

The logo for the Transnational Institute (TNI) consists of the letters 'TNI' in a large, white, serif font, set against a dark grey rectangular background.

Transnational Institute  
<http://www.tni.org/crime>

*Crime & Globalisation Paper*

**Paper presented at:**

**Global Enforcement Regimes  
Transnational Organized Crime, International Terrorism and  
Money Laundering**

**Transnational Institute (TNI)  
Amsterdam, 28-29 April 2005**

---

## **The exceptional and draconian become the norm**

**The emerging counter-terrorism regime: G8 and EU plans for  
"special investigative techniques", the use of "intelligence  
information" in court and new "preparatory" offences**

**By Tony Bunyan  
Statewatch**

1. Introduction
2. G8: How G8 is setting the agenda
3. G8: USA takes over Presidency
4. EU: The initiative launched
5. EU: The Council of the European Union take up the initiative
6. COE: Council of Europe: Draft Convention on Terrorism
7. Conclusions and implications

### **1. Introduction**

This paper examines the new counter-terrorism regime being planned by G8 and EU:

**"Special investigative techniques"** including phone tapping, "bugging" premises, informers, undercover agents and bribes for information. The results of this surveillance would be "available" to agencies across the EU and outside.

**"Intelligence information"** surveillance "products" from more than a dozen sources - including ones from outside the EU - will be presented as "evidence" in court while "protecting" the sources.

**"Preparatory offences"** intended to criminalise people prior to a terrorist act being committed. And as being discussed in the Council of Europe this could cover the crime of *apologie*: *"where the message, although not directly advocating such acts, would be reasonably interpreted to have that effect, inter alia, by presenting an act of terrorism as necessary and justified"*.

The paper tracks the hidden discussions in G8, the Council of the European Union and the Council of Europe and pinpoints the role played by the USA and the UK in shaping the outcomes.

The first is to broaden "terrorist offences" to cover preparatory and associated acts even where no terrorist attack has been carried out or even planned and for *apologie*, condoning or sympathising with terrorism.

Second, within these broader remits to make lawful the use of "special investigative techniques", such as tapping, bugging, informers, bribes, undercover agents, access to all government databases (datamining) and the sharing of this "intelligence" with other agencies - whether inside or outside the EU. Where "obstacles" exist, like requiring judicial authorisation, these should be overcome. "Self regulation" by the agencies, with all the dangers of misuse and abuse, is to be the new norm.

Third, the intelligence gathered should be used in court while ensuring that it is "protected". The "protection" of intelligence will inevitably be counter to the normal rule of law and the rights of defendants in a democracy.

The inexorable build up of "intelligence" is fuelling these demands for new offences where people cannot now be charged and brought before the courts. Armed with "special investigative techniques" and their products the defendant will never know what the evidence is against them, where it came from and how it was gathered.

The USA and the UK invaded Iraq together. The USA and the UK have detained people indefinitely without trial and in defiance of the rule of law.<sup>1</sup> Now in a classic case of "policy-laundering" the USA, backed by the UK, are working through G8 to get these demands agreed in the EU. Indeed they have offered to draw up a list of "obstacles" to "compliance" with them for EU member states to overcome.

---

1. The UK has just passed the Prevention of Terrorism Act 2005 enabling it to place people under "control orders" restricting their movements and communications. This is covered in detail in: <http://www.statewatch.org/news/2005/mar/exceptional-and-draconian.pdf> The Labour Party election manifesto says a new law will be introduced to cover activities which "glorify condone acts of terror".

These new offences, techniques and changes in the legal process are likely to spill-over into the mainstream criminal justice system and establish new norms – the discussion refers to transnational crime and crime in general. For example, nowhere is it suggested that the use of "special investigative techniques" should be limited to tackling terrorism – "terrorism" is simply grounds on which to legitimate their usage. What has been seen as exceptional and draconian becomes the norm.<sup>2</sup>

The paper looks at moves by the USA, G8, the Council of the European Union and the Council of Europe to introduce new preparatory offences including *apologie*, "intelligence information" as "evidence" in court gathered by "special investigative techniques" including from third states.

## 2. How G8 is setting the agenda

The role of the G8 took on a new dimension after 11 September 2001.<sup>3</sup> It is a "global" grouping, which can set global standards. Two of its first demands were for international standards for biometrics on passports and the retention of telecommunications traffic data - the first of which has been agreed by the EU and second is now going through its legislative process. Another was for checking and surveillance of all visitors entering a country - the USA has introduced this and the EU is about to (commonly known as checking "PNR", Passenger Name Records, against "watch-lists").<sup>4</sup> It is also of relevance to note that four G8 members already detained people without charge and trial – USA, UK, Russia and Canada.<sup>5</sup>

As the ideology of the "war on terrorism" deepened, and became permanent, other standards were set out by G8. Notable in this context are the G8 Recommendations on Transnational Crime which were "endorsed" by the G8 Justice and Interior Ministers at Mont-Tremblant in Canada on 13-14 May 2002.<sup>6</sup> Although headed "transnational crime" the Recommendations were directed at "transnational crime and terrorism".<sup>7</sup>

---

2. In response to civil liberties critiques the previous Justice and Home Affairs Commissioner in the European Commission, Antonio Vittorino, said: "We have not created emergency legislation, we did not create special courts, we did not create special regimes of detention. Those are the areas where real, serious limitations to civil liberties might arise" (launch of the "Tampere II" process in July 2004).

3. G8 is comprised of the USA, Canada, France, Germany, Italy, the UK, Japan and Russia. The key G8 working groups are the Roma Group (set up in 1978 and comprised of intelligence and internal security officials, known as the Counter Terrorism Experts Group) the Lyon Group (law enforcement officials dealing with organised crime set up in June 1996) and the judicial cooperation group (there are others on issues like immigration).

4. The construction of terrorist lists were advanced through the UN, USA and EU, and were accompanied by measures to track and freeze funding for suspected terrorist groups.

5. On Canada see: <http://www.cbc.ca/story/canada/national/2004/12/10/security-certificate-041210.html>

6. These were previously known as the "Lyon Group Recommendations".

7. EU combating terrorism or crime? <http://www.statewatch.org/news/2004/jun/08eu-terrorism-and-crime.htm>

Among the key Recommendations is a section on "Strengthening investigative capabilities" including "Investigative techniques". Even among the G8 countries, let alone the EU and the rest of the world, the use of telephone-tapping, bugging and video surveillance, informers, *agent-provocateurs* and undercover agents is stringently circumscribed in law – in many EU countries judicial authorisation is required to carry out covert surveillance.<sup>8</sup>

For example, in seven EU states the police require judicial authorisation to access "documentation of telephone tapping" and in a further nine states they cannot obtain this information without judicial authorisation. For "documentation of room bugging" eight states require judicial authorisation to access it and in a further nine states they cannot obtain this information without judicial authorisation. In nine states "real-time" telecom monitoring requires judicial authorisation to access and in fourteen states they do this without judicial authorisation. As to access to traffic data held by service providers in nine states the police require judicial authorisation and thirteen states cannot obtain this information without judicial authorisation. **"Judicial authorisation" is seen within the G8 plans as an "obstacle" to efficient cooperation between agencies – both internally and externally.**

The use of such investigative techniques is perceived as being exceptional and their everyday use associated with authoritarian states. In May 2002 this G8 meeting agreed on: *"the relevance and effectiveness of special investigative techniques such as electronic or other forms of surveillance technology, undercover operations and controlled deliveries"*.<sup>9</sup>

G8 states were called on to review their: *"domestic arrangements for those techniques, also ensuring any necessary anonymity of undercover agents and to conclude where necessary, appropriate bilateral and multilateral agreements and arrangements for using the special investigative techniques in the context of cooperation at international level..."*

This commitment is immediately followed by the following Recommendation: *"We emphasise the importance of giving the fullest possible protection to sensitive information received from other states. The competent authorities of different states should advise each other as to the requirements regarding the disclosure of information in the course of judicial and administrative proceedings, and discuss in advance potential difficulties arising from those requirements."*

---

8. See survey of current police powers: <http://www.statewatch.org/news/2005/feb/01police-data-exchanges.htm>

9. "Controlled deliveries" is a relatively recent development and describes a police or customs operation which is deliberately set up by the agencies in order to catch perpetrators.

From this point on there is an ongoing link between "special investigative techniques" and how to allow the product of surveillance to be used - whether by other "friendly" agencies or in "judicial proceedings".<sup>10</sup>

The meeting of G8 Ministers of Justice and Home Affairs in Paris on 5 May 2003 (prior to the Evian G8 Summit) reiterated the need to "promote special investigative techniques" and called on their "experts" to "identify the obstacles" to international judicial cooperation in this area.

### 3. USA takes over the Presidency of G8

The USA took over the Presidency of G8 on 1 January 2004 and sent out a questionnaire to its member states drawn up by the "Roma Group". On 23 February 2004 there was a EU-US high-level officials meeting on justice and home affairs under the "New Transatlantic Agenda" held in Dublin. The Irish Presidency Chair of the EU's Article 36 Committee<sup>11</sup>, assisted by officials, met with their US counterparts. The meeting was a: "EU-US Troika JHA Informal/SCIFA Informal Troika" (Troika refers to past, present and next EU presidency).<sup>12</sup> The report on the meeting is peppered with references to on-going work in G8 (of which neither Ireland nor the next EU Presidency, Netherlands, are members).<sup>13</sup>

At the meeting the US took the lead on the topic of: "Terrorism prevention measures" and *"expressed three concerns regarding [EU Member] States abilities to fight terrorism"*:

*"The first concern was that states' legal systems should allow their law enforcement authorities to take action against preparatory acts for terrorism at a stage where no terrorist acts had been committed."*

The second US concern was the ability of EU states to: *"afford mutual legal assistance and extradite persons for preparatory acts."*

---

10. On 25 June 2003 the EU and USA signed agreements on extradition and mutual legal assistance - these have yet to be ratified by the USA and a number of EU member states. The agreement on mutual legal assistance includes the creation of joint investigation teams and requests for "assistance" - for example, to place under surveillance an individual or group and supply the "products" of this to the requesting state. See: <http://www.statewatch.org/news/2003/apr/01Auseuag.htm>

11. The Article 36 Committee is a Coordinating Committee consisting of senior officials that was set up under Article 36 (former Article K.4) of the Treaty on European Union (TEU) to prepare the ground for Council deliberations on police cooperation and judicial cooperation in civil matters.

12. Although the UK was not represented at the Dublin meeting, Home Office, police, MI5 and MI6 officials were at the earlier key meetings in G8 of the Roma and Lyon groups. These officials, together with their counterparts from three other EU states (France, Germany and Italy), had by the time of the meeting on 23 February already agreed on the "concerns", sent out a questionnaire and received replies from all G8 members (including from the UK).

13. EU doc no 6862/04: <http://www.statewatch.org/news/2005/jan/6862-eu-us.pdf>

While the third: *"probably most difficult issue which was raised by the US was how to share intelligence information related to terrorism for use in a criminal proceeding in another country, while ensuring that the intelligence would be protected.*

*"This question is two-pronged: (1) have states the legal ability to protect intelligence information, and (2) how can the (prosecutorial) authorities of a state be informed of the fact that another state holds intelligence information which is relevant to the terrorist case that is being prosecuted. The US clearly signalled that it was seeking to cooperate with the EU and its Member States on this issue. As a first step it suggested drawing up a document that would collate information from the US and the Member States, which would lay out to what extent and how states can protect intelligence information received from another country.*

*The G8 had already started work on this by way of a questionnaire that had been sent out to and replied by all G8 members. The US suggested that the EU might consider following up on this questionnaire in relation to use of intelligence information."*

In summation the USA said that:

1. law enforcement agencies should be "allowed" to take action against preparatory acts for terrorism where no such act has been committed.
2. extradition should be allowed for "preparatory acts".
3. intelligence "information" should be used in court and while ensuring it is "protected".

Even as the USA was canvassing the EU to support these ideas it was preparing to put a series of issues openly and explicitly on the table at the G8 meeting of Justice and Home Affairs Ministers in Washington on 11 May 2004 - it should be remembered that of the now 25 EU member states only the UK, France, Italy and Germany have a say (the European Commission is also in attendance).

The press release from the Washington meeting again linked the use of "advanced investigative techniques" with the "sharing" of intelligence to: *"better prevent and disrupt terrorist activities and to prosecute terrorists"*

There were three detailed Recommendations on:

- "special investigative techniques";<sup>14</sup>
- "enhancing the legal framework to prevent terrorist attacks";<sup>15</sup>
- protecting intelligence in prosecutions.<sup>16</sup>

---

14. "special investigative techniques": <http://www.statewatch.org/news/2004/may/G8justice04-legal3.pdf>

15. "enhancing the legal framework": <http://www.statewatch.org/news/2004/may/G8justice04-legal2.pdf>

16. "protecting intelligence": <http://www.statewatch.org/news/2004/may/G8justice04-legal4.pdf>

The Lyon and Roma groups, under the French and US G8 Presidencies, had conducted a survey of "special investigative techniques" which led to the Recommendation that "legal systems" should "allow" the use of techniques such as: *"use of undercover agents, use of covert filing and listening devices, and covert interception of all forms of electronic communications"*

Seven Recommendations follow, including:

a. the use of *"special investigative techniques to support **criminal proceedings** at national and international levels"* (emphasis added)

b. the creation of a *"legal framework"* which allows the use of *"special investigative techniques"*

c. *"access to a broad array of special investigative techniques for the purpose of international investigation"*

d. here the Recommendation (no 6) makes a direct link between the use of the "techniques" and the use of their product in court: *"Requested States should work with requesting States to maximise the likelihood of admissibility in the requesting State of evidence provided through special investigative techniques."*

*The mere fact that a special investigative technique, carried out by the requested State in accordance with its law, would not be available to the requesting State in similar circumstances, **should not per se bar the use of evidence so acquired in the requesting State's courts**"* (emphasis added)

This could mean for example that the USA could request an EU state to conduct blanket electronic surveillance of a particular group based in the EU and this "intelligence" could be used in the USA where this power may not exist (or at least not the power to produce such intelligence "intercepts" by US agencies in its courts). Similarly, it covers tapes or statements from people held in states where the use of torture or inhuman treatment in suspected terrorist cases is the norm.

The second Recommendation covers creating a "legal framework to prevent terrorist attacks". The emphasis here is on people and groups suspected of preparatory acts requiring action in: *"situations in which the terrorist objective is not yet well defined and an attack may not happen for some time... prevention, investigation and prosecution are complimentary in nature..."*

The objective is to take action against people and groups "prior to terrorist attacks being carried out". What this means is not spelt out. Does this refer to people who are buying, gathering and collecting materials that could be used in an attack? If so this would be understandable. Does it mean people with "radical" views, who may have visited Pakistan or Afghanistan in the past and who consort with others, some of whom have done the same? If so this would be unacceptable.

The Recommendation calls for criminal offences covering "recruiting persons to commit terrorist acts" (which is clear) and providing "directly or indirectly" financial or other "material support" and: *"a person who engages in such conduct should be criminally liable not only where he or she knows or intends that the conduct will facilitate the commission of a specific attack, but also where he or she knows or intends that the conduct will facilitate the commission of future unspecified attacks"*.

The latter category is not clear. Does the giving of a mobile phone to someone constitute such conduct? The person may have "radical views" but in giving the phone how is intention to be judged? Does the giving of a pair of boots, which end up in Chechnia in the hands of a suspected Al-Qaeda group constitute giving "material support"? <sup>17</sup>

Another Recommendation specifically refers to social, religious and charitable groups who should also be subject to "special investigative techniques": *"while duly respecting established legal privileges recognised under domestic law, such as attorney-client or clergyman-penitent confidentiality and respect for diplomatic status, the fact of involvement of entities whether social, religious or charitable in nature, or of their leaders should not per se bar use of investigative techniques"*.

This set of Recommendations calls for i) the use of bribes ("incentives") to gather intelligence; ii) those defined above as "directly or indirectly" suspected of giving material support to be extraditable for "anticipatory or preparatory" offences; iii) states should "assist another country" by conducting "a broad array of special investigative techniques" against targets at their request.

The third set of Recommendations covers the use of "intelligence" gathered through "special investigative techniques" in the "prosecution of terrorists and their associates" while giving: *"appropriate protection to national security intelligence information in criminal prosecutions"*.

The Recommendations call on States to:

1. "adopt legislation" and "procedural safeguards" to "prevent, disrupt and pre-empt" terrorist activities by permitting: *"information sharing among and between their intelligence community, their law enforcement community and their prosecutors, to the fullest possible degree"*.
2. "adopt legislation" to establish "procedural safeguards" which will: *"permit national security intelligence information to be used in the prosecution of terrorists and those who commit associated offences, while protecting such information, including sources and methods by which such information has been acquired; **to the extent***

---

17. See, Observer, 19.12.04, article by Martin Bright. It is alleged that one of the men held in Belmarsh prison did exactly this.

**possible** consistent with a fair trial, such mechanisms, for example, include the use of summaries, substitutions or stipulations" (emphasis added).

What is meant by "summaries"? It implies that the agencies will be able to present an edited version of an intercept or statement from an informer? Does "substitution" means getting rid of juries and introducing judge-only "Diplock" courts? And does "stipulations" mean that defence lawyers will have to be vetted and defendants not allowed to see the "evidence" against them?

3. "adopt legislation" allowing: *"national security intelligence information"* from a third State to be *"used in a criminal proceeding"* subject to: *"the conditions, if any, agreed upon between the competent authorities in the originating State and those in the receiving State"*.

If "legislation" to this effect were adopted the "conditions" agreed between intelligence agencies would override the power of the courts to decide otherwise.

4. in "adopting" this "legislation" States should: *"give due regard to civil liberties and fundamental principles of law"*. Well, enough said.

Taken together these Recommendations would totally undermine any concept of a fair trial and the presumption of innocence. They would "legalise" the pre-emptive detention of those being held in Belmarsh who are being held on unseen "evidence" providing by UK intelligence and security agencies.<sup>18</sup>

The G8 Sea Island Summit in the USA on 8-10 June 2004 simply noted the Recommendations from the Justice and Home Affairs Ministers in Washington on 11 May 2004. The USA handed over Presidency of G8 to the UK on 1 January 2005.

#### **4. The EU initiative is launched**

Just three weeks after the High Level EU-US meeting in Wassenaar, on 28 July 2004, the Netherlands Presidency of the Council sent a questionnaire to the Working Party on Substantive Criminal Law for member states to respond to by 1 September 2004.<sup>19</sup>

The reason for the circulation of the "Questionnaire on prevention of terrorism" was because: *"the US authorities have conveyed several concerns regarding States' abilities to fight terrorism."*

*A first concern relates to the ability of law enforcement authorities to take action against preparatory acts for terrorism at a stage where no terrorist acts had been committed. A second concern related to the ability of states to afford mutual legal assistance and*

---

18. See, <http://www.statewatch.org/news/2004/feb/09gp-guardian.htm>

19. Questionnaire on prevention of terrorism: <http://www.statewatch.org/news/2005/jan/eu-g8-10694.pdf>

*extradite persons for preparatory acts. The third issue which has been raised by the US is how to share intelligence information related to terrorism for use in criminal proceedings in another country, while ensuring that the intelligence is protected".*

It should come as no surprise that the questionnaire sent out to the 25 EU member states was **the same questionnaire already answered by all G8 members.**

The questionnaire is primarily directed at the first and third of the US "concerns" - the introduction of a preparatory criminal offence and the protection of intelligence information in court proceedings.

It opens by asking if it is a crime in their countries to "incite or recruit" for terrorist acts (A.1) and to provide "directly or indirectly" material support (A.2).

The next question (A.3) makes explicit the distinction between current criminal offences in the EU directed at acts committed or knowingly of the planned commission of a terrorist act and the new concept of "preparatory" or "associated" offences. The questionnaire asks: *Can liability also arise where there is a more general mental state, such as where the recruiter/inciter/supporter intends to, or knows that his or her conduct will aid future unspecified terrorist acts?"*

It is also asked whether there are legal limits on action against religious leaders or charitable institutions (A.4) and whether financial inducements before an attack or after are lawful?

The second series of questions opens with the use of "special investigative techniques" (B.1), including: *"can the government overtly or covertly observe conduct taking place in a house of worship or property otherwise belonging to a religious or charitable entity? Can electronic surveillance be conducted in such a location? Are there limitations to executing searches and seizures in such a location?"*

And goes on to ask whether a "religious figure" can be lawfully questioned, information gathered about them or do any "legal privileges" bar gathering such information of evidence? (B.2) And are there any legal limits on detaining or arresting religious figures? (B.3)

The question on the use of "intelligence" in court (B.4) follows: *"To what extent do you have procedures under your law that permit the use in judicial proceedings of national security intelligence information in a manner that protects its source while adequately protecting rights of the defence?"*

The final question asks whether a EU state can assist a non-EU state (eg, the USA) in: *"gathering information and evidence by other countries for use in their criminal investigations or prosecutions?"*

It then explicitly uses as an example the surveillance and bugging of a place of worship.

The term "mutual legal assistance" is a euphemism for acts such as this. For example, can the USA request that an EU member state either place a targeted person(s) under surveillance and give the intelligence "product" to them or, as the above phraseology suggests, allowing (and aiding) US agencies to carry out the surveillance of the "target(s)".<sup>20</sup>

### **- the response to the EU questionnaire**

As far as can be ascertained only 11 out of 25 EU member states have responded to the questionnaire. Some member states responded by setting out the current legal situation in their countries with little further comment (for example, Germany and Portugal).<sup>21</sup>

A number of member states said that the Framework Decision on combating terrorism (13.6.02) already covered terrorist acts including preparatory and accessory acts.

Slovakia said: *"Its practical use would be improved if the American party could be confronted with the same questions too."* The Czech Republic said the same.

Belgium, Ireland and Austria thought it would be "very useful" if the EU G8 members were to inform the rest of the EU of their responses. It also proposed that any questionnaire should be drafted by all the parties so that each could make amendments and that information should be shared between all the partners - including the USA.

Greece was not convinced that these "American style" measures were needed and wanted to know how intelligence information could be protected. It was concerned too over lack of mention of the European Convention of Human Rights (ECHR), reciprocity, the death penalty and data protection.

Austria expressed strong concerns about a "shift" in what is perceived as criminal, which could put the rights of suspects at risk and infringe freedom of religious expression. For example, the line between the procurement of intelligence information and its use in prosecutions not revealing sources.

Germany was the only EU member of G8 to supply the same answers to the questionnaire as it gave to G8 - a basic statement of the current legal position in Germany.

---

20. It should be noted that the EU-US agreements on extradition and mutual assistance have not yet been formally adopted by the USA. However, such "mutual cooperation" can take place under existing bilateral agreements.

21. Responses to the questionnaire: <http://www.statewatch.org/news/2005/feb/terr-quest-12041.04.pdf>

The UK's response - which did not include its response to the G8 questionnaire - is very revealing. The UK's view is that the questions are "pertinent to the concerns of the US" and that: *"the burden of completing such questionnaires can be considerable, and we wonder whether this is the most cost-effective means of addressing this issue. It might be preferable for the G8 to put forward a set of preliminary proposals and invite EU Member States to comment on them, including the extent to which they are already compliant and any legal or other impediments they foresee to their becoming compliant."*

In other words, the UK's view is that G8 should be in charge of initiating these proposals and that EU member states should set out any problems with becoming "**compliant**" to its demands.

**There could not be a clearer expression of how the UK views the EU and how the "Atlantic Alliance" of the UK and the USA reflect their dominant role within G8.**

The Council's Working Party on Substantive Criminal Law discussed the issue at its meeting on 8-9 September 2004 and "number of delegations" asked for clarification as to the aim of the questionnaire. "Certain delegations" also asked for the distribution of the responses of EU members of G8 to its questionnaire. The matter was referred upwards to the Article 36 Committee.

The high-level Article 36 Committee discussed the issue at its meeting on 7-8 October 2004 and concluded that the Presidency should contact the USA to see how it "would like to proceed" and ask for a copy of the US reply to the G8 questionnaire (EU states in G8 should also make their responses available).

This response might seem to indicate a luke-warm response to the US (and UK demand). However, the influence of top JHA officials in the Council (and Commission) who meet and discuss with their US counter-parts regularly, and who take part in G8 working groups, should not be under-estimated.

## **5. Council of the European Union takes up the initiative**

The proposal for using intelligence information as evidence in court was raised within the closed circles of the Council of the European Union in an unreleased review of its work to combat terrorism early in 2004. This report from the Council's General Secretariat to COREPER (the committee of permanent representatives of the member states based in Brussels) said: *"One of the main problems to be addressed is the use of intelligence as evidence in courts in full respect of the right of defence"*.

In an "evaluation report" by Mr de Vries, the EU Counter-Terrorism Coordinator (based in the Council), produced at the end of May 2004, asks: *"How can intelligence be*

*exploited so that it can be used, if necessary by courts in legal proceedings?" [EU doc no: 9876/04]<sup>22</sup>*

A "more integrated approach" is "desirable" to the sharing of information between different state databases (eg: police and customs") and it should be considered whether: *"security services could also have a permanent access to law enforcement databases and to other relevant administrative databases, such as border management ones"*.

The report also noted that some internal security services had legal powers for the "interception of communications or eavesdropping" while: *"In some Member States, there is no specific legal framework relating to special investigative techniques"*.

The updated "EU Plan of Action on Combating Terrorism" agreed at the EU Summit (meeting of prime ministers) in December 2004 reflected developments on some of the issues raised in this analysis (doc no: 16090/04). Two of the seven overall "Objectives" are pertinent.

Objective 3 is "to maximise capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and prevent attacks". These measures include three measures already in the pipeline: i) a draft Council Decision on the exchange of information and cooperation concerning terrorist offences (Council doc no: 15871/04); ii) a draft Decision on the exchange of information extracted from the criminal record (Council doc no: 15281/04); iii) a draft Framework Decision on simplifying the exchange of information and intelligence between the law enforcement authorities of Member States particularly in respect of serious crimes including terrorist acts (original proposal from Sweden, doc on:10215/04) - this is referred to as introducing the "principle of availability" as endorsed by the "Hague Programme" (4.11.04).<sup>23</sup>

This "Objective" contains no reference to the introduction of either intelligence evidence in court proceedings or of "special investigative techniques".<sup>24</sup>

---

22. A related issue to the use of intelligence in court proceedings is that of freezing or seizing the bank accounts of individual and groups on terrorist lists. This raises problems when it is used as a "preventive measure" which has "led to a series of legal questions" (Council doc no: 14180/3/04): *"These questions range from the criteria which should be applied and the evidence which is needed for administrative freezing, the relation of administrative freezing to judicial freezing, seizure and confiscation, to matters of due process, availability of de-listing procedures and the role of intelligence in the designation process."*

23. "The Hague Programme" is a five-year programme for closer co-operation in justice and home affairs at EU level (2005 to 2010). It was agreed by at a EU Summit on 5 November 2004. It follows on from the "Tampere Programme" adopted in October 1999. <http://www.statewatch.org/news/2004/nov/hague-annotated-final.pdf>

24. Though a reference to the possibility of "the adoption of legislation for the use of special techniques for intelligence gathering" was slipped into a Presidency Briefing Note given to the press at the Summit.

Objective 6 "to address factors which contribute to support for, and recruitment into, terrorism" was added in the June 2004 version of the Action Plan (doc no: 10010/3/04, after 11 March bombings).

The June and December Action Plans (2004) contain under this Objective: "*conduct more detailed studies, including academic studies, of recruitment to terrorism in specific contexts such as prisons, in schools, in universities or in mosques; studies into the role of the media, including the internet, in radicalisation or in promoting support or sympathy for terrorists...*" (6.1.3)

Another point concerns investigating "links between extreme religious or political beliefs... and support for terrorism". The December 2004 Action Plan now assigns this task to SitCen (the EU's Situation Centre) to include relevant material in its "assessments".<sup>25</sup>

The concept of "radicalisation and recruitment" is now widely used in EU justice and home affairs documents.<sup>26</sup> The Action Plan notes that: "countering radicalisation and recruitment needs a joint strategy of police and security services". The first ever meeting of the Council's Counter Terrorism Group (CTG) and the Police Chiefs Task Force (PCTF) led to a report making recommendations "to better structure the process of intelligence-gathering".

A report on "recruitment to terrorism" has been completed - though this is not public (6.1.1). However the *European Voice* newspaper reports (9.12.04) that a report drawn up after the discussions between the CTG and PCTF identifies mosques, the internet and prisons as "hot spots" for the recruitment to "extremists" by terrorist groups. It recommends that national security services should increase their intelligence gathering at such locations and that Europol should undertake more "profiling" of "Islamic extremists".

## **6. Council of Europe: Convention**

It is not surprising that these far-ranging developments are echoed in the Council of Europe (CoE, 45 member states). After 11 September 2001 the CoE set up a Multi-disciplinary Legal Group on International Action against Terrorism (GMT). Its final report in November 2002 set out a number of priorities including research on the concepts of "*apologie du terrorisme*" and "incitement to terrorism".

---

25. Solana statement: <http://www.statewatch.org/news/2004/jun/solana-jha-june-04.pdf> See also: Statewatch article: <http://www.statewatch.org/news/2005/jan/06sitcen.htm>

26. See for example Council doc no: 5670/04, dated 6.2.04, which refers to this concept and gathering details on "motives for radicalisation within the EU". The document also suggests looking at "the Richard Reid/shoe bomb case" and the "ricin plot in the UK".

The research project was published on 24 June 2004.<sup>27</sup> It noted that whereas incitement to commit a criminal offence is common in the member states *apologie* of a crime is not. The project used a questionnaire to compile an analysis of the law in the CoE and defined "*apologie du terrorisme*" as: "*the public expression of praise, support or justification of terrorists and/or terrorist acts*".

Of the forty-five states only eight replies met the criteria that their national legislation defined "*apologie du terrorisme*" and/or "incitement to terrorism" as a specific criminal offence - these were Bulgaria, Denmark, France, Hungary, Spain, UK, Italy and Switzerland. Only three states mentioned "*apologie du terrorisme*" as a specific crime - Denmark, France and Spain (Belgium said it intended to). A number of states raised the problem of free expression and freedom of the press if "*apologie du terrorisme*" were to become a crime.

In parallel in February 2003 the CoE's Committee of Ministers set up an "ad hoc Committee of Experts on Terrorism" with the acronym CODEXTER to implement the priorities of "*apologie du terrorisme*" and "incitement to terrorism".

**On 16 May 2005 the Convention on Terrorism was adopted and at 20 May 2005 had been signed by 20 governments (to come into force it has to be ratified and adopted in member states' law.<sup>28</sup>**

The scope is set out in Article 4.1 which says that: "*For the purpose of this Convention, "public provocation to commit an act of terrorism" means the distribution, or otherwise making publicly available, of a message to the public, with the intent to incite the commission of an act of terrorism, including where the message, although not directly advocating such acts, would be reasonably interpreted to have that effect, inter alia, by presenting an act of terrorism as necessary and justified*".

Article 4.2 says a criminal offence as defined in 4.1 should be adopted in domestic law when committed unlawfully and intentionally provided that: "the provocation causes an imminent danger or likelihood of one or more terrorist acts being committed".

Articles 4 and 5 cover recruitment and training for terrorism. Article 7 sets out "ancillary offences" where it would be a criminal offence if a person "participates as an

---

27. "Apologie du terrorisme" and "incitement to terrorism": Analytical report: <http://www.statewatch.org/news/2005/jan/ribbelink.pdf>

28. Council of Europe Convention on Terrorism: <http://www.statewatch.org/news/2005/may/coe-conv-terrorism.pdf>

Explanatory memorandum: <http://www.statewatch.org/news/2005/may/coe-conv-terrorism-expl-memo.pdf>

List of signatories: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=196&CM=8&DF=5/20/05&CL=ENG>

accomplice" in Articles 4-6 or "organises or directs others to commit an offence" under these Articles.

The EU's Action Plan on terrorism (December 2004) records its support for this initiative, which includes "criminalisation of public provocation to commit acts of terrorism" (point 1.3.1).

Although the EU TOOK part in CODEXTER, a meeting of JHA Counsellors (experts on justice and home affairs based in the permanent representatives office of each member state in Brussels) in March recorded that "the vast majority of delegations were sceptical as to a comprehensive convention against terrorism of the Council of Europe" and "preferred to focus, at present, on the UN work in this field".<sup>29</sup>

A report on 4 February 2005 discussed the primary definition in Article 4.1.<sup>30</sup> A majority of EU governments accept the definition as drafted. However "several delegations" wanted to delete the following words at the end: "*by presenting an act of terrorism as necessary and justified*". The result of the discussion was a fudge. The majority position held subject to the addition of a new point 7 in the preamble: "*Recognising that this Convention is not intended to affect established principles relating to freedom of expression and freedom of association in national legal systems*" (which in is the adopted text).

**Whereas the research study in 2004 showed only three EU member states had a law akin to *apologie* now the EU as a whole supports such a law.**

## **7. Conclusions and implications**

In the judgment in the UK in December 2004 on the appeal by 12 men held in Belmarsh high security prison in south London and Woodhill prison under the Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001), Lord Hoffman, one of the nine judges, said that: "*The real threat to the life of the nation... comes not from terrorism but from laws such as these*".

The use of "intelligence information" in court or in "intelligence assessments" for issuing "control orders" - against people for whom there is insufficient evidence to bring criminal charges - would bring fundamental changes to any normal concept of criminal justice systems in democracies.

It could herald, as in the UK, vetted defence lawyers, refusal to let defendants know the evidence against them, *in camera* (closed) court session, the use "intelligence information" from third countries where it will be impossible to question the source

---

29. EU doc no: <http://www.statewatch.org/news/2005/jan/7873-04-coe.pdf>

30. EU doc no: 6049/04

or whether the "information" had been obtained as a result of torture or ill-treatment or "rendition".<sup>31</sup>

The demand for these changes needs to be seen in context. Since 11 September 2001 the EU has adopted measures to introduce its own PNR scheme (passenger name record) recording the movements of all third country nationals who enter as well as the external movements of EU citizens; agreed on the introduction of biometric passports and a huge database carrying personal details; and is planning to introduce the mandatory retention by service providers of all communications traffic data. These measures have little to do with combating terrorism but together seek to make available to the law enforcement and security agencies a mass of personal data over which there are few, if any, controls as to its use.<sup>32</sup> In terms of tackling terrorism there will simply be a bigger and bigger "haystack" in which to find the same number of "needles".

In addition there are new EU proposals based on the so-called "principle of availability" agreed under the EU's "Hague Programme" on justice and home affairs. This means that if information on a person is held in one agency in an EU member state then it can be accessed by any other agency in any other member state. There is also another new "principle" being put forward by the European Commissioner's Director-General, Mr Frattini, who says there is a need for a "principle that information may be passed on with the prior consent of the party forwarding it". This is to enable the passing of personal data to a third state like the USA and the "prior consent" is not that of the individual concerned but the agency which gathered it - it is impossible to control who has access to data in, for example, the USA which has over 1,500 agencies.<sup>33</sup> What may be a supposition or speculation about an individual's activities in one state may be added to or interpreted quite differently in another.

### **- widening the net**

The Council of the European Union has reached "political agreement" on a "Council Decision on the exchange of information and cooperation concerning terrorist offences". This envisages in Article 2.1 the exchange of "information" during investigations and prosecutions concerning terrorist offences as set out in Article 1 to 3 of the

---

31. "Rendition" is practice carried out by the CIA to send suspected terrorists to be interrogated in countries where the use of torture and ill-treatment has been well documented. CIA prisoners 'tortured' in Arab jails. BBC: [http://news.bbc.co.uk/1/hi/programmes/file\\_on\\_4/4246089.stm](http://news.bbc.co.uk/1/hi/programmes/file_on_4/4246089.stm) plus Britain accused over CIA's secret torture flights: [http://news.independent.co.uk/low\\_res/story.jsp?story=609538&host=3&dir=506](http://news.independent.co.uk/low_res/story.jsp?story=609538&host=3&dir=506). "Outsourcing torture": <http://www.cageprisoners.com/articles.php?aid=5200> and Sweden: Expulsions carried out by US agents, men tortured in Egypt: <http://www.statewatch.org/news/2004/oct/05sweden-us-abduction.htm>

32. The EU's Joint Supervisory Authorities for Europol, Schengen and Eurojust have told the UK parliament in evidence that recent proposals involve the: *"processing of personal data from different sources on an unprecedented scale"*.

33 Statewatch, The "principle of availability" takes over from the "notion of privacy": what price data protection?: <http://www.statewatch.org/news/2005/feb/07eu-data-prot.htm>

2002 Framework Decision on combating terrorism.<sup>34</sup> The "information" is to be communicated to Europol and Eurojust (EU prosecutors) and made *"accessible as soon as possible to the authorities of other interested 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 and social 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 *"accessible"* to dozens of agencies across the 25 EU member states.

In April 2004 ten Muslim "suspects" were arrested and held for questioning in the north of England but were 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 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 large-scale protests. It covers, for example, 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 in this way opens the way for abuse and its application to non-terrorist offences.

### **- the effects of gathering intelligence through "special investigative techniques"**

Of direct relevance to the use of "intelligence information" in courts is the legalisation of "special investigative techniques" (eg: tapping and bugging). Techniques which in the past have been limited and very strictly controlled - usually requiring authorisation by a court because they are intrusive, covert and open to abuse - are to become the norm.

From the "security" perspective measures and practices are being introduced to track peoples' movements, to data-mine public and commercial databases, retain and

---

34. Statewatch critique: <http://www.statewatch.org/news/2002/feb/06Aep.htm>

search all telecommunications, create "watch-lists", infiltrate undercover agents in suspect groups and to recruit informers.<sup>35</sup> Undercover agents and informants inhabit a world of "hearsay", manipulation and *agent-provocateurs*. Communities, mosques, individuals and groups are targeted for "disruption" - people are stopped and searched, arrested and released without charge, bank accounts closed without explanation, mysterious burglaries occur and dissension is encouraged by infiltrators to split and divide groups. Already the security agencies have gathered a mass of "intelligence" and information on "suspect" individuals and groups. Many groups and individuals are under "suspicion" and under surveillance but very few so far have been charged with terrorist offences. In the next phase of the internal "war on terrorism" the build-up of "intelligence information" on "suspected" individuals and groups and targeted communities in EU states is going to expand enormously.

There are lessons from history when surveillance based on suspicion (rather than investigation leading to trial) becomes the norm. British Irish Rights Watch observed, when commenting on UK Prevention of Terrorism Bill, that in Northern Ireland: *"Gathering and controlling intelligence took priority over the detection and prevention of crime... The need to recruit, and keep in place, informants meant that some agents were allowed to participate in crimes without being prosecuted, while others were granted de facto immunity in order not to blow agents' cover. As a result many people died needlessly in the name of saving lives."*<sup>36</sup>

The use of "special investigative techniques" aided by undercover agents and informers "hoovers" up "intelligence" on specific "targets" and everyone else who may unknowingly come into contact with them. Such methods carried out covertly and unaccountably (except to the agencies themselves) will lead to an unacceptable intrusion into social and political activity in a democratic society. The lives of the Muslim communities and those who go to mosques to worship become subject to an all pervasive and intrusive surveillance - which, though targeted at potential terrorists, soon extends to all suspected crimes and then to everyday activities.

**These practices, techniques and changes in the legal process are, moreover, likely to spill over into the mainstream criminal justice system and establish new norms.**<sup>37</sup>

---

35. In the UK the surveillance of telecommunications is running at an unprecedented level (see Statewatch's Analysis, 1937-2003): <http://www.statewatch.org/news/2004/jul/uk-tel-tap-rep-2003.htm>. In 2003-04 the law enforcement agencies used/had in place 10,409 CHIS (covert human intelligence sources): <http://www.statewatch.org/news/2005/mar/chis.pdf> and the Special Branch has doubled in size: <http://www.statewatch.org/news/2003/sep/01specbranch.htm>

36. Briefing February 2005. See also: On the Force Research Unit in Northern Ireland, Statewatch bulletin, vol 13 no 5, and on GAL in Spain, Statewatch bulletin vol 9 no 3.4.

37. Similarly these techniques are being brought to bear on "normal" police life in the surveillance of protests, especially where people come together from a number of different EU states.

The inexorable logic of the explosion in intelligence-gathering and targeting undertaken by a host of agencies across Europe is that the demands of the law enforcement and security agencies are going to grow for the detention or criminal prosecution of "suspected" terrorists, "sympathisers" and "apologists". Those who in previous times supported the North Vietnamese and the ANC and a host of liberation struggles in the 1960s and 1970s and those today, including the Palestinian struggle, are liable to be caught up in the surveillance "net".

Communities that house "suspect communities" are targeted and subjected to intensive surveillance. Religious and political activity infiltrated and spied on. And all this based the institutionalised racism of post 11 September 2001 – a racism embedded in the "politics of fear".<sup>38</sup> Privacy, accountability, data protection, respect for fundamental rights and democratic norms disappear for those targeted or innocently caught up in the process.

Since 11 September 2001 governments, ministers and officials at all levels of the EU have maintained that the swathe of new measures introduced have all been "balanced" as between the needs of security and respect for fundamental rights. Concerned civil society groups across Europe know differently as do refugees, those stopped and searched and detained and the communities subject to surveillance.<sup>39</sup>

In a democracy when the rights and freedoms of the few are curtailed so too are the rights and freedoms of us all.

---

38. "Racism in the age of globalisation", A Sivanandan: <http://www.irr.org.uk/2004/october/ha000024.html>

39. In a moment of honesty UK Home Secretary, Charles Clarke, when asked about claims that MI6 played an active role in the kidnapping of a Briton who spent 33 months in Guantanamo Bay, responded: *"I'm all in favour of human rights, but I'm even more in favour of our national security being protected"* (Guardian, 7.2.05)