COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 6.11.2007
SEC(2007) 1425

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

COUNCIL FRAMEWORK DECISION

amending Framework Decision 2002/475/JHA on combating terrorism

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2007) 650 final}
{SEC(2007) 1424}

Summary of the Impact Assessment

SECTION 1: PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

The Commission Legislative and Work Programme for 2007 includes a proposal for the revision of the Framework Decision of 13 June 2002 on combating terrorism (hereafter, "Framework Decision") in order to devise effective solutions towards fighting terrorist propaganda through various media and limiting the transmission of expertise, in particular on explosives and bomb making, for terrorist purposes.

A wide stock-taking exercise was launched in June 2006. The Commission issued three different questionnaires in 2006: a questionnaire to Member States on 26 June 2006; a questionnaire to the media, relevant industry and civil society on 20 November 2006, and finally, a questionnaire to Europol and Eurojust on 11 December 2006. The replies to these questionnaires are summarised in Annexes I, II and III to the Impact Assessment. In addition, conversations and meetings were held with representatives of European media and internet service providers. Finally, a conference was held on 20 March 2007 in order to bring together Member States, Europol, Eurojust and Cepol, present the results of the questionnaires and discuss possible solutions to fight the use of the internet for terrorist purposes.

SECTION 2: DEFINITION OF THE PROBLEM

Modern information and communication technologies play an important role in the development of the threat which is currently represented by terrorism. In particular, the Internet is cheap, fast, easily accessible and has a practically global reach. All these advantages, highly appreciated by law-abiding citizens that benefit from the Internet in their daily lives, are also unfortunately exploited by terrorists, who have perfectly understood the potential of the Internet as a tool to spread propaganda aiming at mobilisation and recruitment as well as to provide for instructions and manuals intended for training or planning of attacks at very low risk and cost.

The Internet serves in this manner as one of the principal boosters of the processes of radicalisation and recruitment: it is used to inspire and mobilise local networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a ‘virtual training camp’. The dissemination of terrorist propaganda and terrorist expertise through the Internet has therefore empowered terrorists, making the terrorist threat grow. Moreover, the importance of such dissemination can only be expected to increase, taking into consideration the fast growing number of users that will make the Internet an even more vital element of modern society than it is today.

Law enforcement authorities are presently in a difficult position to contain the spiral of violent radicalisation and terrorist attacks deriving from the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet. The difficulties stem from insufficient legislation, from lack of capacity and expertise to cope with the volume and plurality of languages in which the terrorist propaganda and terrorist expertise are disseminated as well as from the nature of the Internet itself: its extra-territoriality together with the anonymity it provides seriously hinder the reaction of law enforcement authorities

complicating both the removal of such contents from the Internet and the investigation and prosecution of those responsible for a website and its contents.

The analysis of national legislation reflects that the dissemination of terrorist propaganda and terrorist expertise is not always adequately covered by Member States' criminal law. Insufficient legislation, especially concerning the dissemination of bomb-making and other terrorist expertise, and important divergences between national legal measures, especially concerning the dissemination of terrorist propaganda, demonstrate that there is a security gap to address and harmonisation is required.

EU legislation does not explicitly cover public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism. Furthermore, it is doubtful that the Framework Decision on combating terrorism requires Member States to ensure that a significant part of the dissemination of messages through the Internet encouraging the commission of terrorist offences or providing for terrorist expertise, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, is made punishable.

However, the Council of Europe Convention on the prevention of terrorism tackles the use of the Internet as a means for public provocation to commit terrorist offences, recruitment and training for terrorism. Furthermore, it contains conditions and safeguards ensuring the respect of human rights, in particular the right to freedom of expression. It will lead to the harmonisation of Member States' legislation in this area if all of them sign and ratify the Convention.

Any legislation in this field, dealing with issues which are on the border between the legitimate exercise of freedoms (such as freedom of expression, association or religion) and criminal behaviour would necessarily have a direct impact on fundamental rights. The establishment, implementation and application of criminalisation have to be carried out while respecting fundamental rights obligations. This also implies that all establishment, implementation and application of criminalisation is subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, excluding any form of arbitrariness or discriminatory or racist treatment[1].

SECTION 3: OBJECTIVES

Adopting effective measures to counter the public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism, especially through the Internet, would contribute to the prevention of the development of a stronger and wider platform of terrorist activists and supporters. Such measures should include legal provisions to remedy the insufficient legislation referred to above as well as practical measures to enhance law enforcement authorities' capacities and expertise. These actions would help to reduce the risk of terrorist attacks and to diminish the possibilities for radicalisation and recruitment.

As regards the legal provisions, they should clearly allow law enforcement authorities to investigate the dissemination of terrorist propaganda and terrorist expertise, also through the Internet, and prosecute the terrorist activists and supporters behind such dissemination

[1] See the Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism, points 143-151.

throughout the European Union. Furthermore, law enforcement authorities should be allowed to benefit from all harmonisation that has already been achieved in the fight against terrorism and use co-operation instruments such as the European Arrest Warrant for these new forms of crime.

As regards the practical measures, they should provide law enforcement authorities with adequate training, sufficient equipment and qualified support by experts both on languages and IT, in order to detect and analyse violent radical content on the Internet and trace and identify the individuals behind the dissemination of terrorist propaganda and terrorist expertise.

SECTION 4: POLICY OPTIONS

The options identified to achieve this objective are:

(1) No policy change. This option represents a debatable status quo because of the existence of the Council of Europe Convention on the prevention of terrorism and the associated ongoing process of signatures and ratifications.

(2) Forbidding internet service providers to give access to material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism. This option considerably modifies the regime of the Directive on electronic commerce by introducing a new obligation which generally applies to service providers.

(3) Enhancing law enforcement authorities' capacities and expertise to counter the use of the Internet for terrorist purposes. This option envisages the financing of adequate training, efficient equipment and involvement of experts so that law enforcement authorities can better detect and analyse the material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism and tracing the terrorist activists and supporters behind such material.

(4) Urging Member States to sign and/or ratify the Council of Europe Convention on the prevention of terrorism. This option consists of a political statement aiming at accelerating the process of signature and ratification of the Convention.

(5) Revising the Framework Decision on combating terrorism in order to introduce parallel offences to those foreseen under the Council of Europe Convention on the prevention of terrorism and make public provocation to commit terrorist offences, recruitment and training for terrorism, also via the Internet, punishable.

SECTIONS 5 AND 6: IMPACTS AND COMPARING OPTIONS

The impacts of the policy options on security, economy and human rights are carefully considered. Security impacts focus on the empowerment of law enforcement authorities from either a legal or an operational perspective. Economic impacts include both costs for public authorities and private sector, and make a distinction between direct and indirect impacts. The impacts on human rights include direct impacts on freedom of expression and indirect impacts on right to life and right to physical and mental integrity. Further to careful analysis of the impacts on security, economy and human rights of each of the options, their main advantages and drawbacks have been identified.

Under option 1, the Convention on the prevention of terrorism will bring about some positive impact on security, helping to tackle the issue of the use of the Internet for terrorist purposes. This option implies the empowerment of law enforcement authorities to fight new modus operandi of terrorists, including offences committed through the Internet while fully respecting human rights and implies that there is no need for further regulation at EU level. However, full harmonisation will only be achieved once all Member States sign and ratify the Convention, which can last for many years.

Option 2 is the most extreme of the options examined. It presents the advantage of restricting directly the dissemination of the relevant materials through the Internet. However, it involves serious disadvantages, most importantly, it does not incriminate the behaviour of those producing terrorist propaganda and expertise nor does it fully guarantee compliance with human rights standards.

Option 3 provides for practical solutions to overcome limitations of law enforcement authorities to detect and analyse the messages disseminating terrorist propaganda and terrorist expertise through the Internet. It also helps them to identify the authors of such messages. The information obtained in this manner contributes to understand terrorist trends, anticipate terrorist actions and prevent attacks. However, it does not allow investigating the dissemination of terrorist propaganda and terrorist expertise nor does it allow prosecuting the terrorist activists or supporters behind it, since no legislation is adopted. In consequence, option 3 leads to a partial empowerment of law enforcement authorities, lacking the legal side.

The advantages and drawbacks of option 4 do not present substantial differences from those of option 1.

Option 5 is similar to option 1 as regards its impact on human rights, because it includes conditions and safeguards of the Council of Europe Convention on the protection of terrorism, aiming to ensure the protection of human rights and fundamental freedoms. However, it implies important advantages such as the application of the rules of the Framework Decision on penalties and jurisdiction to the new offences introduced in the Framework Decision on combating terrorism. Additionally, it would guarantee the application of the European Arrest Warrant and allow for the use of specific EU co-operation instruments linked to the Framework Decision on combating terrorism in relation with the new offences. Furthermore, it brings all advantages of EU legislation vis-à-vis international conventions and treaties.

Based on this analysis, it appears that the combination of options 5 and 3 would constitute the most effective policy to counter the new modus operandi of terrorists, in particular their use of the Internet as a means for public provocation to commit terrorist crimes, recruitment and training for terrorism, while fully respecting human rights.

SECTION 7: MONITORING AND EVALUATION

The monitoring and evaluation of the legal measures envisaged under option 5 would be ensured, concerning the revision of the Framework Decision on combating terrorism, by the evaluation of national implementation which is generally applied to verify the transposition of framework decisions, as foreseen under Article 11 of this instrument.

As regards the non-legislative measures of option 3, monitoring and evaluation would be guaranteed by Articles 13 and 15 of the Specific Programme Prevention of and Fight against crime. Article 13 details the monitoring of each of the actions financed under this programme and Article 15 sets out the rules for the evaluation of the programme itself.