



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 5 March 2013

**6090/10
ADD 14 EXT 1**

**ENFOPOL 38
PROCIV 15**

PARTIAL DECLASSIFICATION

of document:	6090/10 ADD 14 RESTREINT UE/EU RESTRICTED
dated:	5 March 2010
new status:	Public
Subject:	Second Round of Peer Evaluation Preparedness and consequence management in the event of a terrorist attack

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



ANNEX

**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 5 March 2010

**6090/10
ADD 14 EXT 1 (05.03.2013)**

**ENFOPOL 38
PROCIV 15**

ADDENDUM TO THE NOTE

from : The Council General Secretariat
to : Working Party on Terrorism

Subject : Second Round of Peer Evaluation
Preparedness and consequence management in the event of a terrorist attack

Delegations will find enclosed the report of the evaluation mission in **Poland** (25-27 February 2009) in the framework of the above-mentioned round of peer evaluation.

1.	EXECUTIVE SUMMARY	3
2.	ARRANGEMENTS IN THE EVENT OF A TERRORIST ATTACK	5
	2.1. Structure and organisational framework of National Crisis Centres	5
	2.2. Rules of internal communication in the event of a terrorist attack	10
3.	TRAINING/EXERCISES FOR TESTING THE NATIONAL CRISIS CENTRE AND COMMUNICATION SYSTEMS IN THE EVENT OF A TERRORIST ATTACK	12
	3.1. Training/exercises for testing the National Crisis Centre and communication systems in the event of a terrorist attack	12
4.	SOFT TARGETS	12
5.	GOOD PRACTICES	14
6.	RECOMMENDATIONS	15
7.	ANNEX	17
	7.1. Speakers	17
	7.2. Expert team	20

1. EXECUTIVE SUMMARY

- In the framework of the second round of peer evaluation covering "Preparedness and consequence management in case of a terrorist attack" an evaluation visit was made to Poland from 25 to 27 February 2009.
- The Polish authorities assess that the terrorist threat in Poland is low since the country is not seen as a primary target for the activities of terrorist groups. The main threat is religiously motivated due to the presence of Polish military forces in international missions, particularly in Afghanistan.
- The threat from right-wing extremism is considered to be lower than in Western Europe. No incidents have occurred that would indicate a development of the activities of such groups towards terrorist action.
- **NOT DECLASSIFIED**
- Generally, there has been significant progress in the development of Poland's counter-terrorism and crisis management structures following the findings of the first round of peer review. Progress has been particularly apparent as regards the internal communications system, the National Border Guard and the Internal Security Agency's Counter Terrorism Centre.
- The Polish system for crisis management is being fully reformed and many recent legal provisions have not been fully implemented or tested in practice.

- The Crisis Management Act (CMA) of 26 April 2007 was ratified and entered into force in August 2007. The full impact of this document has been difficult to assess since its full implementation is still ongoing. The CMA is considered crucial and central to a coordinated deployment of resources, since it establishes the competences and the role of the different bodies involved in crisis management.
- Poland is divided into a four-layer political structure that also reflects the operational reaction levels:
 - national level
 - provincial level (*voivoid*)
 - district level (*powiat*)
 - municipality (*gmina*)
- The Crisis Management Act (CMA) defines four levels of alert that may be activated by the Prime Minister in the entire country or in part of it.
- According to the new legal framework of 26 April 2007, crisis management means the activity of the public administration authorities as an element of managing the national security management system, which consists of preventing crisis situations, preparing to take control over them by way of planned activities, responding in the event of emergencies, and reconstruction of infrastructure or its restoration to its previous state.
- The Polish Administration is fully aware of the fact that they have to build government structures to minimise the threats of terrorism, with the EURO 2012 football championship as a deadline. Planning and reform of current structures has already begun.
- The main recommendations resulting from this evaluation mission focus on the following areas:

NOT DECLASSIFIED

2. ARRANGEMENTS IN THE EVENT OF A TERRORIST ATTACK

2.1. Structure and organisational framework of National Crisis Centres

NOT DECLASSIFIED

Following the recommendation of the first round of peer evaluation that inter-agency cooperation should be reinforced, which was supported by the Prime Minister's directive N°102 of 17 September 2008, the Counter Terrorism Centre (CAT) took up its work on 1 October 2008 and is located within the structures of the Internal Security Agency. Various services are represented in the CAT (police, border guards, fire department, intelligence services, etc).

This has allowed the creation of a level that was missing between the strategic and the operational levels. The CAT's tasks include:

- supporting the decision-making process;
- coordinating operational activities;
- analytical and intelligence activities;

- preparing response procedures;
- supporting the activities of other institutions;
- international cooperation;
- education activities (for example training courses for other institutions).

Nevertheless, its main task is drawing up the assessment of the terrorist threat; doing so reinforces the preventive role of the CAT. Operational reports are received from various institutions and bodies, allowing the drafting of a final overall report that is sent to the Minister. A non-classified version is also sent to the various contributing institutions as feedback.

In the CAT are representatives of the Ministry of Finance (MOF), Ministry of Defence (MOD), National Security Agency (ABW), National External Security Agency (AW), Internal Military Security Service (SWW), External Military Security Service (SKW), police, border guards, Governmental Protection Bureau, State Fire Service, customs as well as other services, institutions, or entities needed for any particular situation.

As a method of work, the CAT has developed a database concerning terrorist events and related information, stored according to 104 situations, incidents or patterns.

NOT DECLASSIFIED

Its core functions in support of decision-makers are: the coordination of information flows and operational activities across the various domestic stakeholders; information and intelligence analysis; the definition of response procedures and algorithms; and international cooperation.

The CTC is equally responsible for the threat assessment and for operating as the central repository where information is evaluated and disseminated to the appropriate authorities. For the threat assessment, a scale of 1 to 4 is used to indicate a particular level at a point in time and it is constantly reviewed. Level 4 is the highest and level 1 the lowest.

The landmark crisis management text is the most important legal framework in the development of a national master plan. This plan is a transposition of the objectives of the 2007 legislation (Crisis Management Act of 26 April 2007) in terms of delineating approaches relating to risk identification, threat analysis, allocation of resources etc. Attached to this document are functional analysis annexes which serve as standard operation procedures tailored for particular sectors or classes of threat.

It was noted that the National Plan was awaiting finalisation at the political level, and undergoing sectoral tailoring by the Council of Ministers. This was keenly looked forward to by the relevant MOI administrators, so that they could proceed with its implementation. A central concern of the National Crisis Management Plan was the coordinated deployment of resources.

The MOI's *EU Coordination Unit* is responsible for integrating an EU dimension into the reflections of the inter-ministerial group, as well as managing input into the Council SitCen and Europol OCTA intelligence instruments.

At national level four bodies are involved in crisis management:

- the Prime Minister (PM);
- the Council of Ministers (COM);
- the Government Crisis Management Team (GCMT);
- the Government Centre for Security (GCS).

As pointed out before, in preparation for a crisis situation the CMA defines the basic guidelines for crisis management and specifies which authorities are responsible for doing what and how they should interact with other institutions. **NOT DECLASSIFIED**

The GCS was established by the Crisis Management Act of 26 April 2007 and its director is directly appointed by the Prime Minister. The main task of the GCS is to provide the Council of Ministers and the Prime Minister with support in the area of crisis management. The GCS is also in charge of:

- civil planning;
- critical infrastructure protection;
- organisation of exercises;
- conducting training;
- threat monitoring.

In the event of a crisis, caused by a terrorist event or otherwise, the strategic level is guaranteed by the Council of Ministers (COM). The Prime Minister is in charge of the COM but in the event of an emergency, the Minister of the Interior can also assume that role, always informing the Prime Minister of his actions.

There is also a consultative body, namely the Government Crisis Management Team (GCMT), which advises the Council of Ministers on the activities to be undertaken in relation to management of the crisis.

The GCMT is led by the Prime Minister and its members are the MOD, the Minister of Foreign Affairs (MOFA) and other ministers and heads of central authorities as appointed by the PM.

Beyond its advisory tasks, the other functions of the GCMT are:

- evaluation of final reports on activities related to crisis management;
- assessment of the National Crisis Response Plan and its presentation to the COM;
- assessment of the national and provincial (*voivoid*) Critical Infrastructures Protection Plan;
- establishment of cooperation with voluntary fire fighting services.

Recent planning aims to centralise information flows from the 16 regions (*voivoids*) and also to ensure consistency of approach in terms of replicating the central CT administrative arrangements at *voivoid* level.

Ministers and central administration authorities whose competences include issues related to ensuring external, economic and internal security, including civil protection, have established crisis management offices to allow a centralisation of all the information that arrives in and leaves their institutions.

In March 2009 the crisis room of the PM's office and the MOI will merge and become part of the GCS.

Concerning the National Police HQ, in July 2008 a re-organisation of police structures established the *department for Combating Acts of Terrorism* (within the Central Investigative Bureau). The main responsibility of this department is the coordination of police activities. Other sections involved in counter-terrorist activities are the contingency planning unit, the suppression of terrorism unit, and the central intelligence investigation unit. It was pointed out that this national structure was replicated in field offices at *voivoid* level.

Before the July 2008 restructuring, a 2004 Order gave the police Commander-in-Chief the authority to establish regional counter-terrorism teams (it is not certain whether this power has been retained).

Participation in these teams was described as an extra duty for regional officers. Teams were created on an ad hoc basis to fulfil the tasks of situation control, intelligence gathering, and threat identification and assessment.

Another important element in the fight against terrorism in Poland is the activities of the National Border Guard. The extent of the internal border (1930,75 km) and external border (1580,77 km) is a significant factor. The organisation employs 16 000 officers and 4 000 civilians and operates throughout the territory of Poland. The Border Guard has an extensive network throughout the country. The organisation has a significant responsibility in the event of a terrorist attack, both in the prevention of entry and detection in the aftermath; therefore, it has a potential role in the ongoing prevention of further attacks by an organised group of terrorists targeting a number of locations.

The border guards can be characterised by their whole-of-territory operations and extensive experience of cooperative working both at domestic level (including with the Polish atomic energy agency, civil aviation authority, and police) and at inter-state level (with the NATO crisis response system, NCRS, and crisis management exercises, NCMX; with NATO Host Nation Support, NHNS – in relation to large scale crises requiring military involvement; with Frontex's Rapid Border Intervention Teams, RABIT – in relation to the deployment of EU border guards to the EU's external borders; and with the Proliferation Security Initiative, PSI – cooperation with DK, SE & RU relating to maritime security). The organisation cooperates with all arms of the law enforcement community during a crisis situation and has an ongoing responsibility to assist the intelligence community by providing access to its main database to the police and the Government Centre for Security. (Recommendation of the First Round Peer Evaluation)

This joined-up approach is illustrated in the Border Guard's *Crisis Management Plan* which operates as the central planning document for dealing with various crisis scenarios, including terrorist threats, legal and illegal migration and asylum flows, infectious diseases, and natural and industrial disasters. This in turn informs an algorithmic approach to coordinating Border Guard functions and actions according to crisis type. Also notable is consideration of EU and international sources of information in the identification and prevention of terrorist threats.

At national, voivodeship, powiat and gmina levels, crisis response plans will be prepared. Crisis response plans will contain the following elements:

- 1) The main plan, consisting of:
 - a) characteristics of threats and a risk assessment, including the risk map and the map of flood threat;
 - b) a register of capabilities and resources, including procedures for the use of state reserves in crisis situations;
 - c) an analysis of the functioning of public administration, its efficiency and the opportunity to use it in crisis situations;
 - d) possible action to be taken in crisis situations;
 - e) procedures for amendment and revision of the plan and the individual functional annexes.

The Polish authorities intend to bring together all these plans so that they may be properly tested, thereby avoiding duplication of effort and trying to create common frameworks in all the regions.

2.2. Rules of internal communication in the event of a terrorist attack

NOT DECLASSIFIED

NOT DECLASSIFIED

3. TRAINING/EXERCISES FOR TESTING THE NATIONAL CRISIS CENTRE AND COMMUNICATION SYSTEMS IN THE EVENT OF A TERRORIST ATTACK

3.1. Training/exercises for testing the National Crisis Centre and communication systems in the event of a terrorist attack

The **National Police** had not been involved in any significant cross-border cooperation or exercises with other Member State police forces or in officer exchange programmes; nor had they availed themselves of CEPOL or Europol resources for support and training purposes.

The **CTC** is currently developing training courses and procedures involving ISA and seconded personnel from domestic security stakeholders. This is viewed as a means of cultivating contacts within stakeholder services who can act as multipliers as to CTC needs and procedures, and also facilitates the processes of networking and exchange of experience amongst stakeholder personnel. That said, there was no evidence of consideration of exchange programmes with other Member State personnel or of linking into EU training and expert resources from Europol and Cepol in consultation with other Member State authorities. Crisis management exercises largely consisted of weekly riot-control training and an annual state-wide exercise – the 2008 exercise involved a hostage-taking scenario at Warsaw airport. The development of scenarios for these exercises is the responsibility of the Government Centre for Security. The police's involvement in this goes in tandem with that of other security stakeholders.

4. SOFT TARGETS

In Poland the distinction between critical infrastructure and soft targets is not taken into consideration for the threat level assessment or for the measures to be adopted for their protection.

The Crisis Management Act defines critical infrastructure as systems contain buildings, devices, installations, and services of major importance for public security and to ensure the appropriate functioning of public authorities, institutions and private companies. A list of targets and critical infrastructure systems is part of the critical infrastructure protection plan.

There is no official definition of “soft targets” in case of terrorist attack. However there is a list of objects (updated on a regular basis) which can be a potential target for terrorist attack. This list is being prepared in cooperation with the relevant local crisis management units (province, district, and commune).

Both sole and dependent owners and holders of objects, installations or machinery regarded as critical infrastructure are required to protect it in accordance with separate provisions, and are obliged to prepare and implement their own critical infrastructure protection plans as appropriate, and to have their own reserve systems to ensure security and maintain the functioning of the infrastructure until it is fully recovered. The law also requests that persons responsible for maintaining contacts with the public administration in the context of critical infrastructure protection should be appointed.

1. Critical infrastructure protection tasks include:

- gathering and processing information on critical infrastructure;
- developing and updating critical infrastructure protection plans;
- developing and implementing procedures for use in the event of threats to critical infrastructure;
- provision for the possibility of critical infrastructure recovery;
- cooperation between public administration and both sole and dependent owners and holders of objects, installations or facilities of critical infrastructure in relation to its protection.

2. Critical infrastructure protection plans are to be developed at national and voivodeship levels.

These critical infrastructure protection plans are to be updated at least every two years.

Critical infrastructures are considered an important issue on the Polish agenda, as shown by the fact that there is a requirement, from the central authorities, to take into account the existence of soft targets in every main city in Poland and on the border with neighbouring countries.

5. GOOD PRACTICES

- 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.
- 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.
- 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.
- 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.

- 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.
- 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.

6. RECOMMENDATIONS

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

7. ANNEX

7.1. Speakers

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

7.2. Expert team

Council General Secretariat

NOT DECLASSIFIED

Police and Customs Cooperation Unit - DG Justice and Home Affairs

European Commission

NOT DECLASSIFIED

Directorate General, Justice, Freedom and Security

Europol

NOT DECLASSIFIED

Serious Crime Department – Counter Terrorism

Ireland

NOT DECLASSIFIED

Major Emergency Management Section, Liaison & Protection

Netherlands

NOT DECLASSIFIED

Deputy director of the National Crisis Coordination Centre (NCC)
