**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 22 October 2010

**13153/2/10
REV 2**

**ENFOPOL 237
PROCIV 102
PARLNAT 78**

NOTE

from:	General Secretariat
to:	COREPER
No. prev. doc.:	13154/10 ENFOPOL 238 PROCIV 103
	8568/10 ENFOPOL 98 PROCIV 47 + COR 1
	6090/2/10 REV 2 ENFOPOL 38 PROCIV 15 + COR 1
	6090/10 ENFOPOL 38 PROCIV 15 RESTREINT UE
Subject:	Information on the content and results of evaluations

The current document sets out the final report of the second round of peer evaluation in the area of counter-terrorism concerning "Preparedness and consequence management in the event of a terrorist attack".

COREPER endorsed the transmission of the report to the European Parliament and national parliaments at its meeting on 22 September 2010.

I   BACKGROUND

1. Following the attacks in the United States on 11 September 2001, the Council of 20 September 2001 launched an assessment of national anti-terrorist arrangements through a peer evaluation, taking into account considerations of a legislative, administrative and technical nature. The main objective was to identify and understand the mechanisms in existence in each of the 27 MS.

2. The evaluation visits were carried out between 2003 and 2005 and resulted in the final report[1] which sets out recommendations addressed to all Member States and to individual Member States for further improvement of their national anti-terrorist arrangements. Moreover, best practices were identified and an overview of the counter-terrorism arrangements in all the Member States was given. Implementation of these recommendations was assessed by the Working Party on Terrorism in 2006[2] and a follow-up report on the implementation of recommendations by the Council of the EU on counter-terrorism measures in the Member States was finalised in 2007[3].

---

[1] 12168/3/05 REV 3 ENFOPOL 109
[2] 95 % of these general recommendations were implemented
[3] 5356/2/07 REV 2 ENFOPOL 30

3. The peer evaluation as an exercise contributed significantly to the reform of counter-terrorism arrangements in the Member States. As a result of this common approach between the Member States developing in the same direction, the EU's collective capacity in this area has been strengthened.

Following these positive results, Member States agreed to conduct a second round of peer evaluation as would serve to continue the implementation of the counter-terrorism strategy in the EU.

II BASIS FOR THE PEER EVALUATION

4. Nine potential topics for the second round, as suggested by the Council Secretariat, the Member States and the Commission, included video surveillance, terrorism financing and countering radicalisation and recruitment. The discussion showed that the vast majority of the Member States (twenty-three) saw a need to further develop the EU's capacity to react appropriately to a possible terrorist attack. As a result, preparedness and consequence management[4] was accepted as the central topic for the second round of peer evaluation.

5. Up to then, national crisis-management arrangements had not been the subject of either in-depth evaluation or policy consideration at EU level. The second round of peer evaluation was to concentrate on those arrangements. It was essential to prevent any duplication of ongoing work as regards civil protection and especially the protection of critical infrastructures which was a broader subject than the protection of soft targets and is being dealt with by a specific working party. That would promote a coherent and compatible approach in the Member States and lay the foundation for a coordinated response to a terrorist attack if more than one Member State were to be targeted.

---

[4]   7188/07 ENFOPOL 39 RESTREINT UE

6.	In May 2007 the Article 36 Committee approved the subject for the second round and designated the Working Party on Terrorism as the working party competent to continue the proceedings, under Articles 2, 3, 4, 5 and 8 of the Council Decision of 28 November 2002[5].

## III	EVALUATION PROCESS

7.	The second round was divided into four phases: the questionnaire, the visits to the countries, the national reports and the final report.

8.	Once consensus had been reached on the general topic it was necessary to define more specific sub-topics, on which the questions would be drawn up. It was considered important to limit the number of sub-topics to a maximum of three, to ensure a realistic and effective exercise.

It was also essential to guarantee the coherence and complementarity of those three sub-topics with a view, in particular, to ensuring that the same evaluation teams had the capabilities and expertise to deal with all the matters.

9.	For those reasons the questionnaire was divided into three sections:
	–	Structures and organisational framework of national crisis centres;
	–	Training/exercises to test national crisis centres and communication systems in the event of a terrorist attack;
	–	Soft targets.

10.	Those three sections were covered by various specific questions, which were intended to collect material for the evaluation visits and the future final report. The questionnaire was sent to the Member States on 1 August 2007 for completion and suggestions. Some of the Member States' suggestions were included in the final version which was endorsed by the Terrorism Working Party on 16 October 2007.

---

[5]	Decision 2002/996/JHA, OJ L 349, 24.12.2002, p. 1.

11. Replies to the questionnaires were used as the basis for meetings and questions raised during the visits to Member States. The Member States, EUROPOL and the Commission were asked to designate experts to make up the evaluation teams. Each expert team normally comprised one expert from the General Secretariat, two experts from Member States, one expert from EUROPOL and one expert from the Commission.

12. These visits lasting an average of three days were prepared by Member States in cooperation with the Council Secretariat. The evaluated Member States were in charge of selecting the institutions and individuals most capable of answering the expert delegations' questions and clarifying doubts, the objective being to obtain a clearer picture of the crisis and consequence management model in place in the country.

13. The order of the visits is set out in annex 1.

14. After each evaluation visit, the experts were asked to prepare a draft report to be sent to the Council General Secretariat. All these draft reports, the replies to the questionnaire and all the material provided by the country[6] were used as sources of information for drafting the national/country reports. The national/country reports were submitted to the relevant Member State for comments. The Member State gave its opinion on the report normally within six weeks and the report was amended where the Member State deemed it appropriate. The national/country reports are set out in addenda 1 to 27 to the current document.

15. The progress of the exercise was presented at several meetings of the TWP and an interim report, set out in document 12287/09 ENFOPOL 199, was delivered in response to a request by the Swedish Presidency.

---

[6] PowerPoint slides, presentations, brochures, plans, etc.

IV MAIN FINDINGS

16. During the visits, numerous differences were found between the systems to be prepared to manage the consequences of a terrorist incident, although they all share the same concern. The systems are adapted to the size, geography and population distribution in the country as well as to the perception of the threat. This threat perception varies from MS to MS depending on historical, political or legal reasons and borders, the social network and the relations with risk countries. The collection of best practices, therefore, shows a multifaceted approach to the topic.

17. The main influencing factor is the legal framework for the different political models among the 27 MS, a fact also reflected in the crisis management. Some countries have very active political structures which intervene down to the operational decision-making level, and in others the political authorities play a more strategic role, establishing the main objectives to be achieved. The first case results in a more or less bureaucratic model, sometimes extremely dependent on a solid communication system, the second distances the political authority from the most important decisions (such as using military forces to reinforce civilian structures).

18. Guidance for and political coordination of the forces and structures involved in crisis management may be directly under the prime minister's office, under different ministries or under one single ministry which is generally the Ministry of Interior or the Ministry of Defence. The results of these different kinds of management models, more or less centralised, can be equally efficient if the coordination process is not too complex or theoretical. In all cases, the first responder teams react immediately, initiating all the normal procedures to deal with a terrorist attack and implementing the emergency plans, when possible or available.

19. Different MS have specific plans to deal with emergencies, of which terrorism is just one. The different plans can be combined and measures across the board can be adopted depending on the needs and the circumstances. These plans sometimes create too rigid a model which can create some difficulties when it comes to adapting the pre-established measure to the actual situation. In other MS there are no specific plans, just one general plan that operates as an "umbrella model" and deals with the consequences of a terrorist attack in the same way as any other crisis.

In this last system the general plan relies on the measures and the organisation model of the various police and emergency authorities, making it more flexible but more difficult to implement.

20. In a few MS a crisis is managed at local level to begin with and only in the case of lack of resources is management of the situation transferred to regional or national level, the so-called principle of subsidiarity. In other MS, crisis management is seen as a national issue and as soon as an emergency is declared the central level assumes leadership. This is often related to the resources available in the country and how they are distributed over national territory. A centralised approach is frequently a country's way of compensating for limited crisis-management resources.

21. Another clear difference between the MS relates to the Crisis Centre. In some cases the Crisis Centre is a permanent structure, with its own premises and staff, playing an important daily role in the crisis management system. In other cases the crisis is managed by an ad hoc committee composed of the main authorities concerned, meeting only in case of need. Finally, there is a third model in some MS, where the Crisis Centre is a physical structure fully equipped for the management of an emergency situation (meeting rooms, communications, IT systems, etc) which does not operate on a day-to-day basis but is only activated to face a particular event (state visits, major sports events, natural disasters, among others).

22. Concerning the training for testing the national crisis centre or arrangements and the communication system in the event of a terrorist attack, different situations were found. All MS organise exercises but in some cases they are only table top exercises which do not involve all the forces, sometimes not even including the first line responders. In some cases the number of exercises in cooperation with neighbouring countries (MS or not) are not sufficient.

23. During the visits, the teams of experts noted that the countries were at very different stages in their transition from analog networks which were sometimes unencrypted to encrypted digital networks. However, no country was without at least a plan for such a move. Some have already completed their full national encrypted digital network or are at the final stage in doing so.

24. With regard to soft targets, a significant number of MS assimilate them to critical infrastructures, adopting the same security approach to both. In some other MS soft targets are seen and dealt with as an autonomous issue. Among those, the soft target issue can be within the competence of a national authority or competence may be delegated to local level. This responsibility includes not only identifying the soft targets but also proposing the relevant security measures and procedures.

V   RESULTS

25. From a national standpoint, the peer evaluation enabled Member States to examine and reassess the structures in existence in their countries. The considerations emerging at the time of answering the questionnaire and in the second phase, during the evaluation visit, brought the various national structures involved in crisis management closer and strengthened the relationship between them. They also made it possible to clarify the competences of each of the bodies involved and to identify failings in the system. In the same way, meetings with the teams of experts in some Member States gave different bodies the opportunity to sit around the same table, thus reinforcing personal and institutional contact which is so important in times of crisis.

26. Each country report sets out specific recommendations which take national legal and political frameworks into consideration and addresses the model in place. These specific recommendations, backed up by procedures already in existence in some other MS, were intended to improve the current mechanisms by suggesting measures to be adopted. They were also intended to give the national authorities an outside view, thus enabling them to question the national crisis and consequence management arrangements.

27. One of the main purposes of this exercise was not just to present recommendations but above all to collect best practices. Those best practices were identified in all of the 27 MS depending on the different models in place and are compiled in annex 2 to this report. From a supranational standpoint, the collation of best practices will enable the MS to use functional solutions from other MS to solve similar problems, thus allowing them to adapt compatible mechanisms to their national model. The identification of best practices in dealing with a problem in one MS will undoubtedly strengthen the dialogue between the EU MS, bringing them together on the vitally important issue of security.

28. On the basis of the specific recommendations and best practices, the current report presents general recommendations which go beyond the national models and structures and aim at improving crisis and consequence management at European level as well as aligning the 27 EU MS crisis management models more closely.

29. The ten general recommendations below are divided into the following four groups:
    (a)   Structural issues;
    (b)   Communications;
    (c)   Improvement of cooperation;
    (d)   Contact with the public.

(a) Structural issues

1. Development of a generic plan for crisis management

Most Member States have specific plans for concrete crisis scenarios, and in some cases a significant number of such plans. It is essential to ensure that all existing plans are compatible throughout the country and also to resolve conflicts of competence between the various bodies involved in crisis management. A generic plan that is compatible with existing plans, and enables any lacunae or doubts engendered by cross-plan situations to be overcome, is an essential document for the satisfactory coordination of crisis management mechanisms.

2. National Crisis Centre

All MS have a national crisis centre or a similar structure for dealing with a major crisis, whether terrorist-related or not. The NCC is organized in different ways in different MS: for some it is a permanent structure, with physical facilities, permanent staff and competences established by law. For other MS, the NCC is a concept, supported by plans that bring its members together in the event of crisis, using the facilities of the organisation that takes the lead for that particular event. It is impossible to assess the relative efficiency of the different models since only a few countries in the EU have suffered the consequences of a terrorist attack. Nevertheless, regardless of which model is in place in the MS, the role of the NCC needs to be clarified. The NCC should be well known nationally and have a clear basic composition and a clear role.

To be able to respond to a terrorist-related crisis, the national organisations involved in crisis and consequence management have to be able to see the NCC as a coordinating body formally established. The NCC should not overlap with existing structures but should focus on its coordinating role at national level.

(b)   Communications

3.   Encrypted digital networks and consequence management in the event of a terrorist attack

3a   Further development or establishment of encrypted digital networks enabling all the emergency services to work together

Technical developments and advances in terrorism now make it impossible for emergency services to work with unencrypted networks. Likewise, the close coordination required between the various parties involved makes encrypted digital networks a technical necessity.

To ensure both an effective service to the public and the security of the various emergency services, it is important that all the Member States complete the conversion of their communication network for the emergency services to an encrypted digital network.

3b   Improving the compatibility of encrypted digital networks in border areas

An effort must be made to find simple solutions to make radio networks compatible in border areas, especially where different technical standards (TETRA or TETRAPOL) are used.
To help advance this issue MS should participate in the expert group set up by *the Council Recommendation on improving radio communication between operational units in border areas*[7] to examine the issues involved in the development of ISI for TETRA and TETRAPOL and draw on the report to the Police Cooperation Working Party (PCWP) on the viability of establishing such interfaces, foreseen for June 2010[8].

---

[7]   Doc. 10141/09 ENFOPOL 143 TELECOM 116 COMIX 421, approved by Council on 4-5 June 2009

[8]   Meetings on the subject are planned for May 2010 and October 2010

4.   Establishment of direct communication between the crisis rooms in the different MS

The crisis rooms have the job of organising all the strategic coordination for the measures adopted to deal with the events for example terrorist-related emergencies. While at internal level most MS have a clear definition of the competences of the different bodies, when it comes to international contacts there are more uncertainties to be resolved.

When a cross-border crisis arises, and where there is a need to coordinate measures between MS affected by the events, it is necessary for the crisis room to be able to contact their counterpart in the other MS. It is therefore recommended to have a clear, complete and up-to-date list of all the crisis rooms and contact points, related with terrorism issues, in the various MS. Such a list was already created in the PROCIV group[9] integrated in the Manual on EU Emergency and Crisis coordination. This list should be updated as frequently as possible, using the existing EU working parties and a proper distribution of this list should be ensured.

There is also a need to establish direct communication between those structures, not only to facilitate joint decision-making, should the need arise, but also to circulate information during the crisis between the MS involved and with other MS.

---

[9]   See doc 7154/10.

(c)   Improving the various forms of cooperation

5.   Private-public partnership

In general, there is a lack of contact between public authorities and the private sector in the MS concerning soft targets. Contact between the private and public sectors in the area of counter-terrorism needs to go beyond granting building permits or carrying out fire inspections. It is necessary to establish a relationship based on trust and dialogue, allowing the private sector to consult the country's authorities for various aspects of their professional activities. This might range from measures to be adopted for passive protection, during the construction of a building or the management of a public space, to agreements with private hospitals on coordination in the event of mass casualties, by way of joint training or assessment.

A significant step forward on the question of soft targets is therefore the existence of an official interlocutor like the National Counter Terrorism Security Office (NACTSO), responsible for dealing with the possible threat and the risk to the target and also for advising the private/public partners on what measures to adopt to protect those targets.

6.   Stepping up cooperation between civilians and the military

There is solid expertise among the country's civilian authorities and military forces in dealing with crisis situations notably because of the experience acquired during interventions abroad in such matters as day-by-day crises and international missions and during training in the use of new equipment. While in most of the Member States, the army represents a reinforcement of civilian forces in the event of a major crisis, there is still room for army and civilian emergency forces to enhance their cooperation upstream by exchanging their experience and knowledge, by improving integration of the army into civilian emergency procedures as well as the procurement and practical use of equipment. This will allow harmonising procedures and ensure that compatible resources are available in the event of a terrorist-related crisis.

7.   Cross-border training

It was clear from all the visits carried out that the need for cross-border cooperation was a matter of concern for all the Member States and one of particular importance for neighbouring states, be they EU Member States or not. Exercises such as those carried out by the ATLAS network for special intervention units should be organized for the different authorities related to crisis and consequence management in case of terrorist attack.

Such exercises give the various interlocutors a chance to get to know each other personally, and that cannot but simplify contacts in the event of a crisis. They also provide an opportunity to update approaches and find solutions to a certain number of difficulties which could have very serious consequences if they were not discovered until a crisis occurred. Such cross-border exercises need to be conducted both with the Member States and with third countries wherever appropriate.

While not a substitute for cross-border exercises, participation by observers neighbouring countries also needs to be developed.

The participation of staff from the emergency services in exercises of neighbouring countries as observers is less costly than cross-border exercises and can be an additional means of maintaining relations and knowledge of each other's intervention resources and techniques.

d)   Communication with the public

8.   Dedicated Internet site for crisis situations

Many of the MS seek to keep the public informed via Internet sites. Such sites are most often the standard government sites on which the crisis information sits alongside structural information, departmental staff lists or declarations by dignitaries. The result is a degree of confusion and priority is not given to access to essential information.

Other MS, however, have opted for dedicated crisis management sites. This gives the public a clearer and quicker access to the important information and an easier monitoring of the situation. The domain name must be clear and easy to remember and the content must relate exclusively to the management of the current crisis (information on developments, advice, etc.). There is no input into such sites outside crisis periods. They must be designed in such a way as to resist all forms of cyber-attack.

9.   Centralise all emergency-related calls at the European emergency number 112

Although all the MS have introduced the central 112 number, in some cases it still operates in parallel with another centralised number. In other cases it operates in parallel with several emergency numbers for different services, sometimes without any interconnection between them. Technical solutions offer the possibility of changing historical habits or overcoming logistical problems. It should be a priority to implement the centralised 112 number, structured in such a way as to allow immediate triage of the types of emergency and capable of responding to requests from the public.

10.   Creation or strengthening of a psychological unit

It is widely recognized that next to the persons suffering physical trauma as a consequence of a terrorist attack, there is an even larger group of psychological victims. It includes those losing a family member, friend or work colleague, or even simply surviving an attack. It is therefore recommended that units of professionals specialising in this type of assistance should be set up, or strengthened to offer both immediate and long-term support to these victims.

Member States	*Dates*
Latvia	*28-30/05/2008*
Czech Republic	*11-13/06/2008*
Greece	*18-20/06/2008*
Hungary	*02-04/07/2008*
Cyprus	*10-12/09/2008*
Malta	*17-19/09/2008*
United Kingdom	*08-10/10/2008*
Bulgaria	*22-24/10/2008*
France	*19-21/11/2008*
The Netherlands	*26-28/11/2008*
Belgium	*21-23/01/2009*
Austria	*28-30/01/2009*
Lithuania	*18-20/02/2009*
Poland	*25-27/02/2009*
Finland	*11-13/03/2009*
Luxembourg	*18-20/03/2009*
Spain	*01-03/04/2009*
Portugal	*15-17/04/2009*
Estonia	*06-08/05/2009*
Sweden	*10-12/06/2009*
Slovenia	*17-19/06/2009*
Romania	*16-18/09/2009*
Italy	*23-25/09/2009*
Denmark	*14-16/10/2009*
Slovakia	*28-30/10/2009*
Ireland	*18-20/11/2009*
Germany	*25-27/11/2009*

BEST PRACTICES ON PREPAREDNESS AND CONSEQUENCE MANAGEMENT IN THE EVENT OF A TERRORIST ATTACK

This Annex compiles the main good practices as contained in the national peer evaluation reports of the Member States evaluated.

1. ARRANGEMENTS IN THE EVENT OF A TERRORIST ATTACK

1.1. National arrangements

1.1.1. Legislative or organisational measures

- The establishment and distribution of guidelines between the different ministries, with the aim of creating a common approach to security and crisis management measures, is a significant improvement. This creation of common standards allows for easier planning as well as more efficient management of any emergency situation. (Austria)

- In the event of a crisis any state authority can request support from the Army, and corresponding agreements exist at Länder level. The Army does not function as a first responder but as a very important provider of support in managing the crisis, with its well trained and extremely well equipped forces. The involvement of the Army with its manpower and up-to-date equipment in general appears to be compulsory for crisis and consequence management and could apply to all EU Member States. In addition, the army can be asked to make use of special expertise in relation to specific types of danger, such as chemical or nuclear weapons. The fact that this cooperation and support is already stipulated in the Constitution represents a forward-looking aspect thereof. (Austria)

- Organisation of the NCC. The NCC organisational structure consists of two main divisions: Operations (Gestion opérationnelle) and Planning (Planification d'urgence). The presence of a planning division reflects the inclusion of emergency planning as one of the NCC's main tasks. This organisational arrangement merits a positive mention. Most importantly, it provides a strong and very important link between emergency planning (essentially a "peacetime" activity) and management activities during a crisis, as efficient crisis management depends on the planning carried out as part of daily business. Furthermore, it ensures guidance for the emergency planners at federal, provincial and municipal level; it facilitates coordination and harmonisation of emergency plans and gives the NCC a thorough knowledge of the quality of the various authorities' emergency planning. Also, the Crisis Centre staff appear to have a philosophy of facilitating coordination between relevant authorities and/or disciplines without seeking to detract from their responsibilities or powers, encouraging a readiness on the part of other departments to work closely and transparently with the Crisis Centre. (Belgium)

- Five "disciplines" are present in all multi-disciplinary forums dealing with incident or crisis management, whether at the physical site of the incident or in the crisis coordination centres at municipal, provincial or national level. The Armed Forces are already integrated in the planning phase of the overall plans within Discipline 4. A deployment can be arranged through the Military Command of the respective province and does not have to go through the whole governmental hierarchy. In terms of best practice, it is also the inclusion of the fifth discipline (information for the public) that deserves attention. This task is quite important, particularly when dealing with large-scale incidents such as terrorism. Therefore, it is very satisfying to see that the Belgian authorities have made "information for the public" an integral part of the crisis management setup in all forums where authorities work together to manage incidents or crises. (Belgium)

- Management of crisis situations and disasters is codified in two legal acts which have been regularly amended (in reaction to experience from implementation and new needs) since their adoption: the Law on the Management of Crises of 2005 and the Law on Protection in the Event of Disasters adopted in 2006. (Bulgaria)

- The law assigns competences to different bodies involved in crisis management as well as command at the scene of the crisis. (Bulgaria)

- Creation in 2008 of the State Agency for National Security including the Counter-terrorism Coordination Centre. (Bulgaria)

- Three-level command arrangement of the police (gold-silver-bronze) is a well-proven arrangement in terrorist and other major incidences and should effectively respond to management-type demands of a crisis organization. The division of tasks for such an arrangement seemed to be well recognized by the police command. (Cyprus)

- A limited number of military staff can be deployed to perform the tasks of Police based on Government regulations. In this case the armed forces are under the command of the police and receive task-related training before deployment. (Czech Republic)

- The existence of the national action plan to combat terrorism. The Czech Republic has a national plan which has been updated five times (once every year since 2002) and establishes not only strategic but also operational objectives. Organizations have been identified and given a timetable for achieving the objective set. For each objective there is a deadline for achieving the result, a responsible body, performance indicators and the estimated amount and sources of funding related to the task. (Czech Republic)

- Estonia has made an effort to reduce the number of agencies involved in a crisis situation by merging various agencies into one emergency body. This will reduce costs, improve the accessibility of the service to the citizen and help to avoid conflicts of interest and competencies. Although Estonia is a comparatively small country, where such an administrative reform might prove easier, the Estonian example may encourage other Member States to examine whether merging agencies may also create synergies and provide clear responsibilities. (Estonia)

- The key players in the Estonian security community seem to know each other very well, which facilitates crisis management. This is due to the fact that there is much exchange of personnel among the authorities. (Estonia)

- The MoI has developed a list of 26 different emergency scenarios in order to prepare individual response plans for each incident. Although the list seems to be very long and may contain some duplication, the concept of developing standard operation procedures for specific scenarios may help to respond more quickly and effectively in an emergency, provided the emergency plans provide for a suitable degree of flexibility. (Estonia)

- In Finland there is a clear intention and effort to simplify the model of crisis management as much as possible. This effort has resulted in extremely effective crisis management. (Finland)

- Terrorism is considered as one type of threat to public security, and therefore as an issue to be dealt with by the Finnish police, and it is dealt with as a crime. Other authorities support the police in fulfilling these tasks, and for that reason the police is entitled to use the resources of the defence forces, as well as any other resources, from any body, which may be considered important to manage a situation related to terrorism. Because of the scarcity of resources, all functions are fulfilled through sharing of resources. The authorisations, which have a strong legal basis, together with regular training and communication, provide sufficient guarantees that resources will be used in the most efficient way possible. Since this management prevents duplication, considerable amounts of money can be saved on the acquisition of equipment as well as on its use in the event of an emergency. (Finland)

- The Special Intervention Team (Karhu) assigns 40 % of its working time to day-to-day police work. This methodology ensures that unit members are kept up-to-date with the general police work, and establishes personal contacts between the unit members and the officers tasked with day-to-day police work. (Finland)

- The regular exchange of staff between the Security Police and the NBI ensures a better understanding of each other's work and tasks and harmonises cooperation in the event of related investigations. (Finland)

- Taken together, the VIGIPIRATE range of intervention plans created under the aegis of the SGDN fully cover the spectrum of the terrorist threat. (France)

- The centralising of a clearly identified hierarchical chain seems particularly effective. The task of manager and coordinator of the Defence Zone Prefect, in the event of a crisis in their area of responsibility, represents a useful mechanism. (France)

- The organisation of the state on a federal basis is conceived in such a way as not to be detrimental to the coherence of overall arrangements and not to cause organisational deficiencies. Coordination between local and federal missions seems to be organised harmoniously and does not give rise to lacunae or overlapping. From the assessment of the threat, then through the planning stage to the organisation of assistance, every aspect appears to be well covered. (Germany)

- The well-prepared Crisis Management and Incident Response System "Polydeukis" and the various levels of threat. This is a live document which is constantly being updated. It makes use of the know-how in the field of crisis management acquired by Greece prior to and during the 2004 Olympic Games. (Greece)

- An interesting assessment structure; the OSINT (Open Sources Intelligence) group in the Ministry of Foreign Affairs. The group was set up in 2007 under the authority of the Ministry of Foreign Affairs. It provides assessments on various topics, particularly information on the safety of Hungarian citizens as well as other subjects related to Hungarian interests abroad such as e.g. terrorist organisations, individuals involved in terrorist activities, proliferation. (Hungary)

- The existence of a document such as the *"A Framework for Major Emergency Management"* allows the coordination and cooperation between all the crisis management authorities under the same guidelines, with a clear definition of competences and the strategic organization. (Ireland)

- The methodology consisting in using an annual questionnaire and the subsequent discussion of the answers with the answering department and authority as a starting point for the annual revision of the plans, and the sending of an annual report to the Government appear to be unique in Europe. (Ireland)

- While the crisis management structure in Italy is complex and based on a number of institutions that developed owing to historical circumstances, the exchange of information and coordination of these institutions (including the civil protection service, fire brigades, etc) seems to function well. In particular, the crisis unit is marked by a high level of flexible arrangements which allow different institutions to be represented in the unit at different times (i.e. depending on the type of the crisis). (Italy)

- The practice implemented by **C.A.S.A** seems to be a particularly useful model of exchanging information between all relevant actors avoiding the duplication of efforts that could arise from such a complex crisis management system.
  The most important thing in any crisis situation, and especially in the event of a terrorist attack, is the need for a good information sharing mechanism: a mechanism that insures that information is quickly distributed to the appropriate organisation, enabling the appropriate actions to be undertaken. Such an institution is C.A.S.A., which enables the threat level to be assessed, based on a continuous flow of information into this mechanism. (Italy)

- The establishment of the Office for Coordination and Planning of Police Forces provides a good instrument with which to optimise and harmonise the services and to plan the activities of the police forces. (Italy)

- The National Counterterrorism Plan (NCTP) defines preventive counterterrorism measures that should be implemented by the State institutions and other organizations. The national plan also defines the role of each of the institutions involved in the fight against terrorism and provides essential guidelines which will be essential in the event of a terrorist attack. The NCTP has to be overviewed once in two years. (Latvia)

- Crisis Centre staff appear to have a philosophy of facilitating coordination among the relevant authorities and/or disciplines without seeking to detract from their responsibilities or powers, encouraging a readiness on the part of other departments to work closely and transparently with the Crisis Centre. (Luxembourg)

- The functioning and content of the VIGILNAT plan is another example of best practice. (Luxembourg)

- The very efficient use of limited resources, existing bodies and available tools, including the Armed Forces. Maltese legislation provides for and regulates the support which the army must provide to the Maltese police and security forces, in particular in terms of managing terrorist incidents. Such support enables resources to be used to the fullest possible extent and avoids the redundancy of equipment and services. The way in which the forces cooperate with each other on a daily basis creates familiarity with the concept of cooperation which could prove to be an advantage in the event of a crisis. (Malta)

- The set-up of five scenarios and their respective checklists provides the commander on the scene and in the command centres with sufficient guidelines but also enough flexibility to respond adequately to any emergency situation. (The Netherlands)

- A very specific feature of the Dutch system that has been set up is its strong reliance on a regional approach, although it became clear that, where a crisis is caused by a terrorist incident, responsibility for managing it will be with the National Counter-Terrorism Coordinator. This structure seems to fit well with the overall Dutch administrative and government culture. It does present some challenges in terms of ensuring a coordinated approach when an attack has cross-regional, national or international ramifications, but these challenges are addressed to some extent by way of exercises involving more than one region, and by way of the coordinating role of the CTC, who is responsible whenever a crisis is of a terrorist nature. (The Netherlands)

- The Crisis Management Act (CMA). The existence of a very comprehensive legal provision that defines the competences and role of each one of the institutions both at a political and operational level is an important step to define the competences and roles of each one of the institutions in the field of crisis management. The plan not only indicates who is involved and what are the tasks of each one of the involved institutions and bodies, but also goes into the detail of setting up time tables with deadlines for the presentation of, for example, plans for the protection of critical infrastructure. (Poland)

- Budgetary provisions for crisis management planning and the handling of crisis situations are laid down in the CMA and define the financial framework including subsidies. Such provisions avoid discussions during or after a crisis and provide a high level of certainty. (Poland)

- Critical infrastructure operators are obliged to prepare and implement their own critical infrastructure protection plans. It is also their responsibility to indicate contact persons to the public administration. Nevertheless all these plans are accessed and coordinated by the central authorities, allowing a more coherent approach to crisis management. (Poland)

- The existence of a Secretary General for the Internal Security System, appointed by the Prime Minister and supported by a legal framework. (Portugal)

- The existence of such a body, with direction and operational command, allows a closer link to be established between the political decision makers and the operational command. In addition, it creates a platform where representatives of all the entities involved in crisis management are present, thus ensuring that planning is more efficient. (Portugal)

- Key first responders are located within the MOI. This not only minimises the possibilities for political disagreement but also guarantees a clear command structure in the event of a crisis. (Portugal)

- The equipment of the ANPC is of a very high standard. Several fully equipped mobile command posts are at the disposal of all first responders. All this equipment can be easily deployed in any emergency, and made available to the entities involved. (Portugal)

- There is a clear vertical organizational framework and a clear distinction between political/strategic, operational/technical and tactical tasks and responsibilities. The tasks at each level are clearly defined and the procedures are laid down in protocols and other provisions. (Romania)

- SNPCT has a very comprehensive structure which permanently includes all relevant actors in the area of preventing and countering terrorism. Based on this structure and on the relevant protocols and legal provisions the existing management system of CCOA guarantees a permanent information flow to and from the relevant organizations within SNPCT. Thus, good preconditions for a timely reaction to an upcoming crisis situation are given. (Romania)

- Besides the continuous collection of intelligence by the SRI and other intelligence services, Romanian authorities are strengthening community policing. The full implementation of this concept will allow the authorities towards preparedness to a large-scale emergency situation. (Romania)

- A full back-up of the police database is located outside the capital Ljubljana. Thus, the possible vulnerability of the system is further reduced. (Slovenia)

- The National Crisis Management Centre (established within the RS Ministry of Defence) provides facilities and technical, information and telecommunications resources for the work of the Government and the National Operative Staff. The NCMC is a good example in terms of a secure environment, communications and IT facilities, which are assets improving coordination among the different actors involved in the management of a crisis. (Slovenia)

- The general cohesion and effective organisation of the entire National Crisis Management System (SNGSC) are in themselves a good practice. The arrangements and mechanisms listed below may, however, also be considered good practice. (Spain)

- A National Crisis Management Centre (CNGSC) for all kinds of crises, in operation twenty-four hours a day and seven days a week, is a guarantee of effectiveness. (Spain)

- The centralised reference database within the CNPIC on critical infrastructure appears to be highly efficient. It also provides the correct contact persons in the event of an incident and a first set of measures to be taken by first responders. (Spain)

- The fact that the law enforcement and the civil protection agencies work with the same four-level system of threat guarantees their sound and coherent understanding of each other's assessments. (Spain)

- The role of NCC is strictly strategic, which helps to avoid attempts to steer the operational processes from government level. (Sweden)

- The concept of merging all emergency and response agencies into one coordinating body called MSB is potentially a good tool for coordination of the response phase in large scale events and international operations. (Sweden)

- Strong local government involvement in crisis and response emergency services provides a good standard of local security systems. The community emergency planning ensures good response standards in limited-size incidents and events. (Sweden)

- The UK Counter Terrorism Strategy (CONTEST2) is foundation for all work on terrorist threats. All competent authorities have to follow 4 points, the so-called 4Ps (prevent, pursue, protect, prepare) and thus ensure consistency in the implementation of the existing programmes and action plans. (United Kingdom)

- The Government Liaison Teams (GLTs) support and advise the local authorities, as well as an important communication and information channel. (United Kingdom)

- As for preparedness for crisis and crisis management, the structure of the police authorities, from the Association of Chief Police Officers (ACPO) to the regional and local headquarters (Gold, Silver and Bronze Commands) provides the ideal basis for optimal planning and carrying out of operations. (United Kingdom)

- Transparent information management by government entities (register accessible on the Internet, threat level, leaflets for different scenarios etc) raises the awareness of the general public and increases understanding of measures to increase security. (United Kingdom)

- The close cooperation between the OSCT, the NaCTSO and the competent government agencies guarantees a balanced set of programmes and measures. (United Kingdom)

- The implementation of the HERMIS plan aims towards the valid and timely briefing of all diplomatic missions in London in cases of incidents with massive losses or other serious events that could happen in the country. This is rightly considered best practice because all embassies are kept informed about the events, leaving the police free to do their job without distractions. (United Kingdom)

1.1.2.   Participation of citizens, NGOs and volunteers

- The principle of involving the individual citizen in crisis management as a result of the great number of volunteers working for the emergency rescue services is positive. This not only automatically raises the awareness of the population with regard to possible disaster risks but also strengthens the individual's capacity to cope with such situations. (Austria)

- Good integration of non-governmental organizations, such as the Red Cross, in rescue work and management of the emergency medical services. (Austria)

- Further to the permanent staff, the additional use of volunteers, has proved to be an effective tool and is considered to be a best practice. Cyprus Civil Defense volunteers contributed effectively during the Lebanon Crisis of 2006, in the relief of thousands of repatriated EU and third country citizens. The same applies for the contribution of Cyprus Civil Defense at several natural disasters and recently during the wild forest fires which occurred in Cyprus and in Greece in 2007. (Cyprus)

- There is a very elaborate volunteering system in the country (Defence League, volunteers who assist the police). To improve co-operation with the police, a framework agreement between the General Staff of the Defence League and the Police Board is concluded annually. According to the agreement, the setting up of public order protection units has been started at all Defence League regional units. The units comprise members of the Defence League with the status of assistant policemen, who help police officers in the protection of public order and in crises can also perform the tasks of the military police. In addition to direct military training, the Defence League provides its members with many other skills and experiences necessary in life. Using the first aid and paramedical skills acquired in the Training Group, members of the Defence League have frequently acted rapidly and decisively, saving many fellow citizens whose life has been in danger. (Estonia)

- The advanced approach with regard to Public Private Partnership certainly appears to be a good practice. The separation of national (political) threat levels as outlined in the DTN from the private sector's alerts system is an asset for valuable cooperation between the two parties. (The Netherlands)

- An interesting dimension to the MOI's outline of crisis management structures was an explicit acknowledgement of the role of non-governmental organisations at both national and regional level. Representation at national level is to facilitate their input into the development of crisis management policy, while at voivoid level this is to be reflected as a list of NGO resources that can be called upon according to the nature of a particular crisis. (Poland)

1.1.3.   Organisation of the work on the spot.

- Organising the work of the police in the event of a terrorist incident. The approach of appointing a bomb scene manager could be introduced at European level. Such a post makes for effective coordination of both the investigative and administrative tasks of the police and contacts between the police and the other emergency services. (Belgium)

- In terms of general investigative competencies, the Finnish police can request any information (including passenger lists) within its mandate without requiring any additional authorisation. (Finland)

- By rationalising and providing a framework for the investigators, the "attack response capability" put in place by the DCPJ facilitates the progress of the critical initial phases of investigation after a terrorist attack has taken place. (France)

- Within the CCOA of the SRI, a telephone hotline as been set up for notifications concerning potential terrorist threats. This hotline is free of charge and available 24/7. Terrorism experts are available to identify hoax calls and immediately assess the (limited) relevant information. (Romania)

- The Police Support Team for the management of major terrorist attacks, created in January 2006 and composed of experts from the CNP and the GC, is very useful in the event of a major terrorist attack. The alternating command of that group by the CNP and the GC is also good practice. (Spain)

- The basic principle – namely keeping responsibility at the most local level possible and having support and strategic consultancy provided by the government – is a useful way of sharing competencies, and avoids complex and long decision-making processes. (United Kingdom)

1.1.4.   Relations with the private sector

- The NCC's links with the private sector via the system put into effect through the FEB (Federation of Belgian Enterprises) appears both flexible and highly effective. Such an approach could also be introduced at European level. (Belgium)

- Obligations concerning the participation and cooperation of natural and legal persons and sole entrepreneurs in crises are set out in the crisis management legislation, sanctions are introduced for non-compliance (and reimbursement of costs incurred while acting on the orders of public authorities in crises). (Bulgaria)

1.1.5.   C.B.N.R.

- Rescue teams in place (by the end of 2008 present in each of the 28 regions) that are equipped for management of CBRN incidents. (Bulgaria)

- The CBRN threat is very well covered in terms of both preventive intervention and intervention following an attack. (France)

- The Armed Forces and the Fire Brigades were provided with the same or at least, compatible equipment to respond to CBRN incidents. This applies to the equipment provided to the first responders in Northern Ireland as well. This cross-border approach indicates the commitment of the Irish authorities towards cross-border and European co-operation. (Ireland)

- The procurement of equipment, in particular with regard to CBRN, is agreed upon among the different bodies involved. This open debate between institutions allows a better understanding of the real needs of each of the bodies, as well as an exchange of experience related to the different equipment. It goes without saying that this more interactive procedure allows better use of the available budget. (Portugal)

- In response to limited CBRN specialist health facilities, the SK Ministry of Health has entered into cooperative arrangements with AT & CZ, and has extended these arrangements to encompass training exercises. The Ministry of the Interior informed the review that it is currently finalising an agreement with the Ministry of Health to prioritise access to such facilities for first responders. This agreement comprises access to public and private healthcare facilities and first aid in the field via the Ambulance Corps. Similarly, Control chemical laboratories of the civil protection of the MoI is investing in mobile centres to provide on-site assistance and testing facilities for CBRN-related incidents. (Slovak Republic)

- The country-wide procurement of basic CBRN equipment ensures compatibility between first responders involved in CBRN matters. It is planned that all 44 fire-fighting units of wide importance (out of which 13 are professional) will be equipped with the quality CBRN equipment by the end of 2013. (Slovenia)

- The Swedish Police Service has developed a unified standard for responding to CBRN incidents. This standard includes common training, procedures and equipment at national level, facilitating a common approach to the topic nationwide. (Sweden)

1.1.6.   Inter - Agency cooperation.

- In order to improve cooperation between the Police, Customs and Border Guard, a joint body has been set up. All three bodies make use of a common database and weekly meetings are held to discuss common issues. (Finland)

- Excellent upstream crisis management system through threat assessment carried out by UCLAT. That threat assessment, which involves all the services concerned, is essential to the process of establishing the threat level for the implementation of the VIGIPIRATE plan. (France)

- The common database at Länder (City of Berlin) level on technical resources and man-power, combined with a list of measures to be taken and an additional set of options appear to be good tools for inter-agency cooperation. (Germany)

- The structure and functioning of GTAZ (Federal Republic of Germany's Joint Counter-Terrorism Centre), combining the counter-terrorism efforts of 40 forces working in Germany on religiously motivated-terrorism, allow an effective assessment of threat. (Germany)

- The cooperation between AGS and the Armed Forces and in particular the involvement of the Armed Forces when it comes to the dismantling of Improvised Explosive Devices (IED). (Ireland)

- Counterterrorism Centre (CTC). The existence of a permanent CTC that can activate an Operational Command Centre in the vicinity of an emergency is crucial. The CTC is also responsible for preparing, updating and implementing the NTCP as well as the developing response plans for specific situations. (Latvia)

- The Security Police as an Intelligence and Law Enforcement Service DP continues to be the main institution for the prevention of terrorism in Latvia. The combination in the same body of police legal capabilities as well as Intelligence services skills, allows efficient preventive work as well as more realistic threat assessments. (Latvia)

- The composition of the Malta Security Service of seconded staff from the police, customs and armed forces improves the flow of information and cooperation between the agencies as well as the efficiency of the functioning of the Malta Security Service. (Malta)

- The existence of a Counter Terrorism Coordinator who takes the coordination role in the case of a terrorist event. Both in terms of technical expertise and in terms of updated procedures it is clear that preparedness for and capability to respond to crises, in particular terrorist ones, have increased considerably as a consequence. (The Netherlands)

- The added-value of CTC information and intelligence analysis capabilities centres on processes of 'verification'. From a presentation it was evident that an elaborate and coherent reporting system (CTC intra-net) was in place and producing operational and situational reports – although a clear demonstration of the detail and added-value of CTC verification was not provided.
The integration of CTC reporting procedures as standard templates across the various domestic security stakeholders would improve the mutual exchange of information and understanding amongst stakeholders. It was noted how bringing various stakeholders together in CTC fora had already resulted in qualitative benefits. (Poland)

- SIRESP is a well-developed structure for inter-agency communication. Opening the use of SIRESP to private partners is an excellent approach allowing fast communication between private and public bodies in the event of an emergency. The participation of all the structures involved in crisis management in a single network means that the most appropriate means can be used in case of need. (Portugal)

- The creation in May 2004 of the National Centre for Counter-Terrorism Coordination (CNCA), which makes it possible to provide the Minister of the Interior with all the intelligence collected by all administrative entities that are involved in the fight against terrorism, is a considerable advantage. (Spain)

1.2. Cooperation about potential cross-border targets

- Cooperation appears to be particularly advanced among the Benelux countries, where information is exchanged on risk analysis, management of emergency situations and implementation of joint exercises. This appeared to be an example of best practice which could potentially be replicated elsewhere on a regional neighbourhood basis. (Belgium)

- Bilateral agreements or Memoranda of Understanding with all neighboring countries for cooperation in crisis situations are in place. (Bulgaria)

- Agreements on cooperation and assistance in preventing, and managing the consequences in the event of, major incidents (including terrorist attacks) exist with all neighbouring countries. (Lithuania)

- Cooperation appears to be particularly advanced among the Benelux countries where information is exchanged about risk analysis, management of emergency situations and implementation of joint exercises. This appeared to be an example of best practice which could potentially be replicated elsewhere on a regional neighbourhood basis. (Luxembourg)

- A distinguishing characteristic of SK crisis response and recovery arrangements is the regional cooperation under V4. This comprises extensive coordination of training and exercises across various stakeholders in accordance with bilateral governmental agreements between, PL, CZ, HU & SK. The V4 formation is notable for the annual meetings between the State parties to discuss work plans, exchange of information and experts, and the organisation of training and exercises. (Slovak Republic)

- Many exercises are carried out, both for national or local services and with neighbouring countries. The debriefings from these exercises provide an opportunity to establish points for improvement and points to be clarified in the intervention plans. (Slovenia)

- There are cooperation and assistance agreements with all neighbouring countries covering prevention and consequence management in the event of a major incident (including terrorist attacks). (Slovenia)

- In terms of cross-border cooperation, the *Vrata Megvarje* operational communications centre can be mentioned as a good example of cooperation with neighbouring countries. This centre, which has already been set up, involves police officers from Italy, Austria and Slovenia, operates round the clock (24 hours a day, every day of the week), and has its own premises and a permanent staff of officers from all three countries. (Slovenia)

1.3. Communications networks and IT systems

- All the security forces (police, fire brigade, ambulances) can communicate on the same digital network (ASTRID). This ensures consistency of relief efforts at all levels. (Belgium)

- The radio network of the Cyprus Police is supported and maintained by a Special Department of the Police which supports and maintains the whole system. In addition, having a private telephone network and issuing a special maintenance contract with providers to support it, is considered to be best practices. (Cyprus)

- The development of the national network of communications will reinforce coordination and cooperation between the regions. (Czech Republic)

- Addressing the issue of obliging the e-mail and internet service providers to keep and provide relevant data to competent authorities This is one of the objectives of the National Action Plan (this does not concern the content of the communications but data such as the sender, addressee and the time of message transmission). Pursuant to existing legislation and in compliance with the EC regulatory framework on electronic communications, those providers are not providers of electronic communications services (i.e. transmission service providers) but rather providers of information society services (i.e. content service providers). (Czech Republic)

- Good practice in the area of communication was observed in the form of KRISEINFO.DK, a robust and overarching website which publishes simple and to-the-point information for the public. It is hosted on servers which are located outside Denmark's borders and which are robust in crisis situations, remaining operational even if the central communication system within Denmark has difficulties. (Denmark)

- A website with a structure similar to that of KRISEINFO.DK would be a best-practice model for other EU States with no structure of this kind. The stated robustness of the KRISEINFO.DK website in communicating basic and vital facts to the public in a crisis situation is to be recommended. (Denmark)

- Maintenance of the radio network which is provided by the Technical Division of the Hellenic Police Headquarters which is responsible for the testing and supervision of all voice communication networks. The Information Technology Division / Hellenic Police Headquarters is responsible for the testing and supervision of all data communication networks.
  The Greek police forces are autonomous as regards means of transmission. They do not have any need for external technical or human resources in this field. (Greece)

- An efficient institution to fight against cyber attack; CERT (Computer Emergency Response Team). The CERT:
  − is the centre handling cyber-crime crises,
  − is responsible for critical information infrastructure protection of government institutions and the private sector,
  − offers training to management and staff of private companies,
  − offers a tailor-made database service according to individual needs,
  − offers periodic (daily/weekly) information on subscription. (Hungary)

- An efficient communication network TETRA. This communication network is digital and encrypted. It is necessary to extend this network to all Hungarian territory. (Hungary)

- The "Computer Communication Command Control for Information (C4I)" Database, developed by the *Guardia di Finanza*, combining a kind of Vessel Tracking System (VTS) with additional analytical features, may be of interest to other Member States, at least those with an extensive coastline. All partners of the *Guardia di Finanza* have access to this database and can add data. The system can also be used as an operations planning tool. (Italy).

- Clear definition of roles among institutions. A clear division of tasks between the existing structures dealing with terrorism is one of the biggest advantages of the Latvian system. This clear division, reinforced by the NCTP, allows better, more efficient prevention and the consequence management of terrorist attacks. (Latvia)

- Malta is well equipped to cope with any IT attack on the communications systems used by the security forces. The existence of the Malta Information Technology and Training Services (MITTS) and its central role reflect how seriously this risk is taken by the Maltese authorities. (Malta)

- The emergency number 112 is used throughout the country. The Police, the Civil Protection Department and the Armed Forces cover each other in operating the system. Emergency numbers used in the past are still in place but are automatically diverted to 112. (Malta)

- Strong emphasize is also given to a well functioning communication and IT-infrastructure including redundant lines for safe communication and backup systems in case of a system failure. There are also exercises to train secure communication. The Special Telecommunications Service which is part of the defence system provides for dedicated communication lines which work independently from public networks. (Romania)

- The Ministry of the Economy uses a software application, EPSIS, to support economic mobilisation during a crisis. The proposed deployment of the EPSIS system (over a secure Internet connection) to Regional authority (Local emergency management agency) should enhance the situational awareness and effectiveness of crisis response. (Slovak Republic)

- WIS: This is a national web-based information system (WIS) that has been developed to facilitate information sharing between the different actors, at every level, in the Swedish emergency management system before, during and after a crisis. WIS enables an efficient shared situations awareness during a crisis. The public and the media also have free access to this website, allowing them to have an overview of the course of events during the crisis. (Sweden)

- The Swedish 112 system operated by SOS alarm, a state-owned enterprise, offers a good and unified standard for answering and handling emergency calls throughout the country. (Sweden)

2. TRAINING/EXERCISES

- The development of Seminars by the BVT focuses on the first response challenges in the event of a terrorist incident. Such seminars are a useful way of bringing together all the expertise needed for the management of the first few hours following incidents. Exchanges of views and open debate promote interaction between different organisations involved in crisis management. The programmes of the seminars range from background information on terrorism, threat assessment and case studies to victim identification and media work. The last one took place in March 2009. (Austria)

- Numerous training courses are organised for all levels involved (from the top political leadership to first responders in regions and municipalities). Results and lessons learned from the training are incorporated into crisis management plans. (Bulgaria)

- The continuous training of the Cyprus police forces including Port and Marine Police and other Authorities of the Republic for a terrorist attack. The Cyprus Police Special forces should be pointed out as a good example to this effort. (Cyprus)

- Cooperation of ordnance services: There are 2 demining forces in the country: one is involved in the emergency service (the largest one; daily activities, public campaigns etc.); another is military (often abroad);. The forces train together, and exercises involving detonations are carried out also in military territory. (Estonia)

- Cooperation of SWAT units. There are 4 forces in the country which, however, engage in joint training activities and - depending on the situation - joint interventions as well: military team (intervenes on its own in purely military situations, often abroad), K-Commando Criminal Police (the most numerous and best equipped team within the Ministry of Interior has its own divers), Law Enforcement Police team (acts independently in cases of street riots), Prison Service team (suppressing unrest in prisons) and KAPO team (acts on its own in cases where the highest confidentiality level is required). As part of the teams' training, various situations are practised. (Estonia)

- "Demanding Situations" frequently occur. Thus, the design and efficiency of the special structure are regularly tested under real conditions. This allows for ongoing and consecutive updates concerning procedures and the resources required. This dynamic process allows of good and efficient coordination between the bodies involved in crisis management. (Finland)

- The operator of Berlin underground makes a fully equipped training facility available to the Police and the FB at one of its stations, including tracks and carriages. It is possible to have training at this facility every week. (Germany)

- The strategic exercises "LÜKEX". These exercises have been organised every two years, whereby the preparation of the exercise stretches over a period of 12-16 months when individual actors (at federal as well as state level, public and private stakeholders, civil and military authorities) are already actively involved and coached for the exercise itself. In this way, the exercise not only serves to test the existing structures, processes and coordination, but also helps develop the capacities of the relevant participating bodies. (Germany)

- Regular counter-terrorism exercises. The continuous importance attached to and the financial resources devoted to the testing of the police crisis management system may be considered as best practice. All relevant services and offices participate in the exercises. For the exercises the budget does not seem to be a problem. (Greece)

- Interesting system of incident evaluation. Greece has a system of evaluating every incident that takes place. The performance of all levels of command is evaluated. Particular importance is attached to trying to identify cumulative mistakes. The material collected and evaluated is subsequently used for training purposes i.e. a practical "lessons learned" approach. (Greece)

- Outcome of the exercises with very concrete measures to be adopted. The Italian authorities avoided concluding that the exercises had necessarily had the positive results which are always wished for and focused rather on the "need for improvement" issues, which allowed them to improve the mechanisms and to clarify the role of each the institutions involved in the management of the situation. (Italy)

- Numerous exercises are carried out, concerning both national or local services and with neighbouring countries. These exercises make it possible, in the course of debriefings, to identify points for improvement and refine action plans. (Lithuania)

- For the purpose of any resulting criminal proceedings, the army and members of the civil protection service receive special training in how to avoid destroying evidence in the event that they are called to the scene of an attack. (Malta)

- The University of Leiden has set up a Chair on Terrorism. As such, the university contributes to the development of expertise in the field of counterterrorism which might be reflected also in an analysis like the DTN. The existence of this discipline in the university allows not only a historical overview of the events that have defined all the security policies of the present but also a comprehensive approach to the problem of terrorism. (The Netherlands)

- Exercises at provincial (voivoid) level are always observed and evaluated by representatives from other voivoids as well as, when possible, by the central authorities. This ensures a high level of objectivity and consequently an exchange on problems and best practices. In addition, key players from different voivoids know each other personally which is of added value for cooperation in real situations. (Poland)

- The approach of integrating basic civil protection and crisis situation skills training into school curricula: The MoI, in cooperation with the Ministry of Education, has developed a contribution to school curricula, which focuses on young pupils and aims at three things:
  (a) Making young members of the population aware of possible threats and educating them to react appropriately if required;
  (b) Motivating young people to develop an interest in the work of the Civil Protection service and other first responders and attracting them to join as young members;
  (c) Using young people as messengers to the older generations, as they will pass on the information gathered and the lessons learned. (Slovak Republic)

- Many exercises are carried out, both for national or local services and with neighbouring countries. The debriefings from these exercises provide an opportunity to establish points for improvement and points to be clarified in the intervention plans. (Slovenia). The use of the Malla B network in everyday work helps to improve users' knowledge of the system and makes its use efficient and easy in the event of a crisis or emergency. (Spain)

- Regular exercises at different levels (national, regional, local) in different regions under different scenarios and also involving other countries, including post-exercise debriefing on the basis of the procedure matrix, permit a continuous improvement of reaction capacities. (United Kingdom)

- A National Counter Terrorist Exercise Programme has been adopted by the responsible political decision makers and covers the period from 2008 to 2012. (United Kingdom)

3.   **SOFT TARGETS**

- Good approach to the best way to protect "soft targets". The Greek authorities consider that the main way to protect "soft targets" is reliable threat assessment. (Greece)

- Government entities and private companies (trade and industry) closely cooperate in the development of technologies for the protection of sensitive areas (crowded places, critical infrastructures). (United Kingdom)

4.   **OTHER**

- Within the MOI there is a "Higher Institute of Emergency Planning", acting as a knowledge centre that develops tools and know-how, establishes networks with academics, experts and centres at European and international level, provides training and a training environment and a discussion forum. Such a specialised centralised body with cross-border links appears to be an excellent tool for the exchange of best practice and knowledge. (Belgium)

- Fire-fighters are fully-trained multi-skilled operators, who are also capable of providing first medical response. As for Civil response, the fact that basic instructions for emergency civilian response are well distributed in phonebooks, is definitely a good practice. (Finland)

- There is a real public-private partnership, with the main (telecommunications, transport and energy) operators very involved. At both planning and implementation levels of the exercises the partnership is based on constant communication. (France)

- The BSI with responsibilities in different areas (public authorities, private enterprises and citizens) is an excellent example of building communication security issues into one body. The BSI appears to have a solid standing as service provider and is not seen as a "data monitoring watchdog". (Germany)

- An interesting practice is the voluntary based operations of the Federal Technical Relief Agency (THW), which provides concrete technical support (on request) in the field of civil protection in dealing with disasters, large-scale emergencies and accidents. Ca. 80 000 of its staff are volunteers and 800 are full time professionals, organised from local to nation-wide levels. While the predominance of the voluntary element may pose certain challenges (concerning e.g. professionalism, availability of volunteers, availability of a wide range of skills), so far, the system has proven its robustness in Germany. The broad volunteer base at the same time represents a considerable outreach to the population and a certain level of awareness and crisis management competences widely spread across the societal structures. (Germany)

- The structure and work of the National Centre for Health Operations. This centre is an efficient example of coordination of the provision of medical aid during a crisis. The very establishment of such an overall stand-by coordination centre in the health sector may be considered as best practice. (Greece)

- By means of a survey, the population expressed their expectations to the Government Ministries and public authorities with regard to crisis management preparedness. One of the key findings was that the population wants to know that a planning was made by the Government and the public authorities. Details of the planning are not of such a major interest for the population. As a result of this survey, each household has been provided with an introduction on "Preparing for Major Emergencies" in English and Irish. (Ireland)

- The facilities to convene the NCC are located and set up well, in particular the three different rooms: one for political decision-making, one for operational staff and another reserved for the media. (Luxembourg)

- Luxembourg struck us as being particularly aware of best practice in other countries, especially neighbouring countries. Based on past experience, Luxembourg has been able to devise individual solutions based on the country's specific features, notably its size. (Luxembourg)

- The installation of radiation detection gates at enterprises handling recycled metal scrap and the national waste recycling plant could become a common European standard. (Luxembourg)

_____