COUNCIL OF THE EUROPEAN UNION

Brussels, 29 November 2010

15894/1/10 REV 1

JAI 918
ECOFIN 688
TRANS 307
RELEX 927
ECO 93
PESC 1399
COTER 84
ENFOPOL 316
COSDP 935
PROCIV 141
ENER 305
ATO 65
DATAPROTECT 81
TELECOM 119

NOTE

from:	EU Counter-Terrorism Coordinator
to	Council / European Council
Subject:	EU Counter-Terrorism Strategy - Discussion paper

Recent aviation security incidents have demonstrated once again that the threat from terrorism remains real, and that, like a virus, it is constantly evolving in response to our efforts to control it. This means that our Counter-Terrorism policy also needs to be dynamic and responsive to new conditions. My role is not simply to co-ordinate the implementation of the EU Counter Terrorism Strategy, but also to call the Council's attention to areas where new or reinforced action would be particularly important and timely. In addition to my regular reporting on the implementation of the Strategy (15893/10 + ADD 1), this paper sets out what I believe to be the most current challenges to be addressed as a matter of priority.

Challenge I

Transport Security

The recent attempted package bombs against civil aviation show that aviation remains a high priority terrorist target. Aviation has a huge symbolic importance, and the system of international mobility it supports is both essential to the modern world but also fragile to disturbance. Unexplained explosions on two aircraft approaching the United States would have had a devastating effect on international aviation.

On 8 November, Ministers of the Interior discussed further action to protect air cargo and this will be taken forward again at their next meeting, in parallel with Ministers of Transport. Much has been achieved on transport security in recent years - but the threat keeps getting more and more diverse. The fact that in the most recent attempts the explosives were hidden in cargo is proof that terrorist are constantly learning, and trying new methods to circumvent security measures. We have to pay constant attention to our systems to protect passengers, employees and the general public against all kind of attacks against means of transport and the relevant infrastructure.

Aside from civil aviation more also has to be done on the less protected area of land transport. Terrorist have targeted European land transport on several occasions and there have been recent arrests in the United States associated with surveillance of public transport. There is the obvious risk that as aviation becomes increasingly more secure, terrorists might switch to targeting land transport e.g. to strike rail access to airports or multi-modal hubs. Furthermore, increasing integration of different means of transport (eg high speed rail and aviation in both freight/cargo and in passenger transportation) creates new challenges for a comprehensive approach on security: a problem with an aircraft could lead to a suspect package being re-directed by road or rail.

Transport security features prominently in the Stockholm Programme, and was also raised in my last Discussion paper on the EU Counter-Terrorism Strategy (doc. 9685/10), issued in June 2010. The Commission has taken up this initiative and announced that enhanced protection of transport will be a priority under its Internal Security Strategy in action. This is a very valuable initiative that needs full support from the Member States. To accompany these efforts I would also propose the following actions:

Recommended action:

- Aviation security (AVSEC) and maritime security (MARSEC) have committees constantly discussing recent developments and new measures for transport security. We should support the Commission to set up as soon as possible a body on land transport security - to close the existing gap in this area of transport and provide an established communication channel to integrate better transport, JHA interests and private partners. Such a body would discuss common minimum standards, extending the exchange of best practices, examine existing common legislation[1] and facilitate input into research.
- In the first half of 2011 a joint expert forum of policy makers on Transport and JHA should discuss the threat to transport facilities to develop an action plan towards better integrated protection of all means of transport in the EU and to analyse future threats and trends.
- With respect to the imminent terrorist threat we need to further analyse gaps in the protection of major components of land transport infrastructure, such as principal stations in Member States capitals, major multi-modal hubs or central connecting stations. The review of Directive 2008/114/EC on European Critical Infrastructures in 2012 will provide an opportunity to further explore how activities at EU level can do this.
- We could consider launching a European exercise day, inviting Member States to hold independent local exercises on land transport on the same day across Europe.

Challenge II

Terrorist Travel

The threat of Europeans travelling to conflict areas or attending terrorist training camps elsewhere and then returning home has become even more apparent in recent months. Several warnings and alerts have lead to an increased public debate. We must face the fact that a growing number of residents of the EU are seeking or have received training in countries like Yemen, Somalia or in the AF/PAK region. The majority of plots detected over the last few years have involved such "foreign fighters". Apart from the operational risk posed by these individuals, they also pose a radicalisation threat, attracting new recruits to the terrorist cause.

[1] Example: Regulation EC 1371/2007, chapter VI: "Security, complaints and quality of service", which came into force on 1/1 2010.

My last discussion paper only mentioned some first steps to address this problem (giving Frontex a limited mandate to process personal data and working more closely with the US through access to Analytical Workfiles). Given the significance of this threat I would like to propose a more strategic approach also at EU level and would like to invite the relevant institutions and structures to find a coherent approach, under the pillars of the Counter-Terrorism Strategy.

Recommended action:

1**) Prevent**

- Develop a counter narrative showing that the "armed struggle" is not as exciting as possible recruits might think. Support and spread information on the reality of life in training camps and in the terrorist theatre of operations (including the reluctance of AQ to involve Europeans in actual fighting).
- Extend our activities under the Prevent work stream projects to make Diaspora communities more resilient: cf. to develop an EU/US project on the Somali communities.

2) Protect

Improve document checks and document security:

- Develop closer operational cooperation with the relevant authorities of the third States constituting target or transit countries with a view to disrupting terrorist travel (cf: invite these countries and the Member States to make more use of the Interpol Lost and Stolen Passports data base. Step up technical assistance to third countries in the areas of document security and identity management).
- In conformity with the existing data protection regulations, using established measures e.g. PNR and biometric technologies to monitor and bar terrorist travel. I welcome the Commission's promise to present a proposal for an EU PNR Directive in January 2011, which should ideally cover also intra EU flights. We should also intensify law enforcement and judicial cooperation with countries of transit (cf: Turkey) and destination (cf: Pakistan, Yemen) and ask for PNR from these countries. This could also be a productive subject to discuss in the political dialogue between the EU and GCC: GCC countries have themselves seen their nationals travel to conflict zones, and are hosts to aviation hubs and airline companies of growing international importance.

- Ensure that Member States are connected to the ICAO Public Key Directory, which gives access to certificates and revocation lists, allowing electronic chip signature validation in biometric passports and speed up the process agreed in the Toledo Joint Statement to work together with the US to make sure that as many countries as possible join the ICAO Public Key Directory.
- We should also analyse the effectiveness of the national visa policy and its practical application in preventing terrorism and take up the German initiative to strengthen the consultation procedure and the initiative under the French Presidency, when the Council adopted Conclusions proposing an alert system within the VISA application procedure (referring to Art. 99 Visa Codex).
- Start an initiative to further develop efficient forgery detection skills for border guards and Consulate staff.

3) Pursue

Information exchange

- Examine how we can better protect our borders by improving the cross checking with data bases when someone enters the EU (making full use of SIS etc.).
- We should step up data sharing between the EU and the US, and continue to work on the proposal to allow the US to get access to Analytical Workfiles and to start a project for Afghanistan similar to the VENLIG project (in which the US shares data collected with Europol) exploiting also data which the US receives from third countries such as Pakistan and Yemen in return for provision of the PISCES frontier control system.

Legislation

- Initiate a discussion on whether the Framework decision on terrorism[1] should be amended so as to make it a crime to attend a terrorist training camps in the EU and abroad.

[1] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism - OJ L 164, 22.6.2002, p. 3 and 2008/919/JHA of 28 November 2008 - OJ L 330, 9.12.2008, p. 21.

International cooperation

- Ask Europol to produce a specific report with Frontex on the link between Islamists and organised crime: look at the routes (the American Somalians were transiting through European hubs), modus operandi (disguising techniques: tourism, pilgrimage, visiting relatives etc.), means of transport, facilitation network, link with trafficking in Human Beings, travel hubs etc.

Challenge III
Cyber Security

The Stuxnet incident in summer has shown again that critical infrastructures can be vulnerable to attacks on their information and communication components. A more intense discussion on cyber security has since started in the EU and the subject is on the agenda of the next Summit with the United States. NATO is including the threat of cyber attack in its new Strategic Concept for the November Summit in Lisbon.

The overall assessment of the cyber threat is that, for the moment, cyber terrorism is not the major hazard. The main risk comes from criminal networks, State driven or State sponsored attacks or individuals. But cyber attacks would be attractive for terrorist groups for the same reasons which attract criminal or other hostile actors. Cyber creates a cheap tool, targets can be attacked from all around the world, a small attack can have huge impact, and the internet still offers anonymity. Like in the field of the CBRN threat we have to start our preparation before terrorists acquire know-how or capacities to target our infrastructures.

When it comes to preventing cyber attacks, the same methods of prevention and preparedness are effective against attackers from all backgrounds. However, to achieve a high level of cyber security and preparedness is a complex and time consuming task. The EU has made major progress in the field of cyber crime, cf. we have common legislation on cybercrime, the relevant Framework Decision will soon be "Lisbonised" and extended to cover botnets. The EU also advocates the establishment of a European Cybercrime Center by 2013, which will include both national and European alert platforms (ICROS - Internet Crime Reporting Online System) to report cyber/internet crime. But we need to do more on the protection of cyberspace as a critical infrastructure.

Through cooperation among Member States and Commission initiatives we have already achieved major progress. The Action Plan endorsed by the Council in December 2009 (Council Resolution on a collaborative European approach to Network and Information security) included several initiatives like a European Forum for Member States (EFMS) and European Public Private Partnership (EP3R), reinforced cooperation between CERT's or national/EU exercises (the first European exercise, "Cyber Europe 2010", was held in November 2010). But there is still a need to come forward with a better integrated approach. From my perspective we first need to clarify what we mean by cyber security and to distinguish clearly our task in the EU from the work done at NATO on the one hand and from cyber crime or content related crime (copyright, illegal content…) on the other. Cyber security in this sense means protection of our vital infrastructures (state and private communication) against attacks in cyber space. This is as much a civilian task as it is a military issue. To achieve a higher level of cyber security we should address the following issues:

Recommended action:

- The EU institutions have been victim to cyber attacks and must be better protected. This is also a challenge for the new created EEAS: Well protected networks are the precondition for sharing sensitive information, including personal data. Therefore I welcome the initiative by Commissioner Kroes to appoint of a group of wise men to explore the set-up of an EU Computer Emergency Response Team (CERT).
- Achieve a minimum level of cyber security preparedness throughout the Union: We could consider some kind of peer evaluation (like for Counter Terrorism): asking whether all Member States have a CERT (24/7), a strategy, some crisis arrangements, regulations to protect their networks and are conducting exercises etc.
- Create and improve the network of institutions and representatives in the EU. There are good networks on technical level and Europol and the law enforcement community have their own networks. What is needed is an integrated approach bringing all aspects together in the form of an EU cyber strategy, endorsed by the European Council.

- We should start a debate on whether we need international common guidelines or a code of conduct for the internet, for example to protect humanitarian infrastructures like hospitals etc against cyber attacks from States. At the same time we need to be careful about a worldwide legally binding treaty regulating the use of the cyberspace. This raises the risk of attempts by a number of States to legitimize controls over content. A better idea is an informal process modelled on the Financial Action Task Force (FATF). This was set up within the OECD to provide informal guidelines for prevention of money laundering, but as these guidelines were adopted in all major jurisdictions, they have become de-facto international standards. An FATF-type process would recognize the dynamism of the Internet (which owes a lot to its decentralisation, openness and soft regulation) together with the need to improve its governance.
- Nevertheless, we cannot neglect the question of content just as we cannot neglect the need to deal with hate speech when we discuss freedom of the press. Al Qaeda propaganda in English - eg Al Awlaki's magazine "Inspire" - hosted in the US, is recruiting EU citizens. We need to develop robust standards against this, including with the US.
- The EU and the Member States should initialise a discussion on the industrial policy aspect. Cyber security needs secure components. In some sectors the EU has already lost its capacities to produce its own components.

Challenge IV

The External Dimension

In my past reports I have written extensively about the need to better coordinate the internal and external dimensions of policy making, and my hope that the new EEAS will be able to ensure this. I need not repeat these arguments here, as the EEAS is now taking form and I look forward to working with it directly. I was happy to be able to accompany the High Representative on her recent visit to India, a country where Counter-Terrorism is of major importance to the strategic relationship that the EU is seeking to build. I look forward to being able to provide similar support in the EU's relationships with other countries for which Counter-Terrorism is a major issue.

One issue, however, that does need to be raised at this point in the process of creating the EEAS is the need to ensure that the EU has adequate resources to support its external Counter-Terrorism effort. During my visit to Yemen last week, I was struck by the fact that the Government of Yemen's complaints were much harsher against European countries which had taken restrictive measures following the recent bomb scares than they were against the US. A major reason for this was the way in which the US was able to balance the restrictive measures needed to protect its internal security with an immediate and public gesture of support to the Government of Yemen. John Pistole, Head of the US Transport Security Administration, visited Yemen within days of the detection of the suspect packages, and the US was also able to send staff and equipment to Yemen within the same time-scale. If the EU were able to respond to future such events in a similar manner, it would significantly increase its influence in the countries where we most need to be effective if we are to achieve our internal security goals.

There needs to be a step change in the amounts which the EU devotes to Counter-Terrorism assistance. Terrorism is one of the major threats to international stability. In Pakistan and in Yemen it is directly challenging the State. In the Sahel, terrorists operate as if the States did not exist. If the EU is to be a serious actor in promoting global stability, and wants to promote a distinctive approach to CT based on the rule of law, it needs to put proper resources behind this. The sums of money potentially involved are not enormous by the standards of development programmes, a lot is already being achieved with very little. It was a major step forward that the 2009-2011 long term IfS introduced even the possibility that the EU could start to get involved in supporting capacity building for CT. The envelope of € 10 – 14 Million is clearly inadequate to the scale of the problem and the dimensions of the role the EU can and should play. But it has enabled a start to be made: in particular in the Sahel. In addition to this, the crisis management IfS has stepped in to fund programmes in Pakistan (€15 Million) and in Yemen (€15 Million). These programmes are just now getting underway. They are by nature high risk, but the price of failure by the Governments we are trying to assist would be borne directly by European citizens facing an increased threat of terrorist attack. It is essential that we learn the lessons from these first projects and use them to build a real expertise going forward. It is also essential for our credibility with the countries concerned that short term actions are seen to have sustainable follow up.

The EEAS needs to be able to use the short term Instrument for Stability (IfS) to intervene in situations like Yemen or Pakistan, coordinated with the actions of other EU Institutions. Just as important, this immediate and coordinated action needs to fit into the broader engagement of the EU in the country concerned. If the short-term actions undertaken are to produce sustainable change for the better, they need to be integrated with a longer-term plan to develop the capacities of the country concerned to fight against terrorism. And both need to be informed by the reservoir of expertise on assistance in this area which is only now being developed. This means that, to the greatest extent possible, both the short and longer term actions should be planned and implemented by the same people, ideally by people based on the ground in the countries concerned.

Recommended action:

- An increase in the funding envelope for Counter - Terrorism in the next Instrument for Stability.
- Programming of the IfS should be undertaken by the EEAS. Implementation of longer term CT funding should be implemented by the same group who will manage funding of the short - term Instrument for Stability.
- Funding of posts within the EEAS in specific countries where Counter - Terrorism forms a major part of the future relationship.

Challenge V

Fighting discrimination and social marginalisation

In addition to the specific focus on fighting radicalization and recruitment, which is counter-terrorism specific, the issue of discrimination and social marginalisation is also relevant and important in the context of the fight against terrorism. It is too simple to say that discrimination and marginalisation lead individuals into terrorism: the processes at work are more complex. However, better social inclusion could contribute to reduce the pool of persons potentially inclined towards violence. Problems of social exclusion can also be exploited as part of the terrorist narrative.

The EU legal framework already prohibits ethnic and racial discrimination in the field of employment as well as in areas such as social protection, education and access to goods and services, including housing[1]. Discrimination on the grounds of religion or belief, by contrast, is currently only prohibited in the field of employment in EU legislation[2].However, in 2008, the Commission submitted a proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation (COM (2008) 426 final), which would also prohibit discrimination on the grounds of religion or belief in areas outside employment. The Council's preparatory bodies are continuing their examination of the proposal, but no agreement has yet been reached.

Recommended action:

- The Terrorism Working Group could start examining the impact on CT policy of the experience of discrimination.

[1] Directive 2000/43/EC.
[2] Directive 2000/78/EC.

Further Challenges

I have listed above some topics on which the EU should be working now. New challenges are already foreseeable for the near future.

We have a successful programme on security related **research**, and are starting to see the first interesting results. It is in our own interests to continue this programme also under the 8th Framework Programme and to guarantee that security related research will have its proper share of the new programme. Budget cuts and the financial crisis make it even more important to share research costs at Union level. We have to look to future priorities. We still need to develop a better capacity within the internal security sector to identify our real needs in the longer term, we need to work better with the private sector in the form of Public Private Partnerships to deliver those needs, and we need to be better at exploiting synergies with the private sector more generally, for example most people trust the company that sells them their anti-virus software with much greater access to their computer than they would be willing to give to the State. We also have to look for possible synergies in both fields military and civilian research. I will table a proposal for this in the first half of 2011.

The implementation of the **Solidarity Clause** also remains a pending task. We all have a vital interest in having a mechanism in place before a future crisis demands the creation of something ad hoc. Given the security concerns of several Member States and the current threat assessment it seems to be even more urgent to have a proposal soon. First discussions to further evaluate the meaning, the extent and the possibilities of this clause are now taking place. There is an urgent need to answer some preliminary questions related to the scope and meaning of Art. 222 TFEU before moving ahead further (eg when does "prevent" start, what is the relation to other mechanisms, what is the military dimension)? Art. 222 TFEU deals with incidents "in the territory of the Member States", but experience so far, for example from the latest CCA exercise, demonstrates that it is crucial to coordinate better the different crisis reaction mechanisms that exist (both internal and external).
