"Sintis" concept of jamming remotely activated improvised explosive devices (RAIED)

Emilian Saslekov, Vladimir Turtansky, Rumen Simeonov
"SINTIS" Ltd, Bulgaria, Sofia-1619, area "Vitosha", residential area "Kniajevo", bul. "Tzar Boris – III" №246, building "A", office №1

ABSTRACT:

This report describes the concept of jamming remotely activated improvised explosive devices implemented by **"SINTIS" Ltd**. It gives reason for our choice of jamming signal, energy parameters, method for protection distance determination and mobile jammers design.

KEY WORDS:

IED - IMPROVISED EXPLOSIVE DEVICES;
BJ - BOMB JAMMER.

Improvised explosive devices **(IED),** led to a significant loss of vital force and technique by the antiterrorist forces. Military commands and security services determine the **IED** threat as one of the main threats in the actions on a foreign, and on their own territory.

Particularly dangerous types of **IED** are those activated remotely via radio channel. Indeed, terrorists can use without restrictions the entire available radio frequency range for technical implementation of communication equipment. Everything that is capable of providing radio communication and that is possible to make or adapt using freely available materials and equipment could be used to create remote activated **IED**.

Examples: mobile phones, remote controls for automobiles, remote controls for toys and models, etc. **Fig.1** shows some common implementations of remotely activated **IED**.

Fig. 1

Protection from remotely activated via radio channel **IED** is performed with radio jamming transmitters. The radio jamming interferes the normal functioning of radio channel to the extent that it cannot be used. Here raises the main issue related to the creation of such radio-jammers - what should be the parameters of the emitted radio-jamming signals in order to ensure that the bomb would not be activated. Illustration of the method of protection via radio jamming is presented on **Fig.2.**

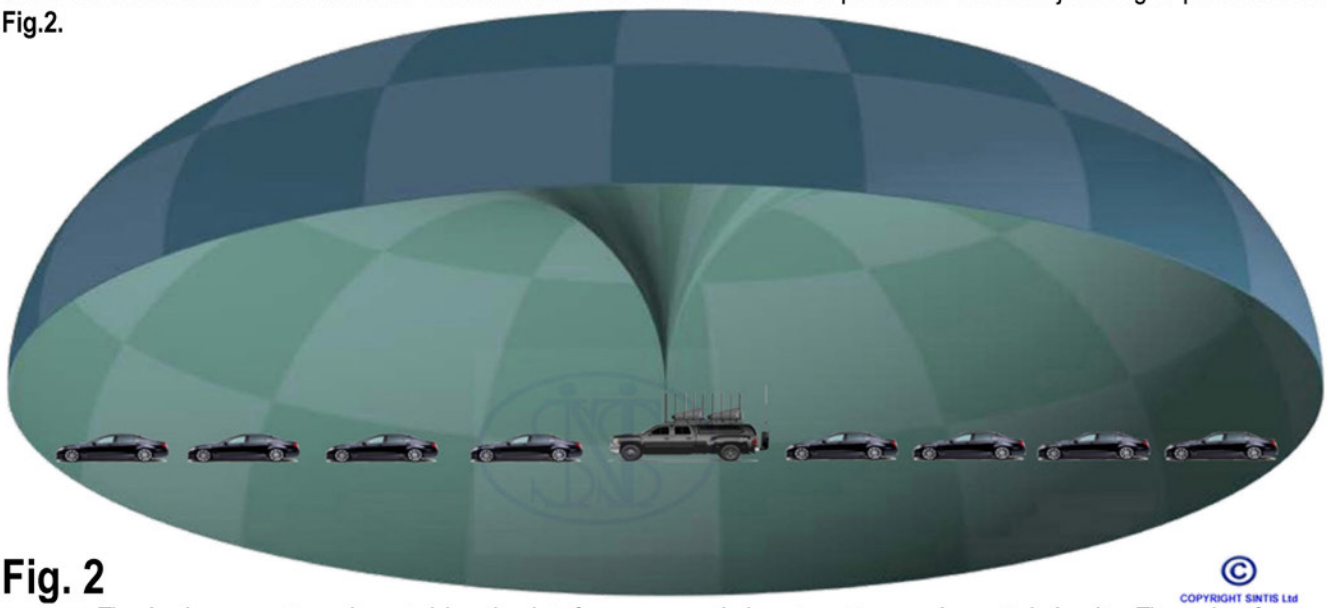

Fig. 2

The basic parameters characterizing the interferences are their nature, type and spectral density. These interference parameters depend on the parameters of the signal used by the terrorists - frequency, type of modulation, coding method, spectral density and polarization. Each one of them, however, the terrorist modulates according to his preferences and capabilities related to both the level of his general theoretical and practical competence in the field of electronics and his access to components and his personal improvisation capabilities.

Finally, nobody is capable to provide acceptable from the standpoint of security restrictions that the alleged terrorist could not overcome. For this reason, it is reasonable to assume that **IED** may be set into operation in virtually all the available for technical use radio spectrum, with all possible methods of modulation, polarization and coding with the only limitation being the power of the appliances used.

Energetic limits are those things that with high certainty set limits for the terrorist. These limits firstly regard the accessible energy sources (batteries) and secondly – the accessible engineer applications of high frequency power. Furthermore for the terrorist it is additionally important the energy sources as well as the powerful end applications to be easily portable.

The energetic limits set also optimization of the emitted interference. The work done by **Sintis Ltd** led to the creation of optimal interference method for generating the optimal interference minimizing the energy consumption for **IED** protection.

The method of **Sintis Ltd** for generating radio frequency interference consists in creating signal, scanning in two directions between the borders of the operating frequency band, and scanning in each direction from one border to the other with accidentally changing speed, during the time of scanning with accidental repetition period. The average scanning time in one direction is much longer than the average scanning time in the other directions and the statistic parameters can be unspecified and only the shortest scanning time can be constant.

The advantages of this method are lack of processing of the radio frequency signal, expanded width, and disruption of the radio jamming signal. Expanded borders for regulation of the spectrum.

From now on the following abbreviation are used in the text:

T	-	time
T_0	-	Average statistic scanning time
ΔT_0	-	Deviation of the average statistic period
τ_f	-	Growth period
τ_t	-	Fall down period
U	-	Tension
U_H	-	High pain limits
U_L	-	Low tension limit
F	-	frequency
f_{start}	-	The starting frequency of the scanning band.
f_{stop}	-	The starting frequency of the scanning band
Δf_{rec}	-	Frequency band of the receiving device.

At **Fig.3** is illustrated signal for control the frequency of the carrier frequency generator.

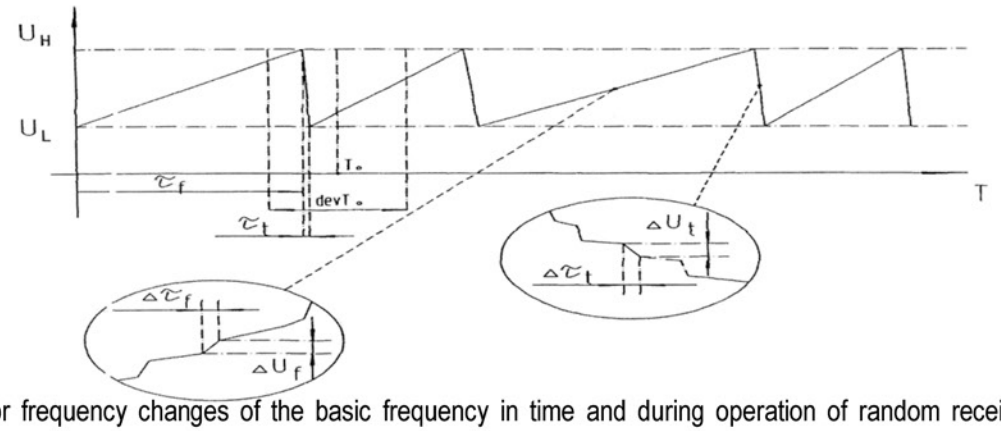

Fig. 3

The generator frequency changes of the basic frequency in time and during operation of random receiver are presented on **Fig.4.**

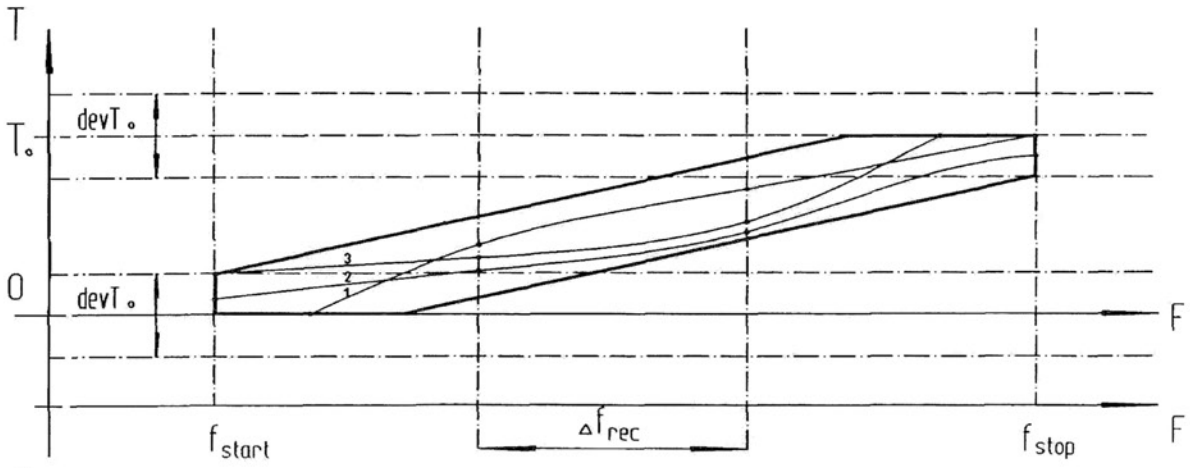

Fig. 4

A particular observation of the radio frequency interference via spectroanalysis is presented on **Fig. 5.**

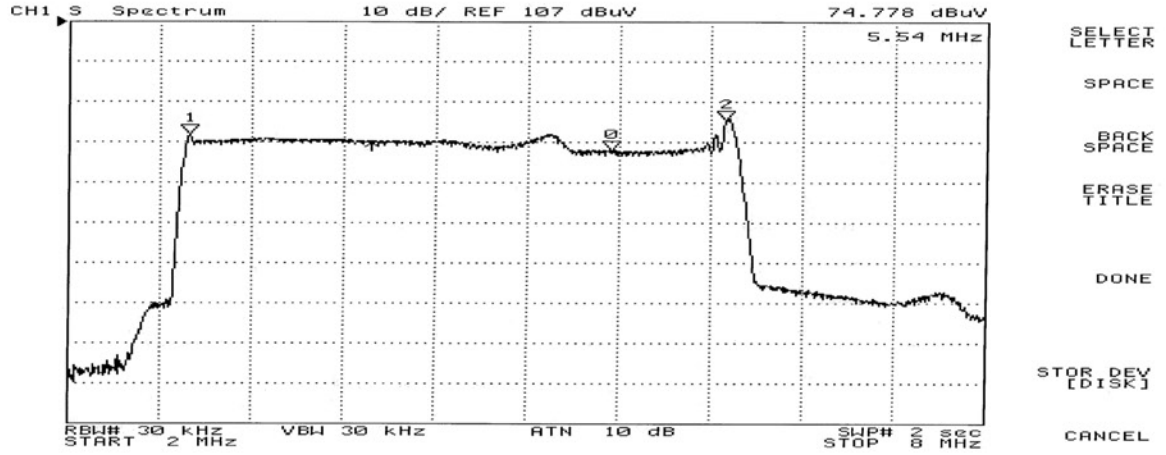

Fig. 5

The frequency scanning control signal is presented on **Fig.3** describing the scanning character of the frequency range. In the particular illustration it is assumed that the control signal is a tension one, which is something usual for scheme realizations of frequency controlled generators of basic frequency. In extremely high frequency generators this signal usually is electrical which doesn't change the figure but in the vertical axis the symbol for electricity **"I"** should be placed. It is also accepted, that the growth period τ_f exceeds many times the fall down time τ_t **-** $(\tau_f >> \tau_t)$**.** If we assume the opposite that τ_t exceeds much more τ_f **-** $(\tau_t >> \tau_f)$, the graph would be a mirror image. The values of deviation - of growth and fall down are not accidental, i.e. τ_f**=var,** τ_t**=var,** the fall down time could be τ_t**=const**.

As this figure shows, the control tension **"U"** in one direction with chaotic speed increases from the value that determines the scanning range U_L, up to the value describing the end of the scanning range U_H. The complex of multiple small and random values of growth elements forms the consecutive front of control tension lasting τ_f. After reaching U_H, the control tension via multiple small and random elements values starts gradually to decrease, and during increase and decrease the process preserves its own direction character with maximum density character and maximum density of the result specter of variation with character. The random one way alteration, formed by the accumulation of multiple small, subsequent and random in value and duration alterations is presented in the two detailed pictured of the curves. The high frequency variation which frequency follows the law of alteration, presented on **Fig.3**, it has equally distributed spectrum closed between the scanning borders – radio frequency interference, with density depending on the statistical characteristics of the increasing and decreasing values forming the scanning law. The non-accomplishment of the motion condition would lead to the appearance of dominating harmonics in the radio frequency spectrum. The non-accomplishment of $(\tau_f >> \tau_t)$ or $(\tau_t >> \tau_f)$, would also lead to the appearance of dominating harmonics or to the so called "lenal" спектър.

Fig.4 shows the variations of scanning frequency measured after periods of time equal to the average statistical scanning period, **"T_0"**. The circled polygon forms the field of the possible realizations of the random scanning process under the condition $(\tau_f >> \tau_t)$, τ_f **= var** и τ_t **= const**. The figure presents also the frequency band Δf_{rec} of hypothetic radio receiver. The particular happenings of the random scanning process **"1"**, **"2"** и **"3"**, illustrate the chaotic time of scanning signal stay in the acceptance band (sensibility) of the receiver, the chaotically distributed moment of signal appearance, the chaotically distributed leaving signal and the chaotic speed alteration.

A particular spectrogram of a radio frequency interference, obtained via the method $(\tau_f >> \tau_t)$, τ_f **= var** и τ_t **= const** is presented on **Fig.5.** The parameters of the regime of the spectrogram are pointed in the figure.

Without a necessity to process the radio frequency signal, and only on the bases of regulations of the law of distribution of the variation values τ_f and τ_t and their statistical characteristics, the spectral density of the radio frequency interference power is directly regulated. The width of the radio frequency band is limited only to the technically reachable range of readjustmen, which is much greater from the spectrum of the phase-module signal. The limits of regulation of the power spectral density are broadened and they are determined directly by the limits of regulation of the spectral characteristics of the scanning law. The maximum operating frequency is each technically possible frequency.

In constructions **Sintis Ltd** apply exactly that method and for each separate case particular statistical parameters of the interference signal are chosen. Thus we achieve the optimum that guarantees protection and reasonable energy consumption.

Regarding the above mentioned, jamming devices should be modular, and the whole frequency band should be divided to sub-bands and each sub-band should be jammed with a separate jamming device. With such approach it is

possible to optimize precisely the jamming signal as the frequency spectrum is used segmented – some parts of it are highly specialized. Such are the sectors for telephone services, TV, navigation, etc.

It is impossible to count on standard applications while using the frequency spectrum for **IED** protection. If for example we use **GSM** sector to activate a bomb, it doesn't mean that the terrorist will use a telephone. There are no reasons that can make the terrorist comply with the international standards. He is free to use the frequency band in a chosen by him way. It is possible to use readjusted **Walky-Talky** with suitable frequency band. In this case the signal would not influence the telephone network operation. The network would ignore it, by determining it as a fixed in terms of frequency interference. The same reaction will have a jammer optimized according to the international standards. The result is – maximum comfort for the terrorist.

The conclusion from the above is that during **IED** protection it is obligatory to use universal and not specialized interference signal. Energetic profits by using „intelligent" jammers are extremely restricted and practically non-applicable. On this basis **Sintis Ltd** uses in the whole applicable frequency spectrum interferences, optimized for the particular mass applied communications as well as for improvised ones.

Finally, the mentioned reasons impose constructive approach based on modular principles. This approach ensures additional energy because of restriction of energy losses in the antennas. In modular constructions the power of each module is much lower the integral power of the whole jammer. It is possible to use well coordinated antennas with better amplifiers, avoiding losses in traditional wideband antennas and diffusion of the emitted signals from wideband antennas.

The lower power of the separate modules allows using more accessible and therefore more electronic elements for the accomplishment of the set parameters.

During the modular approach it is possible to achieve maximum universality and compactness, which leads to flexibility of decisions related to the disposition of the mobile versions of the jammer. Instead of one big corpus, it is possible to diversigy modules, to shorten the antenna cables up to the degree of hteir practical elimination and setting the antena on the modules themselves. A possible vriation in practice is presented on **Fig.6**.

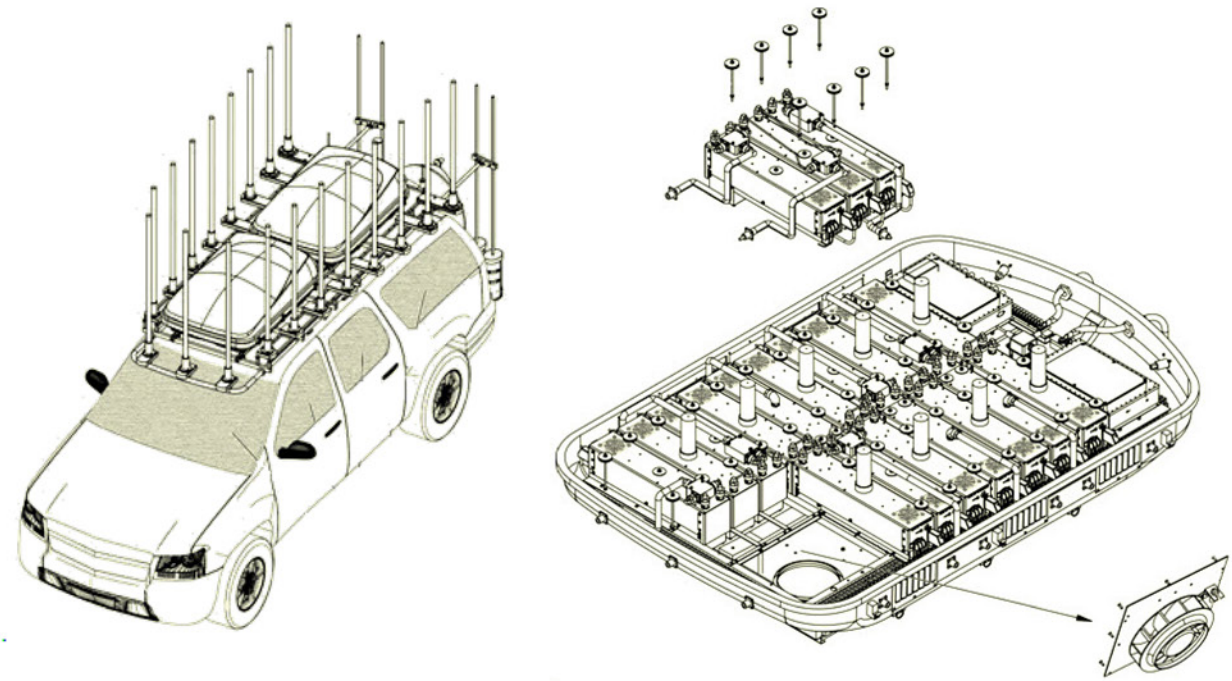

Fig. 6

As shown on the picture, in this case the modules are gathered in a conventional roof boots. A big part of the antennas are integrated with the modules and where it is not possible to achieve, they are brought out on a special frame. The advantage of this approach is that the compartment of the vehicle is free of devices. The temperature separation from the modules is separate inside the compartment and the air conditioning of the vehicle is used only for the people. The disposition on the roof facilitates the cooling of the devices and ensures additional protection for the people from the influence of the emitted radio frequency power.

During its practice, **Sintis Ltd** applies a formal approach for determining the protection radius from **IED**. The criterion is the distance ratio around the jammer, at which the **IED** cannot be activated.

THE NATURE OF THE PROTECTION COEFFICIENT IS DESCRIBED IN FIG.7.

Using the presented in the figure symbols and additionally:

- R_p - protection distance, within the scope of which the **IED** cannot be activated;
- K_p - protection coefficient;

It is defined that protection coefficient is equal to the ratio of the distance around the jammer, in which the **IED** could not be activated and the distance between the terrorist and the **IED**:

$$Kp = Rp / Dtb$$

If we assume that:

- **h** - Efficiency coefficient of interference;
- **n** - Ratio interference/signal at which level the **IED** is not activated;
- P_b - Power of the terrorist transmitter;
- P_j - Power of the jamming device;
- Δf_b - frequency band of the **IED** receiver;
- Δf_j - jammer's spectrum width,

The protection coefficient would be:

$$K_p = \{[h*P_j*\Delta f_b] / [n* P_b*\Delta f_j]\}^{1/4}$$

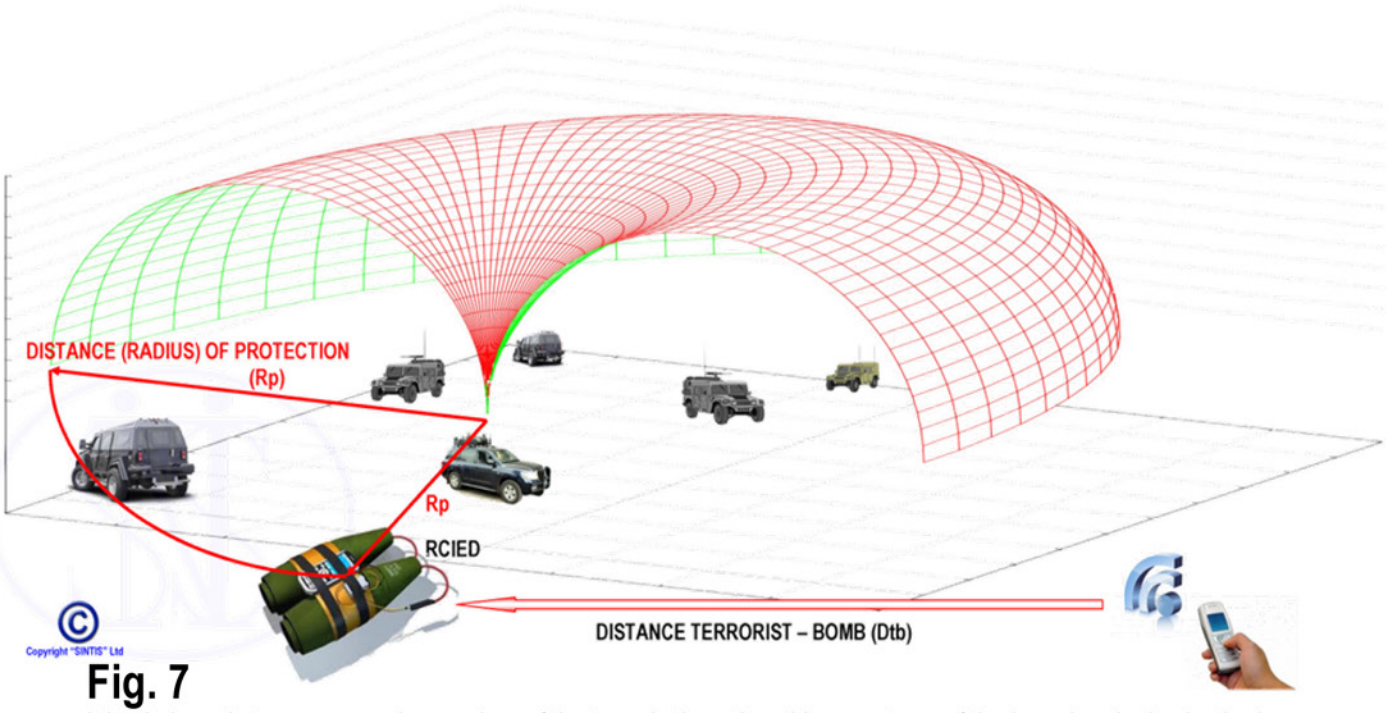

Fig. 7

It is obvious that a narrower the receiver of the terrorist is and a wider spectrum of the jamming device is, the lower the protection coefficient during equal other conditions is. It is also obvious that the increase of the protection coefficient is related to an increase of the jamming quality **„h"**, decrease of the ratio interference/signal **„n"** at the input of the **IED** receiver and naturally – decrease of the jammer spectrum **„Δf_j"** and increase of its power **„P_j"**.

To illustrate the seriousness of the requirements towards the energetic resources of the jammer, without making detailed calculations a suitable example is the serial jammer **SINTIS-BJ™VIP300X2v4KV**. In order to ensure an average protection coefficient of **30%** in a frequency range from **2** to **6000 MHz**, the emitted power is approximately **3000 W**. Such emitted power, regarding the technically achievable efficiency coefficient in the powerful final stages, the consumption of the rest of the electronics, the cooling, the maintenance of the buffer batteries and the reasonable power supply reserves leads to the impressive power of **25KW** of the supply devices.

CONCLUSION:

The concept of **Sintis Ltd** for jamming remotely activated improvised explosive devices **(RAIED)** consists of applying modular principle of creation, separation of the covered range in subranges, each of which covered by moving the devices out of living premises of the bearer and use of differentiated approach while choosing interference signal for each module, based on patent **BG-65591-B1.**

REFERENCES:

1. **Patent BG-65591-B1;**
2. **Catalogue "Sintis Counterterrorism Products".**