## COMMITTEE OF EXPERTS ON TERRORISM (CODEXTER) PROFILES ON COUNTER-TERRORIST CAPACITY

# "THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

March 2010

www.coe.int/gmt

#### **NATIONAL POLICY**

## National Programme for Adoption of the Acquis Communautaire

In 2005, "the former Yugoslav Republic of Macedonia" obtained the status of candidate country for EU membership.

Since 2005, on yearly basis, the Government has adopted the National Programme for Adoption of the Acquis Communautaire (NPAA).

NPAA is a key document for the EU integration process reflecting the dynamics of harmonization of the national legislation with the European law, as well as the adjustment of national institutions to the European administrative structures. It comprises short - and medium-term priorities and activities for harmonization of the national legislation with the EU legislation, the necessary dynamics for institutional strengthening for the implementation of the regulation, as well as the resources required for realisation.

So far, the National Programme for Adoption of the Acquis Communautaire has been revised three times (in 2008, 2009 and 2010). The Programme follows the structure of the Copenhagen and the Madrid criteria, i.e. comprises the following parts: Political criteria; Economic criteria; Ability to assume the obligations arising from membership; Administrative capacities (Public Administration Reform and Preparation of the National Version of the Acquis Communautaire) and Public communication.

The area concerning the fight against terrorism is comprised within the section *Ability to assume the obligations arising from membership*, Chapter 24-Justice, Freedom and Security.

The activities envisaged in this area of the NPAA are systematized in order of the following priorities: harmonization of the legislation in the area of the fight against terrorism, advancement of the cooperation and exchange of data with

EUROPOL and EUROJUST regarding terrorist acts investigations and strengthening the institutional capacities for the fight against terrorism.

#### Revised National Strategy for Combating Money Laundering and Terrorism Financing

Starting from the need to further improve the system for preventing money laundering and terrorism financing, in January 2009, the Government adopted the **Revised National Strategy for Combating Money Laundering and Terrorism Financing** (Hereinafter: Strategy).

With the implementation of measures and activities envisaged in the strategy, the following objectives will be achieved:

- Preventing the use of the financial system for the purpose of money laundering and terrorist financing;
- Harmonization of legislation with the regulations of the European Union and relevant international standards for preventing money laundering and financing of terrorism;
- Harmonization of the domestic legislation with the EU legislation;
- An effective system of inter-institutional cooperation;
- Strengthening of international cooperation; and
- Raising public awareness about the necessity of taking measures to prevent money laundering and terrorism financing.

The National Security Strategy from 2008 and the Strategy for defence from 2010, emphasize that terrorism has the greatest influence upon the national security policy of "the former Yugoslav Republic of Macedonia" and represents a constant, real and serious threat that endangers the peace and security of the country and the world.

#### **LEGAL FRAMEWORK**

#### **Penal law**

#### **Criminal offences of terrorism**

Pursuant to the Strategy for reform of criminal legislation of 2008, a law amending and supplementing the Criminal Code was adopted in September 2009.

Thus, international standards have been implemented in order to improve the criminal-legal framework regarding a number of issues, among which are the confiscation of property and proceeds, criminal liability of legal persons, crimes of terrorism, economic crimes and computer crime.

In relation to the crimes of terrorism, these amendments are made primarily with the goal of harmonization with the following: the Convention of the Council of Europe for the Prevention of Terrorism, the Convention for the Prevention of Financing of Terrorism, the Framework Decision for fighting terrorism (2202/475/JHA) of June 13, 2002, the Framework Decision of the Council of Ministers of the European Union by 2005 and the Council Framework Decision 2005/212/JHA of February 24, 2005 for the confiscation of income, assets and property related to crime.

Specifically, the amendments made in 2008 and 2009 further upgrade the crimes by Article 394-A: a terrorist organization and moreover, two new criminal offences have been introduced: Article 394-B: Terrorism and Article 394-C: Funding terrorism.

In accordance with article 5, 6 and 7 of the Council of Europe Convention on the Prevention of Terrorism, acts of public provocation to commit a terrorist offence, and recruitment and training for terrorism, are included within the above mention amendments: Article 394-a: Terrorist organization, Article 394-b: Terrorism and Article 394-v: Financing of terrorism.

The provisions of the Criminal Code relating to the confiscation of property and proceeds and the removal of objects are supplemented by changes made in September 2009.

Pursuant to the new provisions, the "perpetrator shall be subject to confiscation of the indirect property gain, consisting of the following:

 the property into which the proceeds of crime have been transformed or converted,

- the property acquired from legitimate sources if proceeds of crime have been intermingled, fully or partially, with that property, up to the estimated value of the intermingled proceeds of crime, and
- the income or other benefits derived from the proceeds of crime, from property into which such proceeds of crime have been transformed or converted or from property with which such proceeds of crime have been intermingled, contains the proceeds from a crime, up to the estimated value of the intermingled proceeds of crime."

Moreover, it is provided that: "The proceeds of crime shall be also confiscated from family members of the perpetrator to whom the proceeds were transferred, if it is obvious that they did not provide compensation that corresponds to the value of the obtained proceeds or from third parties, if they fail to prove that they paid an amount corresponding to the value of the proceeds for the item or property."

Furthermore, **extended confiscation** has been introduced and it has particular application to crimes related to terrorism. The provisions provide for confiscation of property which "was acquired within a certain period of time before the court conviction, which the court establishes according to the circumstances of the case, but not longer than 5 years before committing the crime, when based on all circumstances the court is reasonably convinced that the property surpasses the lawful income of the perpetrator and it originates from such an act."

In accordance with international standards, criminal liability for legal persons was introduced in the 2008 amendments and additions to these provisions of the Criminal Code were made with the 2009 amendments.

Namely, in accordance with Article 28-A and B, in the cases determined by law, the legal entity is responsible for the offense done by the responsible person in the legal entity, the name for the account or benefit of legal person.

The legal entity is responsible for a crime committed by his employee or agent of the legal entity, which has realized significant property benefits or has inflicted considerable damage to another under the conditions specified in Article 28-C.

Liability of a legal person does not exclude criminal liability of a natural person as the perpetrator of the offense.

#### Cybercrime

The Criminal Code in Article 251-a criminalizes the acts of **Developing and insertion of computer viruses.** 

The following acts committed by a person are criminalised:

- Developing or undertaking from some other computer virus, with an aim to insert it into someone else's computer or computer network. A fine or prison sentence of up to one year is prescribed.
- Using a computer virus that causes damage to someone else's computer, system data or program. The prison sentence from six months up to three years is prescribed. If major damage is being caused or the act is committed by a group being formed for the commission of such an act, the perpetrator shall be punished with the prison sentence from 1 to 5 years.

As well, the Criminal Code in Article 251-b, criminalises the act of **Computer fraud**, according to which: the one that has an intention for him/herself or for someone else to gain illegal property benefit, by insertion into computer or information system incorrect data, or non insertion of correct data, by changing, deleting or hiding computer data, by falsifying of an electronic signature or in some other manner causes incorrect result in the electronic procession and transfer of data, shall be punished with fine or with prison up to 3 years.

If the perpetrator gained a larger property benefit, the same will be punished with an imprisonment from three months to five years, and if the perpetrator gained a significantly big property benefit, the same will be punished with an imprisonment of one to ten years.

The attempt to commit computer fraud is also punishable.

Criminal liability for legal persons for cyber crime offences was introduced in the Criminal Code amendments from 2009.

**Computer forgery** is a criminal offence in accordance with article 379-a of the Criminal Code, which, in paragraph 1, criminalises the acts of the person who, with an intention to use as authentic, shall without authorisation make, insert, alter, delete or make inapplicable computer data or programs which are determined or suitable to be used as an evidence for the facts that have certain value for the legal relations or

the one that uses such data or programs as authentic. The perpetrator shall be punished with a fine or imprisonment of up to 3 years.

If the act is committed against computer data or programs used in the course of the work of the state bodies, public institutions, companies or other legal and natural persons performing affairs of public interest or in the legal traffic abroad, or if by their usage considerable damage was caused, the perpetrator shall be punished with an imprisonment from one to five years.

Also, with amendments to the Criminal Code of 2009, a new criminal offense was introduced in Article 394-g: "spreading of racist and xenophobic material through computer systems."

In paragraph 1 of this criminal offence, the following acts are criminalised:

"He who through the computer system in the public spreads racist and xenophobic written material, photographs or other representations of the idea or theory which provides, promotes or encourages hatred, discrimination or violence against any person or group based on race, skin colour , national or ethnic origin and religious belief, shall be punished with imprisonment from one to five years."

With the meaning of this paragraph shall be punished who will commit the offence through other means of public information. (Paragraph 2 of Article 394-d)

The person who will commit the offence under paragraphs (1) and (2) of this Article with the misuse of circumstances and authority or for those offences resulting in turmoil and violence against people or property damage from large-scale, shall be punished with imprisonment of one to ten years."

#### Law on criminal procedure

According to the Strategy for reform of criminal legislation, a new draft Law on Criminal Procedure has been prepared. It proposes a new model and a more active role for the public prosecutor in the investigation and in pre-trial procedure. The judicial police are being introduced and would be functionally subordinate to the Public Prosecutor's Office and made available in the detection and prosecution of criminal acts and conduct of investigative procedures.

Also, the action plan for implementing the Law on Criminal Procedure is prepared.

#### **Special investigative measures**

The amendments of the Law on criminal procedure were adopted in 2008 and also concerned the part of special investigative measures.

Namely, the court can order the undertaking of special investigative measures when there are grounds for suspecting that preparation for criminal act has begun, the same is underway or is already committed, when it involves a crime which has a prescribed imprisonment of at least 4 years, as well as for crimes for which there are grounds for suspicion that the same are being prepared, that are underway or that are committed by organized group, gang or other criminal organization, in order to obtain data and evidences necessary for successful conduct of the criminal procedure, which can not be obtained in other way or their provision would be related to big difficulties. (Article 142-b, paragraph 1 of the Law on Criminal Procedure).

Besides the conditions foreseen in the previous paragraph, the court can order the undertaking of special investigative measures and for separately stated criminal acts of the Criminal Code, no matter whether they meet the general conditions foreseen in Article 142-b, paragraph 1 of the Law.

In this regard, the court may order the undertaking of special investigative measures (SIM) for a large number of criminal offences. Among others, SIM can be implemented in relation to acts of terrorism.

#### Law on the interception of communications

In the last period, the State has insisted on finalising the legal framework in order to be able to be able to enhance its institutional and operative capacities in the fight against terrorism.

Therefore, in November 2006, the Law on interception of the communications was enacted ("Official Gazette of the Republic of Macedonia" no. 121/2006) and in 2008, the Law on amendments and supplements of the Law on interception of the communications was also adopted ("Official Gazette of the Republic of Macedonia" no. 110/2008).

These laws determine the conditions and the procedure for the interception of communications aimed at the detection and prosecution of perpetrators of crimes, as well as the conditions and the procedure for the interception of communications aimed at the protection of the

interests and the defence of the country. This led towards the establishment of an important mechanism in the field of prevention of terrorist activities and terrorist threats.

## Law for prevention of money laundering and financing of terrorism acts

A new law on the prevention of money laundering and other proceeds of crime was enacted in 2008.

According to the law, "financing terrorism" includes activities relating to the provision or collection of funds in any way, directly or indirectly, unlawfully and knowingly, with intent that they be used or with knowledge that they will be used wholly or partly because of take-over:

- a) Activity foreseen as a terrorist organization (Article 394-a), crimes against humanity (Article 403-a), the abduction of an aircraft or ship (Article 302), endangering the safety of air traffic (Article 303), terrorism (Article 313), international terrorism (Article 419), taking hostages (Article 421), all of these acts prescribed by the Criminal Code, committed by other individuals or legal entities; or
- b) Any other action taken with intent to cause death or serious bodily injury to civilian persons or any other person who does not participate actively in hostilities in armed conflict, when the purpose of such action, according to its nature or context is to intimidate a population or to compel a government or international organization to do or give up make an action.

Competent entities in the system of prevention of money laundering and financing terrorism, or separately at the request of Office for the prevention of money laundering and financing of terrorism (hereinafter **OPMLFT)**, are required to perform continuous monitoring of the business relationship, including a detailed review of transactions with the aim of confirming that transactions are carried out in accordance with the purpose, business and risk profile and financial condition of customers and update on customer data.

With the aim of a simpler and better risk analysis, the OPMLFT prepares lists of indicators for risk analysis and recognition of suspicious transactions related to terrorism financing, and submitted to the competent entities.

Within its strategic orientation, the OPMLFT pursued a policy of early warning when it executes reception, processing and submission of

lists of terrorists and terrorist organizations (in XML format) developed by relevant international organizations to the competent entities.

According to law, OPMLFT performs inspection and supervision of the competent entities in order to proactively influence the organization and implementation of measures and actions in accordance with the Act, which would have prevented or decreased the risk of transactions and other acts of money laundering and financing of terrorism.

Also, the OPMLFT launched training for all national financial institutions in order to stress the responsibilities and shortcomings, for better training in the area of early detection of suspicious transactions for which there is reasonable suspicion of financing terrorism.

Despite advances in the early detection of cash and non-cash transfers of funds for which there is a reasonable suspicion of financing terrorism, carried out through the banking system and the system of transfer of funds and progress in control of the records of entry and exit of cash by means of border crossings, it is necessary still to emphasize the problem of the circulation of cash within the state, which can be used to finance terrorism.

#### **INSTITUTIONAL FRAMEWORK**

Article 12 paragraph 4 of the Law on Public Prosecutor's Office adopted in 2007, provides for the establishment of the Public Prosecutor for prosecution of organized crime and corruption for the whole territory of "the former Yugoslav Republic of Macedonia".

In 2008, the Public Prosecution Office was established to prosecute organized crime and corruption with jurisdiction throughout state, with the authorities in the area of organized crime and corruption, among which are criminal acts of terrorism.

The central authority in the system to prevent money laundering and terrorism\_financing is the **OPMLFT.** 

OPMLFT has no investigative powers or functions under the law to prevent money laundering and other proceeds of crime and terrorism financing.

The primary responsibilities of the OPMLFT are: collecting, processing, analysis, storage and delivery of information to competent authorities.

Fulfilling its responsibilities, OPMLFT works as an intermediary between entities who undertake measures and actions, and inspection bodies and institutions responsible for the prosecution of perpetrators of crimes.

The OPMLFT is headed by a Director who is appointed by the national Government for a period of four years, at the proposal of the Minister of Finance.

The fulfilment of activities which are planned with the National Strategy for Combating money laundering and terrorism financing will be coordinated by the **Council on combating money laundering and terrorism** financing (hereinafter: Advisory body).

The supervisory body is responsible for monitoring and coordinating the activities of the institutions responsible for implementing the strategy towards meeting the established goals, to promote the functionality of the system and to propose actions to increase its efficiency.

The Academy for Training of Judges and Public Prosecutors is established by the Law on the Academy for Training of Judges and Public Prosecutors published in the "Official Gazette of Republic of Macedonia" No.13/06 on 1 February 2006. The Academy is an independent, autonomous institution, with a set budget, premises, equipment and human resources, managed by the Managing Board in which the institutions which are administrating the judiciary are represented. The basic goal of the Academy is to provide the competent, independent and efficient performance of the judicial and prosecutorial function trough creation of objective system of selection based on precise and measurable criteria.

The second goal of the Academy is to implement compulsory, institutional, financed and continuous professional training for the following target groups: judges, public prosecutors, legal and administrative associates in courts and public prosecution offices, civil servants in the Ministry of Justice and other target groups within the judiciary.

As a part of the continuous training activities, during 2009, the Academy organized a national two-day workshop on "Strengthening the international cooperation in fight against the terrorism" with the participation of international experts who served as trainers, supported by UNDOC, and a two-day Regional Conference in cooperation with Council of Europe (Counter-Terrorism Task Force) with international

participants and experts on the following topic: "Bringing terrorists to justice: promoting the implementation of European standards and documenting good practices".

The prevention of terrorism and anti-terrorist protection training is part of the program for the **training of the police.** The Administration for Security and Counter-Intelligence trains members of the police with specially trained instructors from the Anti-Terrorism Department involved in anti-terrorist and preventive protection.

#### **INTER-AGENCY COOPERATION**

In view of **cooperation and suppression of financing of terrorism**, Memoranda on Cooperation between the Ministry of Internal Affairs and the Ministry of Finance, as well as the Protocol for cooperation in the prevention and fight against terrorism and organized crime between the Administration for Security and Counterintelligence and the Administration for money laundering prevention and financing of terrorism, were signed in 2007.

These bodies continuously exchange information and data of interest for fulfilment of the legal competences of the two bodies and they undertake joint actions for detection and fight against illegal activities in the part of financing of terrorism and money laundering.

#### **INTERNATIONAL LEGAL COOPERATION**

The national Parliament passed the Law on Ratification of the Agreement for cooperation between "the former Yugoslav Republic of Macedonia" and EUROJUST on 15 April 2009.

The agreement allows the direct cooperation of the judicial authorities in "the former Yugoslav Republic of Macedonia" and the EU Member States in the area of judicial cooperation in criminal matters, extradition and transfer as well as acts of organized crime, including terrorism.

On 16 January 2007, "the former Yugoslav Republic of Macedonia" and the European Police Office (**Europol**), signed a Strategic Agreement on Cooperation. The cooperation that is established by this Agreement refers to all areas of crime within Europol's mandate, as well as in the area of terrorism, in compliance with the interest for cooperation between Europol and "the former Yugoslav Republic of Macedonia" in certain concrete cases. Negotiations for the signing of the Operative Agreement with Europol are underway.

An Agreement between "the former Yugoslav

Republic of Macedonia" and the EU on Security Procedures for Exchange of Classified Information was signed as well.

Also, in 2010, the **Law on international cooperation on criminal matters** will be enacted. The purpose of adopting this Act will be to enable the effective implementation of the European Convention on judicial assistance in criminal matters with the two Additional Protocols, the European Convention on extradition of the two Additional Protocols, the Convention on the transfer of sentenced persons with the Additional Protocol and the European Convention for the transmission the penal proceedings.

With the adoption of this law, the provisions of the European Conventions and additional protocols will create a basis for solidarity and international cooperation between countries in the prevention of crime and domestic legislation is fully harmonized with Europe.

#### INTERNATIONAL CO-OPERATION

#### International (multilateral) Cooperation

#### **United Nations**

"The former Yugoslav Republic of Macedonia" actively participates in global efforts to prevent and combat terrorism under the auspices of the UN.

The legal order of the state is supplemented with the following international conventions ratified by the United Nations:

- Nuclear Safety Convention;
- International Convention for the Suppression of Terrorist Bombings;
- International Convention for the Suppression of the Financing of Terrorism;
- Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation;
- Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf;
- Protocol Additional to the Safeguard Agreement with the IAEA.
- Revised Small Quantities Protocol;

In May 2009, the national Government submitted detailed information on the status and implementation of the CTED's recommendations.

#### **Council of Europe**

In the framework of cooperation in the Council of Europe, "the former Yugoslav Republic of Macedonia" fully supported the establishment of the Multidisciplinary Group on Terrorism and its actions in criminal, civil and administrative areas, as well as the current work of the Group on developing international cooperation in criminal matters (Reflection Group on developments in international cooperation in criminal matters).

## Organisation for Security and Cooperation in Europe (OSCE)

In June 2009, "the former Yugoslav Republic of Macedonia" submitted its contribution to the Information exchange on the OSCE Code of Conduct on Politico-Military Aspects of Security.

Since 1998, participating States have exchanged information on the implementation of the Code of Conduct on Politico-Military Aspects of Security established by the Forum for Security Cooperation (FSC) Decision No. 4/98. The information has been exchanged based on a Questionnaire encompassing 10 questions.

#### **NATO**

Cooperation with NATO or with NOS (NATO office for Security), ILU (Intelligence Liaison Office) and TTIU (terrorist threats intelligence units) still involves the regular exchange of intelligence information which is of mutual interest and which is related to the prevention of terrorist threats towards NATO, member countries of the alliance, "the former Yugoslav Republic of Macedonia" and other countries.

#### **Regional (bilateral) Cooperation**

The authorities of "the former Yugoslav Republic of Macedonia" have concluded numerous bilateral agreements with States from the region and other States and international organisations. These

agreements relate to cooperation, *inter alia*, in the fields of fight against terrorism, organised crime, money laundering and other criminal acts pertaining to terrorism.

#### **OTHER INITIATIVES**

On 19 March 2007, "the former Yugoslav Republic of Macedonia" adhered to the Statement of Principles of the Global Initiative to Combat Nuclear Terrorism.

"The former Yugoslav Republic of Macedonia", through active membership of the Administration for Security and Counterintelligence and Intelligence Agency in the South Eastern Europe Intelligence Conference (SEEIC) and Middle European Conference (MEC), participates in the harmonization of interests and the establishment of a joint strategy of the member countries of these conferences for prevention and counter threats arising from international terrorism.

There is active cooperation within regional initiatives such as SECI (South Eastern Europe Cooperation Initiative).

Relevant Council of Europe conventions — "the Former Yugoslav Republic of Macedonia"	Signed	Ratified
European Convention on the Suppression of Terrorism (ETS 90)	08/11/2001	29/11/2004
Amending Protocol (ETS 190)	15/05/2003	14/11/2005
European Convention on Extradition (ETS 24)	28/07/1999	28/07/1999
First Addition Protocol (ETS 86)	28/07/1999	28/07/1999
Second Additional Protocol (ETS 98)	28/07/1999	28/07/1999
European Convention on Mutual Assistance in Criminal Matters (ETS 30)	28/07/1999	28/07/1999
First Additional Protocol (ETS 99)	28/07/1999	28/07/1999
Second Additional Protocol (ETS 182)	08/11/2001	16/12/2008
European Convention on the Transfer of proceedings in criminal matters (ETS 73)	08/11/2001	29/11/2004
European Convention on the Compensation of Victims of Violent Crimes (ETS 116)	-	-
Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS 141)	14/12/1999	19/05/2000
Convention on Cybercrime (ETS 185)	23/11/2001	15/09/2004
Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189)	14/11/2005	14/11/2005
Council of Europe Convention on the Prevention of Terrorism (ETS 196)	21/11/2006	23/03/2010
Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (ETS 198)	17/11/2005	27/05/2009