COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 30 June 2016

CODEXTER (2016) 18

LAST UPDATE morning 30.06.2016

COMMITTEE OF EXPERTS ON TERRORISM

(CODEXTER)

DRAFTING GROUP ON SPECIAL INVESTIGATION TECHNIQUES

DRAFT EXPLANATORY REPORT

OF THE RECOMMENDATION ON "SPECIAL INVESTIGATION TECHNIQUES"

IN RELATION TO SERIOUS CRIMES INCLUDING ACTS OF TERRORISM

Secretariat of the Terrorism Division
Information Society and Action against Crime Directorate, DG I

codexter@coe.int - www.coe.int/terrorism

Draft Explanatory Report
Recommendation on "special investigation techniques" in relation to serious crimes including acts of terrorism

The text reproduced below is the version of the draft Explanatory Report of the Recommendation on "special investigation techniques" in relation to serious crimes including acts of terrorism as consolidated by the SIT Drafting Group at its 2nd meeting (Rome, 13-14 June 2016)

Introduction

1. On 20 April 2005, at the 924th meeting of the Ministers' Deputies, the Committee of Ministers adopted the Recommendation Rec(2005)10 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism.

2. On 14 – 15 May 2013, the Council of Europe hosted in Strasbourg the International Conference on "The Use of Special Investigation Techniques to Combat Terrorism and Other Forms of Serious Crime", in close co-operation with the UN Security Council Counter-Terrorism Committee Executive Directorate (CTED), the Organization for Security and Co-operation in Europe (OSCE) and the League of Arab States. The participants recognised that to protect society from terrorism and organised crime, law-enforcement must apply modern investigation methods such as "special investigation techniques" (SIT). The Conference highlighted that since the adoption of Recommendation Rec(2005)10, the computer and Internet technology made great strides offering new possibilities to criminals and terrorists but also to law enforcement. Therefore, it noted the need for updating the standards and guidelines applicable to the use of SIT.

3. On the basis of its Terms of Reference for 2014 – 2015, at its 25th Plenary Meeting (23 – 24 October 2013), the Committee of Experts on Terrorism (CODEXTER) examined and discussed a document containing proposals for priority areas for its work in 2014-2015. These proposals included, among other things, establishing a sub-groups of the Committee which would focus on "special investigation techniques".

4. At its the 26th Plenary Meeting (6 – 7 May 2014), the CODEXTER decided to establish a drafting group, composed of members of CODEXTER, the European Committee on Crime Problems (CDPC), the Steering Committee on Media and Information Society (CDMSI), the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the Cybercrime Convention Committee (T-CY) and the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), with the task of elaborating a set of draft amendments to Recommendation Rec(2005)10.

5. At the 5th meeting of its Bureau (15 September 2014), the CODEXTER decided to instruct the Secretariat to invite 13 members to participate in the drafting group. Of these, 7 members (including the Chair of the drafting group) should be appointed by CODEXTER, 2 by CDPC and the other Committees should appoint 1 member each. It further instructed the Secretariat to foresee at least 2 meetings with the future drafting group.

6. At its 27th Plenary meeting (13-14 November 2014), the CODEXTER confirmed the decision of the Bureau to appoint Mr Nicola PIACENTE (Italy) as Chair of the drafting group. Prior to this meeting, a letter was sent to members of the CODEXTER calling for candidates with practical experience concerning the application of special investigation techniques for the six remaining seats reserved for CODEXTER in the drafting group.

7. Although CODEXTER had agreed to start with the topic of "special investigation techniques" (SIT) as from the end of 2014 and throughout 2015, the Committee had to postpone its foreseen activities following the request of the Council of Europe Secretary General, at the 27th Plenary meeting of the CODEXTER to play a key role in ensuring the proper and timely implementation of the United Nations (UN) Resolution 2178 (2014) on "Threats to international peace and security caused by terrorist acts". The Committee was encouraged, notably, to adopt the draft terms of reference for an ad hoc committee to elaborate and negotiate a draft additional protocol to the Council of Europe Convention on the Prevention of Terrorism. On 22 January 2015, the Committee of Ministers (CM), at the proposal of the CODEXTER, adopted the terms of reference for the Committee on Foreign Terrorist Fighters and Related Issues (COD-CTE) which drafted the Protocol in a timely fashion. It was adopted by the CM in April 2015 and opened for signature in Riga on 22 October 2015.

8. At its 29th Plenary meeting (17-18 November 2015), the CODEXTER decided that the work on amending Recommendation Rec(2005)10 would start at the beginning of 2016.

9. The members of the CODEXTER Drafting Group on Special Investigation Techniques convened for the first time on 18 February 2016. The Drafting Group examined the draft and discussed the amendments paragraph by paragraph.

10. At the 7th meeting of its Bureau (17 Marc 2016), the CODEXTER examined the preliminary draft prepared by the drafting committee and proposed some amendments to it.

11. At its 30th Plenary meeting (19-20 May 2016), the CODEXTER instructed the Secretariat to submit the draft amended recommendation to the CDPC for their opinion after the second meeting of the SIT Drafting Group.

12. The members of the CODEXTER Drafting Group on Special Investigation Techniques convened for the second time on 13 – 14 June.

General Considerations

13. In line with Recommendation Rec(2005)10, the aim of the updated recommendation is to promote the effective use of SIT by the competent authorities mainly in the framework of criminal investigations in relation to serious crimes, including acts of terrorism, whilst ensuring strict respect for the rights and freedoms of the individual.

14. The amendments aim to balance the existing text by, on the one hand, further emphasising the need to adhere to human rights in the application of all special investigation techniques, and, on the other hand, addressing the new technical capabilities developed since 2005 and the inclusion of cyber investigations and of financial investigation techniques on individuals and, where national legislation so provide, legal entities among the special investigation techniques covered by the recommendation.

15. Therefore, the update of Recommendation Rec(2005)10 was conducted by retaining the majority of the text as it stands in its original version, but, where necessary, in view of bringing the recommendation up to date, introducing new text to supplement the recommendation.

16. The structure is only minimally revised. In the updated Preamble the provisions are systematically presented according to a chronological order. Chapter I of the Appendix reproduces the definitions and scopes of “special investigation techniques” and “competent authorities”. Additionally, it provides the definitions and scopes of “financial investigation” and “cyber investigation”. Chapter II “recalls or provides for some common principles that should be respected when member States are regulating SIT and when they are used by their competent authorities. Chapter III suggests measures to be taken with a view to improving “international and national” co-operation in matters related to the use of SIT.”

17. SIT are particular techniques because of their covert nature. It is because of their nature that they are considered a vital tool in the fight against serious crimes, including acts of terrorism. However, their use may interfere with fundamental rights and freedoms, such as the right to a fair trial, the right to freedom of expression, freedom of communication, the protection of the right of property and the right to respect for private life, including the right to protection of personal data. Therefore, the recommendation seeks to strike a balance between the need to enhance the efficiency of the fight against serious crimes, including acts of terrorism, by promoting the use of SIT, and the need to ensure the protection of fundamental rights and freedoms.

18. The search for a balance is inspired by a similar approach adopted by the European Court of Human Rights (hereinafter “the Court” or “ECtHR”). Any interference with a right guaranteed under the European Convention on Human Rights (ETS No. 5, hereinafter “the Convention”) can only take place under exceptional conditions and must be necessary in a democratic society, in the interests of, inter alia, national security and/or for the prevention of disorder or crime. However, member States do not enjoy an unlimited discretion to interfere with those rights in the application of SIT. Any such interference should be proportionate and necessary to the legitimate aims pursued. Moreover, there must be adequate and effective

guarantees against abuse and access to an effective remedy.[1] Finally the measures have to be subject to authorisation by a competent authority, as defined in Chapter I, paragraph 2 of the recommendation, and, where applicable under national law, to oversight by an independent body. In the context of new technological developments, when applying SIT, special consideration should be given to the relevant Council of Europe standards in the field of protection of private life and freedom of expression as described, inter alia, where applicable, in the provisions of Recommendation 2016 (5) on Internet Freedom.

19. Several instruments of the Council of Europe, such as those listed in the Preamble of the recommendation as well as in paragraph 23 of Chapter III, already deal with the question of SIT. However, these instruments address issues connected with the use of SIT only in so far as these are being used in relation to their respective scope, while the present text offers a comprehensive approach to the use of SIT in connection with all forms of serious crimes, including acts of terrorism.

20. Addressing the use of SIT in connection with not only terrorism but, more generally, with serious crimes, including acts of terrorism, the principles laid down in the recommendation are applicable in a more general context. However, the Committee opted for avoiding the definition of the term "serious crimes" since, for the purposes of the recommendation, it is more appropriate to leave member States a margin of appreciation in setting thresholds for qualifying the seriousness of the crimes. As indicated in the Explanatory Report of Recommendation Rec(2005)10, Article 2 (b) of the UN Convention against Transnational Organised Crime, which provides for a definition whereby '"Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty', can however serve as an indicator for those states that wish to define this notion more precisely. In any event, the term "serious crimes" covers offences related to terrorism and organised crime.

Commentary on the provisions of the Recommendation

Preamble

21. The 4th paragraph identifies three legal instruments adopted by the Council of Europe European Commission for Democracy through Law (Venice Commission) and relevant for SIT. The Opinion on the protection of human rights in emergency situations notes that the security of the State and its democratic institutions "are vital public and private interests that deserve protection, if necessary at high costs." Indeed, the measures of protection may also consist of, or amount to justified limitations of certain human rights or freedoms not only of those who have committed, are suspected of having committed or are about to commit acts against public safety, but of anybody, even potential victims of terrorist acts. The second source recalled in paragraph 8 is the Report on the Democratic Oversight of the Security Services, focusing, inter alia, on different forms of judicial review and authorization of "special investigative measures". Finally, the recommendation recalls the Report on counter-terrorism measures and human rights. The Report considers that national interest and public safety may justify limitations to the enjoyment of certain fundamental rights "of both those who have committed or are suspected of having committed a terrorist act, but also of the population at large, even those of actual or possible victims of terrorist acts."

22. The 7th paragraph refers to the Council of Europe's work in the field of Transnational Organised Crime (TOC). The White Paper of the CDPC includes a list of recommendations aimed at defining which measures should be applied in key areas, including special investigative techniques. On this subject, the White Paper notes that SIT are indispensible to detect and prosecute TOC but their use has to be counterbalanced with adequate measures that guarantee the protection of human rights and prevent abuse. It points out that the lack of adequate rules and legal harmonisation of SIT poses difficulties to the cross-border transfer of evidence.[2] The White Paper therefore identifies two sets of actions that could be taken with regard to the fight against TOC and the use of SIT: (i) to enhance the regulation and efficient use of such techniques and acquiring comprehensive knowledge of the existing legislation in the member States of the

[1] ECtHR, Klass and others v. Germany, Application no. 5029/71, Judgment, 6 September 1978; the Court has reiterated these principles in several occasions, including, Gillan and Quinton v. the United Kingdom, Application No. 4158/05, 12 January 2010; Uzun v. Germany, Application No. 35623/05, Judgment, 2 September 2010; R.E. v. the United Kingdom, Application no. 62498/11, 27 October 2015; and, as a most recent example, in the case of Karabeyoğlu v. Turkey, Application no. 30083/10, Judgment, 7 June 2016.

[2] The CDPC White Paper, p. 32, notes that the "lack of comprehensive regulation and/or the differences existing across the domestic law of Council of Europe member states obviously increases the difficulties in transnational co-operation and the transfer of evidence. The differences in the regulation of certain investigative techniques may hamper their use in a cross-border setting. For example, conducting covert investigations and controlled deliveries in the territory of another state is challenging because of differences in laws, law enforcement systems and institutional priorities."

Council of Europe; (ii) to strengthen human rights protection when resorting to these intrusive investigative measures.

23. In the 8th paragraph, reference is made to the Action plan on "The fight against violent extremism and radicalisation leading to terrorism" adopted by the Committee of Ministers on 19 May 2015. The update of the Recommendation Rec(2005)10 aligns with the objectives of the Action Plan, which are: 1. to reinforce the legal framework against terrorism and violent extremism; 2. to prevent and fight violent radicalisation through concrete measures in the public sector, in particular in schools and prisons, and on the Internet.

24. The 9th paragraph recalls the work of the Council of Europe in the field of data protection, use of the Internet and network neutrality, essential components of SIT. The 2014 Guide to human rights for Internet users is a tool for Internet users to learn about human rights online, their possible limitations, and available remedies for such limitations. The Guide provides that in exceptional circumstances, which are prescribed by law, such as for a criminal investigation, privacy with regard to personal data may be interfered with. However, "accessible, clear and precise information about the relevant law or policy and your rights in this regard should be made available". The 2016 Recommendation on protecting and promoting the right to freedom of expression and communication and the right to private life with regard to network neutrality reiterates that the use of techniques in the context of Internet traffic management which inspect or monitor the content of communications should be in accordance with applicable legislation on the right to private life and personal data protection and be reviewed by the competent national authority in order to assess compliance with legislation. Reference is made also to the Recommendation on Internet Freedom, adopted by the Committee of Ministers on 13 April 2016.

25. Paragraph 11 is reproduced in its totality. The Guidelines on human rights and the fight against terrorism of 2002 remain a valid and essential text with reference to the use of SIT. This was particularly underlined in the discussion paper which suggested the opportunity to reflect, in particular, provisions I (States' obligation to protect everyone against terrorism), V (collection and processing of personal data by any competent authority in the field of State security), VI (measures which interfere with privacy), IX (legal proceedings), and XVI (respect for peremptory norms of international law and for international humanitarian law) of the Guidelines.

26. The aim of paragraph 14 is to further underline the legal framework by stressing provision XVI of the above mentioned Guidelines, which recalls the necessity to fight terrorism while respecting peremptory norms of international law and international humanitarian law, where applicable.

27. In its new formulation, paragraph 20, concerning recommendation to member States, also refers to the need to further strengthen international and domestic cooperation in criminal matters, in particular with regards to the exchange of information and best practices at the operational level.

Appendix to Recommendation

Chapter I. Definitions and Scope

28. Paragraphs 1 and 2 of Chapter I are reproduced in their entirety. Indeed, for the purpose of the updated Recommendation, the meaning of "SIT" and that of "competent authorities" remain unchanged. SIT are techniques applied by the competent authorities in the context of criminal investigations. The consequences of this are twofold: firstly, it means that the use of SIT in a different context, such as national security, does not fall within the scope of the recommendation; secondly, it leads to the fact that SIT that are being used in the context of criminal investigations are covered by the recommendation regardless of the title or identity of the authorities that have been involved in deciding, supervising or using SIT.

29. As clarified in the Explanatory Report of Recommendation Rec(2005)10, SIT are techniques used "in such a way as not to alert the target persons". The use of SIT would be superfluous, and might even be counterproductive, if the target persons were aware about the fact that such techniques are being used with a view to collecting information on their actions or activities. Consequently, SIT are often of a covert nature, which is present where an attempt is made to conceal the on-going criminal investigations.

30. For the purpose of this recommendation, SIT may include: undercover operations (including covert investigations); front store operations (e.g. undercover company); informants; controlled delivery; observation (including cross-border observation); electronic surveillance of specific targets; interception of communications; searches (including of premises and objects, such as computers, cars, etc); cross-border

(hot) pursuits; pseudo-purchases or other "pseudo-offences", covert monitoring of financial transactions and web traffic as they are defined in national laws.

31. Paragraphs 3 and 4 refer to the definition of "financial investigations" and "cyber investigations". These amendments were essential to expressly include these investigation techniques, although not necessarily covert, on individuals and, where national legislation so provide, legal entities among the SIT covered by the recommendation. Through the former investigators can uncover and disrupt criminal and terrorist associations and/or groups, and confiscate their assets. The latter recognises the centrality of cyberspace as an environment through which, and in which, criminal and terrorist activities may take place and at the same time be detected.

32. The definition of "financial investigation" finds its origins in Recommendation 30 (Responsibilities of law enforcement and investigative agencies) of the 2012 Recommendations of the Financial Action Task Force (FATF), an independent inter-governmental body that develops and promotes policies and international standards to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.[3] In 17 April 2015, MONEYVAL presented a "Typologies Report on Laundering the Proceeds of Organised Crime". The Report noted that "at the jurisdiction level there is no generally accepted (or used) definition of "financial analysis" or "financial investigation" and the understanding of those terms range from basic intelligence gathering activities to complex relational networks and money flows, and financial profiling aimed to identify unexplained wealth or disproportionate income compared with apparent lifestyle and sources of wealth." In this context, MONEYVAL agrees that FATF's Operational Guidance on Financial Investigations of 2012 is "a valuable tool in defining the investigative strategy, the objectives, dedicated action, the necessary resources, the training for investigators and use of the legal instruments available for a comprehensive, creative, consistent, and committed manner of conducting effective financial investigations".

33. For the purpose of this recommendation, "cyber investigation" means an inquiry aimed at preventing, suppressing and prosecuting any serious criminal or terrorist act, as well as any criminal offence established by the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Additional Protocol (CETS No. 196).

34. Both financial and cyber investigations contemplated in this recommendation are tools to be used within the framework of paragraph 13 of the Explanatory Report.

Chapter II. Use of SIT at national level

a) General Principles:

Paragraph 5:

35. Over recent years, the Court has been asked to consider the use of SIT in the context of Article 8. [4] This body of jurisprudence has established a clear set of principles governing the deployment of SIT which has been largely reflected in the amended text of the recommendation.

36. Paragraph 5 reiterates that any interference can only be justified if it is provided for by law with sufficient clarity. These wording requires the law providing for the impugned measure has to be accessible to the person concerned and foreseeable as to its effects. In this context, the domestic law must be sufficiently "precise" and "accessible" for an individual to be able to foresee with a reasonable degree of certainty the consequences of his or her actions, or the circumstances in which and the conditions on which authorities may take certain steps. In this regard, the Court stated:

"Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct:

[3] FATF Recommendation 30 gives the following definition as a footnote "A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to: (i) identifying the extent of criminal networks and/or the scale of criminality; (ii) identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and (iii) developing evidence which can be used in criminal proceedings."

[4] Article 8 provides that: "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

he must be able – if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[5]

37. When regulating or using SIT, national authorities need to bear in mind that the use of SIT may affect not only the rights of the person who is suspected of having committed or prepared the offence, but also, directly or indirectly, the rights of other persons or legal entities. In this respect, the appropriateness of a specific SIT may, inter alia, depend on the intrusiveness into the rights of others.

38. As regards more specifically communication interception, the law should at least set out the categories of persons whose communication may be intercepted, the nature of the offences justifying the use of intercepting, the duration of the measure, the procedure for drawing up the summary reports containing intercepted communication, the precautions to be taken in order to ensure the integrity of the communication for possible inspection and assessment by the judicial authorities and the parties, and the circumstances in which they should be permanently deleted (in particular following discharge or acquittal of the accused).

39. More generally, with regard to the compatibility of SIT with the requirements of Article 8, the Court has been called upon to examine a certain number of situations such as:

A) With respect to telephone tapping:

The Court has laid down the principle that telephone tapping must comply with the law, considering that, where it does not, it is prohibited, regardless of whether it is for judicial purposes or for reasons of national security.

B) With respect to searches:

Depending on the scope of the measures and the guarantees provided by domestic law, to allow a non-judicial authority alone to decide on such operations may constitute a violation of the Convention.

In some circumstances, the Convention requires a judicial authority to decide on the appropriateness, number, duration and scope of search operations and for searches to be carried out within the limits of a warrant issued by a judge. In other circumstances, the Court has accepted as lawful a purely administrative search in view of the strict legal framework in which it took place and the proportionate scope of the action.

C) With respect to interception of mail:

The Court has accepted that the existence of legislative provisions granting powers for the covert surveillance of correspondence and other items sent through the mail might be necessary as part of the fight against terrorism, if appropriate and sufficient safeguards against abuse are provided. The Court's appreciation will depend upon the nature, extent and duration of any measures, the reasons required for ordering them, the authorities competent to authorise them, carry them out and review them, and the type of remedy provided for in domestic law. Further protection is granted with respect to correspondence with a lawyer since this type of interference affects the rights of the defence.

Electronic correspondence has introduced a new situation: where investigation of criminal offences or the protection of public order are legitimate reasons for interference, a clearly defined legal framework is required. The particularity of such interference is that it affects not only the secrecy of correspondence but also the secrecy of communications and the right to privacy at home.[6]

D) With respect to photographing and filming:

The Court has accepted the legitimacy of such techniques in the very particular context of the fight against terrorism and during questioning by the security forces. It stressed that this context influenced its assessment of the fair balance between the rights of the individual and the needs of society. However, it is clear that there must be a legal framework whose application is foreseeable, a legitimate aim, and that such techniques must be regarded as having been necessary in a democratic society for the prevention of crime.

E) With respect to the use of informants:

[6] ECtHR, Roman Zakharov v. Russia, Application no. 47143/06, Judgment, 4 December 2015, paras. 227-234.

The Court has accepted that the needs of police action may require the use of informants without that being in violation of Article 8 of the Convention. The police do not have a duty as such to reveal the identity of persons who provide them with information, but the using of such information as evidence before a tribunal will have to respect the right to a fair hearing guaranteed under Article 6 of the Convention.

Paragraph 6:

40. Paragraph 6 reiterates that SIT could result in a limitation of the rights enshrined in the Convention only to the extent in which they pursue a legitimate aim and are necessary in a democratic society. As to the question whether an interference was "necessary in a democratic society", the case law by the Court established that when balancing the interest of the respondent State in protecting its national security and or for the prevention of disorder or crime against the seriousness of an interference, the national authorities enjoy a certain margin of appreciation. However, this margin is subject to supervision by the Court embracing both legislation and decisions applying it. In view of the risk that a system of covert investigative techniques may undermine democracy and the rule of law, the Court must be satisfied that there are adequate and effective guarantees against abuse.[7]

41. As it was clarified in the Explanatory Report of Recommendation Rec(2005)10, the extent to which SIT can be used depends on the degree to which such use is necessary and proportionate in a democratic society. However, paragraph 6 should not be interpreted as an obligation on member States to introduce additional SIT. The SIT that should be available depend on what is considered appropriate by national legislative authorities.

Paragraph 7:

42. Paragraph 7 departs from the Court's assumption that "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[8]

43. Judicial review and supervision of covert surveillance measures may come into play at three stages: when the measure is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of covert surveillance dictate that not only the surveillance itself but also the accompanying judicial review should be implemented without the individual's knowledge. Consequently, it is essential that the procedures established should provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed faithfully in the supervisory judicial procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers.

44. As it was noted in the Explanatory Report of Recommendation Rec(2005)10, the various types of control may be complementary, depending on the degree of intrusiveness in the private sphere occasioned by the use of SIT. For example, in undercover operations, there may be judicial control at the beginning, during and at the end of the operation. At the beginning, the launching of the operation would be subject to there being sufficient reasons or suspicions; during the operation, regular reports would be made and, lastly, a precise description of the conduct of the operation would enable ex post facto control.

Paragraph 8:

45. The ability of individuals and legal persons to challenge the use of SIT and have access to an effective remedy against their misuse before a national authority is a necessary component of the rights and freedoms granted under the Convention, as stated in Article 13. The recommendation has a specific provision recognising such a right where there has been a misuse of SIT. The Court has recognised that the covert nature of SIT should not render them "effectively unchallengeable and outside the supervision of the national judicial authorities and the Court".[9]

b) Conditions of use:

[7] ECtHR, Klass and others v. Russia, op.cit., para. 46.
[8] ECtHR, Klass and others v. Russia, op.cit., para. 56.
[9] ECtHR, Roman Zakharov v. Russia, op.cit., para. 171.

Paragraph 9:

46. Paragraph 9 has been reproduced in its entirety. It should be noted that, as clarified in the Explanatory Report of Recommendation Rec(2005)10, the determination of "sufficient reasons" presupposes the existence of facts or information which would satisfy an objective observer that the person concerned may have committed the offence. However, "what may be regarded as 'reasonable' will depend upon all the circumstances".[10]

47. The reference to a crime "being prepared" covers situations where, although no offence has been committed yet, a person has carried or is carrying out one or more actions that could objectively be considered as contributing to the preparation of an offence.

Paragraph 10:

48. This paragraph underlines the importance and the non-derogative nature of the principle of proportionality when deciding to deploy SIT.

Paragraph 11:

49. This paragraph is reproduced to encourage competent authorities to apply other investigation methods than SIT if such methods enable the offence to be detected, prevented or prosecuted "with adequate effectiveness". The words "with adequate effectiveness" indicate that other investigation methods than SIT should be used if, firstly, they are capable of leading to the same results and, secondly, their implementation does not give rise to significant practical obstacles.

Paragraph 12:

50. The first sentence of the paragraph does not mean that SIT should exclusively be used to obtain information and material that can serve as evidence before the courts. It aims at ensuring that, where appropriate, information or material gained from the use of SIT can lawfully be produced in the course of a trial before national courts and calls on member States to enact appropriate legislation to this end.

51. As indicated in the second sentence of the paragraph, evidence gained from the use of SIT should not be submitted in such a way as to jeopardise the right of the accused to a fair trial, guaranteed by Article 6 of the Convention. In this regard, it should be recalled that, even though Article 6 of the Convention "does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law",[11] the Convention requires the proceedings as a whole, including the way in which evidence is submitted, to be fair. In this context, it should be underlined that paragraph 7 does not prevent member States from excluding the admissibility as evidence of information or material gained by SIT in extraordinary cases, in particular where the SIT has not been used in accordance with national law.

52. In the Lüdi and Teixera de Castro cases,[12] the Court considered that supervised operations and controlled operations were compatible with the rights of the accused only if those operations were conducted in the framework of a judicial investigation and the identity and role of the infiltrated officer were known to the judge. Conversely, action taken without judicial supervision would be unfair and would taint the procedure from the outset.

53. While the Court accepts the use of infiltrated officers whose role is not entirely passive,[13] it condemns provocation to commit offences.[14] There is provocation where the behaviour of the authorities has been decisive in the commission of an offence. The Court also considers that a conviction based substantially on the testimony of "*agents provocateurs*" violates the right to a fair hearing.

54. The use of undercover agents, anonymous informants and anonymous witnesses gives rise to particular legal concerns. The Court has often stated that the Convention does not prohibit the use of

[10] ECtHR, Fox, Campbell and Hartley v. the United Kingdom, Application No. 12244/86; 12245/86; 12383/86, Judgment, 30 August 1990, para. 32; see also ECtHR, O'Hara v. The United Kingdom, Application no. 37555/97, Judgment, 16 October 2001, para. 34.
[11] ECtHR, Schenk v. Switzerland, Application no. 10862/84, Judgment, 12 July 1988, para. 46. García Ruiz v. Spain, Application no. 30544/96, Judgment, 21 January 1999, para. 28.
[12] ECtHR, Lüdi v. Switzerland, Series A no.238, Judgment, 15 June 1992; ECtHR, Teixeira de Castro v. Portugal, Application nos. 44/1997/828/1034, Judgment, 9 June 1998.
[13] ECtHR, Lüdi v. Switzerland, op. cit.
[14] ECtHR, Teixeira de Castro v. Portugal, op. cit.

anonymous informants during a preliminary investigation but that the use of information thus obtained at the trial presents a problem with respect to fairness.[15] The Court takes as its starting-point the principle that evidence must be presented at the trial and debated in the presence of both parties; this does not, however, prohibit the use at the trial of statements made during the investigation, provided that those who made them have been cross-examined by the defence prior to the trial. The use of anonymous testimony by witnesses who do not appear at the trial for security reasons and whose identity remains unknown to the defence, and sometimes even to the trial judge, has to be examined. The admissibility of anonymous testimony depends on the circumstances of the case and on the answer to three questions emerging from the case-law: Is anonymity justified by a compelling reason? Have the resulting limitations on the effective exercise of the rights of the defence been adequately compensated for? Was the conviction exclusively or decisive based on such anonymous testimony?[16]

c) Operational guidelines:

Paragraph 15 and 16:

55. As noted above, the recommendation specifically defines and draws attention to the use of SIT in financial investigations. Such investigations may disrupt the criminal activity, by preventing perpetrators from generating revenues from their conduct, or block access to funds being used to further such activities. In addition, financial investigations may trace the proceeds of the criminality in order to freeze, seize and deprive persons and, where national legislation so provide, legal entities of those assets that result from the activity.

56. It should be also considered that the use of these SIT do not usually jeopardize the relevant fundamental rights as they are envisaged and protected by the Convention.

Paragraph 17:

57. Similarly, the recommendation calls upon member States to utilise SIT in cyber investigations, both to investigate and disrupt criminality occurring in this environment.

Paragraph 18:

58. The retention and the preservation of traffic data and, where legally available, of personal data may be necessary in any investigation into serious crime, including acts of terrorism. For the purpose of this recommendation, it should be recalled that traffic data has been defined in Article 1, d) of the Convention on Cybercrime of 23 November 2001 (ETS No. 185). It should also be noted that service provider has been defined in Article 1, c) of the Convention on Cybercrime (ETS No. 185).

59. Member States should ensure that the access to traffic data retained for other purposes by law enforcement authorities is pursued in accordance with national legislation and international instruments, especially Article 8 of the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

60. However, paragraph 18 should not be read or interpreted in a way that imposes any obligation on member States to introduce legislation on retention and preservation of traffic data that goes beyond obligations that already exist under international or national law.

Paragraph 19:

61. Interception of communications is one of the most commonly used SIT in member States. Paragraph 19 calls for such interception to meet “minimum requirements of confidentiality, integrity and availability”. These requirements mean that the information should be accessible only to certain authorized persons (confidentiality), that the information should be authentic and complete, thus granting a minimum standard of reliability (integrity) and that the technical system in place to intercept communications is accessible whenever necessary (availability).

[15] ECtHR, 20 November 1989, Kostovski v. the Netherlands.
[16] ECtHR, Kostovski v. The Netherlands, Application no. 11454/85, Judgment, 20 March 1990; ECtHR, Van Mechelen and others v. the Netherlands, (55/1996/674/861-864), 23 October 1997; ECtHR, Doorson v. the Netherlands, Application no. 20524/92, Judgment, 26 March 1996; ECtHR, Visser v. the Netherlands, Application no. 26668/95, Judgment, 14 February 2002, para. 46.

Chapter III. National and international co-operation

Paragraph 22:

62. The text of Recommendation Rec(2005)10 was amended as to include reference to national cooperation. This addition aims at reflecting the CODEXTER (2014)1 Discussion Paper on Special Investigation Techniques insofar as it suggests addressing the issue of how to further improve cooperation on information gathering and sharing between the different competent authorities involved in combating terrorism at both international and national level.

63. The terms "international arrangements" in this paragraph include not only multilateral but also bilateral agreements and instruments.

64. States need to ensure that law enforcement has timely access to investigate, including monitoring, financial information on targets, such as: assets, individual and (where national legislation so provide) legal entities and transactions of any kind. The relevant provisions can be sourced from the Warsaw Convention (CETS 198) – Articles 7, 17, 18 and 19.

65. The reference to jurisdiction in connection with the use of SIT on cyber investigations reflects concerns that member States should not exploit SIT to circumvent traditional measures of international co-operation and interfering with the principle of territoriality and the sovereignty of other states. The Convention on Cybercrime (ETS No 185) provides, in Article 32, for two circumstances in which a Party is permitted to access computer data stored in another Party without seeking mutual assistance. Other situations are, however, neither authorised nor precluded.

Paragraph 23:

66. The text was updated as to include most recent fundamental conventions and instruments, such as: the Convention on the Prevention of Terrorism of 16 May 2005 (CETS No. 196) and its Additional Protocol 22 October 2015 (CETS No. 217); the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 16 May 2005 (CETS No. 198); the Additional Protocol to the Council of Europe Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). A specific reference concerns the 2012 Recommendations of the FATF.

Paragraph 24:

67. The reference to the "Council of Europe" that appears in this paragraph, aims at inviting member States to increase their participation in the various existing or future committees of experts set up by the Committee of Ministers, as well as in any future European conferences or meetings to be organised by the Council of Europe in connection with the use of SIT. The amended text further refers to other institutions, courts and tribunals, key partners of the Council of Europe, which have gained valuable experience in using SIT in co-operation with relevant states and organisations.

Paragraph 25:

68. This paragraph was amended in order to further encourage member states to exchange information spontaneously, i.e. without prior requests. It is based on the idea that member States should overcome the practical problems which hamper effective co-operation by reinforcing exchanges at the operational level between competent authorities. Examples of such "practical problems" include those related to working procedures, including undue delays, lack of information, lack of language knowledge, undue bureaucracy, slow transmission of information, inappropriate point of contact, cost related issues and any other relevant technical issues. The paragraph also refers to competent authorities proactively and spontaneously offering information and assistance to other member States, where appropriate. This reflects Article 26 of the Convention on Cybercrime (ETS No. 185), as well as Article 22 of the Convention on the Prevention of Terrorism (CETS No. 196) and Article 22 of the Convention on Laundering, Search, Seizure and Confiscation of the proceeds of crimes and on the financing of terrorism (CETS No. 198).

Paragraph 26:

69. This paragraph is based on the idea that common technical references in the field of SIT should ease international co-operation. As far as "internationally agreed standards" is concerned, particular attention could

be given to the work conducted by the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Service (ITU) on this issue.[17]

[17] For more info: http://portal.etsi.org/li/Summary.asp ; www.etsi.org and http://www.itu.int/en/Pages/default.aspx