COUNCIL OF THE EUROPEAN UNION

Brussels, 3 March 2011

14306/04 EXT 1

ENFOPOL 155

PARTIAL DECLASSIFICATION

of document:	14306/04 RESTREINT UE
dated:	5 November 2004
new classification:	none
Subject:	Interim Report on the Evaluation of National Anti-Terrorist Arrangements

Delegations will find attached the partially declassified version of the above-mentioned document.

ANNEX

COUNCIL OF THE EUROPEAN UNION

Brussels, 5 November 2004

14306/04
EXT 1 (3.03.2011)

ENFOPOL 155

NOTE

from :	General Secretariat
to :	Working Party on Terrorism
Subject :	Interim Report on the Evaluation of National Anti-Terrorist Arrangements

The Declaration on Combating Terrorism (doc. 7906/04) calls on the Council to examine an interim report on the outcome of the process of peer evaluation of national arrangements in the fight against terrorism[1].

The attached provisional report based on the evaluation of 15 Member States, responds to this request[2], on the understanding that the final report will include the 10 other Member States.

[1] Council Decision of 28/29 November 2002, OJ L 349 of 24 December 2002.

[2] cf. doc. 9876/04 from the EU Counter-Terrorism Coordinator on provisional findings of the two peer evaluation mechanisms affecting the Union's fight against terrorism.

Preliminary Comment

1. The characteristics as well as the significance of the threat from international terrorism after 9/11 led most of EU Member States as a matter of urgency to review and/or amend their counter terrorist strategy or to adopt a position with a focus on

- enhanced exchange of information at both national and international level and
- crisis management, including the identification and reduction of vulnerabilities, and consequence management.

2. A wide range of situations exists within the EU because each Member State's counter-terrorism strategy is part of and depends on its own constitutional and legal framework.

Countering terrorism involves law enforcement bodies as well as intelligence agencies and in particular security services within the remit of their responsibilities. This is of particular importance where counter terrorism is mainly intelligence led (e.g. where the security services hold the lead). From a security service perspective, to prevent and disrupt terrorist activities is a top priority in addition to providing the law enforcement bodies with relevant intelligence to be turned into evidence where possible. Coordinating bodies/mechanisms are fully part of the counter terrorism machinery where set up.

In general terms, countries with longstanding experience in fighting domestic terrorism have developed a global counter-terrorism strategy based on a more or less "joined up approach" of the threat from international terrorism and improved the intelligence capacity accordingly.

In most countries, the Minister/Ministry for the Interior or the Minister/Ministry of Justice acts as coordinating Minister/Ministry.

3. Interim Report

The evaluation reports identified good practices in all countries. However, they have to be considered within the local context. This means that, according to different laws and structures, what is good practice in one particular country cannot be fully considered by all countries or cannot be "exported" as such. The interim report refers to specific national arrangements only when needed in terms of best practice, but does not highlight all good practices in all Member States.

Key areas in terms of improvements and related recommendations are :

3.1 Coordination between Law Enforcement Bodies and Security Services
3.2 Security services (information sharing, special techniques for intelligence gathering and recruitment and radicalisation processes)
3.3. Intelligence as Evidence in Court
3.4. Preparedness and contingency plans to deal with terrorist threats CBRN issues
3.6. Public Communication/Information
3.7. Support to moderate Islam
3.8. Europol
4. Other points

3.1 Coordination between Law Enforcement Bodies and Security Services

The exchange of information as well as information sharing at national level is generally accepted as a core element. However, security services and law enforcement agencies are basically operating in two different spheres that aim, respectively, to prevent and disrupt terrorist activities and to support prosecution and provide evidence to the courts. This does not mean that law enforcement bodies do not disrupt terrorist acts when appropriate legal provisions exist and that security services do not provide the police with intelligence. Investigations backed up by intelligence are an effective tool and criminal investigations provide useful focus for intelligence activities, where the police and the security service act in a coordinated manner. **NOT DECLASSIFIED** There is no conflict between the intelligence dimension and the criminal investigation dimension in countering terrorism. In addition to factual channels and partnerships, some Member States have permanent arrangements to ensure that information is shared in terms of day-to-day operational coordination and that the overall response is effectively co-ordinated. From that perspective, the creation **NOT DECLASSIFIED** in the immediate aftermath of the terrorist attacks of 11 March 2004 highlights a posteriori the crucial role of a permanent technical co-ordinating body involving in particular all law enforcement bodies and security services.

A co-ordinating body that promotes unity in diversity is the appropriate forum

- to ensure that the relevant information is provided to all key players,
- to ensure that a common reflection is made as well as to assist each other
- and to promote and implement a common counter terrorism policy on the basis of a common ("joined up") approach to terrorism.

Recommendation 1

In order to ensure sharing and exchange of information, all Member States, should set up a permanent national body. NOT DECLASSIFIED is a valuable source of inspiration in this respect: it has responsibility for day-to-day coordination on operational matters. Law enforcement bodies and security services should be part of this coordinating body.

3.2 Security services

Sharing of information

In order to detect and identify at a very early stage terrorist networks as well as their plans and activities, access to law enforcement databases and other relevant databases to cross information from various sources (**NOT DECLASSIFIED**) including administrative databases is crucial.

Recommendation 2

All Member States should have in place legislation allowing security services to have access to law enforcement databases and other relevant databases while respecting data protection requirements.

Special Techniques

In some Member States, security services have no appropriate legal basis enabling the use of special techniques for intelligence gathering.

Recommendation 3

Member States should provide security services with appropriate legal basis for the use of special techniques for intelligence gathering.

Recruitment and radicalisation processes

Recruitment and radicalisation processes are also key points and the work of security services in these fields is invaluable, in particular when carried out in close partnership with law enforcement bodies.

Recommendation 4
Member States should focus on recruitment and radicalisation processes and should undertake national analysis/assessments annually (on the basis of a common template) with a view to identifying key issues as well as guidelines NOT DECLASSIFIED

NOT DECLASSIFIED

Recommendation 5
The EU should continue to discuss the exchange of information on suspect persons and potential perpetrators of terrorist acts with a view to understanding processes and agreeing on a common approach. NOT DECLASSIFIED

3.3 Intelligence as Evidence in Court

In most Member States intelligence information and in particular covertly obtained intelligence are not admissible as such for use in judicial procedures.

NOT DECLASSIFIED However, intelligence that can be made admissible in court means an enhanced capacity to deal with terrorist cases at a very early stage. This issue, which does not apparently affect all EU Member States in the same way, is under examination in some Member States.

The use of intelligence as evidence in court implies the need to develop a coherent set of laws and procedures to deal with the interaction of intelligence information and the judicial system (in particular through preventive detention) while respecting fundamental rights. This interaction must therefore ensure (through burden of proof standards, procedural guarantees, laws on defence rights, and judicial oversight) that civil liberties are not infringed upon. Another key point relates to the disclosure of information to the judge and the defence. **NOT DECLASSIFIED**

Recommendation 6

The use of intelligence as evidence in court is primarily a national issue to be dealt with by national authorities. However, in order to reinforce the capacity to prevent and disrupt terrorist activities, the use of intelligence as evidence could undoubtedly have a positive impact. Member States are requested to pay further attention to this issue and to take any necessary steps where needed.

Due to the importance of the question of the rule of law and the rights of defence, there should be a specific evaluation of this subject at EU level with a view to identifying a coordinated approach. Such an evaluation could build on the current works in some Member States as well as in other fora (e.g. the G8).

3.4 Preparedness and contingency plans to deal with terrorist threats

Some Member States have established (or are in the process of establishing) specific plans for dealing with disasters, terrorist threats and related warnings in particular.

Recommendation 7

All Member States should consider setting up systems and plans with a view to dealing with terrorist threats. Such plans should address the interoperability of capacities to help other Member States to deal with major terrorist attacks. The objective could be the establishment at European NOT DECLASSIFIED plan (NOT DECLASSIFIED with its flexibility of deployment, which would enable it to be activated in all or in part of the European Union and/or using all or some of its components, depending on the nature of the threat.

In order to respond to a terrorist case including a CBRN event, specific consequence management programmes have sometimes been established with a view to testing in particular the capacity of key players to act together, communication networks and procedures. In this field, it is considered that exercises on the ground are crucial for handling a major disaster.

Recommendation 8

Each Member State should have a national programme including exercises (domestic and cross border) and related assessments. In addition, Member States should have a permanently updated list of national critical infrastructures/sectors or key assets and related protective security measures to be implemented where a major terrorist event occurs including in particular a CBRN attack. Moreover, to be able in case of threats or terrorist attacks to rapidly exchange early warnings, to exchange further information and to coordinate measures with other Member States. Member States should have a national permanent crisis centre, which is linked to all national security and emergency related agencies.

3.5 Terrorist Threat Analysis

Threat assessment is a delicate task that implies actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets in order to take appropriate protective actions/measures and procedures. In terms of readiness posture or response, this means to prompt the implementation of an appropriate set of protective measures in order to reduce vulnerabilities or increase ability to respond to the terrorist case. Consequently, threat assessment aims at disseminating relevant and timely information regarding the risk of terrorist acts to government ministries/departments as well as to key persons both in the public and private sectors and population.

Most Member States establish threat assessments (with a dimension that includes the threat from international terrorism) with various inputs from law enforcement bodies and intelligence agencies that sometimes also deal with separate threat assessments. Consequently, the final threat assessment depends on such contributions and this means that each provider controls the information that is made available. In order to deal with accurate information in a timely manner, a remarkable innovation in this field was the creation of **NOT DECLASSIFIED**

Recommendation 9

As an example of best practice, Member States should pay attention NOT DECLASSIFIED in terms of methodology (working methods) and final products and should establish permanently updated threat assessments on international terrorism (NOT DECLASSIFIED). Additionally Members States should establish specific threat assessments on CBRN issues.

3.6. Public Communication/Information

In connection with threat assessments and preparedness/civil protection programmes, public information is of a particular importance but it is a very delicate task based on a balanced approach (warning and not threatening). This applies to current terrorist threat evaluations, the way to react to a terrorist incident as well as to the initiatives that are taken by governmental bodies in order to improve the fight against terrorism and to protect the population. Some countries already took measures in this area and some others are improving public communication. Information of the public should also target private companies (out of the scope of national critical infrastructure and national assets) in terms of advice.

Due to the particular scale and nature of the threat as demonstrated in Madrid last March, the public expects more and more information from governments. This applies to CBRN threats in particular.

Recommendation 10

Member States should develop an appropriate strategy in the field of public communication with a focus on "awareness", information related to the terrorist threat and consequence management.

3.7 NOT DECLASSIFIED

3.8 Europol

Basically, bilateral police cooperation is considered as the most efficient tool and this probably affects cooperation with Europol, which is considered, on the one hand, as necessary but has to be seriously boosted on the other hand. Law enforcement bodies generally support a more in depth cooperation with Europol (and some Member States are active partners) NOT DECLASSIFIED

Concerning law enforcement bodies, the situation varies from one country to another. The Europol purpose is to deal with "living information" but in terms of ongoing investigations, the police often cannot provide information without the permission of a prosecutor. As a consequence of the evaluation in this field, NOT DECLASSIFIED is considering the creation of a working group that would consist of members of the Police, judicial authorities and Europol. The aim is to identify legal, structural and de facto obstacles to an enhanced cooperation with Europol and to propose solutions including legislative ones.

Recommendation 12

Member States could consider the creation of a working group consisting of law enforcement authorities, judicial authorities and Europol members with a view to identifying and overcoming obstacles to enhanced information sharing.

Concerning the exchange of information between member States' security services and Europol, it is up to each Member State to decide what kind of information can be transferred to Europol **NOT DECLASSIFIED**

4. The evaluation visits raised other concerns as follows:

- The aim of the **NOT DECLASSIFIED** working party, which brings together magistrates, police force and intelligence service, is to identify ways of enabling the two sides to exchange information, particularly of an operational nature, more effectively. This cooperation as well as common police station along borders and the joint investigative teams could provide other Member States with methodology (best practice).

  Member States should pay attention to all aspects of the NOT DECLASSIFIED operational counter terrorist cooperation.

- The fight against the financing of terrorism has become an important topic. However, the identification data on the UN (and other) lists distributed to freeze assets of suspected individuals/organisations, is sometimes incomplete and thus difficult to manage when it comes to ensuring that a name on a list is matching with an identity.

  In this field security services should help identification and a list of persons and organisations whose funds/assets are frozen regardless the legal regime at the origin of the decision should be systematically disseminated.

- To ensure uniform prosecution guidelines based on broadest possible experience some Member States have given exclusive responsibility for the prosecution of terrorist cases to special prosecution offices and in some cases coordination is made at central level.

  National coordination of judicial authorities should be promoted including systematic debriefings from judicial authorities to law enforcement bodies and security services.

- Counter terrorism aspects of border control (possibly with regard to the European Border Agency and illegal immigration[3]) should be developed.

  Border control should include a counter terrorism dimension in terms of intelligence gathering and systematic intelligence sharing with law enforcement bodies and security services.

- In order to develop/enhance a common approach to the threat from international terrorism (International Jihad), it would be relevant to systematically disseminate within the EU analysis and cases study including terrorist acts in third countries. It would also be useful to provide Member States with debriefings about security measures adopted for important events (G8 summit, Olympic Games, Football Cup, etc).

  Terrorist attacks as well as security measures for major events should be systematically analysed and analysis disseminated.

[3] On 18 March 2004, the Regulation (EC) No 491/ 2004 of the European Parliament and the Council Decision of 10 March 2004 establishing a Programme for Financial and Technical Assistance to Third Countries in the Areas of Migration and Asylum (AENEAS) was published (cf. OJ L 080 , 18/03/2004 P. 0001 – 0005).

- As a general idea, the flexible exchanges of staff at national level between all bodies and at EU level between Member States' respective agencies promote mutual understanding.

  Member States are invited to facilitate exchange of staff at national and EU level with a view to enhancing coordination and cooperation especially in cases where formal structures are not applicable.

- Training at European level (CEPOL) in terms of mutual knowledge of existing systems, best practices, etc should be developed.

  The governing board of CEPOL should take into account the EU priorities in its working programme and develop training courses on terrorism with the participation of Europol.

- EU Member States' intervention units could link up to form a European network in the area of training, best practices, interoperability of equipment, etc.