POLISH CHAIRMANSHIP OF THE COUNCIL OF EUROPE

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

18 March 2005

Third High-level multilateral meeting

of the ministries of the Interior

Fight against terrorism and organised crime

to improve security in Europe

Warsaw (Poland)
Hotel Sofitel Victoria

17 -18 March 2005

Report by Mr Nigel Burrowes

President of PC-TI
(Committee of Experts on Special Investigation Techniques)

Practical approaches and techniques to the fight against terrorism and organised crime

General considerations

Special investigations techniques ("SIT") are techniques used for the purpose of detecting and investigating crimes and suspects, aiming at gathering information in such a way as not to alert the target persons. Examples of such techniques include interception of communications, under-cover operations, controlled delivery, electronic surveillance or bugging.

SIT are numerous, varied and constantly evolving and their secret nature means that their application could interfere with fundamental rights and freedoms.

It is widely recognised that SIT constitute crucial tools to investigate acts of terrorism and serious crime. The conditions for their use and how they must be regulated does not vary between the types of crime against which they are used.

Since rights under the European Convention of Human Rights are engaged, the use of SIT must be properly regulated or used in accordance with Convention obligations.

Practical approaches to the use of SIT, and the extent to which they are used, differ, in some cases markedly, between different jurisdictions for many reasons.

In some jurisdictions laws and constitutions either forbid, or do not provide for, the use of particular types of SIT (e.g. interception of communications). Similarly the use of some SIT is more sensitive and controversial for some jurisdictions than they are for others.

Also in some countries certain SIT appear to be used almost exclusively (again, the most notable example is interception of communications) leading potentially to under-use of often equally important and effective SIT (e.g. placing covert listening devices).

The availability of resources often dictates the extent of the use of SIT particularly those which can be technically complex (e.g. interception of communications) or require the use of human resources (e.g. surveillance). For SIT to be used most effectively, they must be properly resourced.

Wider adoption of internationally agreed technical standards and agreement to a common set of requirements would ensure greater co-operation with industry providers (e.g. in the area of interception of communications and communications data) and consequently more effective use of SIT which involve the use of technology. Close dialogue and consultation with industry providers encourages confidence and enhanced co-operation.

The provision of effective training in the use of SIT, by means, for example, of specialised advice from expert practitioners, is a feature of some jurisdictions and should be encouraged. Equally, more intensive use of international networks of contacts can assist in the spread of best practice.

Practitioners of SIT must be aware of their obligations under the European Convention on Human Rights. Without this awareness, the regulatory requirements imposed in law on practitioners may seem unnecessarily burdensome. In certain jurisdictions training in the implications for human rights of the use of SIT is provided.

Police co-operation on an international level, and in accordance with existing multi-lateral and bilateral international agreements, is key to effective use of some SIT. Rapid ratification and implementation of relevant instruments should improve the effectiveness of international co-operation. For example, the Second Additional Protocol to the Convention on Mutual Assistance in Criminal Matters should improve co-operation in a respect of the use of various SITs, including cross border surveillance, controlled delivery and undercover officers.

UK case examples

In common with all other countries which use SIT, the UK regards them as essential tools not only in the fight against serious crime and terrorism but in other areas. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a clear lawful basis for the use of SIT (including interception of communications, access to communications data, use of surveillance, bugging, use of informants and covert agents). RIPA sets out the purposes for which SIT can be used (consistent with ECHR legitimate aims), prescribes authorisation levels reflecting the sensitivity of the use of the SIT and the level of interference with private life, provides for independent oversight of all SIT and a means of redress to an independent tribunal for anyone who believes SIT have been used unlawfully against them.

In the area of interception of communications, the UK is one of very few countries which do not use the material obtained as evidence. This is because its use as an intelligence only tool is very effective and may be undermined if techniques and capabilities were exposed publicly, for example in a trial. The UK also benefits from a uniquely close relationship between law enforcement and intelligence agencies, including in the area of interception. Again exposure of techniques and capabilities in cases where intelligence agencies support law enforcement would undermine the work of all agencies. The UK successfully uses interception of communications to disrupt and prevent serious crime and terrorism. And its use leads to investigators gaining other evidence used to prosecute and convict. In 2003, interception of communications led to:

- seizure of 26 tonnes of illicit drugs;
- seizure of 10 tonnes of tobacco
- detection of £390m of financial crime; and
- 1,680 arrests. (with resulting conviction rate estimated at over 80%)

RIPA is designed to take account of all new technologies in the communications arena.

Accessing communications data (for example telephone numbers called, when calls are made, mobile phone location data etc) is another SIT which UK law enforcement agencies and other public authorities use, in some cases extensively, when such use if justified by the statutory purposes of those authorities. For example most, obviously law enforcement agencies use communications data to prevent and detect crime. But other public authorities are also entitled under RIPA to access communications data for purposes consistent with Article 8 of the ECHR (for example for protecting public health and safety). Law enforcement agencies in particular maintain a close

relationship with communications service providers in order to ensure effective access to communications data. This is assisted by for example, the provision of specialised training by industry and law enforcement experts for those who are entitled to use this SIT, and the designation of Single Points of Contacts in all public authorities to help ensure integrity and consistency in accessing communications data.

The clear experience of the UK is that SIT provides crucial information, which often cannot be obtained by other means, to prevent, detect and prosecute not only serious crime and terrorism but also less serious crimes. At the most serious level, the UK further considers that without effective use of a range of SIT, there would be a greater risk of successful terrorist atrocity.

Importantly, one of the main purposes of RIPA is to ensure that the use of SIT is regulated in a way that is consistent with ECHR obligations, that such use is demonstrably necessary and proportionate, and that there is a proper balance between the interference with human rights that the use of SIT entails and protecting the public.

Draft Recommendation of the Committee of Ministers to Member States on "Special Investigative Techniques in Relation to Serious Crimes Including Acts of Terrorism

At its meeting on 7-11 March 2005 the CDPC approved a draft Recommendation on the use of SIT in relation to serious crime including acts of terrorism, drawn up by the Council of Europe Committee of Experts on Special Investigative Techniques (PC-TI). The aim of this draft recommendation is to promote the use of special investigation techniques by judicial and prosecuting authorities in the framework of their criminal investigations in relation to serious crimes, including acts of terrorism, whilst ensuring strict respect for the rights and freedoms of the individual. To this end, the Recommendation recalls or provides for some common principles that should be respected when the competent authorities use SIT. It also suggests measures to be taken with a view to improving international co-operation between member states in matters related to SIT.

With a view to improving the use and the efficiency of SIT, the draft recommendation contains provisions that seek to make SIT available to a wide extent to competent authorities, to encourage, where appropriate, the use of material obtained from the use of SIT before courts, to promote the provision of technological, human and financial resources to the authorities using SIT, to retain and preserve traffic data collected through the use if SIT, to provide adequate training and specialised advice to the competent authorities, to ensure compliance of technical equipment with internationally agreed standards, to better use international networks of contacts in order to exchange information on national regulations and operational experience, and to implement existing conventions or instruments in the field of international co-operation in criminal matters.

In order to enhance human rights protection when SIT are being used, the draft recommendation contains principles such as the legality principle (the circumstances in which, and the conditions under which, authorities are empowered to resort to the use of SIT should be defined in national legislation), the proportionality principle (proportionality between the effects of the use of SIT on the rights of the individuals concerned and the objective that has been identified) and the subsidiarity principles (less intrusive investigation methods than SIT should be used if such methods enable the offence to be detected, prevented or prosecuted as effectively). The draft recommendation also provides for adequate control of the implementation of SIT and requests that SIT only be used where there is sufficient reason to believe that an offence has been committed, prepared or is being prepared.

Key Questions

ECHR Considerations

Is there a sufficient lawful basis for the use of SIT in all jurisdictions?

Do laws on the use of SIT conform entirely with ECHR requirements (including those relating to proportionality, necessity, legitimate aims, independent oversight/control etc)?

Operational considerations

Are sufficient financial, technological and human resources provided to ensure the most effective use of SIT?

Do laws on the use of SIT take account of new technologies?

Is there sufficient dialogue and consultation with the private sector to ensure the most effective use of new technologies?

Training

Is sufficient training provided on technical, operational, criminal procedure, legislative and human rights issues?

Has the provision of specialised advice (e.g. by experienced practitioners) been considered?

International Co-operation

Are Member States using to the greatest extent possible existing bilateral and multilateral agreements for judicial and police co-operation in the use of SIT?

Are relevant bodies (e.g. Council of Europe, the European Judicial Network, Europol and Eurojust) made use of to the greatest extent that is appropriate?

Are internationally agreed technical standards adopted with a view to overcoming obstacles in the use of SIT in an international context?

ANNEX A

Related Instruments:

1. Resolution No. 1 on Combating International Terrorism adopted at the 24th Conference of European Ministers of Justice where the Committee of Ministers was invited to adopt urgently all normative measures considered necessary for assisting States to prevent, detect, prosecute and punish acts of terrorism;

2. The final report of the Multidisciplinary Group on international action against terrorism (GMT) and the subsequent decisions of the Committee of Ministers recognising the use of special investigation techniques (SIT) as a priority area of the Council of Europe legal action against terrorism;

3. Resolution No. 1 on Combating Terrorism, adopted at the 25th Conference of European Ministers of Justice, which invited the Committee of Ministers, *inter alia*, to pursue without delay work with a view to adopting relevant international instruments on the use of SIT;

4. The Final Report on SIT in relation to acts of terrorism prepared by the Committee of Experts on special investigation techniques in relation to Acts of Terrorism (PC-TI) and the opinion of the Committee of Experts on Terrorism (CODEXTER);

5. Surveys on "best practices" against organised crime carried out by the Group of Specialists on Criminal Law and Criminological Aspects of Organised Crime (PC-S-CO, formerly PC-CO), as well as the reports adopted in the framework of the Council of Europe's technical co-operation programmes for the fight against corruption and organised crime;

6. Recommendation No. (96) 8 on crime policy in Europe in a time of change and Recommendation (2001) 11 concerning guiding principles in the fight against organised crime;

7. Convention No. 108 for the protection of individuals with regard to automatic processing of personal data (28 January 1981) and its additional Protocol No. 181 on Supervisory Authorities and Transborder Data Flows (8 November 2001); Recommendation No. (87) 15 regulating the use of personal data in the police sector; Recommendation No. (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services;

8. Council of Europe instruments dealing with the question of SIT include the Convention on Money Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (Article 4), the Criminal Law Convention on Corruption (Article 23), the Second Additional Protocol to the Convention on mutual assistance in criminal matters (Articles 17-20) and the Committee of Ministers' Recommendation Rec (2001) 21 on the fight against organised crime.

9. Existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other states;

10. The Guidelines on human rights and the fight against terrorism adopted by the Committee of Ministers of the Council of Europe on 11 July 2002.