COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 19 August 2021
[PC-OC/PC-OC Mod/Docs PC-OC Mod 2021/ PC-OC Mod (2021)04E]
http://www.coe.int/tcj

PC-OC Mod (2021)04
English only

EUROPEAN COMMITTEE ON CRIME PROBLEMS

(CDPC)

COMMITTEE OF EXPERTS

ON THE OPERATION OF EUROPEAN CONVENTIONS

ON CO-OPERATION IN CRIMINAL MATTERS

(PC-OC)

SPECIAL INVESTIGATIVE TECHNIQUES: ASSESSING THE NEED FOR ADDITIONAL REGULATION IN THE COUNCIL OF EUROPE'S INSTRUMENTS OF LEGAL ASSISTANCE IN CRIMINAL MATTERS

Discussion Paper

by Mr Pyotr Litvishko (Russian Federation), PC-OC Mod Substitute Member

Contents

I. Introduction

According to the List of decisions taken at the 79th meeting of the PC-OC under the chairmanship of Mr Erik Verbert (Belgium) held by videoconference 4–6 May 2021, the PC-OC decided to ask the PC-OC Mod to continue the examination of the different proposals [for a future update of the 1959 Convention in an additional protocol], based on the discussions held and to present their conclusions to the plenary, and noted the proposal to address the issue of the use of special investigative techniques (hereinafter referred to as "SIT(s)") in criminal matters.[1]

The importance and timeliness of raising this subject can hardly be overestimated. The new reality characterized by such major factors as virtualization, anonymization and pseudonymization leaves the judicial and law enforcement communities no option, calling for equally surreptitious means and methods of their work. The employment of stealthy operations is more than ever gaining on relevance, especially in the online environment, compared to the physical world often being the only way to collect admissible evidence, expose criminals, disrupt and dismantle transnational criminal networks.[2]

This paper explores the nature of SITs, the international global (UN, FATF) and regional (CoE, CIS, SCO and CSTO) as well as domestic legal frameworks, and addresses the challenges of their designation and definitions. It identifies the problems of their coverage in the treaties, and relationships and differences in interpretation and application. The paper concludes with the proposals for the required CoE regulations.

II. Designation/Definition Challenge. Council of Europe Framework: National vs. International SITs

It is common knowledge that names are too often just arbitrary labels which do not reflect intrinsic qualities of things they are attached to. Shakespeare's "What's in a name?" is of relevance when one starts talking about SITs.

For the most part, SITs are associated with law enforcement intelligence[3] which, in turn, is considered an outgrowth of military and national security intelligence that dates back to ancient

---

[1] List of decisions taken at the 79th meeting of the PC-OC under the Chairmanship of Mr Erik Verbert (Belgium). Meeting held by Videoconference 4-6 May 2021. Strasbourg, 17 May 2021 [PC-OC/Docs PC-OC 2021/ PC-OC (2021)05E], p. 3–5, items 3b and 5.

[2] Cf.: para. 24 of the Explanatory report to the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Draft Protocol version 2. T-CY(2020)7_PDP_Protocol_v2b (PDP 12 April 2021) states that "[t]he drafters also considered other measures which, after thorough discussion, were not retained in this Protocol. Two of these provisions, namely, "undercover investigations by means of a computer system" and "extension of searches", were of high interest to Parties but were found to require additional work, time and consultations with stakeholders."

[3] Law enforcement intelligence mainly represents information gathered surreptitiously to prevent, identify and combat criminal offences. SITs can be deployed either for intelligence-gathering or evidential purposes.

Unlike the definitions in the Council Framework Decision 2006/960/JHA of 18 Dec. 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (art. 2), the term "criminal (law enforcement) intelligence operation" as used in this paper is a synonym for a SIT and encompasses the stages both of a criminal intelligence operation *per se* and a criminal investigation, i.e., both proactive and reactive types of investigations.

times;[4] references to it can be found in ancient Chinese writings (Sun Tzu, fl. 4th century BC) and the Bible (Numbers 13).[5]

The methods to transform the product of SITs (the biblical "fruit of the land") into evidence and adduce it in court, as well as the evidential value allocated to materials derived from the deployment of SITs, are different in the existing legal systems.

Various sources generally distinguish the following types of covert SITs:[6]

– interception of communications;

– controlled deliveries;

– surveillance (observation);[7]

– (virtual) covert investigations (undercover operations)[8], such as:

infiltration, i.e., the use of undercover officers,[9] assumed identities (legends);

staging (imitation) of criminal offences, or (reverse) sting operations, like a storefront or other (online) undercover facility, pseudo-purchases (test buys) and sales, other simulated transactions, and other pseudo offences, while as a general rule no entrapments (police incitement) or agents provocateurs are permitted;

integrity testing (simulation of bribery);

financial transaction monitoring;

– deployment of covert human intelligence sources, i.e., confidential informants; in some legal systems, the latter are subsumed under the notion of "undercover (police or intelligence) officers (undercover agents, police operatives)";

– covert obtainment of samples (DNA from a fingerprint, lip smear or other objects, voiceprints, video footage, or malware specimens);

---

[4] M. Peterson, *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: U.S. Department of Justice, 2005), p. 5.

[5] "The LORD said to Moses, "Send men to reconnoiter (in other translations, "search", "explore", or "spy out") the land of Canaan". The men conducted covert observation and sampling, procuring "the fruit of the land". In the end, they presented a misinformative description ("a bad report") of the outcome of their covert investigations.

[6] See, e.g.: *Mutual Legal Assistance Manual* (Belgrade: Council of Europe Office in Belgrade, 2013), pp. 33–36 and 101–109; *Model Legislative Provisions against Organized Crime* (New York: United Nations, 2012), pp. 59–87; *Model legislation on money laundering and financing of terrorism* (United Nations Office on Drugs and Crime, International Monetary Fund, 2005); *Technical Guide to the United Nations Convention against Corruption* (New York: United Nations, 2009), pp. 182–187; Recommendations on Special Investigative Techniques and other Critical Measures for Combating Organized Crime and Terrorism. Meeting of G8 Justice and Home Affairs Ministers, Washington – May 11, 2004.

[7] "Surveillance" is either physical (conventional) (tailing, stakeout, shoulder surfing, aerial covert surveillance using unmanned aircraft (drones) etc.; it may also extend to monitoring bank accounts in financial investigations, monitoring computer activities in cyber investigations (equipment interference)) or technical (electronic). The latter is more intrusive than the former and includes audio, visual, tracking and data surveillance, may be directed (in a public place) or intrusive (involving the installing and using of a covert listening or recording device (wireless transmitter) in residential premises or private vehicles).

"Surveillance" may also be used as an umbrella term for various kinds of SITs. See: *Current practices in electronic surveillance in the investigation of serious and organized crime* (New York: United Nations, 2009), p. 2.

[8] E.g., in virtual investigations by using loggers, such as IP Grabber (Grabify IP Logger), hardware and software keystroke loggers, sniffers to more complex methods.

[9] They include undercover online operatives. Techniques employed by them may include various kinds of misrepresenting their identities, e.g., communicating through the online identity of a cooperating witness (with consent) or appropriating online identity, or lure, or using products of private persons' "digilantism" (Internet vigilantism, or sousveillance) (e.g., those derived from proactive impersonation of a child or of a facilitator of child exploitation online or compromising information systems used for the purposes of child pornography).

– (transborder) remote search in information systems and networks, use of remote forensics (e.g., in forensic virtual asset investigations).

The term of art “SIT” originates in the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 1990. Pursuant to art. 4.2 (“Special investigative powers and techniques”), “[e]ach Party shall consider adopting such legislative and other measures as may be necessary to enable it to use special investigative techniques facilitating the identification and tracing of proceeds and the gathering of evidence related thereto. Such techniques may include monitoring orders, observation, interception of telecommunications, access to computer systems and orders to produce specific documents.”

The Explanatory Report to the 1990 Convention (para. 30) indicates that “[p]aragraph 2 of the article was drafted to make States aware of new investigative techniques which are common practice in some States but which are not yet implemented in other States. The paragraph imposes an obligation on States at least to consider the introduction of new techniques which in some States, while safeguarding fundamental human rights, have proved successful in combating serious crime. Such techniques could then also be used for the purposes of international cooperation. In such cases, Chapter III, Section 2, would apply. The enumeration of the techniques is not exhaustive.”

As one can see, SITs were initially conceived as a mixture of judicial/law enforcement intelligence measures, not necessarily of a surreptitious nature, including such patently overt judicial measure as a production order.

The Explanatory Report to the 1990 Convention may be held to elucidate what was, is and will always be “special” about SITs in art. 4 (also, in comparison with “ordinary” “Investigative measures” in art. 3) and in any other document applying the inseparable words of the term since then – they were “new” and not “common” to all States. (However, it is difficult to accept the novelty (or comprehend how they can otherwise be uncommon or special) of such old-timers as physical surveillance, undercover activities, use of informants, production orders (subpoenas, warrants) and other classical police and criminal justice tools.)

The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 2005 largely reproduces the wording of the 1990 Convention in relation to SITs, and its Explanatory Report (para. 85) again, in 15 years, calls them “new” and not “common” to all States. Currently, after a lapse of another 15 years, in the CoE Member States this is definitely not the case anymore.

It is therefore clear that presently the adjective “special” has no added value, failing to convey its meaning, and the term “SIT” as a whole may be perceived as a misnomer, as vague and lacking legal certainty as it was over 30 years ago encapsulating its “zero-day” vulnerability.

The terminological deficiencies and lack of a uniform concept of SITs also result in the divergent scopes of the relevant measures and inconsistent usage throughout various documents, primarily either equating them with only covert actions[10] or, as was discussed above, including some overt activities in them as well.

In addition, as will be shown further, some countries’ legislation distinguishes between covert and overt criminal intelligence measures (the latter include inspection of premises, vehicles and objects, identification (lineups, identity parades etc.), sampling, interviews etc.), which should be taken into account when developing a definition of a SIT that would be acceptable to those countries, by underscoring the covert type, and its denomination to import secretness in and of itself, which is not the case with the current designation of a SIT.

[10] See, e.g.: Good practices in special investigative techniques. Background paper by the Secretariat. Conference of the Parties to the United Nations Convention against Transnational Organized Crime, Working Group on the Smuggling of Migrants, Vienna, 11-13 Nov. 2013 (UN Doc. CTOC/COP/WG.7/2013/2 of 7 Aug. 2013), para. 8 (“Special investigative techniques, also known as “covert investigation techniques” differ from routine investigation methods, and include both covert techniques and the use of technology”).

At present, there is no universally recognized definition of the legal phenomenon of SITs.

The Legislative Guide to the Organized Crime Convention defines SITs as "techniques for gathering information in such a way as not to alert the target persons, applied by law enforcement officials for the purpose of detecting and investigating crimes and suspects."[11]

A regional CoE definition of SITs was introduced in 2005 and is currently reproduced in the Recommendation of the Committee of Ministers of the Council of Europe to Member States on "special investigation techniques" in relation to serious crimes including acts of terrorism of 2017,[12] which defines SITs as "techniques applied by the competent authorities in the context of criminal investigations for the purpose of preventing, detecting, investigating, prosecuting and suppressing serious crimes, aiming at gathering information in such a way as not to alert the target persons". "Competent authorities" means judicial, prosecuting and investigating authorities involved in deciding, supervising or using SITs in the context of criminal investigations in accordance with national legislation. SITs are applied both in a judicial context and for purposes of intelligence gathering outside of a judicial context. The scope of this Recommendation is only the application of SITs in a judicial context, including for the purposes of financial or cyber investigations.

The Explanatory Memorandum to the 2017 Recommendation gives a non-exhaustive list of SITs: for the purpose of this Recommendation, SITs 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; cross-border (hot) pursuits; pseudo-purchases or other "pseudo-offences", covert monitoring of financial transactions and web traffic as they are defined in national legislation.

This definition may be said to also include purely judicial actions that cannot be considered as such techniques due to their overt character, like examining people other than the subject himself or seizing documents while taking basic precautions not to alert the target through imposing various forms of non-disclosure obligations upon the persons directly involved in those actions, issuing gagging orders, for example, in the legal process preventing default notification by telecom service providers to subscribers whose data are subject of a preservation or production order, or such measures as consensual monitoring or trash runs (dumpster diving).

The CoE's AML/CFT framework (the 1990 Convention (arts. 3, 4, 7 and 8) and the 2005 Convention (arts. 2, 4, 7, 15 and 16)) regulates SITs at the national level only and the international assistance in broad terms with respect to instrumentalities, proceeds and other property.

Other CoE conventions providing (explicitly in their texts or implicitly through their explanatory reports with examples) for domestic-level, but not international-level SITs, are the 1999 Criminal Law Convention on Corruption,[13] the 2011 Convention on the counterfeiting of medical products and

[11] *Legislative guide for the implementation of the United Nations Convention against Transnational Organized Crime* (New York: United Nations, 2004), paras. 442–455.

[12] Recommendation CM/Rec(2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism (Adopted by the Committee of Ministers on 5 July 2017 at the 1291st meeting of the Ministers' Deputies), Explanatory Memorandum thereto. It has replaced Recommendation Rec(2005)10 of the same name, which was the first to establish a SIT definition. As a precursor thereto, one can regard Recommendation Rec(2001)11 concerning guiding principles on the fight against organised crime, which in para. 19 gives national-level examples of "investigative measures (techniques)" (surveillance, interception of communications, undercover operations, controlled deliveries and the use of informants).

[13] Art. 23 ("Measures to facilitate the gathering of evidence and the confiscation of proceeds"), Explanatory Report (para.114) ("this provision includes an obligation for the Parties to permit the use of "special investigative techniques". No list of these techniques is included but the drafters of the Convention were referring in particular to the use of under-cover agents, wire-tapping, bugging, interception of telecommunications, access to computer systems and so on.")

similar crimes involving threats to public health[14], and the 2015 Convention against Trafficking in Human Organs.[15]

The next section will focus on the CoE core treaties – the European Convention on Mutual Assistance in Criminal Matters of 1959 (hereinafter referred to as "the 1959 Convention" or "mother Convention") and its two additional protocols – that do not actually use the term "SIT", but, as distinct from the instruments discussed above, are not sectoral and ordinarily apply to all kinds of criminal offences.

III. To What Extent Are SITs Covered in the 1959 Convention and Its Protocols? Domestic vs. Cross-Border SITs

In accordance with art. 3.1 of the 1959 Convention, "[t]he requested Party shall execute in the manner provided for by its law any letters rogatory relating to a criminal matter and addressed to it by the judicial authorities of the requesting Party for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents."

To ascertain the purpose of the document and properly interpret its authors' intentions, one should refer, among others, to its *travaux préparatoires*.

Pursuant to the Explanatory Report to the 1959 Convention (commentary on art. 3), "[t]he expression "procuring evidence" refers, inter alia, to the hearing of witnesses, experts or accused persons, the transport involved *[sic]* as well as search and seizure."

Down the road, the state of affairs and new developments in crime and in combating criminal offences called for the adoption of the Recommendation of the Council of Europe's Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications of 1985[16] (hereinafter referred to as "the 1985 Recommendation") and then the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 2001 (hereinafter referred to as "the 2001 Protocol"), respectively, to read into the 1959 Convention's scope and further to expressly envisage in the 2001 Protocol, a limited number of covert forms of cooperation as well.

Notwithstanding the presence of the phrase *"inter alia"*, it appears evident that initially, in principle just procedural actions of a public, or overt nature were meant to be included in the scope of the 1959 Convention, since there was no mention of a single clandestine operation to exemplify the inclusion thereof, although at least some of them were undoubtedly existent at the time and could have hardly escaped the drafters' scrutiny. As discussed elsewhere in this paper, it was only in 1990 that the CoE Anti-Money Laundering Convention introduced SITs, labelling them "new". The 1978 and 2001 Protocols changed nothing as regards the "SITless" scope of art. 3 of the mother Convention.

Additionally, the Explanatory Report to the 2001 Protocol in the commentaries on articles concerning SITs states that "the purpose of the drafters when taking account of [the respective covert measures] in this Protocol was not to include police or other forms of non-judicial co-operation within

---

[14] Art. 16 ("Criminal investigations"), Explanatory Report (para. 109) ("Effective investigation" is further described as including financial investigations, covert operations, controlled delivery and other special investigative techniques. These could encompass electronic and other forms of surveillance as well as infiltration operations.")

[15] Art. 16 ("Criminal investigations"), Explanatory Report (para. 102) ("The negotiators noted that conducting effective criminal investigations may imply the use of special investigation techniques in accordance with the domestic law of the Party in question, such as financial investigations, covert operations, and controlled delivery.")

[16] Recommendation No. R(85)10 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies).

the scope of this Protocol, but rather to take in [those measures] as a form of mutual legal assistance". Similar attempts at justification are absent in the Explanatory Report to the 1959 Convention, which, again, allows to argue that covert SITs, domestic or let alone cross-border, were not intended to be covered by the mother Convention.

A CoE publication asserts that "[a]lthough the *European Convention on Mutual Assistance in Criminal Matters* does not specifically address special investigative techniques as a measure of assistance, it is quite clear that co-operation of such measures was envisaged within the context of assistance (See Recommendation No. R (85) 10 sets out fairly detailed rules in relation to requests for interception of communications under the European Convention on Mutual Assistance in Criminal Matters) and subsequently set out in *The 2nd Additional Protocol to the European Convention on mutual assistance in criminal matters* through the following provisions: Article 18: controlled delivery; Article 19: covert investigations; Article 20: joint investigation teams." [17]

This interpretation is far-fetched as it endeavors to stretch the mother Convention out to be comprehensive, which it is not, that fact bringing about the subsequent adoption of sectoral CoE conventions on cooperation in criminal matters, including the 2001 Budapest Convention on Cybercrime, whose harbinger the 1985 Recommendation actually was. The Recommendation means only so much that the States Parties to the 1959 Convention had agreed to deem the Convention applicable to requests for domestic intercepts, and is understandably silent on any other SITs. The circumstance that the 2001 Protocol subsequently extended the mother Convention's scope to encompass some selected cross-border, but not domestic SITs, adds little or nothing to the authors' argument.

Notwithstanding its non-binding soft law character, the 1985 Recommendation has a self-contained régime, enumerating, *inter alia*, the mandatory grounds for refusal of assistance irrespective of those set out in the 1959 Convention, contents of requests, and conditions of their execution.

The 1985 Recommendation and consequently the 1959 Convention may also be considered to envisage the bulk interception of communications, communications data and sharing of their product with foreign judicial and law enforcement counterparts for further data mining, analyzing and filtering for criminal investigation purposes using tasked selectors (search terms), while observing the standards and safeguards similar to those recently determined by the ECHR in respect of intelligence services' activities.[18]

Except for interception of communications, *covert* SITs enumerated in section II of this paper, with no cross-border components, fall outside the scope of the 1959 Convention and its two Protocols and are arguably not available to be performed in the domestic context of the requested States under them.

Unlike domestic and cross-border interceptions of telecommunications, for example, under the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, the 1959 Convention and its Protocols' framework does not cover a cross-border interception of telecommunications, since where the 2001 Protocol does regulate the cross-border forms of assistance, it addresses them explicitly as such in the dedicated provisions, which, in turn, may normally be subject to exclusion and other reservations by Contracting States due to their significant implications for the States' sovereignty. As opposed to art. 3 regime, they are discretionary rather than mandatory and are scarcely applicable to *corpora delicti* that do not satisfy the requirement of dual criminality, non-extraditable or administrative (under art. 1.3 of the 1959 Convention as amended by the 2001 Protocol) offences. All other requested actions under arts. 3, 5 and the rest of the 1959 Convention and its Protocols are assumed, as a general rule, to be domestic (internal) in character, that is, carried out within the requested State's territory in behalf of the requesting State, unless there is a clear indication to the contrary in the texts.

[17] *The Deployment of Special Investigative Means* (Belgrade: Council of Europe Office in Belgrade, 2013), p. 81.

[18] *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, ECHR; *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021, ECHR.

IV. Other International and Domestic Legal Frameworks. Problems of Coverage, Relationship, and Differences in Interpretation and Application: Legal (Judicial) vs. Law Enforcement Assistance

The UN Conventions against Transnational Organized Crime of 2000 (arts. 20 and 27) and Corruption of 2003 (arts. 48 and 50) lay the universal foundations for SITs,[19] while separating them from mutual legal assistance in the dedicated articles. However, their provisions are not "self-executing" for all States as they require further international agreements or arrangements, or purely discretionary decisions on a case-by-case basis, therefore not being a sufficient source of legal authority.[20] SITs may also be considered under other universal sectoral conventions, in the first place, counter-terrorism ones, as well as Security Council resolutions. However, in most cases, because of their general catchall language not expressly indicating covert SITs, they can hardly qualify to create the sufficient binding international obligations with respect to SITs.

The same is true for the FATF Recommendations (31, 37 and 40) which establish the relevant national- and international-level provisions. Under them, countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts.[21]

---

[19] It is sometimes argued that because of its art. 9, the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances may be considered to be a precursor to what would follow in other conventions in terms of introducing SITs. See: H.G. Nilsson, "Special Investigation Techniques and Developments in Mutual Legal Assistance - The Crossroads between Police Cooperation and Judicial Cooperation", in *Resource Material Series No. 65, United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI)* (Fuchu, Tokyo, Japan, Mar. 2005), p. 40.

The same can be said about older treaties, especially bilateral ones, dating back to earlier decades, where their scope was framed in terms of procedural stages of combating crime, such as any assistance in preventing, detecting, suppressing, investigating, solving, prosecuting and adjudicating offences, but without explicitly naming covert means and methods. See, e.g., International Convention for the Suppression of the Circulation of and Traffic in Obscene Publications of 12 Sept. 1923 (with the Agreement for the Suppression of the Circulation of Obscene Publications of 4 May 1910), as amended by the Protocols of 1947 and 1949 respectively.

The 1990 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders and the 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime were the earliest international treaties to expressly deal with this subject matter, and it is the latter that introduced the term "SIT" in art. 4.

At the international level, the 1988 Convention was the first multilateral agreement to endorse the investigative technique and practice of controlled delivery.

[20] In more detail, see: International cooperation involving special investigative techniques. Background paper prepared by the Secretariat. Conference of the Parties to the United Nations Convention against Transnational Organized Crime, Working Group on International Cooperation, Vienna, 7 and 8 July 2020 (UN Doc. CTOC/COP/WG.3/2020/3 of 12 May 2020), paras. 41–51; *Legislative guide for the implementation of the United Nations Convention against Corruption. Second Revised Edition 2012* (New York: United Nations, 2012), para. 650.

[21] FATF (2012-2020), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/recommendations.html

Still, the major deficiencies of the said UN and CoE frameworks regarding SITs stem from their sectoral character, leaving ordinary crime out.

The actions at issue are governed by a number of the European Union supranational instruments,[22] multilateral treaties concluded within other regional and sub-regional international organizations (e.g., CIS, SCO and CSTO),[23] or bilateral interstate, intergovernmental[24] and even interagency agreements and other arrangements[25] governing law enforcement assistance in combating crime, requesting and executing both domestic and cross-border operational measures. These agreements normally do not apply to legal assistance in criminal matters, and many of them explicitly state this, although they may be used to procure both leads and evidence. (Mutual legal assistance may only constitute subject matter of treaties of the interstate level.)

Conversely, in a vicious circle for Russia and many other Commonwealth of Independent States (CIS) countries, legal (judicial) assistance treaties are not applicable to SITs which are the subject matter of those law enforcement assistance agreements, either, unless the treaties themselves, and they are few, like the 2001 Protocol or the 2002 Kishinev Convention, or sources of their authentic interpretation, have provisions to the contrary. Unlike the broad language of art. 3 of the 1959 Convention, for example, bilateral treaties on legal assistance in criminal matters to which the Russian Federation is party normally employ an enumerative approach to measures that may be requested and executed under the treaty, and there are no SITs among them.

This relationship problem was already addressed briefly by the PC-OC back in 2001, mentioning in passing that "[i]t appears that the borders between judicial and police co-operation are not always clear. For example, some see the 2nd Additional Protocol as an unhappy development consisting of introducing police co-operation into the framework of the Convention on Mutual Legal

[22] For the detailed analysis of the main types of SITs, see: *Study on paving the way for future policy initiatives in the field of fight against organized crime: the effectiveness of specific criminal law measures targeting organised crime. Final report, February 2015* (Luxembourg: Publications Office of the European Union, 2014), pp. 221–337.

[23] Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters of 7 Oct. 2002 (Kishinev Convention) (arts. 6–7, 60–61, 63, 104 and 108 ("search for persons and tracing proceeds of crime", "operational measures", "search measures" or "operational search measures", "controlled delivery", and "joint investigative and operational teams")); Agreement on Cooperation between the Governments of the Member States of the Shanghai Cooperation Organization in Fighting Crime of 11 June 2010 ("search for persons", "operational search measures", and "controlled delivery"); Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technologies of 28 Sept. 2018, Protocol on Interaction of the Member States of the Collective Security Treaty Organization in Countering Criminal Activities in Information Sphere of 23 Dec. 2014 ("operational search measures", "coordinated measures and operations for preventing, detecting, suppressing, solving and investigating crimes"); Shanghai Convention on Combating Terrorism, Separatism and Extremism of 15 June 2001 ("operational search measures"); Agreement on Cooperation of the Member States of the Commonwealth of Independent States in the Fight against Illicit Traffic in Narcotic Drugs, Psychotropic Substances and Precursors of 30 Nov. 2000 (as amended by the Protocol of 25 Oct. 2019) ("controlled deliveries", "complex coordinated or joint operational search measures, special operations", and "joint investigative and operational teams").

[24] Agreement between the Government of the Russian Federation and the Government of the United Kingdom of Great Britain and Northern Ireland on Co-operation in Fighting Crime of 6 Oct. 1997 (art. 1; Russian "operational search measures" are translated therein as "inquiries"); Agreement between the Government of the Russian Federation and the Government of the Federal Republic of Germany on Cooperation in Fighting Especially Dangerous Crimes of 3 May 1999 (art. 3 ("coordinated operational measures for preventing, detecting, suppressing and solving crimes")).

[25] Agreement on Cooperation between the Ministries of Internal Affairs in Combating Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 21 Oct. 1992 (concluded by the MoIs of the CIS Member States and the Republic of Estonia) ("operational search measures", "incessant operational surveillance of movements of drug dealers possessing interstate connections", "coordinated measures (operations) for blocking channels of illicit movement of narcotic drugs", "controlled deliveries", and "joint groups for joint operational search measures"); Agreement on Cooperation in the Field of Special Support to Operational Search Activities of 18 Dec. 1998 (concluded by the MoIs of some CIS Member States) ("operational search measures", "operational intelligence", "surveillance subject (target)", and "special support to operational search activities for the purposes of preventing, detecting, suppressing and solving crimes").

Assistance. Others however welcome that same development, considering it rather as a method of controlling police activities by judicial authorities."[26]

As was already mentioned above, the Explanatory Report to the 2001 Protocol in the commentaries on arts. 17–19 (cross-border observations, controlled delivery and covert investigations) flags up rather inconclusively[27] that "the purpose of the drafters when taking account of [the respective covert measures] in this Protocol was not to include police or other forms of non-judicial co-operation within the scope of this Protocol, but rather to take in [those measures] as a form of mutual legal assistance".[28]

There is an exception to the above in relation to the interception of communications. In Russia and some other CIS Member States, wiretapping, "pen registers", "trap and trace devices" using existing software and hardware at the Internet service or telecommunications providers,[29] real-time collection of electronic traffic (transactional, communications) or content data in transit during criminal investigations and proceedings may take the form both of a procedural, judicial action (proceeding) and of a criminal intelligence operation, both being performed for evidentiary purposes and requiring a court warrant.[30] On the other hand, operational measures that involve covert equipment or other property interference other than that using service providers' facilities, such as electronic eavesdropping (bugging of premises, vehicles, i.e., the so-called intrusive covert surveillance, or use of a "body wired" informant to record conversations that take place within his earshot), or deployment of cell-site simulators[31] fall within the exclusive domain of criminal intelligence operations.

Therefore, the application of the 1959 Convention by such countries to domestic interceptions as interpreted by the 1985 Recommendation should not face any legal difficulties. (And the Recommendation concerns the interpretation of requested domestic, but not transnational intercepts.)

Apart from that, SITs are traditionally regulated by multilateral and bilateral treaties and other instruments on mutual administrative assistance in customs matters.[32]

International assistance in operational intelligence investigations is expressly[33] or by implication[34] provided for in Status of Forces Agreements and treaties on similar overseas installations.[35]

---

[26] Judicial collaboration versus police collaboration. Subject submitted for discussion in the PC-OC at its 43rd meeting in 2001 by Mr M. Knaapen (Netherlands). Strasbourg, 30 Jan. 2013 [PC-OC\Docs 2001\20Erev].

[27] *Ibid.*

[28] SITs can also be carried out through another form of legal assistance envisaged in art. 20 of the 2001 Protocol (joint investigation teams).

[29] As well as production orders for their stored wire or electronic communications records, geolocation (cell site location tracking), and cell tower dumps.

[30] Cf.: the Russian Federation's Criminal Procedure Code of 2001, as last amended July 1, 2021, establishing the proceedings for inspection and seizure of postal or telegraphic correspondence, electronic communications or other communications transmitted through telecommunication networks (art. 185); monitoring or recording of telephone or other conversations (art. 186); and obtaining information on connections between subscribers or subscribers' devices (art. 186.1); and Federal Law no. 144-FZ, "On Operational Search Activities", of Aug. 12, 1995, as last amended July 1, 2021, establishing the following operational search measures: control of postal, telegraphic or other communications; wiretapping; capturing information from technical communications channels; and obtaining computer information (art. 6).

[31] IMSI catchers, digital analyzers like a stingray, dirtbox or triggerfish.

[32] Recommendation of the Customs Co-operation Council on Mutual Administrative Assistance of 5 Dec. 1953 ("special watch"); International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offences of 9 June 1977 ("(special) surveillance"); International Convention on Mutual Administrative Assistance in Customs Matters of 27 June 2003, Model Bilateral Agreement on Mutual Administrative Assistance in Customs Matters, as revised in June 2004 ("surveillance, controlled delivery, hot pursuit, cross-border surveillance, covert investigations, and joint control and investigation teams").

[33] Agreement between the Russian Federation and the Republic of Armenia on Jurisdiction and Mutual Legal Assistance in Matters relating to the Stationing of the Russian Military Base on the Territory of the Republic of Armenia of 29 Aug. 1997 ("search for persons", "search actions", and "operational search actions"); Agreement between the Russian Federation and the Republic of Tajikistan on Jurisdiction and Mutual Legal Assistance in Matters related to the Stay of

The dedicated regional SIT-related instruments are also the Agreement on the Procedure for Establishing and Operation of Joint Investigative and Operational Teams in the Territories of the Member States of the Commonwealth of Independent States of 16 October 2015 (“operational search measures”) and the Treaty on the Procedure for the Stay and Interaction of Law Enforcement Officers on the Territories of Member States of the Commonwealth of Independent States of 4 June 1999 (“operational search measures”, “observation”, and “hot pursuit”).

Some but not all CoE countries can cooperate in the field of SITs on the basis of reciprocity. For example, the Russian Federation cannot do this, as this legal basis is not provided for in its Federal Law “On Operational Search Activities”, requiring the treaty basis for executing SITs.

The work on global initiatives concerning the integration of SITs into the mutual legal assistance framework is underway at the United Nations agencies.[36]

One may assert that currently the CoE Member States have a patchwork and insufficient regulation of the subject at stake in terms of it not being streamlined in the framework of the Council’s treaty law and not covering major crime area. It definitely requires the advanced harmonization in a CoE treaty.

Some CoE Member States, in particular CIS countries, have stand-alone laws on SITs, whose concrete denominations vary (the most common one is “On Operational Search Activities”[37]) and which are ordinarily not part of criminal procedure *sensu stricto*.[38] Nor are “operational search activities” a component of “investigative actions” in those countries, as the latter constitute proceedings, are in essence judicial. (Much of this stuff lies, of course, in the nametag terrain of the differing legal systems.) The results of the measures performed pursuant to these laws normally need to pass through a certain validation and legalization process prior to becoming admissible evidence for a criminal case. These actions can be conducted both before the institution of a criminal case and in the course of pre-trial criminal proceedings, for intelligence-gathering and evidential purposes, proactively and reactively.[39]

Military Formations of the Armed Forces of the Russian Federation on the Territory of the Republic of Tajikistan of 21 Jan. 1997 (“search for persons”, “search actions”, and “joint operational and investigative groups (brigades)”).

[34] Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces of 19 June 1951 (art. VII.6.a (“The authorities of the receiving and sending States shall assist each other in the carrying out of all necessary investigations into offences, and in the collection and production of evidence, including the seizure and, in proper cases, the handing over of objects connected with an offence.”)).

[35] Agreement between the Government of the Russian Federation and the Government of the Republic of Kazakhstan on Interaction between Law Enforcement Authorities in Ensuring Legal Order on the Territory of the Baikonur Complex of 4 Oct. 1997 (“operational search measures”, “operational support of criminal cases”, and “joint operational and investigative groups (brigades)”).

[36] Informal Expert Group Meetings on “Updating the UNODC Model Law on Mutual Assistance in Criminal Matters (2007)”, UNODC, Division for Treaty Affairs, Counter-terrorism Learning Platform, URL: https://ctlp.unodc.org/totara/dashboard/index.php, accessed May 9, 2021.

[37] In Russian speaking countries, *operativno-razysknaya deyatel’nost’.* It is sometimes referred to as “operational investigative activities (measures)”, which is not a literal translation.

[38] For instance, the Russian Federation’s Federal Law “On Operational Search Activities” (art. 6) establishes the following exhaustive list of 15 covert and overt operational search measures that are common for intelligence, counterintelligence and criminal intelligence authorities: interview; enquiries; gathering samples for comparative analysis; test purchase; examination of objects or documents (a draft amendment adds computer information thereto); surveillance; identification of persons; inspection of premises, buildings, constructions, areas or vehicles; control of postal, telegraphic or other communications; wiretapping; capturing information from technical communications channels; infiltration; controlled delivery; operational experiment (i.e., a sting operation); and obtaining computer information.

[39] For in-depth analyses of the CIS countries’ domestic legal frameworks and practice, see: N. Kovalev and S.C. Thaman, *Special investigative techniques in post-Soviet states: the divide between preventive policing and criminal investigation*, in: J.E. Ross and S.C. Thaman (eds), *Comparative Criminal Procedure* (Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing, 2016), pp. 453–474; *Analysis of the Legislation of the Kyrgyz Republic on Special Investigative Measures* (B.: United Nations Office on Drugs and Crime, 2014), 122 p.; L.A. McCarthy, *Trafficking Justice: How Russian Police Enforce New Laws, from Crime to Courtroom* (Ithaca and London: Cornell University Press, 2015), 276 p.

At the same time, many CoE Member States have SITs (criminal intelligence operations) incorporated in their laws on criminal procedure and statutes on international mutual legal assistance, thus there appears to be a convergence of procedural and criminal intelligence activities, on the one hand, and of legal (judicial) and law enforcement (police-to-police) international assistance,[40] on the other hand, to some extent, with treaties like the 2001 Protocol following suit.

Currently, we are witnessing the dissolution of boundaries between the procedural pre-trial (preliminary) investigation and operational investigation/intelligence activities in the countries where these institutions have long been separated. These two investigative concepts are integrating mainly due to the incorporation of operational/intelligence activities into criminal procedure.[41]

For example, as a type of procedural activities (proceedings) identical or similar to "operational search measures" *(operativno-razysknyye meropriyatiya)* in Russian law, the Code of Criminal Procedure of Ukraine of 2012 (arts. 246–275) governs the grounds and the procedure for carrying out "covert investigative (search) actions" *(негласні слідчі (розшукові) дії)*;[42] the Criminal Procedure Acts of the Czech Republic of 1961 (§§ 86–87c and 158b–158f) and Slovakia of 2005 (§§ 110–118) (with later amendments) mainly in Ch. "Providing Information" as distinct from the next Ch. "Proof"), while retaining the previous denomination, – "operational search means" *(operativně pátrací prostředky)* and "means of operational search activity" *(prostriedky operatívno-pátracej činnosti)*; the Austrian Criminal Procedure Code of 1975 (§§ 99, 118 and 129–133) governs the actions analogous to "operational search measures" in Sec. "Investigative Measures and Obtaining Evidence" *(Ermittlungsmaßnahmen und Beweisaufnahme)*; the amended German Code of Criminal Procedure of 1950 (§§ 98a–98c, 100c–101, 103, 110a–111 and 163e–163f) in the special section along with seizure, attachment of property and correspondence, and interception of telecommunications; the Swiss Criminal Procedure Code of 2007 (arts. 269–298d) in Sec. "Covert Surveillance Measures" *(geheime Überwachungsmassnahmen)*. Such regulation of the grounds and the procedure for these activities is also typical for criminal procedure laws of the States of the former Yugoslavia. At the same time, for example in Poland, strict separation of "operational intelligence activities" (*czynności operacyjno-rozpoznawcze)* from procedural actions remains in force to the present day.

The transposition of the relevant treaty norms into the national legislation takes various forms. For example, whereas the Act of the Czech Republic "On International Judicial Cooperation in Criminal Matters" of 2013 (§§ 59–65) and the Federal Law of the Republic of Austria "On Extradition and Legal Assistance in Criminal Matters" of 1979, with later amendments (§§ 59b–59c, *besondere Ermittlungsmaßnahmen* ("special investigative measures")) govern the procedure for submitting and performing requests for operational/intelligence actions and classify them as legal assistance (that is, cooperation in the field of criminal proceedings), similar special statutes of Germany and Switzerland, whose criminal procedure codes in this aspect are similar to the Czech and the Austrian ones, do not contain such provisions. At the same time, it can be assumed that in regulating the execution of these incoming requests, the Czech and Austrian competent authorities expect that the requesting party file them through the legal assistance procedure rather than within the framework of law enforcement cooperation.[43] The Ukrainian Criminal Procedure Code regulates controlled deliveries and border pursuit in Ch. "International Legal Assistance in Carrying Out Procedural Actions" (arts. 569 and 570).

There is an example of a CoE country regulating the extraterritorial unilateral use of SITs. The UK Home Office Codes of Practice on Covert Surveillance and Property Interference, Equipment

---

[40] H.G. Nilsson, *op. cit.*, pp. 39–45; P.A. Litvishko, *"The Convergence of Preliminary Investigation and Operational Search Activities in International Cooperation in Criminal Matters"*, in *Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation* (Moscow: Prospekt, 2016), pp. 173–191.

[41] For the concept of "criminal justice finality", see: G. Vermeulen, W. De Bondt, C. Ryckman, *Rethinking international cooperation in criminal matters in the EU. Moving beyond actors, bringing logic back, footed in reality* (Antwerpen-Apeldoorn-Portland: Maklu, 2012), 767 p.

[42] At the same time, the Law of Ukraine "On Operational Search Activities" of 1992 (with further amendments) still regulates operational investigative, intelligence and counterintelligence activities.

[43] For tracing and interception of (tele)communications; agents, informers and infiltration; and cross-border operations, see: the European Judicial Network's practical tool for judicial cooperation "Fiches Belges", URL: https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelges/EN/-1/-1/-1, accessed July 27, 2021.

Interference and Covert Human Intelligence Sources provide for the applicability of authorizations and warrants under the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 to these SITs conducted in overseas areas under the jurisdiction of the UK, such as UK Embassies, UK military bases and detention facilities.[44]

V. Conclusion and Recommendations: Filling the Gaps

The research of the existing frameworks and the considerations set out in the previous sections point to the need for developing the additional regulation of SITs in the CoE instruments of legal assistance in criminal matters as well as to the 1959 Convention being the most appropriate among them to accommodate that.

As the 2001 Protocol is indicative of setting the sovereignty-related thresholds for the feasible cooperation forms in the field of transnational SITs[45] and regrettably, those thresholds seem to be as relevant as they were 20 years ago, back in 2001, when the Second Protocol was adopted, presently it appears advisable to confine the express regulation of SITs to domestic ones.

Since SITs involve either compulsory (coercive) measures (in their broad sense as used in CoE instruments) or deception, decoys and other trickery, most of them are highly intrusive and invade people's privacy, they should be subjected to the restrictive regime of art. 5 of the 1959 Convention, giving the States Parties more latitude in electing or refusing to accede to them.

In view of the above considerations, it is deemed expedient to supplement art. 3 of the 1959 Convention with paragraph 4 expressly stating that *"The provisions of paragraph 1 of this article shall apply to any request for the conduct of covert special investigative techniques that do not have a cross-border character"*, and to amend paragraph 1 of art. 5 of the 1959 Convention so as to read "Any Contracting Party may, by a declaration addressed to the Secretary General of the Council of Europe, when signing this Convention or depositing its instrument of ratification or accession, reserve the right to make the execution of letters rogatory for search or seizure of property, *or for the measures provided for in paragraph 4 of Article 3* dependent on one or more of the following conditions:".

This means, that, firstly, by reference to para. 1 of art. 3, the suggested SITs are only aimed at reactive criminal investigations, prosecutions and judicial proceedings and serve evidentiary purposes, and therefore exclude those employed in secret to prevent, detect or suppress offences, i.e., proactive and disruptive investigations, to say nothing of national security (as opposed to law enforcement) intelligence operations; and, secondly, they do not comprise any individually denominated actions, means or methods.

As art. 3.1 of the 1959 Convention deals with a generic definition of judicial assistance requested and provided solely for evidential purposes, and neither the rest of the Convention nor its Protocols comprise an exhaustive or approximate list of the requested parties' concrete domestic

---

[44] *Covert Surveillance and Property Interference. Revised Code of Practice* (London: Home Office, 2018), p. 12, para. 2.17; *Equipment Interference. Code of Practice* (London: Home Office, 2018), p. 19, para. 3.34; *Covert Human Intelligence Sources. Revised Code of Practice* (London: Home Office, 2018), p. 22, para. 4.9.

[45] Cf.: para. 24 of the Explanatory report to the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Draft Protocol version 2. T-CY(2020)7_PDP_Protocol_v2b (PDP 12 April 2021) states that "[t]he drafters also considered other measures which, after thorough discussion, were not retained in this Protocol. Two of these provisions, namely, "undercover investigations by means of a computer system" and "extension of searches", were of high interest to Parties but were found to require additional work, time and consultations with stakeholders, and were thus not considered feasible within the timeframe set for the preparation of this Protocol. The drafters proposed that these be pursued in a different format and possibly in a separate legal instrument."

Unlike the 1990 Schengen Convention, the 2001 Protocol does not provide for such an intrusive form of cooperation as hot pursuit.

procedural actions, means or methods for rendering that assistance, outlining only those of them that have transnational implications for the requesting parties' proceedings, the requested parties' sovereignty or other essential interests or human rights (safe conduct and other safeguards for the persons concerned etc.), the proposed paragraph 4 should follow this pattern.

These provisions would also help cover particular online covert SITs, which is especially important to countries not party to the Budapest Convention on Cybercrime.

Another solution could be for the Committee of Ministers to issue a dedicated Recommendation to the Member States to this effect by analogy with the 1985 Recommendation.