

**ZENITHAL REACTIVE JAMMER****CROSS-REFERENCE TO RELATED APPLICATIONS**

5 This patent application claims priority from European patent application No. 20425047.6 filed on November 5, 2020, the entire disclosure of which is incorporated herein by reference.

**TECHNICAL SECTOR OF THE INVENTION**

10 The present invention relates, in general, to the field of Electronic Countermeasures (ECM).

More specifically, the present invention relates to a zenithal reactive jammer, i.e., a reactive-type jamming device for the protection against radiofrequency (RF) remote  
15 sensing sensors or systems operating at high elevation angles (such as, for example, radar-type sensors/systems (e.g., imaging radars), Synthetic Aperture Radars (SARs) or the like, installed on space or air platforms - e.g., satellites, aircrafts, drones, etc.).

20

**BACKGROUND**

As is known, the aim of a jamming system for the protection against radar or SAR sensors/systems is to protect an area, a site (e.g. either of the civil or military type)  
25 or a set of assets of interest by inhibiting the capability of an enemy sensor to recognise and/or extract relevant information.

In the specific case of SAR sensors, the aim is to degrade the quality of the images as much as possible, so as  
30 to de-focus or otherwise cover the area of interest and thus offer an appropriate protection in either maritime or terrestrial contexts.

For example, US 10,852,391 B2 relates to a method and a relative device for jamming synthetic aperture radars.  
35 Specifically, US 10,852,391 B2 describes a method for jamming airborne SAR-type radars implemented by means of a radar

jamming device including a group of at least two cooperating units surrounding an area on the ground to be protected, wherein:

• at least two units of said group provide a radar  
5 detection function;

• at least one unit of this group provides a radar jamming function;

• each unit providing the radar detection function comprises a receiving and processing module configured to  
10 analyse the received signals;

• each unit providing the radar jamming function is configured to generate and transmit jamming signals; and

• each unit is interlinked by at least one two-way data link and is synchronised by a common clock.

15 More specifically, the method according to US 10,852,391 B2 comprises:

• identifying whether the received signals correspond to SAR signals;

• characterising the SAR signal received during a  
20 predefined duration that is shorter than the duration of a recurrence of the SAR signal;

• computing a filter adapted to the pulses of the received SAR signal;

• carrying out a pulse compression of the received SAR  
25 signal on each recurrence using said adapted filter, thus obtaining the Doppler history linked to the movement of the platform carrying the radar;

• periodically and iteratively characterising the received signal over a predefined duration that is longer  
30 than a recurrence of the SAR signal so as to establish, from one recurrence to the next, the displacement speed of the radar and the distance between said radar and the area to be protected;

• computing the jamming signals to be transmitted for  
35 each point of the area to be protected so as to jam the SAR-type radar coherently on the distance axis and on the Doppler axis; and

- transmitting the computed jamming signals.

In this context, it should be noted that, given the peculiarities of both the SAR technology (in terms of both the physical characteristics of the SAR sensors and the SAR processing and imaging process) and the air or space/satellite platforms (in terms of kinematic characteristics) generally used for the installation and transport of such sensors, the effective success of the jamming action is unfortunately not guaranteed.

Furthermore, similar limitations inherent in the effects of the processing on jamming effectiveness can also be found in the case of high-resolution imaging radar sensors, which have found increasing use in recent years.

In addition thereto, the kinematic profile of the aforesaid platforms, which is particularly challenging for the traditional electronic defence systems, is a further limiting factor.

Basically, the jamming systems of the known type do not have the architectural flexibility and the reactivity that are necessary to ensure a simultaneous coverage of all the multiple aspects that need to be taken into account when countering the aforesaid types of threats.

In fact, in order to ensure the effectiveness of the electronic defence in such contexts, several factors need to be addressed.

In particular, the technical difficulties relate to several aspects, such as:

- long distance (particularly in the case of contrast with satellite sensors);
- the elevation angles of interest for such threats (either satellite or aerial); and
- processing of the receivers.

With regard to the first aspect, this requires, from the point of view of the threat detection capability, a high sensitivity of the receiver used.

The need to provide the countermeasure with timings compatible with those of the evolution of the ongoing threat

must then be taken into account. This is true, in principle, for a whole range of platforms with a rapidly evolving kinematic profile, against which, therefore, the alarm and engagement times are very short.

5 In addition, in naval/maritime or land contexts, whether it is a matter of point defence (e.g., protection of a single naval platform, coverage of a single base, site and/or land convoy, etc.), or whether it is a matter of defence of larger areas (e.g., coverage of a fleet of ships, protection of a  
10 set of bases, sites and/or land convoys, etc.), the elevation angles involved are not those typical of commonly used electronic defence systems, which do not have the flexibility to provide effective protection even against such threats.

Another highly challenging aspect is the high power  
15 required from the jamming system in order to make the countermeasure effective. In fact, the latest generation high-resolution imaging radars have a high process gain in the coherent integration of the signals reflected from the soil/target during the illumination time of the observed  
20 area. Therefore, a jamming system, in order to be effective, must be able to compensate for this gain.

#### **OBJECT AND SUMMARY OF THE INVENTION**

In view of the foregoing, object of the present invention  
25 is to provide an innovative jamming device for the protection against remote sensing sensors or systems operating at radiofrequency (RF) and at high elevation angles (e.g., satellite/airborne radars or SARs), which is capable of overcoming or alleviating, at least in part, the drawbacks  
30 and limitations of the currently known jamming technologies.

This and other objects are achieved by the present invention as it relates to a jamming device, according to what is defined in the attached claims.

In particular, the present invention relates to a jamming  
35 device for the protection of targets on the earth's surface against radiofrequency (RF) threats of the space, satellite or air type;

said jamming device comprising:

- RF threat detection means;
- RF jamming means; and
- a control system;

5 wherein the RF threat detection means include:

- a plurality of receiving antennas;
- an RF threat detection unit; and
- one or more predefined RF-threat-related libraries;

10 wherein the receiving antennas are configured to receive RF signals having elevation angles of arrival that are equal to, or greater than, a minimum elevation angle, thereby providing an elevation angle coverage of interest;

wherein the RF threat detection unit is configured to:

- detect the presence of an RF threat based on the RF
- 15 signals received by the receiving antennas and on the predefined RF-threat-related library(ies); and,
- in case of detection of an RF threat,
  - determine a respective type of the detected RF threat based on the RF signals received by the receiving
  - 20 antennas and on the predefined RF-threat-related library(ies),
  - estimate a respective direction of arrival of the detected RF threat based on the RF signals received by the receiving antennas and
  - 25 - alert the control system about the detected RF threat, providing said control system with the respective type and the respective direction of arrival of said detected RF threat;

wherein said predefined RF-threat-related library(ies)

30 contain(s) information related to one or more RF threats of interest so as to enable the RF threat detection unit to detect the presence of said RF threat(s) of interest and to determine the respective type thereof based on the RF signals received by the receiving antennas;

35 wherein the control system includes:

- a control unit; and
- one or more predefined RF-jamming-actions-related

libraries;

wherein the control unit is configured, in case of detection of an RF threat by the RF threat detection unit, to:

- 5       • determine an RF jamming action to be performed against the detected RF threat based on the respective type determined by the RF threat detection unit and on the predefined RF-jamming-actions-related library(ies); and
- 10       • operate the RF jamming means so that said RF jamming means perform the determined RF jamming action against the detected RF threat;

wherein said predefined RF-jamming-actions-related library(ies) contain(s), for each RF threat of interest inserted in the predefined RF-threat-related library(ies),  
15       respective information related to one or more respective RF jamming actions to be performed against said RF threat of interest;

and wherein the RF jamming means are operable by the control unit in case of detection of an RF threat by the RF  
20       threat detection unit and include:

- a plurality of transceiver antennas configured to
- also provide said elevation angle coverage of interest,
  - track the detected RF threat and
  - 25       - transmit RF jamming signals against said detected RF threat so as to perform the RF jamming action determined by the control unit; and
- an RF jamming signal generation unit configured to generate the RF jamming signals to be transmitted by the  
30       transceiver antennas against the detected RF threat so as to perform said RF jamming action.

#### **BRIEF DESCRIPTION OF THE DRAWINGS**

For a better understanding of the present invention,  
35       some preferred embodiments (provided purely by way of explanatory, but absolutely not limiting, let alone binding example) will now be shown with reference to the accompanying

drawings (not to scale), wherein:

- Figure 1 schematically shows a jamming device according to a preferred embodiment of the present invention;

- Figure 2 schematically shows RF threat detection means of the jamming device of Figure 1;

- Figure 3 schematically shows an example of pointing of receiving antennas of the RF threat detection means of Figure 2 for detecting satellite SAR signals;

- Figure 4 schematically shows an embodiment example of said receiving antennas for detecting satellite SAR signals;

- Figure 5 schematically shows a control system of the jamming device of Figure 1;

- Figure 6 schematically shows RF jamming means of the jamming device of Figure 1;

- Figure 7 shows an embodiment example of the jamming device of Figure 1 for use on naval platforms to detect, and to counter, satellite SAR signals; and

- Figures 8 and 9 show, respectively, an example of a satellite SAR image and an example of a corresponding SAR image obtained in the presence of jamming provided by the jamming device according to the present invention in a satellite anti-SAR configuration.

#### **DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION**

The following description is provided to enable a person skilled in the art to comprehend, make and use the invention. Various modifications to the embodiments set forth will be immediately clear to persons skilled in the art and the general principles herein disclosed may be applied to other embodiments and applications without, however, departing from the scope of protection of the present invention as defined in the enclosed claims.

Therefore, the present invention should not be understood as limited to the sole embodiments described and shown, but it must be given the widest scope of protection in accordance with the characteristics defined in the appended claims.

The present invention relates to a jamming device for the protection of targets on the earth's surface, whether mobile or fixed, such as land or naval platforms (e.g., land vehicles, naval units, etc.), areas or sites of interest or  
5 the like, against radiofrequency (RF) threats such as radar or SAR sensors or systems, RF remote sensing sensors or systems or the like, of the space, satellite or aerial type.

For a better understanding of the present invention, Figure 1 shows a block diagram schematically representing a  
10 high-level functional architecture of a jamming device (denoted overall by 1) according to a preferred embodiment of the present invention.

In particular, the jamming device 1 (which, for the sake of brevity, will hereafter be referred to simply as the  
15 jammer) comprises:

- RF threat detection means 11;
- RF jamming means 12; and
- a control system 13.

In this respect, it is important to note that the jammer  
20 1 is preferably constituted by a single apparatus/device which said RF threat detection means 11, said RF jamming means 12 and said control system 13 are integrated into.

Furthermore, as shown in Figure 1, the jammer 1 is preferably connected, in a wired or wireless mode, to user  
25 interface means 2 that are external to said jammer 1 (e.g. a computer, a laptop, a station specifically dedicated to the control of the jammer 1 by a user, i.e. an operator, etc.).

The RF threat detection means 11 represent the passive  
30 part of the jammer 1 dedicated to monitoring a predefined angular sector (in azimuth and elevation) to detect the presence of RF threats (e.g., satellite/airborne SAR sensors/systems, satellite/airborne radar sensors/systems, satellite/airborne RF remote sensing sensors/systems, or the  
35 like) that transmit microwave signals or, more generally, RF signals that illuminate a target to be protected (e.g., an area or site of interest, a land or naval platform, or the

like) at which the jammer 1 is installed.

The RF jamming means 12 represent, instead, the active part of the jammer 1 dedicated to the delivery of RF countermeasures such as to compromise/impede the extraction  
5 of relevant information (e.g., position, distance, shape, etc.) related to the target to be protected.

Finally, the control system 13 provides:

- management of the RF threat detection means 11 as regards the surveillance of the area of interest; and
- 10 • activation and appropriate operation of the RF jamming means 12 as soon as an alarm is received from the RF threat detection means 11.

In this respect, it is worth noting that the integration of said RF threat detection means 11, said RF jamming means  
15 12 and said control system 13 into a single apparatus/device (i.e., the jammer 1) contributes to reducing the latencies in the delivery of the countermeasures.

Figure 2 shows a block diagram schematically representing a high-level functional architecture of the RF  
20 threat detection means 11, which include:

- a plurality of receiving antennas 111;
- an RF threat detection unit 112; and
- one or more predefined RF-threat-related libraries 113, wherein said predefined RF-threat-related library(ies)  
25 113 may be conveniently stored in an internal memory of the RF 112 threat detection unit or in a memory external thereto.

More in detail, the receiving antennas 111 are configured to receive RF signals having elevation angles of arrival which are:

- 30 • equal to, or greater than, a given minimum elevation angle (conveniently equal to, or greater than,  $20^{\circ}$  - preferably comprised between  $20^{\circ}$  and  $65^{\circ}$ );
- or, preferably, within a given angular range in elevation defined by the given minimum elevation angle and  
35 by a given maximum elevation angle greater than said given minimum elevation angle (e.g., elevation angles of arrival within the range  $20^{\circ}$ - $40^{\circ}$  or  $20^{\circ}$ - $45^{\circ}$  related to avionic RF

threats, or within the range  $30^{\circ}$ - $60^{\circ}$  or  $30^{\circ}$ - $65^{\circ}$  or  $30^{\circ}$ - $70^{\circ}$  related to satellite RF threats, or within the range  $60^{\circ}$ - $90^{\circ}$  or  $65^{\circ}$ - $90^{\circ}$  related to zenithal or quasi-zenithal RF threats).

Thus, the receiving antennas 111 (and, therefore, the RF threat detection means 11) provide an elevation angle coverage with respect to RF signals having high elevation angles of arrival with respect to the jammer 1 (more precisely, with respect to a given horizontal reference plane of said jammer 1), wherein said elevation coverage may conveniently also be zenithal or quasi-zenithal.

Preferably, said receiving antennas 111 are configured to receive RF signals having said elevation angles of arrival and azimuth angles of arrival in the range  $0^{\circ}$ - $180^{\circ}$  or  $0^{\circ}$ - $360^{\circ}$ , thereby providing, in addition to said elevation angle coverage, also an azimuth angle coverage of  $180^{\circ}$  or  $360^{\circ}$  around a zenith direction of the jammer 1 (wherein said zenith direction is orthogonal to the aforesaid horizontal reference plane).

The receiving antennas 111 can be conveniently realized by means of a predefined number of antennas that:

- have predefined operating characteristics (in terms of directivity, gain, antenna or radiation/power pattern, etc.);
- are installed/mounted at predefined positions of the jammer 1; and
- are pointed according to predefined pointing directions;

wherein said predefined number, said predefined operating characteristics, said predefined positions and said predefined pointing directions are such that to guarantee the aforesaid elevation and azimuth angle coverages (or, more generally, elevation and azimuth angle coverages of interest).

Conveniently, the receiving antennas 111 are directional antennas, preferably with high gain.

Moreover, said receiving antennas 111 preferably also have suitable characteristics in terms of weight and bulk so

as to allow or, in any case, facilitate the integration/installation of said receiving antennas 111 in/on the jammer 1.

Figure 3 schematically shows an example of pointing of the receiving antennas 111 for detecting satellite SAR signals.

In particular, Figure 3 shows a three-dimensional (3D) Cartesian reference system defined by:

- a vertical axis  $z$  corresponding to the zenith direction of the jammer 1; and
- two horizontal axes  $x$  and  $y$ , orthogonal to each other and perpendicular to the axis  $z$ , which define the given horizontal reference plane of said jammer 1, so that the latter is positioned at an intersection point  $O$  of said axes  $x$ ,  $y$ ,  $z$  (so-called origin of the 3D Cartesian reference system).

In addition, Figure 3 also schematically shows respective pointing directions of four groups of receiving antennas 111 together with the respective radiation patterns.

In particular, Figure 3 shows the orientation of the four groups of receiving antennas 111 in the four quadrants in azimuth (so as to guarantee an azimuthal coverage of  $360^\circ$  around the zenith direction) and at an elevation such that to cover the typical directions of illumination of the SAR satellites.

In this regard, it is important to note that, depending on the type of threat of interest, the pointing of the receiving antennae 111 can be conveniently redefined in an appropriate way, so as to focus on specific sectors (and, therefore, threats), or so as to cover sectors that are common to several types of threats. In addition, the pointing can be conveniently squinted further, so as to provide coverage even against diving avionics threats, and/or with kinematics that are quasi-orthogonal with respect to the jammer 1.

Referring again to the example shown in Figure 3, Figure

4 also schematically shows an embodiment example of each individual group of receiving antennas 111, wherein each group of receiving antennas 111 is conveniently realized by means of three horn antennas (denoted by 111A, 111B and 111C, respectively) that guarantee full-band coverage with respect to the typical frequencies of satellite SAR sensors/systems.

Finally, as regards the receiving antennas 111, it should be noted that the use of four groups of receiving antennas 111, like in the case of the example just described, in addition to guaranteeing the elevation and azimuth angle coverages of interest, also makes it possible to obtain a rough estimate of the direction of arrival of the RF signals which, in the absence of intelligence data on the orbit of the satellite or on the trajectory of the aircraft (e.g., drone, plane, etc.), makes it possible to appropriately point the RF jamming means 12 towards the detected threats.

On the other hand, as regards the RF threat detection unit 112 (conveniently implemented by means of a digital receiver), the latter is configured to:

- 20 • detect the presence of an RF threat based on the RF signals received by the receiving antennas 111 and on the predefined RF-threat-related library(ies) 113; and,
  - in case of detection of an RF threat,
    - determine a respective type of the detected RF threat based on the RF signals received by the receiving antennas 111 and on the predefined RF-threat-related library(ies) 113,
    - estimate a respective direction of arrival of the detected RF threat based on the RF signals received by the receiving antennas 111 and
    - alert the control system 13 about the detected RF threat, providing said control system 13 with the respective type and the respective direction of arrival of said detected RF.

35 In this respect, it is important to explain that said predefined RF-threat-related library(ies) 113 contain(s) (i.e., store(s)) information related to one or more RF

threats of interest (e.g., SAR sensors/systems, radar sensors/systems or, more generally, RF remote sensing sensors/systems) so as to enable the RF threat detection unit 112 to detect the presence of said RF threat(s) of interest and to determine the respective type thereof based on the RF signals received by the receiving antennas 111.

Preferably, said predefined RF-threat-related library(ies) 113 contain(s) (i.e. store(s)) information and/or data that is/are:

- related to various types of RF threats of interest; and
- indicative of respective operating parameters of said RF threats of interest (e.g., frequency, Pulse Repetition Interval (PRI), pulse width, agility, etc.).

Figure 5 shows a block diagram schematically representing a high-level functional architecture of the control system 13, which includes:

- a control unit 131; and
- one or more predefined RF-jamming-actions-related libraries 132, wherein said predefined RF-jamming-actions-related library(ies) 132 may be conveniently stored in an internal memory of said control system 13.

More in detail, the control unit 131 is configured, in case of detection of an RF threat by the RF threat detection unit 112, to:

- determine an RF jamming action to be performed against the detected RF threat based on the respective type determined by the RF threat detection unit 112 and on the predefined RF-jamming-actions-related library(ies) 132; and
- operate the RF jamming means 12 (providing the latter with appropriate commands indicative of, inter alia, the direction of arrival of the RF threat estimated by the RF threat detection unit 112), so that said jamming means RF 12 perform the determined RF jamming action against the detected RF threat.

In this respect, it is important to explain that said predefined RF-jamming-actions-related library(ies) 132

contain(s) (i.e., store(s)), for each RF threat of interest inserted/indicated/defined in the predefined RF threat library(ies) 113, respective information related to one or more respective RF jamming actions to be performed against said RF threat of interest.

Preferably, said predefined RF-jamming-actions-related library(ies) 132 contain(s) (i.e., store(s)), for each RF threat of interest inserted/indicated/defined in the predefined RF threat-related library(ies) 113, respective information and/or respective data that are:

- related to one or more respective RF jamming techniques to be implemented (conveniently, the most appropriate and effective jamming techniques) against said RF threat of interest; and

- indicative of respective operating parameters to be used to implement said respective RF jamming technique(s) against said RF threat of interest, wherein said respective operating parameters are conveniently related to one or more of the following characteristics:

- noise band to be used,
- number of jamming pulses to be generated for each received SAR/radar/RF pulse,
- amplitude modulation(s) to be used,
- frequency modulation(s) to be used.

Figure 6 shows a block diagram schematically representing a high-level functional architecture of the RF jamming means 12, which are operable by the control system 13 (in particular by the control unit 131) in case of detection of an RF threat by the RF threat detection means 11 (in particular by the RF threat detection unit 112) and include:

- a plurality of transceiver antennas 121 configured to
  - also provide the same elevation and azimuth angle coverages as the receiving antennas 111,
  - track the detected RF threat (conveniently by receiving RF signals coming from the detected RF threat) and

- transmit RF jamming signals against said detected RF threat so as to perform the corresponding RF jamming action determined by the control system 13 (in particular, by the control unit 131); and
- 5       • an RF jamming signal generation unit 122, preferably of the Digital Radio Frequency Memory (DRFM) type, configured to generate (conveniently, after storing and processing of the RF signals coming from the detected RF threat received by the transceiver antennas 121) the RF jamming signals to
- 10 be transmitted by said transceiver antennas 121 against the detected RF threat so as to perform said corresponding RF jamming action.

Conveniently, the transceiver antennas 121 are such as to provide:

- 15       • a high gain; and
- high capabilities (in particular, in terms of agility, flexibility and accuracy) of pointing of the receiving and transmitting beams and, hence, of aiming at the detected RF threats.

20       Preferably, said transceiver antennas 121 are made by means of Active Electronically Steered/Steerable Antennas (AESAs) - sometimes also referred to as Active Electronically Scanned Arrays (AESAs).

25       Preferably, the jammer 1 comprises, or is coupled to, a mechanical pointing system that is configured and operable to vary the elevation pointing of said receiving antennas 111 and of said transceiver antennas 121 so as to modify the elevation angle coverage of the jammer 1.

30       Conveniently, said mechanical pointing system is configured and operable to vary the inclination of the entire jammer 1 so as to vary the elevation pointing of the receiving antennas 111 and of the transceiver antennas 121 and, thereby, to modify the elevation angle coverage of said jammer 1.

35       As regards, instead, the user interface means 2, the latter are conveniently configured to allow a user/operator to:

- monitor and control the operation of the jammer 1;
- define/set the elevation angle coverage of said jammer 1, i.e. of the receiving antennas 111 and of the transceiver antennas 121 (specifically, by defining/setting the  
5 aforesaid given minimum and maximum elevation angles);
- define, programme, set, modify, etc., the predefined RF-threat-related library(ies) 113 and the predefined RF-jamming-actions-related library(ies) 132; and
- operate the mechanical pointing system to vary/modify  
10 the elevation angle coverage of the jammer 1.

In the light of what has just been explained, it is also possible to define a jamming system that comprises the jammer 1 and the user interface means 2 (and, in the case of a mechanical pointing system external to said jammer 1, also  
15 said mechanical pointing system).

Figure 7 shows an embodiment example of the jammer 1 for use on naval platforms to detect, and to counter, satellite SAR signals.

In particular, in such embodiment example, the  
20 transceiver antennas 121 dedicated to the delivery of the jamming are realized by means of two pairs of AESA 121A, 121B, wherein:

- each pair of AESA 121A, 121B operates in a respective frequency band; and
- 25 • for each pair, the two respective AESAs 121A or 121B of said pair provide, each, an azimuth angle coverage of 90°, whereby each pair provides a total azimuth angle coverage of 180°.

In addition, the receiving antennas 111 dedicated to the  
30 detection of satellite SAR threats comprise a plurality of groups of antennas which also provide, as a whole, an azimuth angle coverage of 180°, wherein each group of antennas can be conveniently realized by means of three horn antennas of the type shown in Figure 4 and previously described (i.e.,  
35 horn antennas 111A, 111B, 111C).

Conveniently, a 45° polariser can also be used advantageously.

Therefore, by using a jamming system comprising two jammers realized according to the example shown in Figure 7 and just described, and suitably installed/mounted one with respect to the other on one and the same naval platform, it is possible to obtain a total azimuth angle coverage of 360° around a zenith axis of said jamming system, for both the detection of satellite SAR threats and the delivery of the jamming against such threats.

In this regard, it is important to note that the embodiment example shown in Figure 7 and just described must absolutely not be construed as limiting, much less binding. In fact, the jammer 1 can be advantageously exploited:

- in the maritime field, either for naval or coastal installations; and
- in the terrestrial field, for either fixed or mobile installations.

In particular, depending on the type of mission of interest, the jammer 1 can be conveniently customised and scaled up, also to meet the different requirements (of installation and not only) typical of the different application scenarios.

In the example shown in Figure 7, i.e. in the case of a satellite anti-SAR configuration of the jammer 1, the latter conveniently provides protection against low-orbit satellite platforms.

In this case, a fast reaction is preferable, since the instant of illumination by the SAR sensor is unknown and the sensor in orbit moves at extremely high speeds.

Therefore, it is important to react quickly, because the SAR integrates the signal during the observation time so that the jamming, in order to be maximally effective, must act from the beginning to the end of the illumination window.

In use, the RF threat detection means 11 have, therefore, the task of intercepting the pulses from the electromagnetic environment, recognising pulses belonging to a possible RF threat of interest (in the case of a SAR threat, for example), of roughly estimating the direction of arrival and

then of alerting the control system 13 by providing the latter with the estimated direction of arrival, so as to activate the delivery of the countermeasure via the RF jamming means 12. At first, it is convenient to prioritise the speed of jamming delivery over the measurement/estimate accuracy of the direction of arrival of the RF threat. Thereafter, during the delivery of the jamming, a fine tuning of the measurement/estimate of the direction of arrival can be conveniently performed to maximise both the pointing accuracy of the RF jamming means 12 (in particular of the respective transceiver antennas 121) and the power level of the delivered jamming.

This effect can be more or less felt also in the case of contrast to avionic platforms. In particular, in the case of airborne sensors, the illumination times are sometimes significantly longer, so the visibility time interval is greater than in the satellite case. Sometimes, however, for example in the case of avionic platforms approaching the target to be protected, the useful times for the effective delivery of the jamming are reduced, so that the situation is similar to the satellite case.

In addition, in the various usage scenarios, the problem of the process gain of the imaging sensors remains, typically higher than that of the "classic" sensors.

The SAR waveform is usually made up of pulses modulated with a linear (chirp) frequency modulation (FM) with a rather wide bandwidth in order to have a resolution in a range comparable to that in azimuth; this also adds, besides the large distance, also further constraints on the detection technique.

The limitations that generally remain in these contexts are overcome by the jammer 1 thanks to the use of the receiving antennas 111 dedicated to the detection of SAR signals, oriented so as to ensure coverage in the required elevation angular sector. This also allows the coverage to be guaranteed against other categories of RF threats originating from particularly high elevation angles.

Figures 8 and 9 show, respectively, an example of a satellite SAR image and an example of a corresponding SAR image obtained in the presence of jamming delivered by the jammer 1 in the satellite anti-SAR configuration described above.

From the foregoing disclosure, the many innovative characteristics and the innumerable technical advantages of the present invention are immediately evident for a person skilled in the art.

In particular, it is important to point out that the jamming device according to the present invention is based on the coordination of two subsystems, namely:

- a receiving subsystem dedicated to the detection of threats, which alarms reactively upon illumination by threats coming from non-typical elevation angles of arrival; and

- a jamming subsystem, which inhibits the extraction of sensitive information operated by the enemy sensor (such as, for example, imaging information or the angle and distance coordinates of one or more targets).

The appropriate mechanical structure and the appropriate orientation of the antennas optimise the ability of the jamming device to detect radar transmissions coming from these classes of sensors and to maximise contrast effectiveness. The characteristics of the threat, as well as the most suitable countermeasure strategy, are appropriately determined, modulated and managed on a library basis, conveniently as a function of the mission in progress.

The architecture of the jamming device allows to best meet particularly stringent mission requirements and, for this reason, this device can be advantageously exploited not only for anti-SAR applications, but also for the defence against diving threats or in any case with quasi-zenithal flight profiles and high kinematic evolution.

Furthermore, the architecture of the jamming device according to the present invention provides for a deep integration between the aforesaid two subsystems and allows

the use of state-of-the-art transmission and processing technologies, which make this architecture particularly reactive and flexible, in addition to guaranteeing the maximum effectiveness of the contrast delivered.

5        These characteristics are winning in all those application contexts wherein the speed of response, the power involved and the effectiveness of the countermeasure delivered are fundamental.

10        The jamming device according to the present invention arises from the Applicant's extensive experience in jamming radar systems which requires the use of panoramic receivers with a high probability of interception, a fast reaction and the delivery of a coherent jamming.

15        The present invention is capable of meeting stringent electronic defence requirements, either against satellite SAR sensors or, more generally, against a wide range of avionic-type RF threats from high elevation angles (up to profiles close to the zenith).

20        Furthermore, the use of state-of-the-art DRFM devices, such as those of the Applicant, enables the jamming device to be able to deliver a wide range of possible coherent countermeasures and to synthesise effective countermeasures extremely quickly.

25        Furthermore, the jamming device according to the present invention is characterised by an extremely flexible control architecture.

More specifically, the subsystem dedicated to the jamming delivery:

30        • operates in real time with respect to the RF threat, reducing processing losses at the enemy sensor and thus increasing the effectiveness of the countermeasure;

• operates on a pulse basis, thus allowing consistency to be maintained at each instant of radar sensor transmission; and

35        • operates on a modulation basis, making it possible to control the characteristics and thus the effects of the jamming injected in the enemy receiver.

In practice, this translates into:

- an increase in the effects of the jamming delivered and, therefore, in the consequent inhibition of the enemy sensor's ability to extract relevant information; and
- 5       • an ability to control the jamming distribution in the resulting image (SAR or more generally radar).

The traditional naval and land electronic defence systems currently known are not designed to ensure an elevation angle coverage suitable for the defence against  
10       satellite or avionic SAR threats of the zenithal or quasi-zenithal type. In fact, the traditional configuration of such systems typically ensures an elevation coverage of  $[-5^\circ, +55^\circ]$ . Conversely, the jamming device according to the present invention is capable of ensuring a coverage for high  
15       elevation angles, even azimuthal or quasi-azimuthal. Furthermore, according to a preferred embodiment of the invention, the jamming device may advantageously include, or may advantageously be coupled to, a mechanical pointing/tilting system capable of orienting the antennas or  
20       the entire jamming device, even in real time, towards the desired pointing direction, held fixed throughout the mission duration. This directionality is also successful in case of detecting, and countering, SAR threats installed on avionic platforms that also operate close to these angles of  
25       view.

A further configuration may conveniently include positioning the antennas so that, once the jamming device has been suitably tilted, the final pointing is quasi-orthogonal so as to ensure the coverage of the sector at the  
30       zenith.

The set of technical features described above makes the use of the jamming device according to the invention particularly advantageous for countering both satellite and avionic SAR sensors, as well as a wide range of radar or  
35       aerial RF threats with various flight profiles, since it is able to meet the typical requirements of both types of operating scenarios.

In fact:

• in the case of defence against satellite SAR, the use of the jamming device according to the invention is advantageous because this device has a high reactivity; this characteristic, together with the possibility of programming, modifying and, therefore, using various countermeasure techniques, guarantees high operating efficiency and effectiveness of the device which is always able to counter satellite SAR threats, cancelling the high processing gain of the SAR receivers;

• in the case of defence against avionic SARs (e.g. installed on aircrafts, drones, etc.), the use of the jamming device according to the invention is advantageous because such a device has a flexible architecture that allows programming, modifying and, therefore, using highly effective contrast techniques; this guarantees an efficient electronic defence to be delivered, since the possibility of detecting SAR-type threats is always guaranteed;

• in the case of defence against avionic RF threats with zenithal, quasi-zenithal profiles or, more generally, with high angles of view, the use of the jamming device according to the invention is advantageous because such device has the capacity to configure the angle of view by means of the mechanical pointing system, so that it is always possible to obtain a suitable configuration such as to guarantee the coverage of zenithal angle elevation sectors or those close to 90°; this guarantees the delivery of an electronic defence that is either efficient or effective, since

- the ability to detect threats with zenithal or quasi-zenithal flight profiles is guaranteed,
- high speed of response delivery is guaranteed and
- effective jamming techniques can be used.

Finally, it is important to draw attention once again to the fact that the present invention makes it possible to equip naval or land platforms with an electronic defence system that is extremely effective against satellite or avionic SAR threats and, more generally, against various

types of avionic RF threats at high angles of view.

In fact, the jamming device according to the present invention:

- can be configured to meet the needs of different mission categories, such as
  - satellite anti-SAR missions,
  - anti-platform avionic missions and,
  - more generally, it can offer an effective countermeasure against radar (imaging or otherwise with high process gain) on aerial platforms at elevation angles up to the zenith (depending on the mission configuration);
- ensures a rapid response against various types of threats, as it
  - provides for a receiving subsystem specifically dedicated to the function of detecting threats of interest, and
  - also integrates the jamming subsystem for the delivery of countermeasures into the same device;
- is preferably provided with a mechanical pointing system so that it makes it possible to
  - maximise or optimise the elevation angle coverage and
  - optimise the power of the jamming delivered;
- has capabilities of high threat tracking and maximising the jamming power delivered;
- has a highly flexible control architecture.

In conclusion, it is important to note that, while the above described invention refers in particular to very specific embodiments, it must not be intended as limited to such embodiments, including within its scope all the variants, modifications or simplifications covered by the enclosed claims.

### CLAIMS

1. Jamming device (1) for the protection of targets on the earth's surface against radiofrequency threats of the space, satellite or air type;
- 5 said jamming device (1) comprising:
- radio-frequency threat detection means (11);
  - radio-frequency jamming means (12); and
  - a control system (13);
- 10 wherein radio-frequency threat detection means (11) include:
- a plurality of receiving antennas (111);
  - a radiofrequency threat detection unit (112); and
  - one or more predefined radiofrequency-threat-related
- 15 libraries (113);
- wherein the receiving antennas (111) are configured to receive radiofrequency signals having elevation angles of arrival that are equal to, or greater than, a given minimum elevation angle, thereby providing an elevation angle
- 20 coverage of interest;
- wherein the radiofrequency threat detection unit (112) is configured to:
- detect the presence of a radiofrequency threat based on the radiofrequency signals received by the receiving
- 25 antennas (111) and on the predefined radiofrequency-threat-related library(ies) (113); and,
- in the event of detection of a radiofrequency threat,
    - determine a respective type of the detected radiofrequency threat based on the radiofrequency
- 30 signals received by the receiving antennas (111) and on the predefined radiofrequency-threat-related library(ies) (113),
- estimate a respective direction of arrival of the detected radiofrequency threat based on the
- 35 radiofrequency signals received by the receiving antennas (111) and
- alert the control system (13) about the detected

radiofrequency threat, providing said control system (13) with the respective type and the respective direction of arrival of said detected radiofrequency threat;

5        wherein said predefined radiofrequency-threat-related library(ies) (113) contain(s) information related to one or more radiofrequency threats of interest so as to enable the radiofrequency threat detection unit (112) to detect the presence of said radiofrequency threat(s) of interest and to  
10        determine the respective type thereof based on the radiofrequency signals received by the receiving antennas (111);

         wherein the control system (13) includes:

         • a control unit (131); and  
15        • one or more predefined radiofrequency-jamming-actions-related libraries (132);

         wherein the control unit (131) is configured, in case of detection of a radiofrequency threat by the radiofrequency threat detection unit (112), to:

20        • determine a radiofrequency jamming action to be performed against the detected radiofrequency threat based on the respective type determined by the radiofrequency threat detection unit (112) and on the predefined radiofrequency-jamming-actions-related library(ies) (132);  
25        and

         • operate the radiofrequency jamming means (12) so that said radiofrequency jamming means (12) perform the determined radiofrequency jamming action against the detected radiofrequency threat;

30        wherein said predefined radiofrequency-jamming-actions-related library(ies) (132) contain(s), for each radiofrequency threat of interest inserted in the predefined radiofrequency-threat-related library(ies) (113), respective information related to one or more respective  
35        radiofrequency jamming actions to be performed against said radiofrequency threat of interest;

         and wherein the radiofrequency jamming means (12) are

operable by the control unit (131) in case of detection of a radiofrequency threat by the radiofrequency threat detection unit (112) and include:

- a plurality of transceiver antennas (121) configured to
  - also provide said elevation angle coverage of interest,
  - track the detected radiofrequency threat and
  - transmit radiofrequency jamming signals against said detected radiofrequency threat so as to perform the radiofrequency jamming action determined by the control unit (131); and
- a radiofrequency jamming signal generation unit (122) configured to generate the radiofrequency jamming signals to be transmitted by the transceiver antennas (121) against the detected radiofrequency threat so as to perform said radiofrequency jamming action.

2. The jamming device of claim 1, wherein:

- the receiving antennas (111) are configured to receive radiofrequency signals having elevation angles of arrival that are included in a given elevation angle range defined by the given minimum elevation angle and by a given maximum elevation angle greater than said given minimum elevation angle; and
- the given elevation angle range corresponds to the elevation angle coverage of interest.

3. The jamming device according to claim 1 or 2, wherein the given minimum elevation angle is equal to, or greater than, 20°.

4. The jamming device of claim 2, wherein the given minimum elevation angle is comprised between 20° and 65°, and the given maximum elevation angle is comprised between 40° and 90°.

5. The jamming device according to any preceding claim, wherein:

- the receiving antennas (111) are configured to receive radiofrequency signals having said elevation angles of

arrival and azimuth angles of arrival in the range  $0^{\circ}$ - $180^{\circ}$  or  $0^{\circ}$ - $360^{\circ}$ , whereby said receiving antennas (111) provide an azimuth angle coverage of  $180^{\circ}$  or  $360^{\circ}$  around a zenith direction of the jamming device (1); and

- 5       • the transceiver antennas (121) are configured to also provide said azimuth angle coverage.

6. The jamming device according to any preceding claim, wherein the predefined radiofrequency-threat-related library(ies) (113) contain(s) information and/or data which  
10 is/are:

• related to various types of radiofrequency threats of interest; and

• indicative of respective operating parameters of said radiofrequency threats of interest;

15       and wherein the predefined radiofrequency-jamming-actions-related library(ies) (132) contain(s), for each radiofrequency threat of interest inserted in the predefined radiofrequency-threat-related library(ies) (113), respective information and/or respective data which is/are:

20       • related to one or more respective radiofrequency jamming techniques to be implemented against said radiofrequency threat of interest; and

• indicative of respective operating parameters to be used to implement said respective radiofrequency jamming  
25 technique(s) against said radiofrequency threat of interest.

7. The jamming device according to any preceding claim, comprising, or coupled to, a mechanical pointing system operable to:

30       • vary the pointing in elevation of said receiving antennas (111) and of said transceiver antennas (121) so as to modify the elevation angle coverage of interest; or

• vary the inclination of the entire jamming device (1) so as to vary the pointing in elevation of said receiving antennas (111) and of said transceiver antennas (121), thus  
35 modifying the elevation angle coverage of interest.

8. The jamming device according to any preceding claim, wherein:

- the receiving antennas (111) are horn-type directional antennas;

- the transceiver antennas (121) are active electronically steered/steerable high-gain antennas;

5       • the radiofrequency threat detection unit (112) is a digital receiver; and

- the radiofrequency jamming signal generation unit (122) is based on Digital Radio Frequency Memory technology.

9. The jamming device according to any preceding claim,  
10 consisting of a single apparatus/device which the radiofrequency threat detection means (11), the radiofrequency jamming means (12) and the control system (13) are integrated into.

10. Jamming system for the protection of targets on the  
15 earth's surface against radiofrequency threats of the space, satellite or air type, comprising:

- one or more jamming devices (1) as the one claimed in any preceding claim; and

- user interface means (2) connected to said jamming  
20 device(s) (1) and configured to allow a user/operator to

- monitor and control operation of said jamming device(s) (1),

- set the elevation angle coverage of interest of said jamming device(s) (1) and

25       - define and modify the predefined radiofrequency-threat-related library(ies) (113) and the predefined radiofrequency-jamming-actions-related library(ies) (132) of said jamming device(s) (1).

11. Jamming system for the protection of targets on the  
30 earth's surface against radiofrequency threats of the space, satellite or air type, comprising two jamming devices (1) as the one claimed in claim 5; wherein each jamming device (1) is configured to provide a respective azimuth angle coverage of 180° around a respective zenith direction of said jamming  
35 device (1); and wherein said jamming devices (1) are arranged with respect to each other so as to provide as a whole an azimuth angle coverage of 360° around a zenith axis of the

jamming system.

12. Jamming system for the protection of targets on the earth's surface against radiofrequency threats of the space, satellite or air type, comprising:

- 5       • one or more jamming device(s) (1) as the one claimed in claim 7;
- in the case of a mechanical pointing system external to said jamming device(s) (1), also said mechanical pointing system; and
- 10       • user interface means (2) connected to said jamming device(s) (1) and configured to allow a user/operator to
  - monitor and control operation of said jamming device(s) (1),
  - set the elevation angle coverage of interest of said
  - 15       jamming device(s) (1),
  - define and modify the predefined radiofrequency-threat-related library(ies) (113) and the predefined radiofrequency-jamming-actions-related library(ies) (132) of said jamming device(s) (1)
  - 20       - operate the mechanical pointing system to modify the elevation angle coverage of interest of said jamming device(s) (1).

13. Land or naval platform, either fixed or mobile, equipped with the jamming device (1) as claimed in any claim 25 1-9 or with the jamming system as claimed in any claim 10-12.