aerial lobe will also hit the ground or water surface below the target. The radar receiver will therefore pick up ground and water echoes in addition to the target echo, and under certain conditions the target may be completely concealed.

If air-to-air missiles are used, their radar homing device will be disturbed by ground and water echoes in the same way.

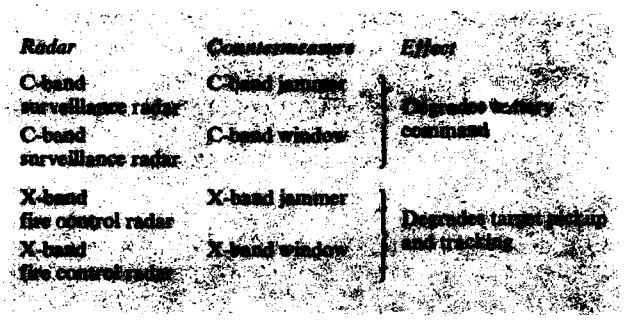
The maximum target altitude at which this form of interference occurs depends on the lobe width and pulse length of the radar and on the terrain, among other factors. The effectiveness of fighter defence is greatly reduced against attacking forces flying at altitudes below 300—500 m since neither radar nor missiles with radar homing head can be used under such circumstances.

The echo from the target aircraft is concealed by the ground echo when the aircraft is attacked at low altitude.

The effectiveness of A.A defence can be reduced by jamming

Several of the forms of jamming discussed in the previous sections are effective also against the A.A. artillery.

The rough effect of countermeasures which the attacker may be presumed to possess against the A.A. artillery are tabulated below.



Strike aircraft can carry jamming equipment only to a very limited extent owing to lack of space, and the attacker is therefore forced to make a choice among the conceivable alternatives.

One possibility is to procure various alternative countermeasures with the aim of changing jamming tactics during the war so as to make it more difficult for the defence to develop effective counter-countermeasures. Different countermeasures, of course, can also be allotted to different aircraft within a formation.

Means available to the air defence to jam the attacker's electronic equipment

In air attacks against ground targets of limited extent—bridges, harbours, certain military establishments—combat economy is greatly dependent on the possibility of precise navigation. Uncertainty concerning the aircraft's position at the moment of bomb release—and therefore concerning the point of impact of the bombs—must be compensated for by a larger quantity of bombs. This necessitates a greater risk of losses. In good visibility the location of a target is a comparatively simple problem, while in poor visibility navigational aids are required of an entirely different quality than, for example, the classic method of dead reckoning. If the distance to the target area is not too great (less than 400 km), radio navigation is a method which, at the stage of technical development today, allows location within a margin of error of 50—500 m. An alternative is inertial navigation, which, at present, however, is very much more expensive and is less accurate, with margins of error of 1—3 km. Another is bombing radar, which has high precision but can only be used against targets that can be clearly distinguished on the radar screen. The radar, however, by denying the attacker through its own signals.

Radio navigation systems are therefore very important aids against geodetically located targets—particularly if the attacker, owing to fighter opposition for example, is forced to attack in poor visibility or from a low altitude, at which visual location of the target is also difficult.

The defence can substantially reduce the effect of such attacks, however, by denying the attacker the advantages of radio navigation. This can be done by jamming, which may have the effect of impairing precision, entire saturation or deception, according to the power and character of the jamming equipment.

The following simplified example, together with the sketch on the next page, illustrates how such jamming may be organized and the effect it may have under favourable conditions.

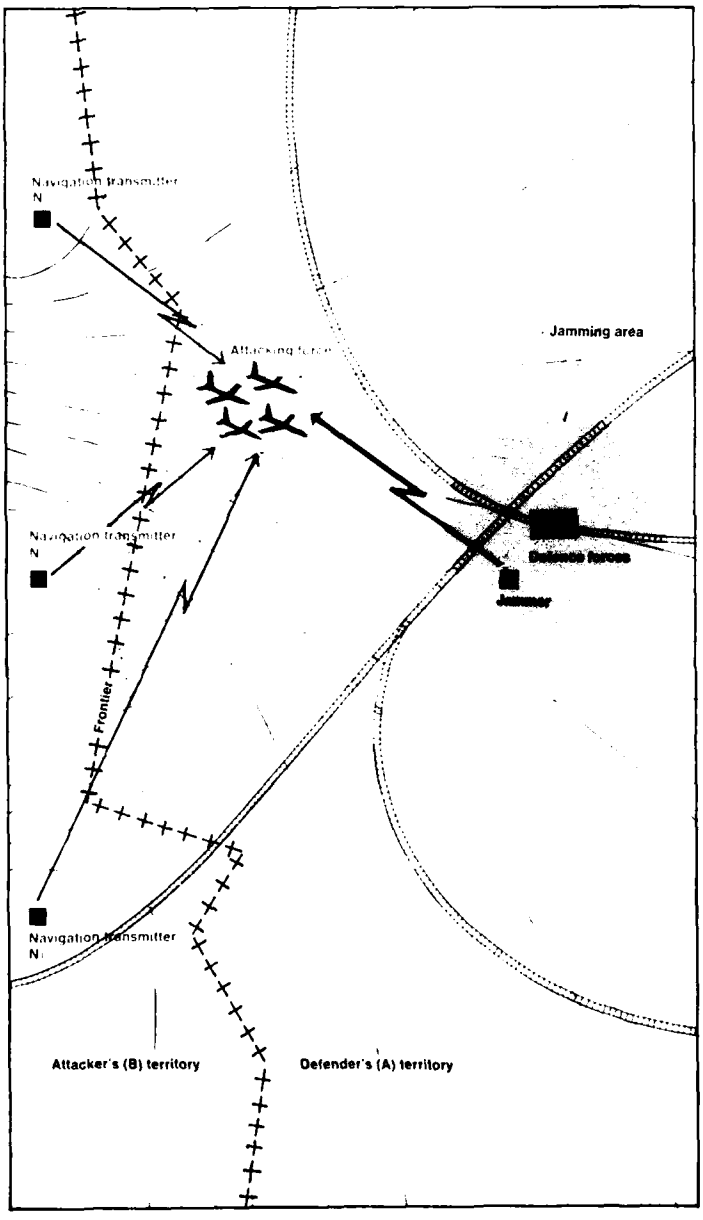
In the softening-up stage the attacker (B) aims to destroy a strategically important railway junction by air attack. B judges A's air defence to be so strong that he must make the attack at low altitude at nighttime in order to reduce his aircraft losses. He can do this by using his radio navigation system consisting of the three navigation transmitters N_1, N_2 and N_3; these generate a hyperbolic coordinate system which normally allows location in the target area with a probable error of about 200 m. B calculates that he must use ten bombers in order totally to destroy the marshalling yard with 90 per cent probability.

The defender knows that the navigation system exists and feels threatened by its potential precision. He has therefore prepared a number of jammers, the signals from which can prevent or interfere with the reception of the navigation signals within strategic areas.

The jammers are comparatively weak and their ranges are therefore rather restricted, but the existence of jammers will also be difficult to detect by monitoring from B's territory.

Nor are they used except when absolutely necessary.

When threatened with invasion, however, A starts up the jammer protecting the railway junction, with the result that the navigation indicators in the attacking aircraft are disturbed and cease to function at some distance from the target. The navigators must have recourse to dead reckoning during the last 50 km or so. If it is their first encounter with the phenomenon, some of them may wait so long before going over to dead reckoning that they badly miss the target. More experienced personnel make the best of the situation, and the spread in the target area may then be increased to about 2.5 km. This greatly reduces the effect of the attack and in all probability the marshalling yard will not be rendered unusable. Thus, in the short run, the jamming has had the same result as a fighter or A.A. action with very high neutralizing effect.



To attain his goal, B must make a renewed attack, this time with better stand-by navigation precision, e.g. using advanced inertial navigation apparatus with which the error over the same distance will be perhaps 500 m. For the same effect on the target a considerably larger number of planes are then required, and more expensively equipped, than the ten which took part in the first attack. An alternative is a daylight attack with visual target location and visual bombing, which involves the risk of heavy losses from fighters and A.A. unless B has air supremacy. As a third alternative B can play about with the signal frequencies and transmitter powers of the navigation system in order to avoid jamming. A's jamming organization must in such case have effective signal interception and transmitter flexibility for rapid adjustment of the jamming to B's countermeasures.

In conclusion, therefore, it may be said that, through their precision, radio navigation systems permit a very high efficiency of air attack within certain range limits. The defence can in such case appreciably reduce the effectiveness of attack by suitable jamming and compel the attacker to adopt more costly measures for a given result. Jamming may be interfered with by changes of frequency and other antijamming measures, which calls for a great flexibility in the jamming organization. In many situations an effective jamming organization, as auxiliary to air defence, can give a high yield in relation to its procurement and running costs.

The attacker's (B) evaluation of his penetration aids and choice of strategy

From the preceding sections it will be apparent that the attacker has a very wide range of aids and methods for penetrating the defences. The problem is to decide *which* to use and *how* to mix and combine them with other measures in order to achieve the desired end in the most effective way.

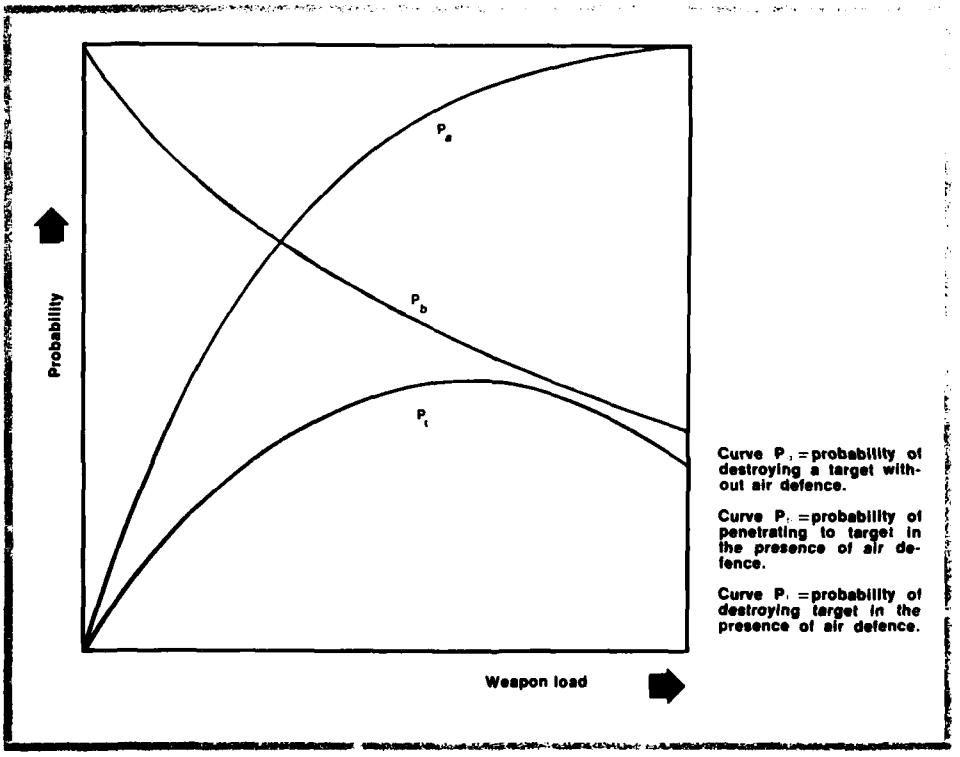
Certain combinations are fairly obvious, e.g. the combination of attack and jamming against the air defence's surveillance radar system. This combination is effective because it is very difficult for an air defence to procure radar stations which are both mobile (and therefore difficult to destroy) and resistant to jamming.

If the attacker knew the disposition of the defence in detail, and also the efficiency of his penetration aids, the problem would be fairly simple. But this is not the case. The defence capacity is not definitely known. It is especially difficult for the attacker to know the disposition and effect of the special electronic counter-countermeasures that may exist. The effect of the penetration aids is thus to some extent unknown. The evaluation is also complicated by the fact that the aircraft weapon load, and also the number of weapon-carrying aircraft, must be reduced in proportion to the use of penetration aids.

To get to grips with this situation it is necessary for the attacker, when planning a mission, to make extensive studies on the basis of various sets of assumptions concerning the target characteristics, the efficiency of different components of the air defence, and the effect of the attacking weapons and penetration aids.

The rising curve P_a (in the figure below) represents the probability of knocking-out a target in the absence of air defence.

Curve P_b represents the probability of penetrating to a target despite air defence. This is a falling curve: the smaller the complement of penetration aids, the greater the quantity of weapons that can be carried, but the



less, too, is the probability of successful penetration of the air defence.

The product of these two curves yields the third curve P_t, the probability of knocking out the target in the presence of air defence.

The number of critical parameters is very great, and the study is complicated by the number of parameter values that must be varied. But an estimate can be made of the probability of penetration for a given set of penetration aids. The attacker has thereby come a step further and obtained a valuable basis for his choice of strategy.

No actual study has been made for the present example and, therefore, one can only have an intuitive idea of what might be an effective strategy for the attacker.

One possible estimation might give priority to the following measures:

before the outbreak of war to concentrate *electronic* and other *military intelligence* on locating the air defence P-band surveillance radar and S-band low-altitude surveillance radar,

in conjunction with the outbreak of war and in the immediately following period to *destroy* the air defence P-band surveillance radar and S-band low-altitude surveillance radar,

to protect bombing missions by *barrage jamming* of surveillance radar on the L and S bands, by *jamming* of fighter command radiocommunication and by *dropping of window* (L-, C-, X-band),

to protect strike aircraft by dropping of window (X-band),

to engage A.A. missile units with *anti-radiation missiles* (L-band),

after the outbreak of war to concentrate *electronic intelligence* on checking the effectiveness of combating P-band surveillance radar and S-band low-altitude surveillance radar.

It appears, however, as though various other alternatives might be equally effective: the attacker should perhaps refrain from measures against the air defence surveillance radar and use the corresponding combat power for attacking fighter aircraft at their bases, concentrating electronic intelligence perhaps on locating the A.A. missile units, etc.

Decision facing the defence, and possible countermeasures

The decisions open to the defence are essentially limited by its inherently defensive character.

The attacker has the initiative in all respects and can plan his attacks on the basis of fairly complete information concerning the air defence and its weak points, while himself being able to a large extent to keep secret even the main features of his plan.

The defence cannot know what parts of the air defence the attacker intends to attack with weapons, what types of radar stations will be engaged with anti-radiation missiles, what jamming methods may be used, and so on.

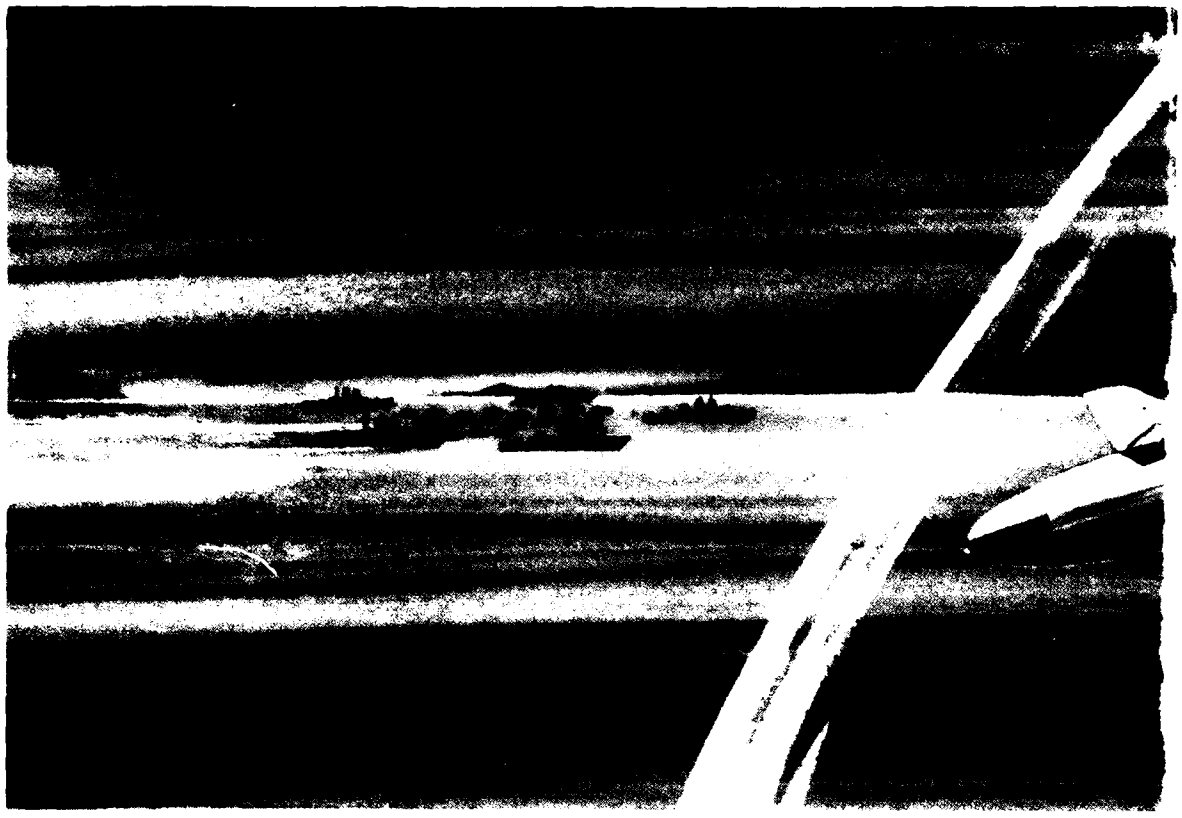
The planning of the use of the existing air defence organization and the longer-term planning for improved systems must therefore be based on alternatives, so that the air defence will be *equally* effective whatever the form of attack.

The defender realizes that, if he leaves any gap in his defences, the attacker can get to know of and exploit it. The defender must therefore guard against all alternatives.

The counter-countermeasures which the defender can take against the attacker's countermeasures are *tactical* in the form of restrictive transmission from certain radar stations, shutting-down of radar stations under the threat of attack by antiradiation missiles, variation of frequency, regrouping or the like, and of *longer-term measures* such as modifications and new procurements of equipment.

In conjunction with the weak points discussed, the following examples of long-term measures may be noted:

Weak point	*Action*
Surveillance radar vulnerable to self-protective jamming.	Establishment of a passive direction-finding system (jamming aircraft located by taking cross bearings on their jamming signals).
Fixes radars easy to attack with weapons, as they can be located even in peacetime.	Addition of a set of mobile, e.g. airborne, surveillance radars.
Difficulty of attacking low-altitude targets with fire control radar on account of ground and sea clutter.	New radar of doppler type which allows suppression of ground echoes.
A.A. missile system susceptible to deception of homing device.	Introduction of ECCM in homing device. Procurement of alternative guidance systems which cannot be jammed by the same means.



Invasion over the sea is one of the forms of aggression which every sea-girt country must consider when trying to achieve a well-balanced defence.

The defence of and attack against an invading naval force offers excellent examples of electronic warfare and illustrates the tactical considerations which must be made on both sides in view of the increasingly important role of electronics in modern warfare.

Out at sea an invasion fleet can be fought with a number of weapons: submarines, coastal and naval missiles, and strike aircraft with different armaments. Nearer the home coast other weapons may be used: mines, coastal and naval artillery, short-range missile systems. The invading force naturally seeks to build up a defense system that is effective against all forms of weapons, but obviously attaches more importance to those which are judged to constitute the most serious threat.

How, then, is an invader likely to reason when attempting to gain optimum protection against a particular weapons system? And, viewing the situation from the side which is going to fight the invasion fleet, what can be done to reduce the effect of the invader's protective measures? A number of steps in the long sequence of reasoning leading up to the final choice of defence system must naturally be omitted in a short study, but the main factors involved might nevertheless be illustrated.

The strategic and tactical considerations underlying the broad plan for the invasion may be disregarded. It may be assumed that the targets to be protected are grouped in a number of separate and identical configurations or convoys. Each convoy is assumed to consist of a large number of identical vessels. To simplify the calculations in the example to be presented below, one may assume that each convoy is of circular form.

For the main protection of each convoy against air attack there are a number of destroyers equipped with A.A. missiles. Since the convoy is gathered within a circular area, the guided missile-armed destroyers are grouped in a circle (see drawing above).

The main weapon for engaging the convoys is assumed to be strike aircraft equipped with air-to-surface missiles. The invader is assumed to have cognizance of this. The missiles have a given

range and, after being launched, are guided to the target by an active radar homing device. This means that the strike aircraft can return as soon as they have launched their missiles.

The contest to be fought may be divided into a series of duels, of which three will be studied. The first is a range duel, the main factors in which are the ranges of the air-to-surface missiles and A.A. missiles, and the ranges of their respective radar equipment. In the second duel a study will be made of how jamming of the A.A. missile system by the strike aircraft affects their chances of survival. The third duel concerns the jamming of the homing devices in the air-to-surface missiles. This study also shows how a given number of jammers should be grouped for optimum protection.

The range duel

It is here assumed that the range of the air-to-surface missiles is fixed and cannot be changed, but that the opposing side does not know their range with absolute certainty. Since these missiles are assumed to constitute the main threat it is natural that the invader tries to group the destroyers at a distance from the convoy which gives the maximum A.A. missile effect against the strike aircraft, from whichever direction the attack comes. This latter condition suggests a symmetrical grouping of the destroyers. The grouping must, however, not be so critical as to yield a considerably inferior effect if the range of the air-to-surface missiles is not exactly that which is judged to be most probable.

An A.A. missile unit has a given effective intercept zone within which its missiles can hit a target. The outer limit of the intercept zone is affected by several factors; in this study, however, we shall assume the only limiting factor to be the range of the missile engine, the outer limit thus being a circle. Adjoining the A.A. missile unit is a dead zone, where one cannot count on a hit as the missile cannot be guided during its acceleration phase. The dead zone may often be approximated to a circle.

It is often impossible to utilize the outer part of the intercept zone owing to the detection range being too short or the system's reaction time, in relation to the speed of the targets, being too long. As a rule, moreover, certain firing restrictions

are imposed by the locations of one's own units. In general, of course, the longer a target remains within the intercept zone of an A.A. missile unit, the more shots the unit can fire with a prospect of hitting the target. In this case the targets consist of strike aircraft which turn back at a given distance from the convoy. An A.A. missile unit which gets a target within its intercept zone, therefore, should achieve the greatest effect if located at a distance from the convoy equal to the distance at which the aircraft turn about, as firing in the rear 180 -sector, where its own ships are, would be impermissible. With a given number of destroyers, on the other hand, a larger number of units should be able to engage a target if the destroyers are grouped close together, as the intercept zones then overlap. Which of these two alternatives should be adopted can hardly be decided on general grounds.

In the example given below, the situation has been analysed quantitatively. The measure of the destroyers' A.A. missile effectiveness has been taken as the number of missiles fired with prospect of hitting a target. The number of prespective hits (engagements) is calculated under given conditions. This number is denoted E.

Assuming ideal operations control, so that perfect target allocation is achieved and no double engagements occur, the *number of shot-down aircraft* will be

$$L = E \cdot p_0$$

where p_0 is the probability of hit by A.A. missiles under unjammed conditions.

In the example E is found to be 6. If p_0 is taken as 0.7, the losses will be 4.2 aircraft. As 8 aircraft are assumed to be used in each attack, only 3.8 aircraft would survive the attack. This corresponds to a survival probability of 0.48, altogether too low a figure to be acceptable. Measures to increase the probability

BATTLE EXAMPLE

This example will present the results of calculations of the number of prospective A.A. missile hits under given assumptions. The A.A. missile system is assumed to have the following data.

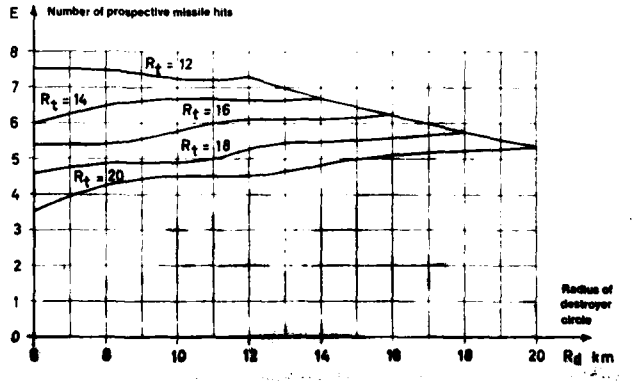
Max. range 25 km.
Min. range (dead zone) 3 km.
Average velocity 600 m sec.
Time delay from detection to first launching 20 sec.
Time delay from intercept to next launching 10 sec.
Surveillance radar range 40 km.

The missiles are of semi-active homing type and travel on an ideal straight path to the calculated point of impact. Every guided-missile-armed destroyer has been allotted a firing sector limited by the bearings to its neighbouring destroyers. One round consists of one A.A. missile.

The attacks on the convoy are made on a squadron basis, i.e. with 8 aircraft. The squadron is divided into four pairs, but these are so closely grouped that the longitudinal and lateral dispersion of the squadron may be disregarded. The aircraft fly at 300 m sec.

The range of the air-to-surface missiles is such that the launching aircraft can turn at a distance of 16 km from the centre of the convoy. This distance is denoted R_t. After the aircraft have turned, no A.A. missile is assumed to be able to obtain a hit.

The number of destroyers is of no concern for the purpose of the study and will be taken as 6. By fairly simple methods one can now calculate the number of prospective hits by A.A. missiles as function of the distance of the destroyers from the centre of the convoy. This distance is the radius of the destroyer circle and is denoted R_d. The exact position of each destroyer is not known to the attacking aircraft, and we must therefore make calculations for a number of alternative and equally probable directions of surface-to-air missile attack. By then forming a



of survival must therefore be taken. One such measure is to operate with larger formations, but this will not be discussed here. Another is to jam the A.A. missile system. The duel between the jammers in the strike aircraft and the A.A. missile system will be studied in the following section.

A.A. missile-jammer duel

An A.A. missile system of the kind described is for its proper function dependent on a number of electronic systems, which are more or less susceptible to different kinds of jamming. The first electronic systems to come into operation are the surveillance radars. Jamming of these delays and may even prevent detection of the attack, which, of course, limits the number of A.A. missile engagements and so reduces the losses.

The surveillance radar stations can be jammed in many different ways, some of which will be described below. One of the more obvious methods—the effect of which can be reasonably well predicted—is barrage jamming, e.g. with wide-band noise. This "drowns" the aircraft echoes in the jammed sectors on the radar indicators.

This method of jamming, however, involves certain difficulties and risks. A modern naval vessel is usually equipped with more than one surveillance system, and they generally work within different frequency bands. A considerable amount of jamming equipment is therefore needed to cater for all systems. The radar stations may also be equipped with auxiliary apparatus which determines the bearings of the jammers. By combining the bearings measured from different jammed radars, the locations of the jammers can be determined with sufficient accuracy to direct fire control and illumination radars onto them. If the jammers are carried by aircraft in the attacking force, there is clearly a great risk of their being engaged.

If the jamming comes from special jamming aircraft, which, for example, may fly-in behind the attacking force (stand-off jamming), the attacking force may perhaps go in unscathed. If the jamming aircraft keep outside the range of the A.A. missiles, they, too, can operate in safety. An analysis of this case, however, shows, that very great tactical difficulties arise in the coordination of jamming and attack operations.

In view of the large distances effective jamming of a particular surveillance radar can be counted on only when its aerial lobe bears upon the jammer. This is a very serious limitation, as a strike aircraft is sure to escape detection by a surveillance radar only when it is within a sector around the radar-jammer bearing, the width of which is equal to the radar aerial lobe, i.e. of an order of 2—10°. Since the guided-missile-armed destroyers are spread over a fairly wide area, not only must there be a large number of jammers but their locations must be successively adjusted as the strike aircraft approach the destroyers if detection is to be effectively prevented. There are other electronic systems which can be jammed by other methods which are very much less exacting both tactically and in respect of the quantity of jamming equipment. It is natural, therefore, that the choice should fall primarily on such methods.

The illuminating radar of a semiactive homing A.A. missile system could also be jammed in several ways. Pure barrage jamming of the illuminating radar, of course, affects the homing device as well, as the latter normally operates on illuminating radar signals reflected from the target. A modern homing device is often designed to switch over to passive tracking and home on the jamming signals. Clearly, therefore, barrage jamming of illuminating radar from the strike aircraft cannot be considered to afford protection. Stand-off jamming is also conceivable in this case, but the tactical requirements on the jamming aircraft are even greater than for jamming of surveillance radar, since an illumination radar has a narrower aerial lobe than a surveillance radar.

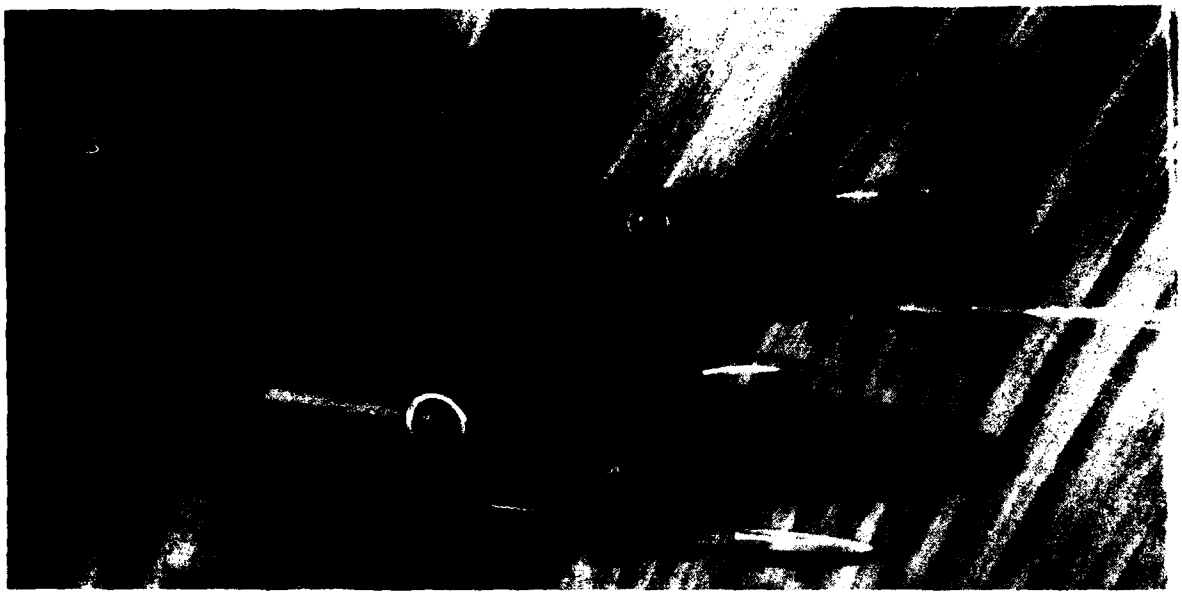
Both illumination radars and homing devices can be opposed by different forms of deceptive jamming. These are usually very effective and require only a moderate quantity of jamming apparatus, one reason being that it is hardly necessary to counter more than one kind of A.A. missile system. Deceptive jamming

---

mean value over all directions, the *anticipated* number of hits is obtained for attack on the convoy from an arbitrary direction.

As the opposing side does not exactly know the range of the air-to-surface missiles, which is what determines the turning distance, the calculation procedure must be repeated for turning distances of 12, 14, 18 and 20 km. The results of the calculations are presented diagrammatically (below left), where the number of A.A. missile hits (E) is plotted as function of the radius of the destroyer circle (R_d) with turning distance (R_t) as parameter.

It will be seen that the maximum number of hits is obtained if R_d is equal to R_t (exception $R_t = 12$). If the invader is absolutely sure that $R_t = 16$ km, he chooses $R_d = 16$ km. He cannot be 100 per cent sure, however, and so must adopt some kind of risk criterion in the selection of R_d. In this case $R_t = 16$ km and one sees that the number of A.A. missile hits is roughly the same if R_d is somewhere in the interval 12—15 km, where E is very close to 6.

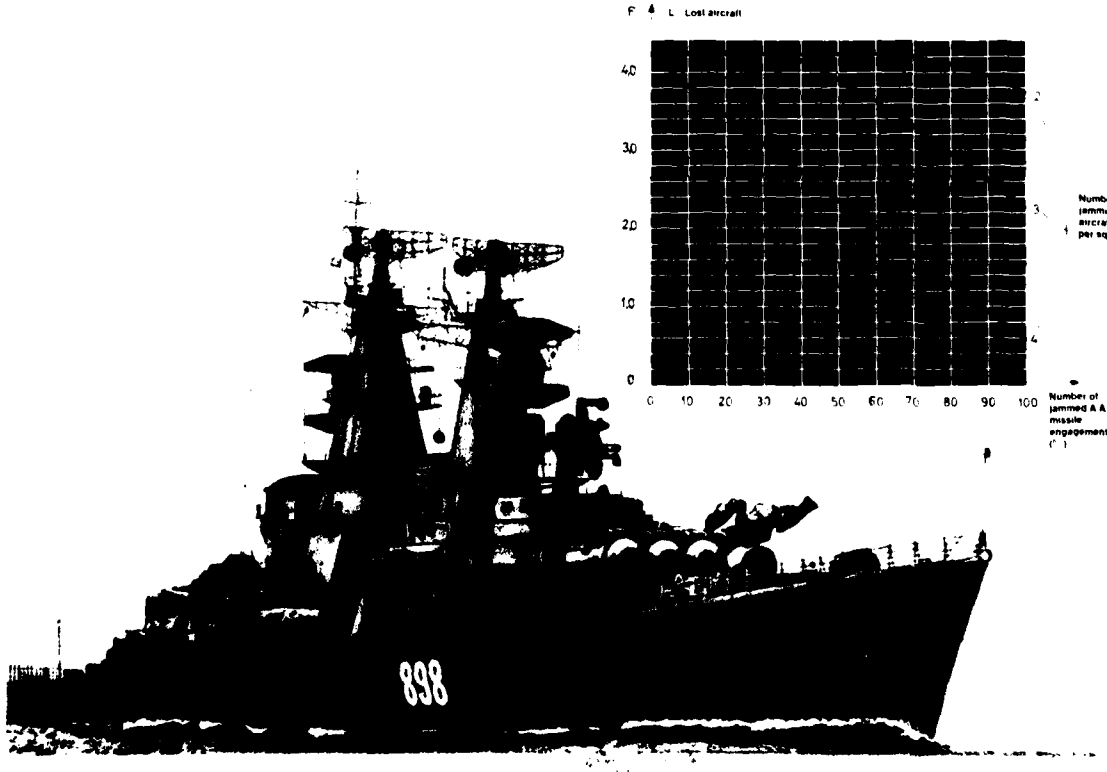


The Swedish strike aircraft A 32 Lansen in twin formation. Each plan carries two air-to-surface missiles type RB 04.

can be done in many ways, but the characteristic feature of this form of jamming is that the jamming signals resemble the true echo signals but are distorted so that the radar is given false information in some important respect. The most common forms are range deception, angular deception and speed deception.

The main effect of deceptive jamming is reduction of aircraft losses, which means that a larger number of air-to-surface missiles can be launched.

Factors affecting the effect of jamming are the tactics adopted by the attacking aircraft, the

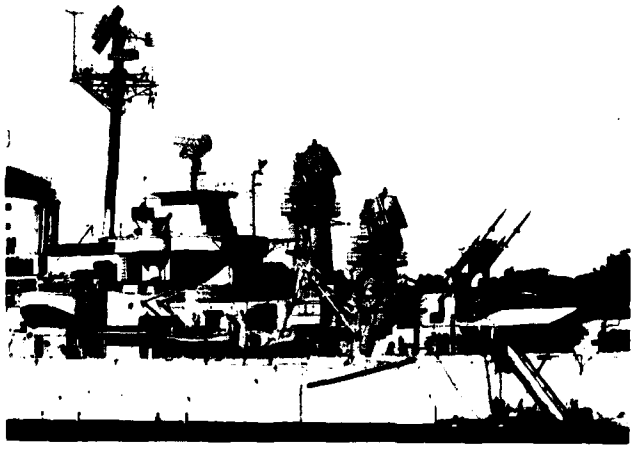


number of aircraft carrying jammers, and the jammer performance, e.g. output power and aerial system. The diagram (left) shows how the losses of aircraft in a particular case depend on the number of jammer-carrying aircraft and on the effectiveness of the jammers. This can be measured in percentage of A.A. missile launchings which can be jammed.

This second study has shown that ECM can reduce losses and increase the number of air-to-surface missile launchings. The next study will illustrate what the invading force can do about the air-to-surface missiles which, after being launched, are on their way towards the convoy with their homing devices in operation.

Duel between air-to-surface missiles and jammers

What can the invading force do to guard against the air-to-surface missiles? The A.A. guns on some landing craft or on other



The United States and the Soviet Union both possess several types of A.A. missile equipped ships. (Left) A Soviet guided-missile armed destroyer of Kynda class, (right) the U.S. light cruiser Galveston with Terrier surface-to-air missile system.

vessels in the convoy, e.g. minesweepers or submarine chasers, will shoot down some of the missiles. An air-to-surface missile is a small target, however, and is not so easy to hit, especially at low altitude. Other protective measures must be taken, therefore, apart from pure firepower. One effective method is to jam the missile homing device.

These homing devices—like those in A.A. missiles—can be jammed in many different ways, which will not be discussed here. We consider, instead, that the invading force has decided to employ barrage jamming to prevent the homing missiles from locking on target. As the convoy configuration is circular and an attack may be expected from any direction, it is natural that the jammers, too, should be grouped in a circle.

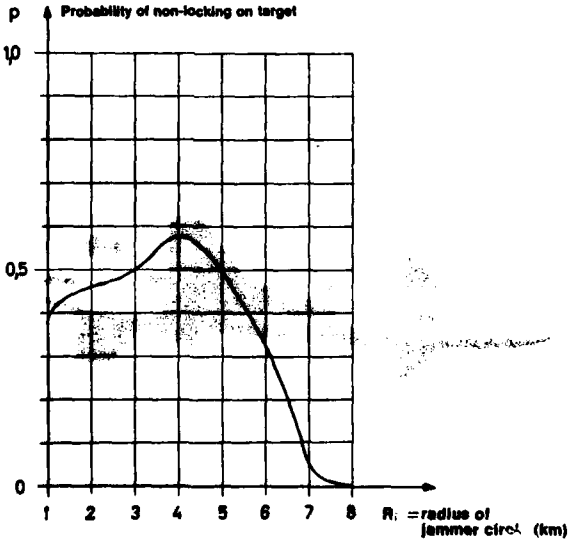
The invading force cannot know exactly the characteristics of the air-to-surface missile and must therefore be very careful in the choice of carriers for the jammers. Whether a homing device can be switched over to passive tracking of jammers is practically impossible to discover by electronic intelligence. The invader must consider this possibility and should therefore avoid placing jammers in the landing craft. Otherwise the jammers might attract air-to-surface missiles and prove a greater hazard to the carrier vessel than if it contained no jammer. The number of jammers, moreover, would be quickly decimated. One alternative is to place the jammers in special vessels so constructed that they do not trigger-off the proximity fuzes of the air-to-surface missiles. This would involve practical difficulties, which, however, will not be discussed here; instead we simply assume that the jammers are not silenced by the missiles.

This reasoning shows how the invader is forced into adopting measures which have both operative consequences and may involve an economic sacrifice owing to his lack of knowledge of the characteristics of the homing device.

The factors determining the effectiveness of jamming in this case are the performance of the homing device and the characteristics and geometrical arrangement of the jammers. For given characteristics of homing device and jammer the positioning of a given number of jammers can be found which ensures the greatest jamming efficiency. The efficiency may be measured, for example, in terms of the probability of preventing a homing device from locking on target irrespective of the direction of attack.

The diagram below shows the result of a calculation with fictive homing devices and jammers. The object is to illustrate that there is an optimal length of radius (R_j) of the circle along which the jammers are assumed to be grouped.

There are several other elements in the sketched situation, each of which can—and often must—be subjected to detailed study and optimization analysis. The intention here has been merely to give examples of duels which may arise in complicated battle situations, and to show that electronic warfare can be studied by the same methods as other forms of warfare.



This diagram shows how it is possible to find the optimal radius of the circle on which the jammers are placed.

Tele-communication Systems in Land Warfare

On the short-wave band space wave propagation via the ionosphere can provide a large range, but there is a severe congestion of stations on the frequency scale.

In land warfare electronics is used, among other purposes, for *communication*, *reconnaissance* and *location*.

Communication

—the transmission of orders, reports etc.—can take place by wire or radio. In quickly changing situations there is often no time to establish wire communication, and a wire network may also be damaged by enemy action. Radio communication is therefore vital. The threat of atomic weapons necessitates wide dispersion and mobility of units and places great demands on the range of radio stations.

Several frequency bands are used for radiocommunications (p. 17). Thanks to ionospheric reflection *short wave* can be used over long distances, e.g. for communication between Staff H.Q.s. Communication may be by teleprinter, telegraphy, telephony or video transmission.

With small heights of aerial the *lower VHF band* is usable over short distances (generally not more than 20 km or so) and is employed between small units. Communication is usually by telephony.

Higher frequencies are used for communication over radio links which, with suitably placed directional aerials, can cover shorter or longer distances in one or more hops.

Radio link communication is used chiefly between higher staffs and may be by teleprinter, telephony or video transmission.

Good communication becomes increasingly important with greater mobility and dispersion of units.

Small radio stations operating on the VHF band are used by small units, e.g. for battle command or fire control.

A radio link can be used over long distances and in broken country and can transmit large quantities of information.

Interception and jamming of radio communication

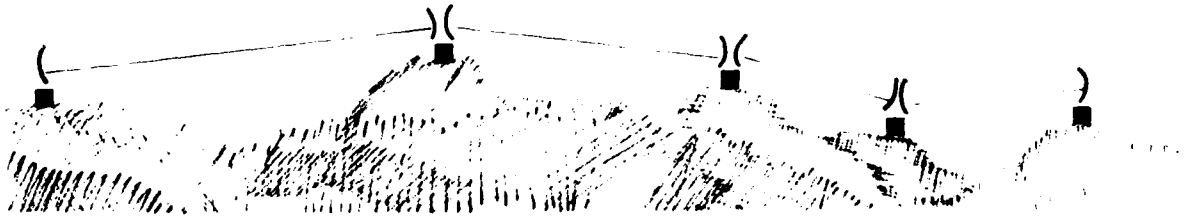
can be done in different ways according to the wave propagation and the tactical situation.

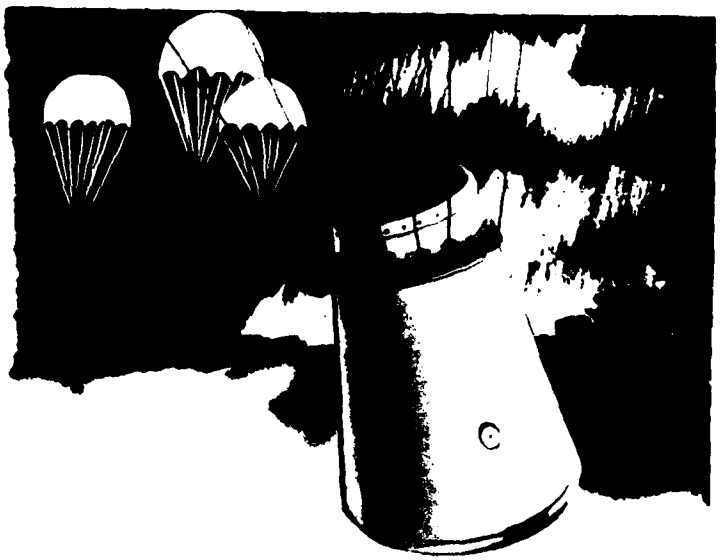
At a conquered bridgehead, for example, mobile stations can be established for signal interception and jamming. Small portable direction finders can be used by commando units for making their way to staff headquarters or other locations equipped with transmitters, and light jammers can be dropped in large numbers by parachute around radio communication centres.

On the short wave band the attacker can use ionospheric reflection and operate from ground stations in his own territory. From these he can both intercept and jam the defence's short wave communications.

On the VHF band and at higher frequencies much can be gained in signal strength if the

"Hidden transmitter hunt"—with portable DF receivers—is in many countries a sport with direct military associations. The picture shows an American DF receiver.





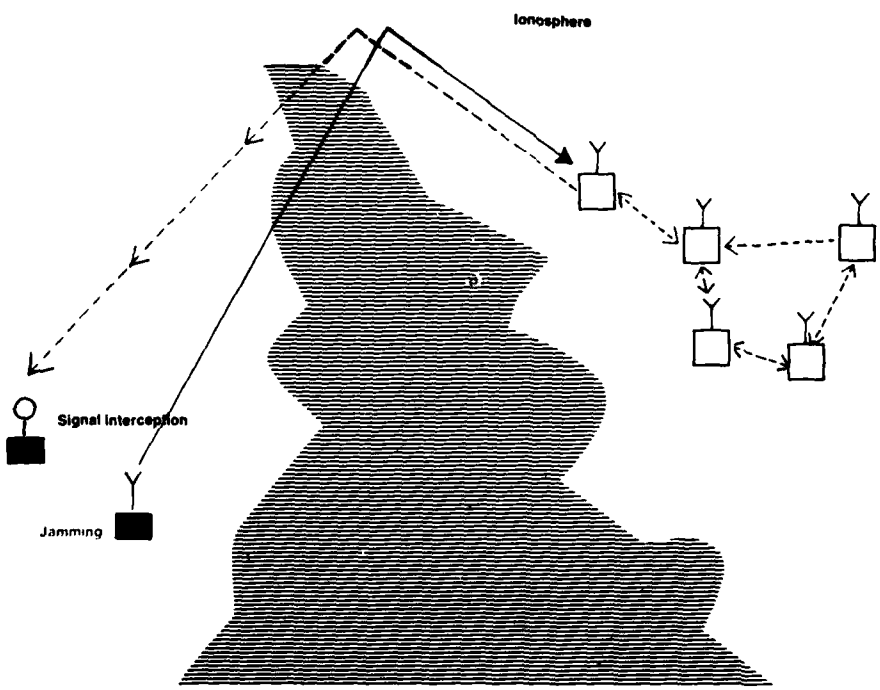
The development of semiconductor components and integrated circuits favours a mass effort with, perhaps, first-sized jammers against radio communication centres and staff headquarters.

ground wave attenuation can be reduced by procuring a reasonably free line of sight to the transmitter.

This can sometimes be achieved by placing the signal interception or jamming station on a hill or mounting the aerial on a high mast. Very great advantages can be gained through the wave propagation on these bands if the apparatus is placed, for example, in a helicopter circling at a suitable altitude.

In operating against radio links there is the added problem that the link stations use directional aerials. At least for jamming, therefore, one must usually make sure that the jamming signal enters the main lobe of the link aerial.

On the short-wave band signal interception and jamming via ionospheric reflection can be effected over large distances. But the same wave propagation conditions also involve a great risk of conflicts with one's own short-wave communications at other places.



For jamming on the VHF band it is of great value to operate from a fair height so as to diminish the ground wave attenuation, in which case a small-power jammer will often suffice. Anchored, electrically driven helicopters have lately been developed for several purposes, e.g. carrying of aerials or complete jamming equipments.

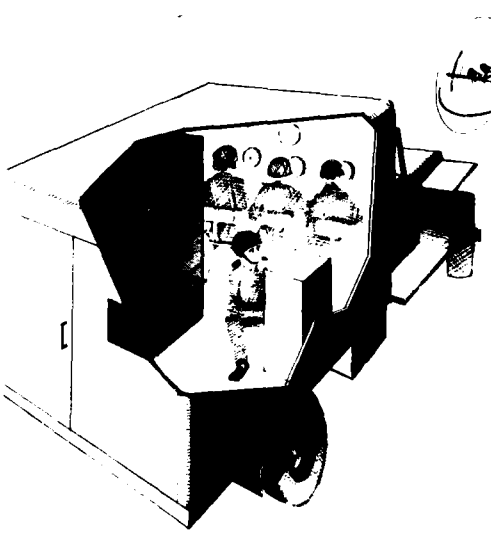
Interception of radiocommunication may serve three purposes, viz.

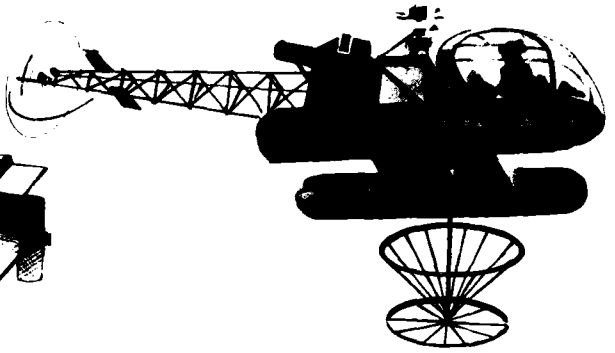
- Interception of orders or reports for the sake of the information they contain.
- Direction-finding for location of transmitters, and so often of staffs or units.
- Frequency identification for jamming operations.

As already noted, jamming

For jamming of a radio link the jammer must generally be in the main lobe of at least one of the link aerials and preferably of the line of connection between the stations. This may cause difficult technical and tactical problems. Interception of radio link signals can, on the other hand, sometimes be done also in the side lobes of the aerials.

For narrow-band jamming on a frequency band used by both parties, a signal analysis equipment and skilled operators are usually required. Ground-based jammers must generally have a high power output.





For jamming of parts of the VHF band used solely by the enemy in a given area, use can be made of automatic narrow-band, wide-band or repeater apparatus. This may be of "black box" type suspended under a helicopter, which has the advantage of reduced ground wave attenuation.

can be done from ground stations or aircraft. Narrow-band, wide-band or repeater jamming may be used according to need and the facilities possessed.

Narrow-band jamming may be advisable on short wave or when the home forces' and enemy traffic channels are mixed within the same band. Wide-band or repeater jamming may be adopted, for example, in the VHF range when, at least temporarily, the enemy alone is forced to use the band in a particular area.

Ground-based jammer stations usually require high outputs, while airborne jammers on the VHF band can generally operate at low powers. The apparatus may be manually or automatically operated.

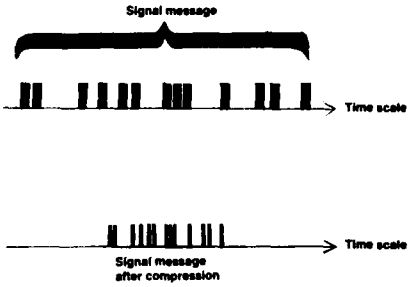
The development of semiconductor components, integrated circuits etc. favours automatic types of equipment, such as airborne jammers—also small inexpensive jammers for mass use around staff headquarters etc.

Counteraction of signal interception

If messages are coded, the enemy has greater difficulty in interpreting intercepted signals, and the time delay may prevent use of the information gathered.

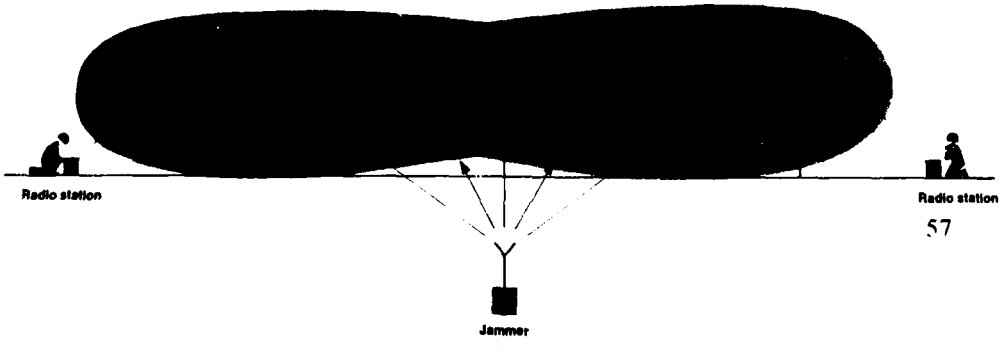
If a message is stored in a suitable way and then transmitted very rapidly, the risk of discovery is reduced.

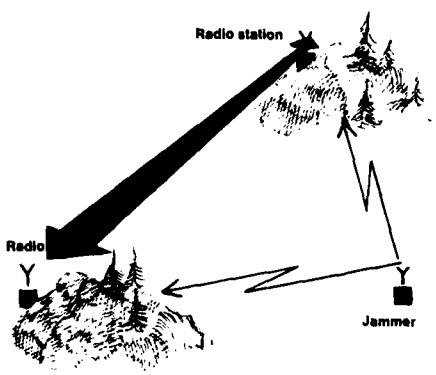
Good radio discipline precludes unnecessary leakage of information and cuts down the transmission time, thus reducing the possibility of interception and jamming.



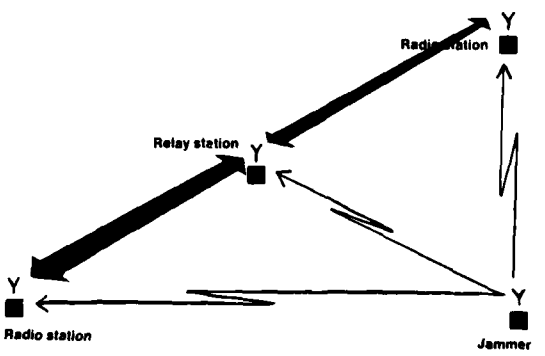
High-speed transmission reduces the risk of interception and protects against many types of jamming. A message of some seconds in length can be compressed to a few hundredths of a second.

The effect of jamming can be reduced by using directional aerials. The aerial gain in the main lobes increases the traffic signal, while the jamming is attenuated in the side lobes. Signal interception is also more difficult in the latter.





On the VHF band and at higher frequencies one can attempt to utilize the terrain to reduce the effect of jamming.



By installing a relay station one can reduce the distance between communicating stations, increase the strength of the traffic signal and so the resistance to jamming.

The effect of jamming can be reduced

The ability of a radio transmitter to override jamming can be increased by suitable choice of the type of radio signal, by raising the power and by the use of a directional aerial.

The radio receiver can be equipped with an aerial which attenuates signals from certain bearings.

By rapid changes of channel certain types of jamming can be avoided at least for short periods.

An appropriate location of the station can often reduce the effect of jamming. As regards the VHF band and higher frequencies, for example, the station can be placed close to a hill which shields it against the jammer but not against the communicating station. Sometimes, too, the distance between communicating stations can be reduced by means of intermediate (relay) stations, so rendering the traffic less sensitive to jamming.

Problems of communication jamming

Signal interception and jamming of radio communications cannot generally be conducted simultaneously. Not only does the flow of information cease if the jamming is effective, but often the jamming masks the radio signal in the interception receiver as well.

If both contestants use the same frequency band and the traffic channels are mixed or even identical, this must naturally be taken into account so that the jamming signals do not prevent important communications of one's own.

On the short wave band ionospheric reflection can make a jamming signal effective at altogether different places from those intended. On the VHF band and at higher frequencies the range of the jammer is quite effectively limited by the "radio horizon"; it is therefore possible within a limited area to jam certain channels or frequency bands which in another area are used for one's own communications. At high frequencies (generally those used on radio links) efficient directional aerials can be used for jamming. This has the advantage of a strong jamming signal in the aerial lobe and of reduced risk of jamming of one's own communications, even if they use the same channels or frequency bands.

In every tactical situation the use of jamming involves the following decisions:

- Should interception or jamming of radio communication be adopted?
- Will one's own vital communications be injured by one's own jamming?

Often the decision is an easy one. Communications between higher staffs are frequently of such a nature that the delay—of an order of hours—caused by the jamming is of no great significance. VHF communications between lower units, on the other hand, are often vital during short periods, e.g. for artillery fire control. In this case much can be gained by jamming during suitable phases of the operations when the jamming side is not in urgent need of radiocommunication within the particular frequency range and sector of territory. There may also be frequency bands within the VHF range, for example, which are used by one contestant alone, and in such case the other can jam these bands without disturbing his own communications.

END

DATE
FILMED

03-82

DTIC