ENERGETIC RESOURCES TO PROTECT AGAINST REMOTELY ACTIVATED IMPROVISED EXPLOSIVE DEVICES (IED)

Vl. Turtansky, E. Saslekov, R. Simeonov

ABSTRACT:

Provision of the adequate energy sources needed for transmitters jamming improvised explosive devices **IED** is examined. The theoretical and practical inadequacy of the attempts to offer jammer using energy-saving "intelligent" interference is proved.

KEY WORDS:

IED - IMPROVISED EXPLOSIVE DEVICES;
BJ - BOMB JAMMER;

The 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 realization 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 parameters of the emitted radio-jamming signals it should have in order to ensure that the bomb would not be activated.

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 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 able 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 the **IED** may be set in 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 used appliances.

The energy limits are the point that can be claimed with high probability to set restrictions for the terrorist - restrictions primarily set by the available power sources (batteries), and secondly by the available engineering implementations of high frequency capacities. However, for the terrorist is additionally important both the energy sources and the terminal devices to be easily portable.

The mentioned most common reasons given a sufficiently clear idea of the complexity of the **IED** protection. Furthermore we will show energetic dependence in creating radio-jammers for **IED**, known as "bombjammers". A typical scheme of remotely activated **IED** is shown in **Fig.2.**

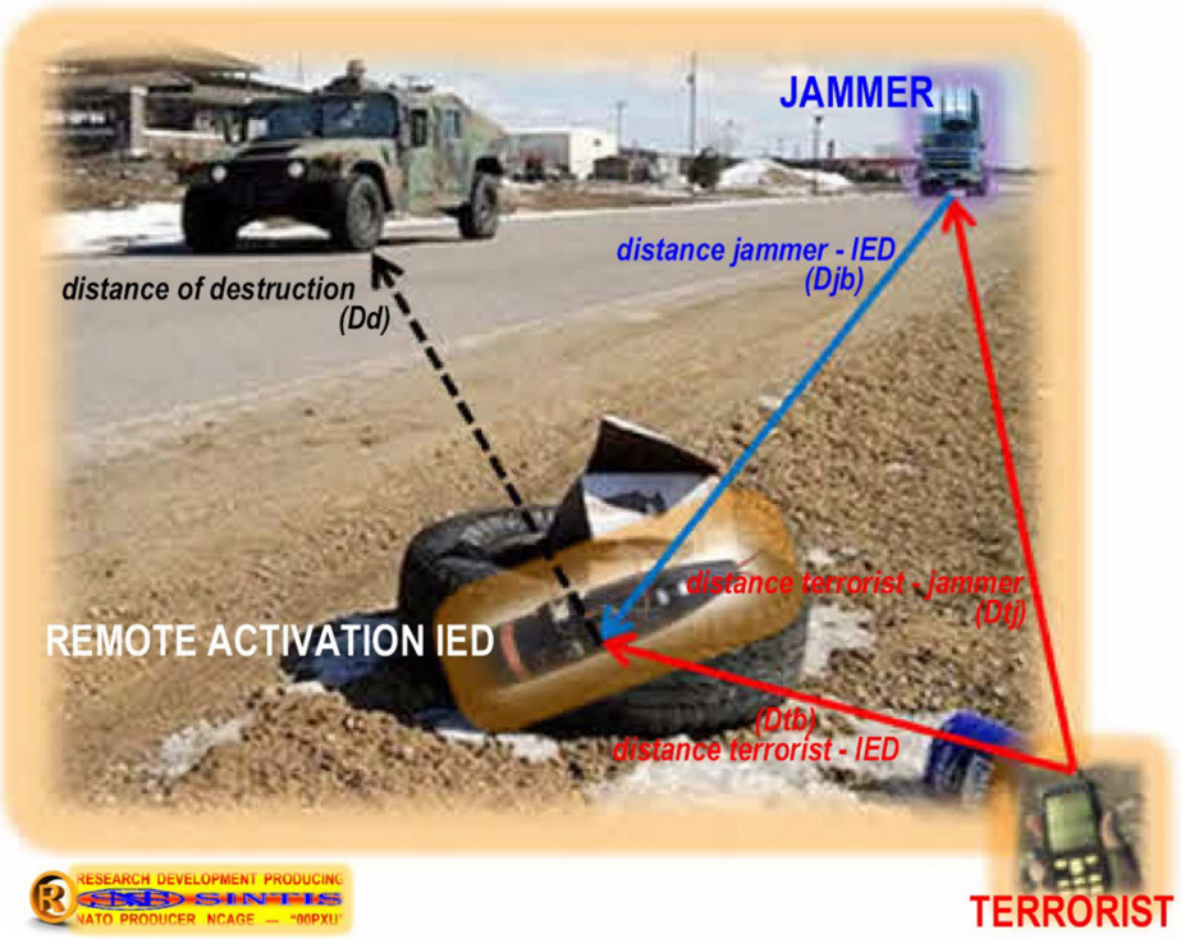

Fig.2.

Using for orientation the symbols shown in the figure and additionally:

D_{jbp} - 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**:

$$K_p = D_{jbp} / D_{tb}$$

If we assume that:

h - Coefficient of radio jamming efficiency;

n - Ratio interference/signal where **IED** is not activated;

P_b - Power of the terrorist transmitter;

P_j - Power of the jammer;

Δf_b - Frequency band of the **IED** receiver;

Δf_j - Frequency band of the jammer.

The protection coefficient would be:

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

It is obvious that the narrower the receiver band of the terrorist and the wider the spectrum of the jammer, the lower the protection coefficient would be under equivalent other conditions. It is clear also that the increase in protection coefficient is related to improving the interference quality "h", reducing the ratio of interference/signal "n" at the entrance to the **IED** receiver and of course — shrinking the jammer spectrum „Δf_j" and increasing its power "Pj".

To illustrate the seriousness of the requirements related to the jammer energy sources, without making detailed calculations, suitable example is the serial jammer **SINTIS-BJ™VIP300X2v4KV**. In order to ensure an average protection coefficient of **30%** in the frequency range from **2** to **6000 MHz**, the emitted power is approximately **3 000 W**. This emitted power, regarding the technically achievable efficiency coefficient in the powerful terminal 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.

With such discouraging conclusions, the idea of "intelligent" interference is often advocated. In this way the low power capacities are justified and an extremely commercial goal is chased. The truth is that "intelligent" interference fit for all cases does not exist - there is "optimal" interference according to specific criteria. Such is the interference according to patent **BG-65591-B1**.

Another popular claim for "intelligence" is the statement that the jammer "traces" the entire frequency spectrum, it registers the signal for activation of the **IED** and it immediately activates an interference signal on the detected frequency. In order to reveal the incapability of such "intelligence", it is enough to examine the operation of the remotely activated **IED**.

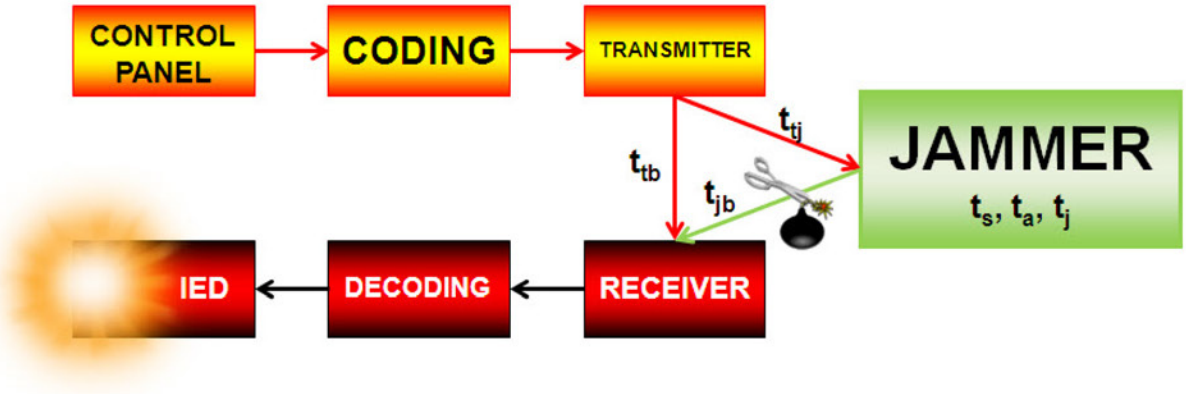

Fig.3.

The time necessary for obtaining the **IED** activating signal is t_{tb}.

The time necessary for obtaining the interference signal is a sum of the following times:

t_{tj}	-	time for obtaining the activating signal by the jammer;
t_s	-	time for registering the signal in the spectrum analysis;
t_a	-	time for analysis and danger distinction;
t_j	-	time for generating and emitting jamming signal;
t_{jb}	-	time for interference receiving by the receiver of the **IED**.

The condition for efficiency of the discussed method is:

$$t_{tb} \leq t_{tj} + t_s + t_a + t_j + t_{jb}$$

The physical incapability of the **„intelligent"** jamming through spectrum monitoring is obvious.

CONCLUSION:

Ensuring protection of remotely activated **IED** requires energy source proportional to the protection coefficient.

SOURCES:

1. Patent **BG-65591-B1**,
2. Catalog **"SINTIS Antiterrorist Jammers"**.