General Secretariat of the Council

Brussels, 16 July 2014

CM 3624/14

LIMITE

ENFOPOL

**COMMUNICATION**

**REQUEST FOR CONTRIBUTION**

| | |
|---|---|
| From: | Presidency |
| To: | Delegations |
| Subject: | The use of malicious means/methods to carry out acts of terrorism |

## 1. INTRODUCTION

A Europol analysis has revealed that a total of **794 terrorist attacks (including failed or thwarted attacks)**[1] have been carried out over the period 2010-2013 in EU countries. Most of them have been committed by means of explosives - a large majority of which being "low" explosives /limited offensive potential – or incendiary devices.

During the period under review, terrorist attacks have caused a total of **34** deaths. In three cases, however, the only victim was the perpetrator and as to a fourth case, an Islamic extremist was killed in a shoot-out with the French police.

[1] Data provided by Europol TE-SAT reports published in 2011, 2012, 2013 and 2014.

A lack of consistency has been noticed in the number and frequency of terrorist incidents and the amount of damage caused, especially with regard to human lives lost. This seems to confirm that terrorists deliberately choose to mount low-profile attacks.

Quite apart from their origin and the actual damage caused, low-profile attacks are intrinsically capable of multiplying their effects and spreading general terror when they are directed, with an unexpected and unforeseeable *modus operandi* and at a very low cost, against targets not considered to be vulnerable to violent actions.

In the eyes of terrorists, acts are more important than the material damage caused. Terrorists are in fact aware that any attack (or even the mere announcement of an attack) *per se* forces the intended target to live in terror, change his/her habits and lifestyle and direct efforts and resources towards self-protection.

It will be recalled in this connection what *Inspire* published in 2010 in its "special issue" dedicated to the so-called *Operation Haemorrhage* relating to the "1,000 cuts strategy": "*America has spent time, effort, and money to prevent a large scale attack such as 9-11 from ever occurring again (…). However, to bring down America we do not need to strike big. In such an environment of security phobia that is sweeping America, it is more feasible to stage smaller attacks that involve less players and less time to launch and thus we may circumvent the security barriers America worked so hard to erect. The strategy of attacking the enemy with smaller, but more frequent operations is what some may refer to as the strategy of a thousand cut. The aim is to bleed the enemy to death*".

This strategy has long been pursued by pro-insurrection anarchist groups who systematically resort to a particularly ingenious and effective terrorist technique: the use of ordinary mail to hide an improvised explosive or incendiary device that is activated by the victim, unaware of its presence, when opening a parcel/envelope.

In the course of time this modus operandi has increasingly characterised the pro-insurrection movement in Italy, i.e., the "Informal Anarchist Federation - F.A.I.", claiming responsibility for parcel bombs sent in 2003 to a number of representatives of institutions, including Europol, the Central European Bank, Eurojust and the European Parliament. In 2010 a similar device caused the death of George Vassilakis, a close aide to the Greek Interior Minister, Michalis Chrisochoidis.

Moreover, as mentioned in recent Europol analytical reports, these methods/means have been used to carry out terrorist attacks in a number of EU countries, including Corsica, Northern Ireland and Spain.[2]

It may be worth remembering that these methods are not necessarily associated with a specific political background, as was the case, for example, with attacks carried out by individuals suffering from psychoses or with deviant behaviour (*Theodore Kaczynski* in the US or the so-called *Italian Unabomber*, who hit indiscriminate targets in north-west Italy between 1993 and 2006).

## 2. SUBJECT OF THE ANALYSIS AND PROJECT GOALS AND OBJECTIVES

This project intends to identify best practices to prevent attacks perpetrated using malicious means/methods. This will be achieved by sharing investigative and/or intelligence experiences, by analysing monitoring and controlling procedures as well as the technical equipment used.

The idea behind this project is that the main characteristic of terrorist attacks carried out using malicious means and/or methods is the capability of spreading terror and insecurity due to the fact that perpetrators can launch attacks whose purpose is to surprise the intended targets.

The use of apparently harmless items makes these acts of terrorism particularly difficult to identify and neutralise beforehand.

This project mainly focuses on attacks carried out by means of the so-called *Victim-Operated I.E.D.*s, such as *booby traps*[3].

In this case, we are dealing with incendiary or explosive devices which, disguised as, or hidden inside, ordinary items, are unknowingly triggered by the presence or actions of the victim.

The same method can be applied to CBRN attacks, when a biological agent, like anthrax spores, concealed inside a package is opened by the unaware victim.

---

2 TE-SAT 2014, page 28

3 Booby-traps are "devices designed to cause the activation of an IED by an action of the victim. Also known as Victim-Operated Switches, these devices are designed, constructed or adapted to kill or injure when a person disturbs or approaches an apparently harmless object or performs an apparently safe act" (Europol Explosives Lexicon, Version 2, 5 March 2014).

Our analysis also covers attacks carried out using particularly malicious techniques such as *double bombs*, i.e. two explosive devices timed to go off within a short time one of the other. The goal is taking by surprise police officers and rescuers called to the scene for the first bomb alert, who will be injured by the second explosion, much more powerful than the first.

In view of the relevance of this type of threat, we think it is advisable to make a closer examination of the means and techniques employed to carry out similar attacks.

In this connection, it may be particularly interesting to specify which terrorist groups utilize, or advocate the use of, malicious means and methods, as well as investigate how the relevant technical know-how is disseminated for the preparation of attacks.

The Italian Presidency intends to contribute to a better understanding of this threat and explore possibilities for putting in place adequate measures to counter it by proactively sharing the experiences gained in Member States.

The aim is to take an integrated approach to malicious techniques/means in order to reinforce prevention through more effective synergy among all actors potentially involved, at both public and private levels, and increase potential targets' awareness.

When considering, for instance, the above cases of parcels being delivered containing a device or a dangerous biological agent, public and private services for the transportation and delivery of mail (air, land, marine, rail carriers and couriers) will be those initially and directly exposed to risk.

Being fully aware of the dangers involved, many of them have developed independent prevention and risk assessment systems which the Italian Presidency would like to evaluate in order to identify and share best practices.

Other useful elements of interest could be provided by public and private bodies that, having been targeted by terrorist attacks committed using malicious means/methods, have adopted specifically cautious procedures.

Finally, interaction with the following bodies will certainly contribute to the development of the project:

– Europol and its EU Bomb Data System containing technical information and intelligence on devices and CBRN threats provided by individual Member States;
– the Commission that recently produced a Communication on a new EU approach to detection and mitigation of CBRN-E risk[4];
– IntCen for a general analysis of the phenomenon;
– the EU Counter-Terrorism Coordinator could contribute to the identification of potential policy gaps.

## 3. PHASES OF THE PROJECT

- In order to highlight the different experiences acquired and security procedures established in each country, not only by national counter-terrorist authorities but also by public/private entities dealing with the matter, Member States are requested to fill in the enclosed questionnaire and send their replies to the e-mail address twpita14@dcpp.interno.it no later than 18 September 2014. We believe that identifying possible synergy between public and private sectors can make prevention and protection activities much more effective.
- Based on the knowledge acquired during this initial exploratory phase, we intend to further develop this aspect during an *ad hoc* seminar scheduled for 2-3 October 2014 in Rome. Representatives of Member States and relevant EU bodies and institutions will be invited to take part, as well as executives from private companies who have acquired significant experience having been the "targets" of attacks. Experts from other countries involved in efforts to combat terrorism will also attend.
- At the end of the Seminar, a final document will be drawn up to be submitted to the Council for consideration.

[4] 9550/14

## 4. QUESTIONNAIRE

| |
|---|
| 1. In recent years, did any terrorist incidents occur in your country using malicious means and/or techniques?<br><br>If so, please provide relevant statistical data (if available). |
| 2. In case incidents of this kind actually occurred, please provide a brief description of the most relevant cases and specify if the attacks were perpetrated by means of:<br><br>• Victim-operated switch (*i.e.*, incendiary/explosive parcels, letters, envelopes, packages and other similar devices);<br>• parcels, letters, envelopes, packages containing biological/radiological agents or toxic chemicals;<br>• "double bombs";<br>• Hoax Bomb (IED incident that involves a device fabricated to look like an IED and is intended to purposely simulate one in order to cause a response from law enforcement);<br>• CBRN contamination of food and/or beverages;<br>• others. |
| 3. What targets were aimed at?<br><br>• government officials/personalities and offices;<br>• persons and/or companies of the public/private sector;<br>• others. |
| 4. Can you indicate the origin of attacks committed by using these means/techniques? In particular, which of them and how many of them have been claimed by or can be attributed to:<br><br>• terrorist groups/individuals<br>• individuals suffering from psychoses or with deviant behaviour<br>• other (please, specify). |

| |
|---|
| 5. What is the role of police forces, in particular national counter-terrorist authorities, in preventing this kind of attacks?<br><br>What steps, if any, have been taken in your country to sensitize citizens to the procedures to be followed in case of suspicious envelopes or packages (for example by organizing periodic meetings or distributing booklets)? Does the same apply to categories particularly exposed to the risk of attacks committed by using the afore-mentioned means/techniques (for example air, land, marine, rail carrier employees or couriers delivering the mail)? If yes, what public or private bodies have taken such awareness raising initiatives? |
| 6. Based on your knowledge, are the radiological controls or, more generally, the control to detect potential risks inside parcels, envelopes, packages, etc. systematic in your country? In the affirmative, could you specify which methods and what equipment are used? |
| 7. Do the companies in charge of the collection/transportation/sorting out/delivery of mail conduct such controls? In the affirmative, please specify if they conduct them systematically, randomly, or on the basis of specific mail characteristics (dimensions of parcels/envelopes, type of addressees, carriers used, etc); |
| 8. Are there any interactions (formal or informal agreements, regulations) between public security authorities and public/private bodies involved in these activities? |