Statewatch

Submission to the
Select Committee on the European Union
Sub-Committee F (Home Affairs)

INQUIRY INTO EU COUNTER-TERRORISM ACTIVITIES

Call for evidence

Sub-Committee F (Home Affairs) of the House of Lords Select Committee on the European Union is conducting an inquiry into counter-terrorism activities in the EU. It will examine proposals that have been made since the Madrid bombings of 11 March, in particular for changes in the institutional arrangements and for facilitating data exchange within the EU [Footnote 1].

Questions on which the Sub-Committee would particularly welcome views include the following:

Examples of concern:

Justification

Q: Does the fight against terrorism require much greater operational co-operation and freer exchange of data between law enforcement authorities (both national and EU)?

In our Scoreboard produced in March 2004 we identified 56 proposals in the EU counter terrorism plans that followed the Madrid bombings. Our analysis found that 27 of these proposals which were a danger to civil liberties or had little to do with combating terrorism. This is available at: http://www.statewatch.org/news/2004/mar/swscoreboard.pdf

There have been a number of developments since this was published.

Exchanging information on terrorist investigations

There certainly is a need for greater operational cooperation between law enforcement agencies in the fight against terrorism. However, this cooperation should a) be limited to terrorism and b) ensure that the rights of suspects are observed.

For example, the Commission proposal (COM (2004) 221) provides for the information gathered during the investigative phase being communicated to Europol, Eurojust and agencies in the 25 member states.

It is sensible that such information should be made available. However, the proposal contains no provision for the "information" to be removed/deleted should a person be found innocent. There is no provision for the "information" passed over on those caught up in a "criminal investigation" but never charged or convicted to be removed/deleted. This is especially worrying as an "investigation" into a suspected terrorist offence would embrace not just the subject but their family, friends and work associates to see if there were any links to the suspected offence. A typical investigation could

involve 20-40 other people who are found to be quite innocent but "information" on them could be "immediately" transmitted to dozens of agencies across the 25 EU member states.

In April ten Muslim "suspects" were arrested in the north of England but never charged - this could have led to several hundred names and personal details being put into EU-wide circulation with no obligation for this data to be deleted. If there is no obligation to delete the names and details of innocent people they could find themselves on "watch-lists" for years to come.

There is another problem with the draft Decision. The intention is to widen the scope from those persons, groups and entities placed on updated lists of terrorist groups on formally adopted EU lists (see: Lists) to all those investigated under Articles 1 to 3 of the controversial Framework Decision on combating terrorism (2002) which, despite some amendment, is still ambiguous as to where the line is drawn between terrorism and, for example, large-scale protests. It covers those acting with the aim of:

"unduly compelling a Government or international organisation to perform or abstain from performing any act" (Art 1.ii)

To broaden the scope of cooperation on terrorism to this much broader definition open the way for abuse and its application to non-terrorist offences.

INTELLIGENCE-GATHERING THROUGH "SITCEN"

In June 2004 Javier Solana, the EU High Representative for defence and foreign policy, announced that internal security services (eg: MI5 in the UK) are to provide intelligence on terrorism to the Joint Situation Centre (SitCen) - part of the EU's emerging military structure. At the same time he revealed that the external intelligence agencies (eg: MI6 and GCHQ in the UK) had been cooperating with SitCen since "early 2002". These moves were clearly needed as attempts to bring together meaningful intelligence on terrorism through Europol was doomed to fail - internal security and external intelligence agencies are loath to share information with police agencies. However sensible this initiative may be it still begs the question of accountability and scrutiny. It would be almost inconceivable at the national level for a body whose role was military to have its remit extended "at a stroke" to include anti-terrorism without a formal procedure being undertaken - and to ensure that a chain of accountability and scrutiny both to government and parliament was set out.

SitCen's job is to produce assessment reports on "the terrorist threat (internal and external)" but it is also to provide reports that cover:

"the broad range of internal security and survey the fields of activity of services in the areas of intelligence, security, investigation, border surveillance and crisis management" (Dutch Presidency Note to the Informal Meeting of the JHA Council in October, unpublished doc no: 12685/04)

The overall concept has, however, swiftly shifted from dealing solely with "anti-terrorism" to "internal security" which embraces all the agencies of the state from the military to the host of agencies who maintain "law and order", from biometric passports to border controls. It is the same in the draft "Hague Programme" on justice and home affairs (the successor to the "Tampere programme"), which refers to internal security as covering: "*national security and public order*."

SitCen will send "advisory reports" to the Justice and Home Affairs Council, reporting "any necessary action", and will cooperate with a host of JHA bodies, including the Strategic Committee on Immigration and Frontiers and Asylum (SCIFA) and the Article 36 Committee (CATS, senior national interior ministry officials), and representatives from the Commission, Europol, Eurojust, the European Border Agency (EBA), the Police Chiefs' Task Force, the Counter Terrorism Group (CTG) and a new "internal crisis management" working party. The EU Police Chiefs operational Task Force, which was set-up in 1999, still has no legal basis for its activities, it is unacceptable that there should be any extension of this groups mandate or remit until this issue is resolved

Under the EU Constitution, SitCen will also report to an "Internal Security Committee" (Article III-261)

which will deal with "operational cooperation on internal security". An ad hoc "Internal Security Committee", comprised of the chairpersons of the JHA bodies above, is to be set-up in the near future, before the Constitution comes into force. Under Article III-261, the European and national parliaments will only be kept "informed" of the new committee's activities - which on past experience will be bland, general reports. There is no guarantee that documents from this Committee will be accessible and little prospect of the interim, ad hoc Committee being accountable.

THE EUROPEAN BORDER AGENCY

The EU Border Police is developing in an ad hoc fashion. Before the Regulation establishing an EU Border Management Agency had even been agreed the EU had established a Common Unit of senior border police, operational centres on sea, land and air borders, and a risk analysis centre. Now, before the Regulation has even entered into force (1 May 2005), a broad expansion of the agencies remit and powers is planned. First, through the creation of a "rapid reaction force of experts" available to "temporarily" increase "external border control capacity" (including "intercepting and rescuing illegal immigrants at sea"). Second, through the creation of a "common European border police corps". Third, consideration of whether it should assume a wider roles for "security, customs" as well as:
the management of large information systems (such as Eurodac, VIS and SIS II) (Dutch Presidency Note to the Informal Meeting of the JHA Council in October, unpublished doc no: 12714/04)

Data exchange

Q: The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement authorities in the EU. To what extent would this challenge fundamental legal and constitutional principles of Member States?

This proposal is present in COM (2004) 429 and has been widely criticised. It proposes a free, open, market for criminal data and intelligence held by the hundreds of law enforcement agencies in the EU - an idea unlikely to find favour with governments or the agencies themselves (see, Home Office EM, 6 July 2004).

Inside sources say that this proposal is unlikely to survive in this form and that a proposal based on specific requests (on named individuals or groups) is likely to replace it (see for example, COM (2004) 664 on the exchange of information extracted from the criminal record).

The “Hague Programme” speaks in general terms of the “availability” of investigative information from 2008.

Q: The Commission calls for the interoperability of EU databases. What are the implications of a facility for transferring data between databases? Is there a case for a centralised EU database for all law enforcement purposes?

The EU uses the term to mean that the various EU databases can be linked or accessed by all law enforcement agencies (the Hague programme refers to SIS, VIS and Eurodac).

The fundamental assumption in the 1990 Schengen Convention is that only those agencies which input data should have access to data in their field. For example, data put onto the SIS by immigration officials would be accessible by them for the purpose of excluding those not to be granted entry.

The change came to a head, after 11 September 2001, when internal security agencies (like MI5) wanted access to all SIS databases. The problem was that such agencies could not abide by the data protection provisions of Schengen. In some states internal security agencies simply submitted searches via police agencies. The solution was "interoperability", namely that a database created for one purpose could be accessible and used for other purposes.

Data protection rights for data held on the SIS are almost unworkable at the moment. Only in a few cases has individuals learnt that action taken against was based on information derived from the SIS.

Complaints then have to be made not against the SIS but the state which placed the information on the SIS. Even if erroneous information is deleted by that state there is little chance of tracing and eliminating the "paper-trail" whereby other states have used the information on their national databases.

Any links between Eurodac and other databases should be strictly limited to searches relating to the question of which Member State is responsible for considering an asylum-seeker's application. This would mean that an asylum-seeker's fingerprint sent to Eurodac could be checked against the fingerprints in the VIS of persons who have been issued visas, because that is one of the criteria for allocating asylum responsibility, but not against the fingerprints of persons who have requested visas or whose applications have been refused. Even in the first case a Eurodac/VIS link would have to be denied for the UK, since we have opted out of participation in the VIS and should not be permitted to participate through the back door.

A Eurodac/SIS link should be totally out of the question even when fingerprints are held in the SIS, because the categories of data in the SIS are not comparable to the grounds for allocation of responsibility for asylum applications. In particular it is not relevant for allocating responsibility that a person is listed in the Article 96 category as a person to be denied admission. Nor should it be possible to have links to this data (or other SIS categories) for the purposes of deciding on the asylum application on the merits, since a prior decision that a person should be refused entry to a Member State should clearly not be relevant to deciding whether a person has a valid claim to be a refugee or in need of other protection. Given the weak procedural rights for individuals in relation to the SIS, this would weaken procedural protection for asylum applicants to an even more unacceptable level.

As to the idea of a "*a centralised EU database for all law enforcement purposes*" it can be argued that the SIS in the form of SIS II is developing in this direction. However, it is not intended to cover criminal records which would require "harmonisation" through a standard European Criminal Record - which is many years away.

Data protection

Q: Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third Pillar, as advocated by the Commission?

The question makes an assumption in asking whether "*current data protection arrangements continue to provide an adequate level of protection for the individual*". In our view the current arrangement offer little protection at the moment - this is true of data protection in general (see the Commission's first and so far only review of the 1995 Directive) and certainly as regards the third pillar. The planned functionalities of SIS II and "interoperablility" make the prospect of protection and rights look even less likely than under the present quite unacceptable situation.

What is intriguing about the final version of COM (2004) 429 on "enhancing access to information by law enforcement agencies" is that the draft discussed by the full Commission in May also included the phrase:

"and related Data Protection issues"

And equally intriguing is Chapter III of COM 429 which refers to data protection but in the sense of preparing a Framework Decision::

"in order to empower access to all relevant law enforcement data by police and judicial authorities"

There is no mention of a measure on data protection and the third pillar in the "Hague Programme". The hope for a legal framework covering the third pillar may, it seems, have to wait until the Constitution enters into force and the commitment for data protection covering all EU activities is put

into practice.

Footnote:

The issue of data protection in the "third pillar" (justice and home affairs: policing, immigration and asylum and judicial cooperation) has long been recognised as a "gap" in EU policy (the 1995 Directive on data protection does not cover this area). The issue of data protection in the "third pillar" was first raised in the Council of the European Union (the 15 governments) in May 1998. The German Presidency of the European Union, 8 June 1998, said to the: "search for the (lowest) common denominator in this field is not new". However, the "Action Plan of the Council and the Commission on how best to implement the provisions of Amsterdam establishing an area of freedom, security and justice" (13844/98) said that data protection issues in the "third pillar" should be: "developed with a two year period" (IV.47(a)). It was not until August 2000 that a draft Resolution drawn up by the Working Party - this was revised five times, the last being on 12 April 2001 under the Swedish Presidency of the EU (6316/2/01) when agreement appeared to have been reached - and the Article 36 Committee was asked to address outstanding reservations. This draft, although peppered with exceptions and derogations, could have been the basis for a public debate. However, since 12 April 2001 there has been silence - and under a rationalisation of the Council's working parties from 1 July 2002 (6582/1/02 REV 1) (reducing the number of Working Parties from 26 to 15) the Council's Working Party on data protection was abolished without explanation.

Immigration and asylum legislation now makes reference to the data protection directive – however, the Commission has long being saying that it plans to set out standard rules on third pillar data protection, but has never done so.

Q: Should there be common standards for the transfer of personal data from EU bodies and the Member States to third countries/bodies, including Interpol?

Yes there should be but it depends on the "common standards". Europol is now authorised to exchange personal data with a host of countries and agencies. This authorisation based on reports on data protection from the intended third states - these are uniformly based on the "legal position" and not on the practice.

"Common standards" have to be based on the fundamental principles of the 1995 Directive, the 1981 Council of Europe Convention and recommendation on policing data, Article 8 ECHR, relevant case law of the European Court of Human Rights, along with the specific right to data protection set out in the EU Charter of Fundamental Rights.

Such standards would, for example, have ruled out the EU-USA agreement on PNR (passenger name records). The USA does not have a data protection law covering EU citizens and has the clear intention of using the data for purposes other than for which it was collected.

The role of the EU

Q: Is there a need for an EU intelligence policy, as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?

This question should perhaps be more specifically defined. We presume it refers to an intelligence role in relation to terrorism and not a general intelligence role.

There is a clear and legitimate role for the EU to have an intelligence-gathering capacity in order

to combat terrorism. However, any extension of this role to cover "any threats" (as we have seen in a recent Council document) would raise major questions of accountability and decision-making (see the answer to the first question).

Q: How important is it for the EU to speak with one voice in the international arena in matters involving counter-terrorism co-operation?

This is hard to envisage. Firstly, there is the special relationship between the UK and the USA dating from 1947 (UKUSA agreement) and their sharing and gathering of intelligence through GCHQ and Echelon. Second, many major policy initiative are formulated in G8 (and its working parties).

We believe that there is another major issue which needs to be addressed in this context, namely the growing influence of the USA over EU justice and home affairs policy-making. During each six-monthly Presidency cycle there are at least 40 high-level meetings (some by video-conferencing) on JHA issues.

These meetings are not simply exchanging views or ensuring operational cooperation but are leading to issue of "concern" to the USA being placed high on the EU agenda (eg: preparatory offences related to terrorism). We will be happy to elaborate on this aspect orally.

Q: The United Kingdom recently hosted a summit of five Member States ("G5") to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?

It is interesting to note that membership of the "G5" group set up last year - UK, Germany, France, Italy and Spain - overlaps with EU membership of G8 - UK, Germany, France and Italy (with the exception of Spain, then under Aznar).

G5 because is not subject to any form of accountability or public or democratic scrutiny and appears to be having a growing role in driving the JHA agenda. It does not meet the criteria for enhanced cooperation since it does not follow the obligation to apply EC or EU processes (which would entail some degree of accountability and scrutiny) and it does not meet the criteria for minimum participation by Member States (at least 8). Why should the large and powerful interior ministries of these member states be able to dictate to the Commission, the European Parliament, national parliaments and smaller member states.

Institutional arrangements

Q: What is the added value of the post of EU Counter-terrorism Co-ordinator? What should his role be?

The value of having a Coordinator is perhaps not so much the post itself but an indication that there is an intention to coordinate the different initiatives in a way that was clearly not the case before 11 March 2004 (Madrid) - three days prior Mr Solana had produced a lengthy report on the many shortcomings in anti-terrorist planning, coordination and operations.

Q: What changes are called for in the EU's institutional arrangements (including Eurojust, Europol, the Chief Police Officers' Task Force, and the Terrorism Working Group) in order to combat terrorism more effectively?

The current plans, and the creation of the Article 261 Committee under the Constitution, should provide the means necessary to combat terrorism. The problems will arise if the Article 261 Committee and SitCen take upon themselves - as there is a clear intention to - a wider role. This is to say all the ramifications of "internal security" as distinct from counter-terrorism.

The Article 261 Committee on operational cooperation on internal security presents its own problems of accountability. European and national parliaments are only to be kept informed of it's activities and whether the Regulation on access to EU documents will apply to it or whether a standard exception under Article 4.1.a will be routinely used is not clear.

Note prepared by Tony Bunyan, Steve Peers and Ben Hayes. 12 November 2004