

Interim Report on the Evaluation of National Anti-Terrorist Arrangements

The Declaration on Combating Terrorism¹ 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.

The attached provisional report based on the evaluation of 15 Member States, responds to this request², on the understanding that the final report will include the 10 other Member States.

¹ Doc. 7906/04

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.

1. Foreword

- 1.1.** On 20 September 2001, the JHA-Council¹ "in the light of the attacks in the United States of 11 September 2001", decided on a peer assessment of national anti-terrorist arrangements on the basis of considerations of a legislative (...), administrative and technical nature.
- 1.2.** At its meeting of 23/24 January 2003, the Article 36 Committee agreed to the subject of the first evaluation: To assess the exchange of information in all domains relating to terrorist activities between law enforcement and intelligence services and all other bodies dealing with various aspects of terrorism, including the co-ordination among those services and between these services and their counterparts in the other Member States on how best to exploit this information. The evaluation should mainly focus on information and co-ordination concerning Islamic extremist terrorist groups and their activities².
- 1.3.** The evaluation reports identified good practices in all Member States. However, they have to be considered within the national context. This means that, according to different laws and structures, a good practice in one particular Member State cannot be considered in full by other Member States or cannot be exported as such to other Member States. Consequently, the interim report does not mention all national good practices.
- 1.4.** National good practices with a significance for all or most other Member States were identified as best practices and dealt with as recommendations in this report.
- 1.5.** Some recommendations may presuppose amendments or adjustments of existing legal or structural arrangements.

¹ Doc. 12156/01 JAI 99 of 25 September 2001

² Cf doc. 5838/03 LIMITE ENFOPOL 8

1.6. Recommendations aim at providing added value and new instruments to law enforcement bodies and security services with a view to taking into account the characteristics and significance of the threat from international terrorism. The interim report suggests neither a uniform implementation in Member States nor a common position as such but it recommends similar approaches. From that perspective, strengthened national anti-terrorist arrangements in each Member State directly or indirectly enhance the security of the EU as a whole. And vice versa¹.

1.7. In most cases, recommendations are issues to be dealt with by national authorities.

2. Preamble

2.1. The characteristics as well as the significance of the threat from international terrorism after 11 September 2001 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.

2.2. 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 framework². Other variables are historical background and respective perceptions of the terrorist threat.

Countering terrorism involves law enforcement bodies and security services as well as intelligence agencies within the remit of their responsibilities.

¹ Cf doc. 14292/04 CONCL 3.

² Cf doc. 5339/1/03 REV 1 LIMITE ENFOPOL 2

In general terms, Member States 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.

3. Interim Report

The report is divided in two parts, the first deals with formal recommendations referring to the field for evaluation as mentioned above, the second part includes additional suggestions on the basis of the evaluation reports.

Key areas in terms of improvements and related recommendations are:

- 3.1.** Coordination between Law Enforcement Bodies and Security Services at National Level
- 3.2.** Security services
 - 3.2.1** Information Sharing
 - 3.2.2** Intelligence as Evidence
 - 3.2.3** Special Techniques
 - 3.2.4** Recruitment and Radicalisation Processes
 - 3.2.5** Suspect Persons and Potential Perpetrators
- 3.3.** Europol Cooperation with Law Enforcement and Security Services
- 3.4.** Border Control
- 3.5.** Terrorism Threat Analysis
- 3.6.** Staff Exchange
- 3.7.** CEPOL
- 3.8.** Prosecution at National Level
- 4.** Additional Suggestions
 - 4.1.** Support to Moderate Islam
 - 4.2.** Contingency Plans
 - 4.3.** Consequent Management Programme
 - 4.4.** Public Communication/Information

3.1. Coordination between Law Enforcement Bodies and Security Services

The exchange of information as well as information sharing at national and international level is generally accepted as a core element of anti-terrorist efforts. 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.

In addition to factual channels and bilateral partnerships, some Member States have permanent arrangements at national level to ensure that information is shared in terms of day-to-day operational coordination and that the overall response is effectively co-ordinated.

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

- to ensure that the relevant information is made available and timely and properly provided to all key players,
- to ensure that a common attitude exists to think as well as assist each other,
- to promote and implement a common counter terrorism policy on the basis of a joined up approach to terrorism while respecting the powers, tasks and goals of all players.

Coordinating bodies/mechanisms are fully part of the counter terrorism machinery where set up.

Recommendation 1

Permanent national arrangements to ensure that all competent authorities have access to the information and intelligence are needed.

For that purpose, Member States should set up a national coordination body/ mechanism responsible for the day-to-day exchange of information in the field of prevention, disruption and investigation that should involve all security services and law enforcement agencies engaged in counter-terrorism.

3.2. Security services**3.2.1 Information Sharing**

International terrorism is a threat to national security. To detect, identify and facilitate profiling at a very early stage terrorists, terrorist networks and individuals supporting them as well as their plans and activities, access to law enforcement and other relevant administrative or government agencies databases (e.g. police and border guards, social security, employment office) to cross information from various sources (data mining process) is crucial in particular in the course of the pre-investigative phase.

Recommendation 2

In order to detect, identify and profile terrorists, terrorist networks and individuals supporting them as well as their plans and activities at a very early stage, Member States should have in place a procedure based on legislation/regulation allowing security services to have access to law enforcement and relevant government agencies/bodies' databases. This access would be strictly restricted to the need to know and should respect data protection requirements.

3.2.2 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.

In order not to damage national security, Security services are reluctant to disclose elements that may lead to the identification of sources and the disclosure of certain special techniques. Another key point relates to the disclosure of information to the judge and the defence. This may imply that the security service's members will have personally to testify in court as privileged witnesses in the framework of an open or closed session, etc. However, intelligence that can be made admissible to court means an enhanced capacity to reinforce criminal investigations and prosecution. 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 while respecting fundamental rights. In this area, the response of the state should be proportionate to the threat and a reasonable balance should be maintained between the civil rights of the individual and the rights and obligations of the state to protect citizens.

Recommendation 3

The use of intelligence as evidence in court is primarily an 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 this issue with regard to fundamental rights, there should be a specific evaluation of this subject at EU level with a view to identifying best practices and national approaches. Such an evaluation could build on the current works in some Member States as well as in other fora (e.g. the G8).

3.2.3 Special Techniques

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

Recommendation 4

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

3.2.4 Recruitment and Radicalisation Processes

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

Recommendation 5

Member States should focus on the processes behind radicalisation and recruitment to terrorism as well as activity after recruitment. They should undertake and exchange national assessments of the key issues behind these processes. This should take into account ongoing works in other fora and should be done in connection with third countries' contributions.

3.2.5 Suspect Persons and Potential Perpetrators

In the area of exchange of information, attention should be paid to:

- persons to be deported, suspect persons that have been trained and suspect persons travelling to or coming from sensitive regions
- identification/detection at an early stage of potential perpetrators in connection with recruitment matters.

Recommendation 6

The security services should deepen and widen the exchange of information on suspect persons and potential perpetrators of terrorist acts.

Keeping in mind ongoing works within the G8, the EU should continue to discuss how this exchange can be improved with a view to agreeing on a common approach.

3.3. Europol Cooperation with Law Enforcement and Security Services

Basically, bilateral police cooperation is considered as the most efficient tool and this probably affects cooperation with Europol. Law enforcement bodies generally support a more in depth cooperation with Europol (and some Member States are active partners) but security services are reluctant to provide information.

Concerning law enforcement bodies, the situation varies from one country to another. In addition to longer-term analysis and assessment, 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, France 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 7

Member States should support and make best use of Europol's existing terrorism analytical workfiles, while optimising their bilateral intelligence exchanges.

Member States should examine whether they are making optimum use of the various multilateral mechanisms available for exchanging information and intelligence, including Europol. In order to remedy any shortcomings, Member States should consider the creation of an ad hoc working group at national level involving representatives of the competent authorities as well as Europol.

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 without endangering investigations and intelligence gathering in the long run. The establishment of a security service dimension within SitCen and the involvement of the Counter Terrorism Group (CTG) will have a positive impact in this field.

3.4. Border Control

Counter terrorism aspects of border control (possibly with regard to the European Border Agency and illegal immigration) are essential.

Recommendation 8

Counter terrorism aspects of border control should be developed and include an intelligence dimension in terms of gathering and systematically intelligence sharing with law enforcement bodies and security services.

3.5. Terrorist Threat Analysis

Threat assessment is a delicate task that implies information in order to define an appropriate strategy and procedures accordingly.

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. The finalised threat assessment depends on such contributions and this means that each provider controls the information that is made available.

Recommendation 9

Assessment of the threat is a key component of the risk analysis process. Member States should ensure that national arrangements allow a coordinated assessment of the terrorist threat including CBRN issues, drawing on all available sources. Assessments should be disseminated in a timely fashion to national stakeholders responsible for activating specific or general protective measures, with a view to reducing the risk.

3.6. Exchange of Staff

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.

Recommendation 10

Member States should 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.

3.7. CEPOL

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

Recommendation 11

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.

3.8. Prosecution at National Level

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.

Recommendation 12

Where appropriate national coordination of judicial authorities (prosecution) should be promoted as well as systematic exchange of information from judicial authorities to law enforcement bodies and security services.

4. Additional Suggestions

4.1. Support to Moderate Islam

In Member States that consider being at risk and whose population includes in particular a Muslim community, support to moderate Islam (and the promotion of intercultural dialogue) is seen as a fundamental issue and as a part of a national counter terrorism programme. Addressing the underlying causes of terrorism and preventing the next generation of terrorists from emerging are other issues in this field.

Member States should exchange experiences and good practices in the area of support to moderate Islam (promoting integration, multicultural dialogue).

4.2. 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 and in particular in the area of terrorist threats and related warnings.

All Member States should consider setting up systems and plans with a view to dealing with terrorist threats.

4.3. Consequence Management Programme

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, exercises on the ground in addition to classroom exercises are crucial for handling a major disaster.

In the field of consequence management programmes, each Member State should have a specific consequence management preparedness and training programme (domestic and cross border) and related assessments. A crucial dimension in case of threats or terrorist attacks is to rapidly exchange early warnings and further information as well as to coordinate measures.

To determine readiness posture or response, 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, Member States should have a national programme. It should consist of 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.

Member States should operate national permanent crisis/situation arrangements, which is linked to all national security and emergency related agencies. This recommendation is to be examined in connection with EU existing policy and bodies¹.

4.4. Public Communication/Information

In connection with threat assessments and preparedness/civil protection programmes, public information is of a particular importance but it is a complex topic and a very delicate task based on a balanced approach to avoid creating public paranoia or panic. There is also the risk of stirring up hostility to minorities assumed to be potential sources of threat.

Public information 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.

¹ Cf in particular doc. 14292/04 CONCL 3, doc. 13941/1/04 REV 1 (widened CBRN Programme) and doc. 14422/04 (Draft Council conclusions on Prevention, Preparedness and Response to terrorist attacks), the relevant European Commission's Communications to the Council and to the European Parliament

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.

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. A consistent approach between Member States would be helpful in this domain.

Dates of the visits**Document numbers:**

France:	24-27 June 2003, 8 September 2003	10373/04 ENF 71
Spain:	15-17 September 2003	11348/04 ENF 95 + REV 1 + ADD 1 REV 1 + ADD 2
Portugal:	18-19 September 2003	11352/04 ENF 96+ REV 1 + ADD 1 REV 1 + ADD 2 REV 1
Belgium:	22-26 September 2003	9216/04 ENF 47
Greece:	14-16 October 2003	12633/04 ENF 118 + ADD 1 + ADD 2
Denmark:	10-12 November 2003	11078/04 ENF 91 + ADD 1 + ADD 2
Ireland:	13-14 November 2003	9770/04 ENF 55
Germany:	08-12 Dec 2003, 09-13 Feb 2004	13946/04 ENF 147 + ADD 1 + ADD 2
Luxembourg:	12-13 January 2004	12597/04 ENF 116 + REV 1 + ADD 1 REV 1 + ADD 2
Austria:	14-16 January 2004	13944/04 ENF 146 + ADD 1 + ADD 2
Netherlands:	02-04 February 2004	12247/04 ENF 113 + ADD 1 ADD 2 + ADD 3
Sweden:	24-27 February 2004	13510/04 ENF 138 + ADD 1 + ADD 2
Finland:	09-12 March 2004	13927/04 ENF 144 + ADD 1 + ADD 2
United Kingdom:	17-19 May 2004	12471/04 ENF 161 + ADD 1 + ADD 2
Italy:	28-30 April 2004	12716/04 ENF 124 + ADD1REV1 + ADD 2 +ADD 2 COR 1