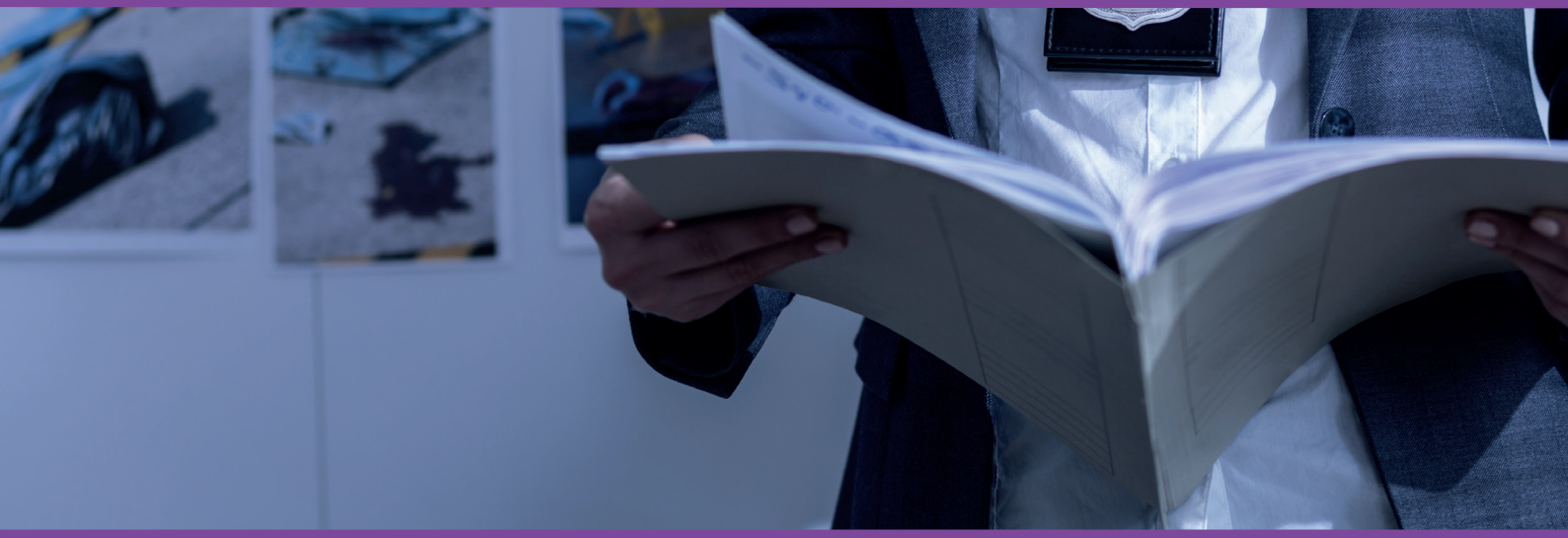
EUROMED JUSTICE

A programme funded by the European Union

EUROMED JUSTICE

Legal and Gaps Analysis
Special Investigation Techniques



CrimEx
EuroMed Justice Group of Experts in Criminal Matters

ALGERIA, EGYPT, ISRAEL, JORDAN, LEBANON, MOROCCO, PALESTINE, TUNISIA

EuroMed Justice Expert: Mr Daniel Suter, UK

Lead Firm /Chef de file

FIIAPP COOPERACIÓN ESPAÑOLA

EIPA

CILC Center for International Legal Cooperation

JCI Justice Coopération Internationale

AUTHOR(S):
This Legal and Gaps Analysis has been written by Mr. David Mayor Fernandez (Spain), in collaboration with: Mr. Dan Suter (Director iJust International - United Kingdom), Mr. Giel Franssen (The Netherlands), and Professor Dr. Mohamed Elewa Badar (Egypt- United Kingdom).

EDITOR AND COORDINATOR:
Virgil Ivan-Cucu, EuroMed Justice Key Expert, Senior Lecturer EIPA Luxembourg.

LINGUISTIC VERSIONS
Original: EN
Manuscript completed in November 2017.

DISCLAIMER

The information contained in this Legal and Gaps Analysis is based on the research and data provided by the senior experts assigned, and the representatives of the Southern Partners Countries in the framework of the work carried out under the EuroMed Justice Project, except for Lebanon. In conformity with Lebanese Law none of the Lebanese judges and representatives contributed to the work in any mean or way. The Consortium implementing this EuroMed Justice project cannot be held responsible for the accuracy, actuality or exhaustiveness of the analysis, nor can it be made liable for any errors or omissions, contained in this document.

This publication has been produced with the assistance of the European Commission. The contents of this publication can in no way be taken to reflect the views of the European Commission.

COPYRIGHT

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged, according to the following model: "EuroMed Justice is an EU project fostering international judicial cooperation in the Euro-Mediterranean area". Furthermore, please inform EuroMed Justice and send a copy at: info@euromed-justice.eu.

www.euromed-justice.eu

Contents

Abbreviations

BC	Budapest Convention on Cybercrime of the Council of Europe
CISA	Convention Implementing the Schengen Agreement
CITO	Arab League Convention on Combating Information Technology Offences
CSPs	Communication Service Providers
EIO	European Investigation Order
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedure
ICT	Information and Communication Technologies
INTERPOL	International Police
MLA	Mutual Legal Assistance
MS	EU Member States
SIT	Special Investigation Technique
SPC	Southern Partner Country
UNCAC	United Nations Convention Against Corruption
UNTOC	United Nations Convention Against Transnational Organized Crime
Vienna Convention	United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988

Introduction

Special Investigation Techniques (SITs) are an essential mechanism to ensure that terrorists and serious organized crime groups are covertly monitored and their communications intercepted. As crime becomes more sophisticated and complex, so SITs are increasingly important investigative tactics. SITs may need to be authorized quickly as opportunities arise to infiltrate criminal enterprises and prevent terrorist attacks. An efficient procedure to react to fast-paced criminality across borders must be balanced with protections against unwarranted breaches of privacy and collateral intrusion.[1] The legal and gap analyses will focus on the harmonization of SPC legislation to ensure SITs can be deployed effectively, with the necessary safe-guards.

1. The risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation - Covert Surveillance: Code of Practice (UK) http://www.gov.scot/Publications/2003/03/16695/19535

Methodology

This paper reviews the differences and similarities of the national legislation of Southern Partner Countries (SPCs) and maps their implementation of relevant treaties and conventions for international cooperation (Legal Analysis). Secondly, recommendations on legal frameworks will be suggested to enable or enhance investigations using SITs (Gap Analysis). This paper is prepared following:

1. Responses to questionnaires on use of SITs in each SPC
2. SPC presentations at the CrimEx session in Masstricht on 8 May 2017
3. Research completed by scientific consultants in the SPCs

Legal Analysis

This paper will analyze the SPC legislation that prescribes the use of SITs, any procedural rules governing the admissibility of evidence and appropriate safeguards. SPC application of the following international conventions will be considered:

1. *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988 ('Vienna Convention');*[2]
2. Budapest Convention on Cybercrime of 23 November 2001 (ETS No. 185);[3]
3. United Nations Convention against Transnational Organized Crime of 15 November 2000 and the Protocols thereto;[4]
4. United Nations Convention against Corruption of 31 October 2003[5]

The following international instruments, standards and good practices provide guidance in this area:

1. United Nations Office on Drugs and Crime, Vienna, 2009 Crime scene and physical awareness for non-forensic personnel (ST/NAR/39).
2. Madrid Guiding Principles on Stemming the Flow of FTFs (2015) (S/2015/939), Guiding Principles 26-27.
3. United Nations Office for Disarmament Affairs information hub on IEDs134
4. INTERPOL, Guidelines concerning transmission of Fingerprint Crime Scene Marks
5. INTERPOL Handbook on DNA Data Exchange and Practice: Recommendations from the INTERPOL DNA Monitoring Expert Group, Second Edition 2009.
6. European Network of Forensic Science Institutes, Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01, November 2015.

2. Algeria ratified 9 May 1995, Egypt ratified 15 March 1991, Israel 20 March 2002, Jordan ratified 16 April 1990, Lebanon acceded 11 March 1996, Morocco ratified 28 October 1992, Tunisia ratified 20 September 1990
3. Israel acceded 9 May 2016 and Morocco invited
4. Algeria ratified 7 October 2002, Egypt ratified 5 March 2004, Israel ratified 27 December 2006, Jordan ratified 22 May 2009, Lebanon ratified 5 October 2005, Morocco ratified 19 September 2002, Palestine acceded 2 January 2015, Tunisia ratified 19 June 2003
5. Algeria ratified 25 August 2004, Egypt ratified 25 February 2005, Israel ratified 4 February 2009, Jordan ratified 24 February 2005 Lebanon acceded 22 April 2009, Morocco ratified 9 May 2007, Tunisia ratified 23 September 2008

7. Organization for Security and Co-operation in Europe, Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers.
8. Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police Officers (United Kingdom), Available from INTERPOL Guidelines concerning Fingerprints Transmission

The *Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions*[6] of the UN Security Council Counter-Terrorism Committee Executive Directorate lists a series of issues for consideration for States regarding SITs:

Enabling legislation:

1. Does the State's legislation allow for the use of special investigative techniques?
2. Is the legislation sufficiently broad to cover the available special investigative techniques?
3. Are the circumstances under which special investigative techniques may be used clearly defined in law?
4. Is there adequate control of their use by judicial authorities or other independent bodies through prior authorization, supervision during the investigation, and ex post facto review?
5. Which is the competent authority for deciding, supervising, or using special investigation techniques?
6. Is there a time limit on the use of special investigative techniques?
7. What are the provisions or systems in place, through a legislative body or otherwise, to review both draft and existing counter-terrorism legislation, including any amendments to ordinary criminal procedures, in order to ensure that they comply with human rights obligations?
8. Do the laws and procedures in place take into account new technologies?
9. Does the national legislation grant a power to enable competent authorities to order or similarly obtain the expeditious preservation of specified digital data?
10. Do national laws include an obligation for Internet Service Providers (ISP) and other ICT firms to retain client data for a specified period?
11. Do national laws explicitly empower the competent authorities to order a person on its territory to submit data under its possession or control?
12. Does the national legislation explicitly include a power to search computer hardware or data?
13. Do national laws explicitly provide for a power to seize computer hardware or data?
14. Does the national legislation explicitly include a power to obtain real-time collection of data?
15. Do national laws explicitly provide for a power to intercept content data?
16. Do national laws explicitly provide that electronic evidence/records are admissible in court proceeding and provide for a process for authentication rules?
17. Do national laws explicitly include a power to obtain subscriber information?
18. Does the law ensure that competent authorities apply less intrusive investigative methods than special investigative techniques, if such methods are adequate for the offence to be detected, prevented or prosecuted?
19. How does the State take into account the need to prevent arbitrary or unlawful interference with privacy?
20. Are there procedural rules governing the production and admissibility of such evidence and safeguarding the rights of the accused to a fair trial?

6. https://www.un.org/sc/ctc/wp-content/uploads/2017/09/Technical-Guide-2017-with-cover.pdf, p. 45.

International cooperation in the field of special investigative techniques

1. Does the State have in place domestic mechanisms to allow for international cooperation in special investigative techniques, including, as appropriate, creation/use of joint investigation mechanisms?
2. Does the State have in place bilateral and multilateral arrangements for international cooperation in special investigative techniques (especially with neighbouring States)?

Gap Analysis

The review of the SPC national legislation will consider the following:

1. Definition of the SIT, its scope, and the legislative basis for its use.
2. Assessment of approaches to the implementation of the SIT. There is typically more than one model that law enforcement authorities use for implementation. Some models have their advantages above others and may make the SIT more effective.
3. Evaluation of the mechanism for judicial or other oversight of the SIT. This is important as excessive or burdensome oversight process may limit effectiveness and oversight remains an essential element for the correct functioning of the SIT.
4. Analysis of the issues and problems that typically limit the effectiveness of the SIT.
5. Recommendations to improve cooperation between the SPCs and EU Member States

Where gaps are identified that inhibit effective and efficient investigations, prosecutions and trial, this paper will make recommendations. These are only suggested recommendations and the SPCs will have to determine the viability based on resources and priorities. For the purposes of this paper the following SITs will be considered:

Surveillance

The use of law enforcement agents to observe the activity of suspects

Interception of Communications

The use of technology to intercept information and communications technology, telecommunications and postal mail

Covert Audio or Visual Devices

The use of listening or video devices to record the activities and conversations of suspects. These devices can be in vehicles, vessels, transitory objects (i.e. shipping containers) or private dwellings

Tracking Devices

The use of technology to monitor where vehicles or packages (i.e. for controlled deliveries) are located and their movements

Controlled Deliveries

Interception of contraband before its intended receipt. Law enforcement may replace contraband with a dummy package or it is allowed to proceed intact to its delivery address. Controlled deliveries are often combined with the use of other SITs to monitor activity (i.e. by tracking or covert devices) and to confirm the recipient/s

Informants

Provision of information from persons with knowledge about criminal enterprises

Undercover Officers

Law enforcement agents acting under the guise of an assumed identity to detect criminality

Context

Definition of SITs

Special investigation techniques have been defined as techniques applied by competent authorities[7] for the purpose of detecting and investigating serious crimes and suspects, aimed at gathering information in such a way as not to alert the target persons.[8]

Article 20 of the United Nations Convention on Transnational Organized Crime (UNTOC) refers to special investigation techniques, including '*electronic or other forms of surveillance and undercover operations*', as well as '*controlled delivery*'. Article 50 of the United Nations Convention Against Corruption (UNCAC) also provides for the use of SITs to combat corruption. Article 11 of the United Nations Convention Against Illicit Traffic and Narcotic Drugs and Psychotropic Substances ('Vienna Convention') also refers to the use of '*controlled delivery*'.

In accordance with Article 20 of UNTOC, each state shall:

1. Establish controlled delivery as a method of inquiry available at the domestic and international levels, if permitted by the basic principles of its domestic legal system;
2. Have the legal capacity to provide international cooperation on a case-by-case basis in respect of controlled deliveries, where it does not conflict with the fundamental principles of its domestic legal system
3. Establish, where appropriate, electronic surveillance and disguised operations as an available means of investigation both domestically and internationally

Arab League Convention Against Transnational Organised Crime

This convention neither defines nor explicity refers to the use of SITs. Albeit, Article 37 states that, States can conduct "*investigations necessary to monitor the movement of proceeds of crime, goods, materials or other instruments used or intended to be used in the commission of these crimes.*"[9]

7. "competent authorities" means judicial, prosecuting and investigating authorities involved in deciding, supervising or using special investigation techniques in accordance with national legislation.
8. 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 (Adopted by the Committee of Ministers on 20 April 2005 at the 924th meeting of the Ministers' Deputies)
9. Jordan ratified 8 January 2013, Palestine ratified 21 May 2013, Tunisia signed 21 December 2010, Algeria signed 21 December 2010, Egypt signed 21 December 2010 and Morocco signed 21 December 2010

EU Legislative Basis

Several main treaties, as well as other initiatives, work to facilitate and foster cross-border cooperation at the EU level. Some of the major frameworks include:

Schengen Agreement

The Schengen Agreement provided for the binding abolition of national borders and effectively assured the free movement of persons and goods among its parties. This, in turn, necessitated the introduction of compensatory measures to ensure and safeguard member state (MS) security. Article 40 of the Convention Implementing the Schengen Agreement (CISA) provides for both pre-planned cross-border surveillance, when activities proceed after authorisation from the host state, and for urgent cross-border surveillance, which may proceed without prior authorisation from the host state.

The Prüm Decision

The Prüm Treaty built upon several bilateral and regional EU best practices to widen the scope of cross-border cooperation and information exchange, particularly in the field of terrorism and organised crime.

The Naples II Convention

This Convention on mutual assistance and cooperation between customs administrations (Naples II) was adopted in 1997 to regulate cross-border cooperation in the prevention, investigation and prosecution of certain infringements of both the national legislation of MS and Community customs regulations. Article 16 of Naples II provides for both planned and spontaneous cross-border surveillance of suspected national and/or community customs infringements and money laundering.

EU Convention on mutual assistance in criminal matters between MS

This Convention creates binding provisions that have a direct impact on exchange of information collected through interception. It mandates that a MS is obliged to respond to an interception request made by another state party to the Convention.

Other Agreements

Bilateral arrangements between neighbouring states often offer the most comprehensive of scopes to cross-border cooperation, including surveillance and are the preferred instrument for conducting cross-border cooperation, including surveillance. Therefore, the value of bilateral and regional frameworks in facilitating cross-border surveillance lies in complementing the already established EU wide standard and in providing best practices.

There exist regional initiatives and formats both outside and within the EU that have developed and fostered specific cross-border cooperation activities. The Task Force of Organized Crime in the Baltic Sea region is perhaps the most prominent example of cross-border integrated maritime surveillance, including among MS, that is outside the immediate EU jurisdiction.

The Task Force Mediterranean is the European response to growing concerns over migrant pressure and the growth of organised criminal networks in the Mediterranean region. The initiative generally provides for enhanced maritime cooperation, including surveillance, in managing migrant flows and combatting transnational crime in the region.

With a few exceptions, surveillance is regulated in the statutes of MS. In some MS, the regulations are part of the Criminal Procedures Codes, in others special legislation governing the use of special investigative tools has been passed. Many MSs have gradually adopted specialised legislation on the use of covert investigation tools to improve control, prevent misuse and assure transparency and accountability. This is in part a result of a generally negative and suspicious public perception of surveillance techniques used by the MS, which has generated sufficient public pressure. That pressure has materialised on the EU level as well in the adoption of Directives aimed to safeguard personal privacy and data. They often work to counter and balance the scope and effect of special investigative means. Most States work with a framework that includes a combination of specialised and non-specialised legislation, in conjunction with binding EU Directives on personal privacy and data protection, and conventions such as CISA, NAPLES II and Prüm.

EIO

The Directive of the European Parliament and the Council regarding the European Investigation Order in criminal matters (EIO) was proposed in April 2010, by: Austria, Bulgaria, Belgium, Estonia, Slovenia, Spain and Sweden. The EIO replaces the existing legal framework applicable to the gathering and transfer of evidence between the MS and allows a competent authority in one MS (the issuing authority) to request specific criminal investigative measures be carried out by an authority in another MS (executing authority).

The EIO contains several significant innovations over existing procedures. The EIO focuses on the investigative measure to be executed, rather than on the type of evidence to be gathered. The EIO has a broad scope – all investigative measures are covered, except those explicitly excluded. In principle, the issuing authority decides on the type of investigative measure to be used. However, flexibility is introduced by allowing, in a limited number of cases, the executing authority to decide to have recourse to an investigative measure other than that provided for in the EIO. Clear time limits are provided for the recognition and, with more flexibility, for the execution of the EIO. The EIO innovates by providing the legal obligation to execute the EIO with the same celerity and priority as for a similar national case. The EIO provides for the use of a form that should be used in all cases. Compared to the European Evidence Warrant and to Mutual Legal Assistance, the EIO provides for rationalization of the grounds for refusal, and the right of the issuing authority to request that one or several of its officials assist in the execution of the measure in the executing State.

LEGAL and GAP ANALYSIS

A legal analysis is provided in this section of current national laws and a gap analysis with recommendations for each SPC. More than one SIT maybe operationally used together. For example the use of surveillance, tracker, undercover agent for a controlled delivery. The legal and gap analyses, however, will consider each SIT separately.

Algeria		
SIT	**National Legislation**	**Comments**
Surveillance	**Code of Criminal Procedure** **Article 16 bis** **Ordinance 05-06 of 23 August 2005 related to the fight against smuggling** **Article 40**	**Legal Analysis** This SIT is available for investigations for the following in Algeria: 1. Drug trafficking 2. Organised cross-border crime 3. Attacks of the automated data system 4. Money laundering 5. Terrorism 6. Offences connected with exchange legislation. The Criminal Code details the offences of category 3 (attacks of the automated data system) in Articles 394bis to 394bis2 (three offences). Ordinance 96-22 of 09-07-1996 as amended and completed by Ordinance 03-01 of 19-02-2003 and Ordinance 10-03 of 26-08-2010 details category 6 (offences connected with exchange legislation) in Articles 1, 1bis, and 2 (one single offence). There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor surveillance There are no provisions confirming if the information collected can be adduced in evidence Cross-border surveillance is not possible. Article 16 of the Code of Criminal Procedure authorizes the public prosecutor to oppose a procedure of surveillance if it is not justified or (s)he considers it to be abusive. Hot-pursuit may be available in relation to a controlled delivery applying Law 05-17 of 23/08/2005 on the fight against smuggling (Article 40) and pursuant to the prevention and fight against corruption (Article 56) **subject to specific agreement** with the country concerned, applying UNTOC and the Vienna Convention Article 16 bis of the Code of Criminal Procedure authorises the establishment of surveillance mechanisms after informing the public prosecutor and without prior authorization.

Algeria		
SIT	**National Legislation**	**Comments**
		Gap Analysis **Recommendations:** Harmonisation of legislation in the SPCs and developing a SPC wide instruments for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 or 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters re cross-border observations (Article 17), The following minimum standards are suggested: 1. To ensure consistently whether the surveillance is not justified or abusive pursuant to Article 16 of the Code of Criminal Procedure, apply the following tests: a. **Necessity:** The public prosecutor or examining magistrate should be satisfied that the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate should be satisfied the surveillance measure is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate should be satisfied the surveillance is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties 2. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the Requesting State has a lower penalty threshold than the Requested State. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance 3. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for surveillance than the requested state. The Requesting State should apply for the maximum period for the requesting state

Algeria		
SIT	**National Legislation**	**Comments**
		4. **Review:** Ensure there is a process to justify the continued use of surveillance and to extend where appropriate 5. **Urgency:** For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 6. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 7. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to begin surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Algeria or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 8. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 9. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Interception of communications (computer)	**Law No. 09-04 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies**	**Legal Analysis** Article 3 allows for real-time collection of content – this would also include the traffic data. There are no safeguards to prevent collateral intrusion or to assess if the use of this SIT is necessary, proportional and reasonable. This measure must be ordered in compliance with the provisions of the Code of Criminal Procedure upon authorization by the public prosecutor or examining magistrate. This authorization must include all the elements allowing the identification of the communications to be intercepted, the offence justifying the resort to this measure, as well as its length (4 months, renewable). This measure cannot undermine professional secrecy. Article 10 of 'Act n°09-04 of 05-08-2009 on the special rules relating to the prevention and the fight against ICT-related offences' compels CSPs to provide support to the authorities responsible for judicial inquiries to collect or record content data in real-time of communications; if not, they may be prosecuted for obstruction of justice or violation of the secrecy of the investigation. Articles 1 and 2 of 'Act n°09-04 of 05-08-2009 on the special rules relating to the prevention and the fight against ICT-related offences' extend this measure to all offences committed or facilitated by computer or electronic communication systems.

Algeria		
SIT	**National Legislation**	**Comments**
	Article 3 In accordance with the rules laid down in the Code of Criminal Procedure and this Law and subject to the legal provisions guaranteeing the secrecy of Correspondence and communications, provision may be made for technical requirements for the protection of public order or for the purposes of investigations or judicial information in progress to **carry out electronic communications surveillance operations, Collection and recording of their content in real time,** as well as searches and seizures in a computer system. **Code of Criminal Procedure** Article 65 bis 5	There is a specific and independent power to collect traffic data real-time as provided by the provisions of presidential decree 15-261 of 08-10-2015 on the composition, organization and functioning of the national body for the prevention and the fight against ICT-related offences (Official journal n°53 of 08-10-2015). **Gap Analysis** **Recommendations:** The following minimum standards are suggested: 1. To ensure consistently whether the interception is justified and to prevent collateral intrusion apply the following tests: a. **Necessity:** The public prosecutor or examining magistrate should be satisfied that the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate should be satisfied the surveillance measure is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate should be satisfied the surveillance is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties
Interception of Communications	**Code of Criminal Procedure** **Articles 65a 5 to 65a 10**	**Legal Analysis** This SIT is available for investigations for the following in Algeria: 1. Drug trafficking 2. Organised cross-border crime 3. Attacks of the automated data system 4. Money laundering 5. Smuggling 6. Terrorism 7. Offences connected with exchange legislation 8. Corruption The Criminal Code details the offences of category 3 (attacks of the automated data system) in Articles 394bis to 394bis2 (three offences). Act 05-17 of 31-12-2015 on the fight against smuggling provide details about the offences of category 5 in Articles 10 to 15 (five offences)

Algeria		
SIT	**National Legislation**	**Comments**
		Ordinance 96-22 of 09-07-1996, as amended and completed by Ordinance 03-01 of 19-02-2003 and Ordinance 10-03 of 26-08-2010, details category 7 (offences connected with exchange legislation) in Articles 1, 1bis, and 2 (one single offence). There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor interception Pursuant to Article 65 bis 10 of the Code of Criminal Procedure, the information collected (correspondence, conversations) must be described or recorded in the official report made by the legal police officer authorized by the examining magistrate. This report is added to the case file. Authorisations are given in writing for a maximum duration of 4 months, which may be renewed depending on the needs of the investigation or the requirements in terms of form and duration applying Article 65 bis of the Code of Criminal Procedure. The Code of Criminal Procedure insists on the exceptional nature of this measure (the needs of the inquiry) and entrusts the public prosecutor or examining magistrate with its monitoring. The measure must be authorized by the public prosecutor or examining magistrate. This authorization must include all the elements allowing the identification of the communications to be intercepted, the offence justifying the resort to this measure, as well as the length of the measure. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested 1. **Necessity:** The public prosecutor or examining magistrate should be satisfied that the proposed interception is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 2. **Reasonable:** The public prosecutor or examining magistrate should be satisfied that interception is the least intrusive technique for the purpose of collecting the targeted information – this includes consideration whether the interception will be of the subject or a specific telephone number 3. **Proportionality:** When invading personal privacy the public prosecutor or examining magistrate should be satisfied the use of interception is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties.

Algeria		
SIT	**National Legislation**	**Comments**
		The right of professional secrecy is preserved in Article 45 of the Code of Criminal Procedure – but unclear if there is any other minimization of any privacy intrusion of innocent parties 4. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize interception. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of interception. 5. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for interception than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 6. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner interception is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 7. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 8. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to intercept domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Algeria or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 9. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 10. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Algeria		
SIT	**National Legislation**	**Comments**
Covert audio or visual devices	**Code of Criminal Procedure** **Articles 65a 5 to 65a 10**	**Legal Analysis** This SIT is available for investigations for the following in Algeria: 1. Drug trafficking 2. Organised cross-border crime 3. Attacks of the automated data system 4. Money laundering 5. Smuggling 6. Terrorism 7. Offences connected with exchange legislation 8. Corruption The Criminal Code details the offences of category 3 (attacks of the automated data system) in Articles 394bis to 394bis2 (three offences). Act 05-17 of 31-12-2015 on the fight against contraband provide details about the offences of category 5 in Articles 10 to 15 (five offences) Ordinance 96-22 of 09-07-1996 as amended and completed by Ordinance 03-01 of 19-02-2003 and Ordinance 10-03 of 26-08-2010 details category 6 (offences connected with exchange legislation) in Articles 1, 1bis, and 2 (one single offence). There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor covert devices Pursuant to Article 65 bis 10 of the Code of Criminal Procedure, the information collected (images, audio and video recording) must be described or recorded in the official report made by the legal police officer authorized by the examining magistrate.This report is added to the case file. The Code of Criminal Procedure insists on the exceptional nature of this measure (the needs of the inquiry) and entrusts the public prosecutor or examining magistrate with its monitoring. The measure must be authorized by the public prosecutor or examining magistrate.This authorization must include all the elements allowing the identification of the communications to be intercepted, the offence justifying the resort to this measure, as well as the length of the measure. Article 65 bis 5 of the Code of Criminal Procedure authorizes –the installation of the device – the entry on any dwelling or similar, including outside of the hours authorized for searches, and without the knowledge and consent of the owners of the property.

Algeria		
SIT	**National Legislation**	**Comments**
		Gap Analysis **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for cross- border deployment of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested 1. **Necessity:** The public prosecutor or examining magistrate should be satisfied the proposed covert device is absolutely necessary for the purposes of the investigation, by demonstrating all other means have either been exhausted or are inapplicable. 2. **Reasonable:** The public prosecutor or examining magistrate should be satisfied the covert device is the least intrusive SIT for the purpose of collecting the targeted information 3. **Proportionality:** When invading personal privacy the public prosecutor or examining magistrate should be satisfied the use of the covert device is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm to third parties 4. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize the use of covert devices. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for deploying covert devices 5. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for covert devices than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 6. **Review:** Ensure there is a consistent process to routinely justify the continued use of covert devices and to extend where appropriate 7. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.

Algeria		
SIT	**National Legislation**	**Comments**
		8. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 9. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Algeria or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 10. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 11. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Tracking devices	**Law 06-01 relative to the fight against corruption** **Article 56**	**Legal Analysis** Law 06-01 relative to the prevention and fight against corruption envisages a provision enabling tracking or electronic surveillance (Article 56). This issue is also governed by the Code of Criminal Procedure in the chapter titled "*interception of correspondences of sounds and image freezing*"[10] No further information is available on the framework for authorization. To this end, the feasibility of such a process is not excluded cross-border, **subject to specific agreement** with the requested state concerned, under the scope of multilateral conventions such as UNTOC, UNCAC and the Vienna Convention. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for authorisation are suggested for the domestic legislation 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly

10. EuroMed Fiche 2014 page 50

Algeria		
SIT	**National Legislation**	**Comments**
		2. **Necessity:** The public prosecutor or examining magistrate should be satisfied that the proposed tracker is necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 3. **Reasonable:** The public prosecutor or examining magistrate should be satisfied that the tracker is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties by the public prosecutor or examining magistrate 5. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor and examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Algeria or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused

Algeria		
SIT	**National Legislation**	**Comments**
		11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Controlled deliveries	**Law 05-06 on the fight against smuggling** **Article 40** **Law 06-01 relative to the fight against corruption** **Article 56**	**Legal Analysis** Algerian anti-smuggling law permits controlled delivery operations, but does not allow the full or partial substitution of smuggled goods – Article 20(4) UNTOC, Article 50 United Nations Convention against Corruption and Article 11 of the Vienna Convention state controlled delivery methods that may be applied at the international level include the interdiction or permitting of goods to proceed intact, or to intercept and replace the goods in whole or in part, leaving the choice of method to the State party concerned. The method applied may depend on the circumstances of the case in question. Therefore, it is possible to have a controlled delivery in accordance with a specific agreement with the countries concerned, applying UNTOC, Vienna Convention, UNCAC or applying the principle of reciprocity. Act 05-17 of 31-12-2015 on the fight against contraband provide details about the offences of category 5 in Articles 10 to 15 (five offences) - but does not expressly include laundered proceeds of crime. There are no standard operating procedures. **Gap Analysis** **Recommendations:** 1. **Other contraband:** For example expressly include controlled deliveries for cash 2. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use a controlled delivery and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Algeria or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused

Algeria		
SIT	**National Legislation**	**Comments**
		3. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 4. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 5. **Substitution:** This should be considered appropriate on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue 6. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 7. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 8. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[11]
Informants	**Code of Criminal Procedure, Article 65 bis 12** **Law 06-01 on the prevention and the fight against corruption**	**Legal Analysis** Algerian law does not allow for infiltration measures to be carried out by informants. Infiltration in accordance with the Code of Criminal Procedure can only be carried out by a legal police agent or officer acting under the responsibility of a legal officer in charge of coordinating the operation Article 65 bis. It is a measure that can only be taken on the written authorisation of the public prosecutor or examining magistrate Algerian law does not yet have a legal framework for the management of informants. It is possible, however, to receive international requests for criminal assistance in order to use the declarations made by informants or receive their declarations and to notify them of specific requests made by the requesting countries, whilst taking preventive measures (such as confidentiality and safety)

11. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412

Algeria		
SIT	**National Legislation**	**Comments**
		Gap Analysis **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency The following minimum standards for legislation are suggested 1. Legislation should consider the following: a. **Necessity:** The public prosecutor or examining magistrate should decide that the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate should decide that the sought-after infiltration is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy the public prosecutor or examining magistrate must decide that the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of infiltration and to extend where appropriate g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or examining magistrate – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.

Algeria		
SIT	**National Legislation**	**Comments**
Undercover Agents	**Code of Criminal Procedure** **Articles 65a 5 to 65a 10**	**Legal Analysis** This SIT is available for investigations for the following in Algeria: 1. Drug trafficking 2. Organised cross-border crime 3. Attacks of the automated data system 4. Money laundering 5. Smuggling 6. Terrorism 7. Offences related to foreign currency legislation 8. Corruption 9. Money laundering The Criminal Code details the offences of category 3 (attacks of the automated data system) in Articles 394 bis to 394 bis 2 (three offences). Act 05-17 of 31-12-2015 on the fight against contraband provide details about the offences of category 5 in Articles 10 to 15 (five offences) Ordinance 96-22 of 09-07-1996 as amended and completed by Ordinance 03-01 of 19-02-2003 and Ordinance 10-03 of 26-08-2010 details category 7 (offences connected with exchange legislation) in Articles 1, 1bis, and 2 (one single offence). These operations are authorised for a renewable period of 4 months. There are no standard operating procedures – this gap could increase the possibility of entrapment Infiltration is a measure that can only be taken by agents of the Algerian State, who must be legal police officers, and only in very special situations (Articles 65 bis 11 to 65 bis 18 of the Code of Criminal Procedure). The law does not allow foreign agents to carry out infiltration on Algerian territory. However, it is possible to allow the presence of foreign agents in Algerian territory under a MLA request entailing an infiltration mission to be carried out by Algerian agents. Article 65 bis 1 of the Code of Criminal Procedure protects the identity of the police officer or agent who conducts the infiltration. Their identity shall not appear at any stage of the procedure. Criminal sanctions are likewise foreseen against the persons who reveal the identity of the police officer or agent. The Code of Criminal Procedure grants a certain immunity to the legal police officers and other people involved in an infiltration operation who commit the offences foreseen in article 65 bis 14 of the Code of Criminal Procedure.

Algeria		
SIT	**National Legislation**	**Comments**
		Gap Analysis **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. **Entrapment:** Ensuring there are SOPs and tasking instructions to reduce the impact of entrapment 3. Disclosure: A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused, unless to do so would prevent the accused having a fair trial 4. **Urgency:** Legislation to allow for emergency authorisation when opportunities for operations suddenly arise. This could be verbal authorization, with retrospective written authorization. 5. **Timeframe:** An appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 6. **International cooperation:** The lack of a common definition of an, '*undercover agent*', and the inclusion of 'citizens' and 'informants' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There may be a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state in appropriate circumstances 7. **Cybercrime:** Consideration should be given to including cybercrime offences in the list of offences to allow for *'remote searches'* or the tasking of an undercover agent online

Egypt		
SIT	**National Legislation**	**Comments**
Surveillance	**No legislation**	**Legal Analysis** This is a preventive measure taken by the police to follow individuals for crimes prepared outside the Egyptian territory or to follow the criminals fleeing from Egypt's borders - implemented under Security Co-operation and Extradition Agreements[12] Cross-border hot pursuit that starts in territorial water of Egypt may continue outside the territorial water. This matter requires coordination with the neighbouring state or with the state through which such pursuit is made, in order to respect the principle of the state sovereignty over its territory. This measure may be executed under the United Nations Convention on the Law of the Sea, without prejudice to the domestic laws of the requested state. [13] There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor surveillance. There are no provisions confirming if the information collected can be adduced in evidence **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 **or** 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters re cross-border observations (Article 17) The following minimum standards for application are suggested: 1. **Necessity**: The public prosecutor or investigating judge should be satisfied the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable.

12. EuroMed Fiche 2014 page 76
13. Ibid

Egypt		
SIT	**National Legislation**	**Comments**
		2. **Reasonable**: The public prosecutor or investigating judge should be satisfied the sought-after surveillance measure is the least intrusive one for the purpose of collecting the targeted information 3. **Proportionality:** When invading personal privacy the measure must be proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties 4. **Threshold:** The public prosecutor or investigative judge should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance 5. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for surveillance than the requested state. The requesting state should apply for the maximum period for the requesting state 6. **Review:** Ensure there is a process to justify the continued use of surveillance and to extend where appropriate 7. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner surveillance is obtained retrospectively without prior consent from the public prosecutor or investigating judge should be satisfied or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 8. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 9. **Spontaneous Information:**[14] Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to begin surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Egypt or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused

14. Ibid p58 reference is made to the Ministry of Justice completing the preparation of the draft law on the free flow of information – it is unknown if this has been promulgated

Egypt		
SIT	**National Legislation**	**Comments**
		10. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 11. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Interception of Communications (computer)	**Criminal Procedure Code** **Articles 95, 206 and 206 bis** **Article 95** The investigating judge may order the seizure of all letters, correspondences, newspapers, publications and packages found at post offices and all telegrams found at telegram offices and may order the surveillance of telecommunications or recording of conversations taking place in a specific place whenever deemed necessary for the revelation of the truth in a crime or misdemeanor punishable by incarceration for no less than a three-month period. In all cases, the acts of seizure, inspection, surveillance or recording shall be on the grounds of a justified warrant, for a period of time no longer than thirty days subject to renewal for another equivalent period or periods of time	**Legal Analysis** The investigative judge/or the public prosecutor (through a judicial decree issued by a judge) can issue an order to record wired and unwired conversations in certain circumstances. The Criminal Procedure Code does not refer to conversations made through the internet or computers and the issue has not been adjudicated upon by the Egyptian Court of Cassation. As Article 19 requires all information requested to be provided, this could include interception. MLA requests are sent to the international cooperation office at the Public Prosecution. If the Attorney General approves the request it is sent to the Department of information and documentation at the Egyptian Ministry of Interior, which proceeds on the interception request through trained police officers. These officers will prepare a report about the outcome, without giving any details about the steps and technicalities of the interception. The police officers who carry out the interception of emails, IP addresses and social networking accounts must do so without infringing the privacy of other individuals (i.e. collateral intrusion). The grounds for each act of interception is written in the Criminal Procedure Code with the required conditions for issuing such a decree from the investigative judge. **Gap Analysis** **Recommendations:** 1. Specific provision should be made to compel CSPs in Egypt to cooperate with real-time collection of content and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 29 of CITO (Egypt has ratified) and section 26 HIPCAR and incorporating language in national legislation 2. There should be a separate and specific power to collect traffic data real-time with safeguards to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The language from section 25 HIPCAR could be considered

Egypt		
SIT	**National Legislation**	**Comments**
	Communications Act 10/2003 **Article 19** All entities and companies working in the telecommunication field shall provide the NTRA (National Telecommunications Regulatory Authority) with whatever requested of reports, statistics or information related to its activities except for matters related to National Security **Article 64** Telecommunication Services Operators, Providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities, and this shall not apply to encryption equipment of radio and television broadcasting. With due consideration to inviolability of citizens private life as protected by law, each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law.	**Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or • authorize a [law enforcement] [police] officer to collect or record that data through application of technical means. 2. A country may decide not to implement section 26. **Article 29 CITO - Interception of Content Information** 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology.

Egypt		
SIT	**National Legislation**	**Comments**
	The provision of the service shall synchronize in time with the availability of required technical potentials. Telecommunication Service Providers and Operators and their marketing agents shall have the right to collect accurate information and data concerning Users from individuals and various entities within the State.	2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.
Interception of Communications	**Criminal Procedure Code** **Articles 95, 206 and 206 bis** **Communications Act 10/2003** **Articles 19 and 64**	**Legal Analysis** Articles 95, 206 and 206 bis allow the investigative judge/or the public prosecutor (through a judicial decree issued by a judge) to issue an order to record wired and unwired conversations in certain circumstances. The process re computer interception for MLA requests also applies for interception of communications Article 95 of the Criminal Procedure Code confirms that a justified warrant for thirty days. There is no definition of a "justified warrant" or the grounds for authorizing. The initial warrant can be for a maximum of thirty days and be renewed for the same period. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for authorization are suggested: 1. **Reasonable**: The legislation must prove the sought-after interception is the least intrusive one for the purpose of collecting the targeted information – this includes consideration whether the interception will be of the subject or a specific telephone number 2. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for interception than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 3. **Review:** Ensure there is a process to justify the continued use of interception

Egypt		
SIT	**National Legislation**	**Comments**
		4. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner interception is obtained retrospectively without prior consent from the public prosecutor or investigating judge or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 5. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 6. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to intercept domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Egypt or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 7. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 8. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Covert audio or visual devices	**Criminal Procedure Code** **Articles 95, 206 and 206 bis** **Communications Act 10/2003** **Articles 19 and 64**	**Legal Analysis** Articles 95, 206 and 206 bis allow the investigative judge/or the public prosecutor (through a judicial decree issued by a judge) to issue an order to record unwired conversations in certain circumstances. The process re computer interception for MLA requests also applies for covert or audio probes. Article 95 of the Criminal Procedure Code confirms that a justified warrant for thirty days. There is no definition of a "*justified warrant*" or the grounds for authorizing. The initial warrant can be for a maximum of thirty days and be renewed for the same period. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for use of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for authorization for domestic legislation are suggested:

Egypt		
SIT	**National Legislation**	**Comments**
		1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly 2. **Reasonable:** The public prosecutor or investigating judge should be satisfied that the covert device is the least intrusive one for the purpose of collecting the targeted information 3. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for covert devices than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 4. **Review:** Ensure there is a process to justify the continued use of covert devices 5. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or investigating judge or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 6. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent a fair trial 7. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 8. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 9. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Egypt		
SIT	**National Legislation**	**Comments**
Tracking devices	**No legislation**	**Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for authorisation are suggested for the domestic legislation: 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly to install the tracker 2. **Necessity:** The legislation must demonstrate that the proposed tracker is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 3. **Reasonable:** The public prosecutor or investigating judge should be satisfied the tracker is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the use of the tracker must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** The public prosecutor or investigative judge should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or investigative judge or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.

Egypt		
SIT	**National Legislation**	**Comments**
		9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Egypt or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Controlled deliveries	**No legislation**	**Legal Analysis** As UNTOC, the Vienna Convention and UNCAC have been ratified by Egypt they can be the basis for any ad hoc arrangement with another state. **Gap Analysis** **Recommendations:** 1. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to determine if a controlled delivery is appropriate if drugs or other contraband are being transmitted in their state – this may lead to them commencing their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 2. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 3. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Egypt		
SIT	**National Legislation**	**Comments**
		4. **Substitution:** This should be considered appropriate in legislation on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue 5. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 6. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 7. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[15]
Informants	**No legislation**	**Legal Analysis** Egyptian law does not allow for infiltration measures to be carried out by informants and does not yet have a legal framework for the management of informants. However, the Court of Cassation case law provides that this measure can only be conducted by a police officer without disclosing his identity to prevent risk of harm **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency The following minimum standards for legislation are suggested: **Legislation should consider the following:** 1. **Necessity**: The public prosecutor or investigative judge should decide that the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 2. **Reasonable**: The public prosecutor or investigative judge should decide that the sought-after infiltration is the least intrusive one for the purpose of collecting the targeted information

15. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412

Egypt		
SIT	**National Legislation**	**Comments**
		3. **Proportionality:** When invading personal privacy the public prosecutor or investigative judge must decide that the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties 4. **Threshold:** The public prosecutor or investigative judge should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant 5. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 6. **Review:** Ensure there is a process to justify the continued use of infiltration and to extend where appropriate 7. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or investigative judge – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or investigative judge or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.
Undercover Agents	**No equivalent**	**Legal Analysis** The law does not allow for the use of domestic or foreign agents to carry out infiltration on Egypt. Although the court of cassation case law accepted in several cases. Article 19 of the Communications Act 10/2003 allows for all types of assistance to be provided by communication service providers or operators – this could include an undercover agent. **Gap Analysis** **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. **Entrapment:** Ensuring there are SOPs and specific instructions for a case (or tasking instructions) will reduce the impact of entrapment

Egypt		
SIT	**National Legislation**	**Comments**
		3. **Legislation should consider the following:** a. **Necessity**: The public prosecutor or investigative judge should be satisfied that the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. **Reasonable**: The public prosecutor or investigative judge should be satisfied that the infiltration is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or investigating judge should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an undercover officer. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an undercover officer. e. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial f. **Witness anonymity:** When an undercover agent is required to give evidence it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise.

Egypt		
SIT	**National Legislation**	**Comments**
		g. **Immunity:** Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents 'are allowed to acquire, possess, transport, dispense or deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and *telecommunications*.'[16] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations h. **Urgency:** Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization by the public prosecutor or investigating judge i. **Time limit:** Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected j. **International cooperation:** The lack of a common definition of an, 'undercover agent', and the inclusion of 'citizens' and 'informants' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There may be a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state k. **Cybercrime:** Consideration should be given to a specific provision (rather than the all-encompassing Article 19 of the Communications Act 10/2003) allowing an undercover agent online.

16. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Israel possesses legislation and procedures that allow a broad scope of special investigative techniques which are designed to maximize law enforcement efficiency while still protecting all legitimate individual rights as enshrined in Israel's Basic Laws. At present the security situations prevailing on Israel's land borders render any more specific legislative framework for cross-border law enforcement and cooperation unfortunately impractical. Israel, however, does have the ability to cooperate and does cooperate in specific cases.

Israel		
SIT	**National Legislation**	**Comments**
Surveillance	**Basic Law: Human Dignity and Liberty** **Article 7:** (a) All persons have the right to privacy and to intimacy. (b) There shall be no entry into the private premises of a person who has not consented thereto. (c) No search shall be conducted on the private premises of a person, nor in the body or personal effects. (d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.	**Legal Analysis**[17] Observation, surveillance in the public domain with or without technical means, is permitted by the Police if conducted (1) in compliance with *'the general principles/values of the State*'; (2) has a worthy objective; (3) is not excessive (proportionality test) Article 8 of the Basic Law. The International Legal Assistance Law 5758-1998 applies to MLA as outlined below for interception **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 **or** 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters re cross-border observations (Article 17), The following minimum standards for application are suggested 1. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 2. **Review:** Ensure there is a process to justify the continued use of surveillance and to extend where appropriate 3. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner surveillance is obtained retrospectively without prior consent from the authorisation body or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.

17. EuroMed Fiche 2014 pages 86

Israel		
SIT	**National Legislation**	**Comments**
		4. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 5. **Spontaneous Information:**[18] Consider the application of Article 18(4) UNTOC and section 32 of the Legal Assistance Between Countries Law -5758 -1998 to allow for information to be shared with another state to allow them to begin surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Israel or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 6. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 7. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Interception of Communications	**Wiretapping Law 1979** **(telephone)** **Criminal Procedure (Arrest and Search) Ordinance, 1969.** **(mail)**	**Legal Analysis**[19] The Wiretapping Law, 1979 permits monitoring, recording or copying of conversations of others without the consent of any of the participants. The Wiretapping Law 1979 was amended in 1995 to allow the balancing of interests and rights, with the right to privacy through judicially authorized wiretapping. The 1981 Law Protecting Privacy defines lawful and unlawful limitations to privacy. that include: reasonable limitation of privacy by a security authority in completion of its duties (i.e. police investigations). The right to privacy will have priority and unlawfully obtained evidence will not be admitted into evidence; unless in exceptional cases for maintaining the rule of law.[20] A conversation is defined in the law as speech, telephone, mobile phone, radio waves, fax, telex and teleprinter. The measure may be used when necessary for the discovery, investigation, or prevention of an offence in the category of felony (offences punishable by at least 3 years of imprisonment), or for the discovery or capture of criminals who have committed such offences, or in an investigation for purposes of confiscating property connected to these offences.

18. Ibid p58 reference is made to the Ministry of Justice completing the preparation of the draft law on the free flow of information – it is unknown if this has been promulgated
19. EuroMed Fiche 2014 pages 82-84
20. HCJ 3815/90 Gilat v. Minister of Police and Others; 3816 Yefet and Others v. Minister of Police and others

Israel		
SIT	**National Legislation**	**Comments**
		The President of the District Court or his authorized deputy is the body authorized to permit interception of telecommunications by a warrant. An application for a warrant shall be filed by a police officer with a rank of commander (Nitzav Mishneh) and above. The application shall be filed using a standard form, and shall specify, inter alia, the factual foundation upon which the application is based, the reasons for the application, and the details of the action requested and the application shall be heard ex parte. The permit in the warrant shall be given after the competent body has considered the severity of the infringement of privacy, and the measure is necessary for the discovery, investigation, and prevention of an offence in the category of felony (offences punishable by at least 3 years of imprisonment), or for the discovery or capture of criminals who have committed such crimes, or in an investigation for purposes of confiscating property connected to such offences. The permit shall specify the identity of the person, the identity of the line or the installation, place or type of conversations and the methods of wiretapping. The duration of the permit shall be for a period of up to three months, and it may be extended from time to time. Once a month, the Police Commissioner will report on the permits issued. The Police Commissioner is authorised to issue an urgent permit for 48 hours when there is no time to obtain a permit and it is necessary for the prevention of a felony and the discovery of its perpetrator. The Commissioner shall report to the Attorney General immediately upon issuing the permit and the latter has the authority to revoke it. The Criminal Procedure (Arrest and Search) Ordinance, 1969 permits the seizing of objects, including postal items, when it is necessary in order to ensure the presentation of the object for purposes of investigation, trial or other proceeding. The police may apply to the court to issue a search warrant. The application shall include, inter alia, the details of the offence in respect of which the search warrant is requested, the details of object requested and the place where the search is to be conducted. The warrant is issued ex parte, specifying the place where the search will be conducted, the details of the object looked for and its effective date. By law, MLA requests may be received by the Directorate of Courts, the Director of the Department of International Affairs of the State Attorney's Office or the Inspector General of the Israel Police or the Head of the Intelligence Division. In practice, requests are sent to the Directorate of Courts and then forwarded by them to the Legal Assistance Unit of the Israel Police who oversees the execution of the requests by the competent authorities. In certain cases, the Legal Assistance Unit will consult with the Department of International Affairs regarding the execution of a

Israel		
SIT	**National Legislation**	**Comments**
		The President of the District Court or his authorized deputy is trequest. While decisions regarding the execution of MLA requests may be made by the Department for International Affairs of the State Attorney's Office and by the Legal Assistance Unit, only the Minister of Justice is authorized to deny a MLA request. A MLA request must specify the type of proceeding for which the assistance is requested, the facts that constitute the foundation for the suspicion of the commission of an offence, and the connection to the assistance requested. In a request for assistance of this kind, consideration shall be had, inter alia, to whether it complies with the requirements of Israeli law for issuing a warrant for wiretapping, as stipulated above The Police execute the measures requested within the framework of the request. There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor interception. **Gap Analysis** **Recommendations:** 1. Harmonization of legislation in the SPCs and developing a SPC wide instrument for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations. 2. **Disclosure**: A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 3. **SOPs**: SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 4. **Spontaneous Information**: Consider the application of Article 18(4) UNTOC and section 32 of the Legal Assistance Between Countries Law -5758 -1998 to allow for information to be shared with another state to allow them to use interception domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused

Israel		
SIT	**National Legislation**	**Comments**
Interception of communications (computer)	**Wiretapping Law 1979**	**Legal Analysis**[21] The Wiretapping Law, 1979 permits monitoring, recording or copying of conversations of others without the consent of any of the participants – subject to protection of privacy (see above re interception). A Conversation is defined in the law as speech, telephone, mobile phone, radio waves, fax, telex, teleprinter, **and communication between computers.** The measure may be used when necessary for the discovery, investigation, or prevention of an offence in the category of felony (offences punishable by at least 3 years of imprisonment), or for the discovery or capture of criminals who have committed such offences, or in an investigation for purposes of confiscating property connected to these offences. The International Legal Assistance Law 5758-1998, applies to MLA as outlined above for interception of telecommincations. **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Israel to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 21 BC and section 26 HIPCAR and incorporating language in national legislation. Further, there should be legal provision to collect real-time traffic data. Article 20 BC and section 25 HIPCAR are applicable precedents: **Article 20 BC -** **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

21. EuroMed Fiche 2014 pages 82-84

Israel		
SIT	**National Legislation**	**Comments**
		2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. 3. A country may decide not to implement section 25.
Covert audio or visual devices	**Wiretapping Law 1979**	**Legal Analysis**[22] The Wiretapping Law, 1979 permits monitoring a conversation, its recording or copying by way of an appliance without the consent of any of the participants, when it is necessary for the discovery, investigation, or the prevention of an offence in the category of felony (offences punishable by at least 3 years of imprisonment), or for the discovery or capture of criminals who have committed such crimes, or in an investigation for purposes of confiscating property connected to such offences. The body authorized to permit monitoring as stated, is also permitted to allow intrusion into a private place to install the means necessary for that purpose.

22. EuroMed Fiche 2014 page 84

Israel		
SIT	**National Legislation**	**Comments**
		The International Legal Assistance Law 5758-1998 applies to MLA as outlined above for interception. **Gap Analysis** **Recommendations:** 1. Harmonization of legislation in the SPCs and developing a SPC wide instruments for use of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 2. **Disclosure**: A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 3. **Spontaneous Information**: Consider the application of Article 18(4) UNTOC and section 32 of the Legal Assistance Between Countries Law -5758 -1998 to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 4. **SOPs**: SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Tracking devices	**No legislation**	**Legal Analysis** While there is no specific legislation to allow tracking devices, the legislation in Israel is designed to prevent violations of individual privacy, so that actions taken by law enforcement authorities, including the police, in pursuit of legitimate and lawful enforcement of the law, are excepted from such prohibitions. Therefore, use of special investigative techniques (such as tracking devices) by law enforcement are permitted in appropriate circumstances **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations.

Israel		
SIT	**National Legislation**	**Comments**
		The following minimum standards for application are suggested for the domestic legislation if conducted in a reasonable manner taking into account Articles 7 and 8 of the Basic Law: Human Dignity and Liberty: 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly 2. **Necessity**: The legislation must demonstrate the proposed tracker is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable**: Whosoever authorizes must be satisfied the tracker is the least intrusive method to collect the targeted information 4. **Proportionality:** When invading personal privacy the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** Whosoever authorises should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** *Ensure there is a process to justify the continued use of a tracker and to extend where appropriate* 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the authorisation body or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial

Israel		
SIT	**National Legislation**	**Comments**
		10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC and section 32 of the International Legal Assistance Law 5758-1998 to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Israel or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Controlled deliveries	**No legislation**	**Legal Analysis** As UNTOC, the Vienna Convention and UNCAC have been ratified by Israel they can be the basis for any ad hoc arrangement with another state. **Gap Analysis** **Recommendations:** 1. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC and section 32 of the International Legal Assistance Law 5758-1998 to allow for information to be shared with another state to allow them to determine if a controlled delivery is appropriate if drugs or other contraband are being transmitted in their state – this may lead to them commencing their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 2. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 3. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Israel		
SIT	**National Legislation**	**Comments**
		4. **Substitution:** This should be considered appropriate on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue 5. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 6. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 7. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[23]
Informants	**No legislation**	**Legal Analysis[24]** An "*Informer*" may be activated on a long term or one-time basis, and a privilege is imposed on his identity. Despite the above, in accordance with the Evidence Ordinance, 1971, the court, at the request of the defendant, may order the disclosure of the identity of the informer if it is crucial to the defence of the defendant. In that situation, the prosecution has the choice of either revealing the identity of the informer or withdrawing the indictment. It is unknown if there are SOPs or management of informers. The International Legal Assistance Law 5758-1998 applies to MLA as outlined above for interception. **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency

23. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412
24. EuroMed Fiche page 89

Israel		
SIT	**National Legislation**	**Comments**
Undercover Agents	**No legislation**	**Legal Analysis**[25] An agent may be a policeman or a citizen (who may also be a criminal who is prepared to cooperate with the police). A Police-agent is an agent who is secretly activated in order to gather information, and once completing this activity, continues to serve as a policeman. A Source, or a citizen agent, is a criminal, intelligence source or other person secretly activated by the Police in the gathering of evidence. His activation is managed within the framework of a "*Activation Agreement*" The activation of an agent is dependent upon the fact there is a basis for the suspicion that the target against whom the agent is activated is involved in the commission of criminal offences, generally in the category of felony (offences punishable by at least 3 years of imprisonment). The International Legal Assistance Law 5758-1998, applies to MLA as outlined above for interception. The Police execute the measures in a MLA request and the investigating unit escorts the activities of the agent by way of "*activators*" (policemen trained for that purpose), and reports on his activities to the District Attorney's Office. The agent is obligated to give a report to his activators concerning every act that he does. This includes agents of the requesting state who are appropriately authorized under Israeli law. It is unknown if there are SOPs for activation of undercover agents. **Gap Analysis** **Recommendations:** 1. A region wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. **Entrapment:** Ensuring there are SOPs and specific instructions for a case (or tasking instructions) will reduce the impact of entrapment 3. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial

25. EuroMed Fiche 2014 pages 87-88

Israel		
SIT	**National Legislation**	**Comments**
		4. **Witness anonymity:** When an undercover agent is required to give evidence it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise. 5. **Immunity:** Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents '*are allowed to acquire, possess, transport, dispense or deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and telecommunications*.'[26] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations 6. **Urgency:** Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization. 7. **Timeframe:** Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 8. **Cybercrime**: Consideration should be given to allowing an undercover agent online

26. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Jordan		
SIT	**National Legislation**	**Comments**
Surveillance	**No legislation**	**Legal Analysis** There are no provisions allowing for the use of surveillance. There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor surveillance There are no provisions allowing hot-pursuit and cross-border surveillance. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 or 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters refers to cross-border observations Article 17) The following minimum standards for application are suggested 1. **Legislation should consider the following:** a. **Necessity:** Any authorization by the competent court or public prosecutor must demonstrate that the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. **Reasonable:** The competent court or public prosecutor should be satisfied that the surveillance measure is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The competent court or public prosecutor should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance

Jordan		
SIT	**National Legislation**	**Comments**
		e. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for surveillance than the requested state. The requesting state should apply for the maximum period for the requesting state f. Review: Ensure there is a process to justify the continued use of surveillance and to extend where appropriate g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner surveillance is obtained retrospectively without prior consent from the public prosecutor or competent court or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 2. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 3. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to conduct surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 4. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 5. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Interception of Communications	**Jordanian Constitution Article 18**	**Legal Analysis**[27] The national law refers to the privacy of communications (Jordanian Constitution Article 18 and Communications Act Article 56) prohibitions to prevent breaches of privacy (Communications Act Article 65 and Article 71). Article 88 of the Criminal Procedure Code allows for the monitoring of telecommunications and interception of mail – but does not determine the process or standards to intercept communications. This raises the following questions:

27. EuroMed Fiche 2014 pages 120-123

Jordan		
SIT	**National Legislation**	**Comments**
	All postal and telegraphic correspondence as well as telephone calls and other means of communication shall be considered confidential not subject to control, check, arrest or confiscation except by judicial order in accordance with the provisions of the Jordanian Constitution. **Communications Act, as amended, No. 13 of 1995** **Article 56** The phone calls and private communication are considered confidential that may not violate the subject to legal liability. **Article 65** A. The commission shall have the right to track down the source of any radio waves to verify the license of that source without considering it as a breach of the confidentiality of messages or violation of the provisions of the applicable laws. B. Dissemination or rumour that the content of messages that have been captured in during the tracing of the source of the letter under paragraph A of this Article, the employee who publishes or rumour that the content of those messages shall be punished as prescribed by the law.	1. Is there a legal test that considers the following: a. Proportionality between the effects of an SIT – namely an evaluation in the light of the seriousness of the offence and taking account of the intrusive nature of interception? b. Consideration of less intrusive SITs before ordering interception? c. Consideration of collateral intrusion? 2. Are there any safeguards on the use of interception as evidence – for example privileged material is inadmissible? 3. Are there appropriate measures to ensure that the technology required for interception of communications, meets minimum requirements of confidentiality, integrity and availability? 4. Is there any procedure for protecting sensitive techniques, methodology and sources? 5. Is it interception of a subject or a telephone number? **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for domestic legislation are suggested 1. **Necessity:** The legislation must demonstrate the proposed interception is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 2. **Reasonable:** The legislation must prove that the interception is the least intrusive SIT for the purpose of collecting of the targeted information – this includes consideration whether the interception will be of the subject or a specific telephone number 3. **Proportionality:** When invading personal privacy, the interception must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 4. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize interception. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of interception.

Jordan		
SIT	**National Legislation**	**Comments**
	Article 71 Whoever posted or disseminated the content of any communication by a public or a private telecommunications network or a telephone message seen by virtue of his job or was recorded without legal basis, shall be punished by imprisonment for not less than one month nor more than one year or a fine of not less than 100 dinars and not more than 300 dinars, or both penalties. **Code of Criminal Procedure:** **Article 88** The prosecutor may control at all post offices correspondence, letters, newspapers, publications, parcels and at all telegraphic offices the telegraphic letters, and may also monitor the telephone conversations when it had use to show the fact.	5. **Timeframe:** A practical issue for international co-operation is what happens when a requesting state has a longer timeframe for interception than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 6. **Renewal:** A standard procedure for renewal to justify the continued use of interception. 7. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner interception is obtained retrospectively without prior consent from the public prosecutor or competent court or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 8. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 9. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to intercept domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 10. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 11. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Interception of communications (computer)	**Cybercrime Law No.27 of 2015** **Article 13**	**Legal Analysis** This Article allows the Judicial Police to intercept communications with permission from the Attorney General **Gap Analysis** Recommendations: Provision should be made to compel CSPs in Jordan to cooperate with real-time collection of content for all crimes; and safeguards should be incorporated to ensure that interception and the collection is legal, necessary, reasonable and proportionate in the circumstances.

Jordan		
SIT	**National Legislation**	**Comments**
	A. Taking into account the terms and conditions prescribed in the legislation in force and taking into account the personal rights of the defendant, Judicial Police employees may, after obtaining permission from the Attorney General concerned or of the competent court, access anywhere with indications of being used to commit any of the offences set forth in this law, also they may inspect the equipment, tools, programs, regulations and the means by which the evidence suggest that they are used to commit any of those crimes, and in all cases, the employee who inspected shall draw up the minutes of this and submit it to the competent prosecutor. B. Subject to paragraph (a) of this Article, taking into account the rights of others bona fide, excluding those licensed under the provisions of the Telecommunications Law, who did not participate in any offence under this Act, Judicial Police employees may control the devices, tools, programs, systems and the means used to commit any of the crimes stipulated or covered by this law and the money earned from them and reserve the information and data relating to commit any of them.	Consideration should be given to reviewing Article 29 of CITO, Article 21 BC and section 26 HIPCAR and incorporating language in national legislation **Article 21 BC** **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. i to collect or record through the application of technical means on the territory of that Party, or ii. ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or • authorize a [law enforcement] [police] officer to collect or record that data through application of technical means.

Jordan		
SIT	**National Legislation**	**Comments**
	C. The competent court may rule to confiscate the equipment and tools, stop or disrupt the work of any information system or website used to commit any of the offences set forth or covered by this law, confiscate the money earned from these crimes, and decide to remove the violation at the expense of the perpetrator.	2. A country may decide not to implement section 26. **Article 29 CITO - Interception of Content Information** 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.
Covert audio or visual devices	**No legislation**	**Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for use of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for legislation are suggested 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly to install a covert device 2. **Necessity:** The legislation must establish the proposed covert device is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** Any authorization pursuant to the legislation must prove the covert device is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy. the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties

Jordan		
SIT	**National Legislation**	**Comments**
		5. **Threshold:** The public prosecutor or competent court should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize the use of covert devices. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for deploying covert devices 6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for covert devices than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of covert devices and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or competent court or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Jordan		
SIT	**National Legislation**	**Comments**
Tracking devices	**No legislation**	**Legal Analysis** The Jordan questionnaire confirms that tracking devices can be used – no legal basis for this has been provided **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested for the domestic legislation 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly to install a tracker 2. **Necessity:** The legislation must demonstrate the proposed tracker is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** The public prosecutor or competent court is satisfied the tracker is the least intrusive measure for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** The public prosecutor or competent court should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the authorisation body or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.

Jordan		
SIT	**National Legislation**	**Comments**
		9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Jordan or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Controlled deliveries		**Legal Analysis**[28] A controlled delivery may happen when a neighbouring state is aware that there is smuggling or drug supply. Jordan, with its security organs, whether the police or Al-Badiah or the Customs Department, shall prosecute that person and try him on a charge pursuant to the Code of Criminal Procedure, the Customs Act, the Narcotics and Psychotropic Substances Act, as amended, No. 11 of 1988. As UNTOC, the Vienna Convention and UNCAC have been ratified by Jordan they can be the basis for any ad hoc arrangement with another state where there is no bilateral treaty. **Gap Analysis** **Recommendations:** 1. Spontaneous Information: Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to determine if a controlled delivery is appropriate if drugs or other contraband are being transmitted in their state – this may lead to them commencing their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused

28. EuroMed Fiche page 156

Jordan		
SIT	**National Legislation**	**Comments**
		2. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 3. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 4. **Substitution:** This should be considered appropriate in legislation on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue 5. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 6. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 7. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[29]
Informants	**No legislation**	**Legal Analysis** Jordanian law does not allow for infiltration measures to be carried out by informants. Or provide a legal framework for the management of informants. **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency. The following minimum standards for legislation are suggested 1. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or competent court should decide that the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable.

29. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412

Jordan		
SIT	**National Legislation**	**Comments**
		b. **Reasonable:** The public prosecutor or competent court should decide the infiltration is the least intrusive SIT for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or competent court must decide that the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or competent court should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of infiltration and to extend where appropriate g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or competent court – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or competent court or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.
Undercover Agents	**No legislation**	**Legal Analysis** The law does not allow for the use of domestic or foreign agents to carry out infiltration in Jordan **Gap Analysis** **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents –e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. Entrapment: Ensuring there are SOPs and specific instructions for a case (or tasking instructions) will reduce the impact of entrapment

Jordan		
SIT	**National Legislation**	**Comments**
		3. **Legislation should consider the following:** a. **Necessity:** The applicant must demonstrate the proposed infiltration is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or competent court should be satisfied that the infiltration is the least intrusive measure for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or competent court should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an undercover officer. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an undercover officer. e. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial f. **Witness anonymity:** When an undercover agent is required to give evidence, it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise.

Jordan		
SIT	**National Legislation**	**Comments**
		g. **Immunity:** Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents '*are allowed to acquire, possess, transport, dispense or deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and telecommunications.*'[30] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations h. **Urgency:** Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization. i. **Timeframe:** Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 4. **International cooperation:** The lack of a common definition of an, 'undercover agent', and the inclusion of '*citizens*' and '*informants*' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There maybe a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state 5. **Cybercrime:** Procedure for an undercover agent online

30. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Lebanon		
SIT	**National Legislation**	**Comments**
Surveillance	**No legislation**	**Legal Analysis** There are no provisions allowing for the use of surveillance. The Criminal Procedure Law will allow the General Prosecutor of the Court of Cassation (or in cases of urgency a Public Prosecutor) to allow this SIT on an ad hoc basis. There is no proscribed procedure but the following basic information is required for a LOR to be executed on the basis of reciprocity: Name of subject of surveillance; length of use of surveillance and case summary confirming why surveillance is necessary There are no provisions allowing hot-pursuit and cross-border surveillance. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 or 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters refers to cross-border observations Article 17) The following minimum standards for application are suggested 1. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or examining magistrate is satisfied the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate is satisfied the surveillance measure is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties

Lebanon		
SIT	**National Legislation**	**Comments**
		d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of surveillance and to extend where appropriate g. **Urgency:** For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 2. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 3. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to conduct surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 4. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 5. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Lebanon		
SIT	**National Legislation**	**Comments**
Interception of Communications	**Law 140/99, amended by the Law 158/99.** **Articles 2, 3 and 9**	**Legal Analysis**[31] Law 140/99, as amended by Law 158/99 allows for interception, listening, and surveilling of communication, of all means of communication (telephones, mobiles, fax, e-mails) Interception can only take place after a judicial or an administrative decision has been taken as prescribed by Articles 2 and 3 of Law 140/99 for a maximum period of two months, which is renewable. Article 2 allows for interception in very urgent cases, for offences that are sanctioned for a duration of imprisonment not less than a year. Article 9 allows the Minister of Defence and the Minister of Interior to order interception, after the approval of the Prime Minister to collect information for terrorist and organized crime offences. This raises the following questions: 1. Is there a legal test that considers the following: a. Proportionality between the effects of an SIT – namely an evaluation in the light of the seriousness of the offence and taking account of the intrusive nature of interception? b. Consideration of less intrusive SITs before ordering interception? c. Consideration of collateral intrusion? 2. Are there any safeguards on the use of interception as evidence – for example privileged material is inadmissible? 3. Are there appropriate measures to ensure that the technology required for interception of communications, meets minimum requirements of confidentiality, integrity and availability? 4. Is there any procedure for protecting sensitive techniques, methodology and sources? 5. Is it interception of a subject or a telephone number, email etc? **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations.

31. EuroMed Fiche 2014 page 160

Lebanon		
SIT	**National Legislation**	**Comments**
		The following minimum standards for domestic legislation are suggested 1. **Necessity:** The legislation must demonstrate the proposed interception is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 2. **Reasonable:** The legislation must prove interception is the least intrusive approach for the purpose of collecting the targeted information – this includes consideration whether the interception will be of the subject or a specific telephone number 3. **Proportionality:** When invading personal privacy, the interception must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 4. **Timeframe:** A practical issue for international co-operation is what happens when a requesting state has a longer timeframe for interception than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 5. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 6. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to intercept domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 7. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 8. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Lebanon		
SIT	**National Legislation**	**Comments**
Interception of communications (computer)	**Law 140/99, amended by the Law 158/99.** **Articles 2, 3 and 9**	**Legal Analysis** Law 140/99, as amended by Law 158/99. allows for interception, listening, and surveilling of communication, of all means of communication including e-mails – it is unclear if this includes the interception of messaging apps **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Lebanon to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 21 BC and section 26 HIPCAR and incorporating language in national legislation. Further there should be legal provision to collect real-time traffic data. Article 20 BC and section 25 HIPCAR are applicable precedents: **Article 20 BC -** **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. i to collect or record through the application of technical means on the territory of that Party; or ii. ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Lebanon		
SIT	**National Legislation**	**Comments**
		Section 25 HIPCAR - Collection of Traffic Data 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. 3. A country may decide not to implement section 25.
Covert audio or visual devices	**No legislation**	**Legal Analysis** The Criminal Procedure Law will allow the General Prosecutor of the Court of Cassation (or in cases of urgency a Public Prosecutor) to allow use of covert devices on an ad hoc basis. There is no proscribed procedure but the following basic information is required for a LOR to be executed on the basis of reciprocity: Name of subject of covert devices; length of use of covert device and case summary confirming why covert device is necessary **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for use of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for legislation are suggested 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a covert device 2. **Necessity:** The legislation must establish the proposed covert device is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** A public prosecutor or examining magistrate should be satisfied that the covert device is the least intrusive one for the purpose of collecting the targeted information

Lebanon		
SIT	**National Legislation**	**Comments**
		4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize the use of covert devices. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for deploying covert devices 6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for covert devices than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of covert devices and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Lebanon		
SIT	**National Legislation**	**Comments**
Tracking devices	**No legislation**	**Legal Analysis** The Criminal Procedure Law will allow the General Prosecutor of the Court of Cassation (or in cases of urgency a Public Prosecutor) to allow tracking devices on an ad hoc basis. There is no proscribed procedure but the following basic information is required for a LOR to be executed on the basis of reciprocity: Name of subject of tracking device; length of use of tracking device and case summary confirming why tracking device is necessary **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested for the domestic legislation 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a tracker 2. **Necessity:** A public prosecutor or examining magistrate should be satisfied the proposed tracker is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** A public prosecutor or examining magistrate should be satisfied that the tracker is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** Another practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes

Lebanon		
SIT	**National Legislation**	**Comments**
		7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Jordan or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Controlled deliveries	**Law No. 673/1998** **Article 73**	**Legal Analysis**[32] Law No. 673/1998 on narcotics introduced a procedure for controlled circulation in article 2, 73,[33] and 220[34] - these provisions do not include any other contraband such as money or allow for substitution. Lebanon has acceded to the Vienna Convention and UNCAC and ratified UNTOC and can be the basis for any ad hoc arrangement with another state.

32. EuroMed Fiche 2014 page 156
33. EuroMed Fiche 2014 page 183
34. EuroMed Fiche 2014 page 184

Lebanon		
SIT	**National Legislation**	**Comments**
		Gap Analysis **Recommendations:** 1. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to determine if a controlled delivery is appropriate if drugs or other contraband are being transmitted in their state – this may lead to them commencing their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 2. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 3. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 4. Substitution: This should be considered appropriate in legislation on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue 5. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 6. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 7. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[35]
Informants	**No legislation**	**Legal Analysis** Lebanese law does not allow for infiltration measures to be carried out by informants. Or provide a legal framework for the management of informants. Although the police may use informants.[36]

35. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412
36. EuroMed Fiche 2014 page 163

Lebanon		
SIT	**National Legislation**	**Comments**
		The Criminal Procedure Law will allow the General Prosecutor of the Court of Cassation (or in cases of urgency a Public Prosecutor) to allow informants on an ad hoc basis. There is no proscribed procedure but the following basic information is required for a LOR to be executed on the basis of reciprocity: Name of informant; period of time for informant to be managed and case summary confirming why an informant is necessary **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency The following minimum standards for legislation are suggested 1. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or examining magistrate should decide the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate should decide that infiltration is the least intrusive method for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate must decide that the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of infiltration and to extend where appropriate

Lebanon		
SIT	**National Legislation**	**Comments**
		g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or examining magistrate – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission.
Undercover Agents	**No legislation**	**Legal Analysis** The law does not allow for the use of domestic or foreign agents to carry out infiltration in Lebanon. The Criminal Procedure Law will allow the General Prosecutor of the Court of Cassation (or in cases of urgency a Public Prosecutor) to allow deployment of undercover agents on an ad hoc basis. There is no proscribed procedure but the following basic information is required for a LOR to be executed on the basis of reciprocity: Name of subject of covert operation; length of use of undercover agent and case summary confirming why an undercover agent is necessary **Gap Analysis** **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. Entrapment: Ensuring there are SOPs and specific instructions for a case (or tasking instructions) to reduce entrapment 3. **Legislation should consider the following:** a. Necessity: The public prosecutor or examining magistrate must decide that the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. Reasonable: The public prosecutor or examining magistrate is satisfied that the infiltration is the least intrusive one for the purpose of collecting the targeted information c. Proportionality: When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties

Lebanon		
SIT	**National Legislation**	**Comments**
		d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an undercover officer. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an undercover officer. e. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial f. **Witness anonymity:** When an undercover agent is required to give evidence, it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise. g. **Immunity:** Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents '*are allowed to acquire, possess, transport, dispense or deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and telecommunications*.'[37] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations h. **Urgency:** Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization.

37. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Lebanon		
SIT	**National Legislation**	**Comments**
		i. **Time limit:** Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 4. **International cooperation:** The lack of a common definition of an, 'undercover agent', and the inclusion of 'citizens' and 'informants' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There maybe a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state 5. **Cybercrime:** Consider process for authorizing undercover agents online

Morocco		
SIT	**National Legislation**	**Comments**
Surveillance	**No legislation**	**Legal Analysis** There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor surveillance and no provisions allowing hot-pursuit and cross-border surveillance. **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 **or** 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters refers to cross-border observations Art.17), The following minimum standards for application are suggested 1. **Legislation should consider the following:** a. **Necessity:** The examining magistrate or senior public prosecutor must be satisfied the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable.

Morocco		
SIT	**National Legislation**	**Comments**
		b. **Reasonable:** The examining magistrate or senior public prosecutor must be satisfied the surveillance measure is the least intrusive method for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the examining magistrate or senior public prosecutor must be satisfied that the measure must be proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The examining magistrate or senior public prosecutor should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of surveillance and to extend where appropriate g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner surveillance is obtained retrospectively without prior consent from the examining magistrate or senior public prosecutor or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 2. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 3. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to conduct surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused

Morocco		
SIT	**National Legislation**	**Comments**
		4. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 5. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Interception of communications (computer)	**No legislation**	**Legal Analysis** This power is essential for national legislation – and there must be safeguards and requirements/procedures to compel CSPs cooperation to collect or record content data in real-time of specific communications in Morocco. **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Morocco to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 21 BC and section 26 HIPCAR and incorporating language in national legislation. Further there should be legal provision to collect real-time traffic data. Article 20 BC and section 25 HIPCAR are applicable precedents: **Article 20 BC -** **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

Morocco		
SIT	**National Legislation**	**Comments**
		3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
		Section 25 HIPCAR - Collection of Traffic Data 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. 3. A country may decide not to implement section 25.
Interception of Communications	**Code of Criminal Procedure**	**Legal Analysis** The law considers interception as an exceptional procedure and an examining magistrate can order on where the needs of an investigation require it. In a case that has not been submitted to an examining magistrate, the senior public prosecutor for the Crown (procureur général du Roi, hereinafter the senior public prosecutor) may order this measure following authorisation by the President of the Court of Appeal (Premier Président) in the case of serious crimes undermining the safety and security of the State. The senior public prosecutor may also, if the needs of the investigation require this, refer in writing to the President of the Court of Appeal with a petition to order the interception, recording, reproduction and seizure of telephone calls and any other long-distance communications if the crime under investigation undermines State security or concerns organised crime, murder, poisoning, abduction and the taking of hostages, counterfeit money or securities, drug trafficking and narcotics, the trade in arms, munitions and explosives or the protection of health.

Morocco		
SIT	**National Legislation**	**Comments**
		However, the senior public prosecutor may in, an emergency, in writing and on an exceptional basis, order the interception, recording, reproduction seizure of telephone calls and any other long-distance communications whenever the needs of the investigation call for urgent action in order to avoid losing evidence in a case concerning State security, drug trafficking, narcotics, arms, munitions and explosives or abduction or the taking of hostages. Within twenty-four hours the latter will issue a decision confirming, amending or overruling the decision taken by the Senior public prosecutor. The law determines the duration of interception to guarantee protection for the privacy of individuals and to ensure that this measure is not implemented illegally, by providing sanctions in the case of breaches.
		Gap Analysis **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested 1. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 2. **Renewal:** A standard procedure for renewal to justify the continued use of interception. 3. Disclosure: A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 4. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to intercept domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 5. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 6. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Morocco		
SIT	**National Legislation**	**Comments**
Covert audio or visual devices	**No legislation**	**Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for use of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for legislation are suggested 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a covert device 2. **Necessity:** A public prosecutor or examining magistrate must establish the proposed covert device is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** A public prosecutor or examining magistrate should be satisfied that the covert device is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize the use of covert devices. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for deploying covert devices 6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for covert devices than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of covert devices and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent a fair trial

Morocco		
SIT	**National Legislation**	**Comments**
		10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Tracking devices	**No legislation**	**Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested for the domestic legislation 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a tracker 2. **Necessity:** A public prosecutor or examining magistrate must demonstrate the proposed tracker is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 3. **Reasonable:** A public prosecutor or examining magistrate should be satisfied that the tracker is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker

Morocco		
SIT	**National Legislation**	**Comments**
		6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Jordan or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Morocco		
SIT	**National Legislation**	**Comments**
Controlled deliveries	**Code of Criminal Procedure** **Article 82-1**	**Legal Analysis** Article 82-1 of the Code of Criminal Procedure defines controlled delivery as "*a method, consisting of allowing, under the supervision of the competent authorities, the passage from Moroccan territory of an illicit dispatch or one suspected of being illicit without being seized or after having been removed and replaced in full or in part with a view to identifying the final destination of said dispatch, investigating an offence and identifying and arresting the perpetrators and incriminated parties.*"[38] Coordination between the Moroccan "*services de lutte*" and their foreign equivalents are needed to guarantee the success of a controlled delivery operation. In practice, foreign authorities (through their liaison officer) will request authorisation of the passage of an illicit dispatch (drugs) through Moroccan territory without being seized at the border posts. The requests will indicate the probable date of the passage, the make of vehicle used, its registration number and the identity of the party who will be driving it. This request is transmitted to the Ministry of Justice and Liberty, Department of Criminal Matters and Exonerations and, the Minister for Justice and Liberty will agree to the request and transmit it to the competent public prosecutor who will authorise the execution of the controlled delivery while continuing to coordinate with the foreign authorities to obtain all the information concerning criminal networks to be used in investigations undertaken by the Moroccan security and judicial authorities.[39] UNTOC, the Vienna Convention and UNCAC have been ratified by Morocco and can be the basis for any ad hoc arrangement with another state if there is no bilateral treaty. **Gap Analysis** **Recommendations:** 1. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 2. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries

38. EuroMed Fiche 2014 page 227
39. EuroMed Fiche 2014 page 228

Morocco		
SIT	**National Legislation**	**Comments**
		3. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 4. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[40]
Informants	**No legislation**	**Legal Analysis** The domestic law does not allow for infiltration measures to be carried out by informants. or a legal framework for the management of informants. Articles 82-9 and 82-10 of the Code of Criminal Procedure, guarantee the protection of informants who reveal certain crimes threatening the security and stability of society to the police and judicial authorities. These protections include for his or her identity to be concealed, for him or her to be given a borrowed identity, to have a special telephone number made available to him or her, to have his or her telephone line placed under surveillance, for his or her personal protection and that of family. **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency The following minimum standards for legislation are suggested 1. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or examining magistrate should decide that the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate should decide the infiltration is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate must decide that the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties

40. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412

Morocco		
SIT	**National Legislation**	**Comments**
		d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of infiltration and to extend where appropriate g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or examining magistrate – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.
Undercover Agents	**Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching** **Articles 54-65** **Organic Law No. 2016-61 of 3 August 2016 related to the Prevention and Combating of Trafficking in Persons** **Articles 27-43**	**Legal Analysis** Undercover agents are not provided for in Moroccan law. The draft Code of Criminal Procedure, has included this procedure, but is yet to be promulgated. There are no SOPs or procedures managing handling of undercover agents. **Gap Analysis** **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. Entrapment: Ensuring there are SOPs and specific instructions for a case (or tasking instructions) will reduce the impact of entrapment 3. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or examining magistrate is satisfied the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable.

Morocco		
SIT	**National Legislation**	**Comments**
		b. **Reasonable:** The public prosecutor or examining magistrate is satisfied that the infiltration is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an undercover officer. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an undercover officer. e. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial f. **Witness anonymity:** When an undercover agent is required to give evidence, it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise. g. **Immunity:** Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents 'are allowed to acquire, possess, transport, dispense or *deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and telecommunications.*'[41] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations

41. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Morocco		
SIT	**National Legislation**	**Comments**
		h. **Urgency:** Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization. i. **Time limit:** Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 4. **International cooperation:** The lack of a common definition of an, 'undercover agent', and the inclusion of 'citizens' and 'informants' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There maybe a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state 5. **Cybercrime:** Consideration should be given to allowing an undercover agent online

The draft resolution on the Palestinian Police Law, which will grant wide powers to the police in the use of investigative techniques and information exchange, is yet to be promulgated. This legal and gap analysis is prepared on the basis of the law presently in force.

Palestine		
SIT	**National Legislation**	**Comments**
Surveillance	**Decree Law No. 18 of 2015 on Combating Drugs and Psychotropic Substances:** **Article 10** The Anti-Narcotics Department shall prepare, in coordination with the competent authorities, the basic reference to combating drug crimes, and shall have the following responsibilities:	**Legal Analysis** This measure is only possible for drug trafficking investigations and when known drug traffickers have entered Palestine. The meaning of, "…*monitoring the movements and relations*" is not explicit. Although the functions of the Anti-Narcotics Department, are explicit in Article 10. Thus, t*he movements and relations under observation* can be reasonably inferred to be all functions listed in Article 10 that contribute to the prosecution of drug traffickers, based on the information, records and lists prepared by the Anti- Narcotics Department. The information obtained from such monitoring and follow-up may be used as evidence during the trial, provided that the information has been obtained in accordance with the law and properly and by a competent person in accordance with the law.

Palestine		
SIT	**National Legislation**	**Comments**
	5. Follow-up with border crossings and reporting on any person whose name is listed as traffickers in narcotics to facilitate the **monitoring of their movements and relations** during their stay in the territory of the State.	There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor surveillance It is unclear if there are any provisions to ensure control, to prevent misuse and assure transparency and accountability Hot-pursuit and cross-border surveillance are not available and remains a sensitive issue in the West Bank. **Gap Analysis** **Recommendations:** Harmonisation of legislation in the SPCs and developing a SPC wide instruments for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 **or** 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters refers to cross-border observations Art.17), The following minimum standards are suggested 1. **Necessity:** Any authorisation must demonstrate that the proposed surveillance measure is necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 2. **Reasonable:** The authorization should ensure that the surveillance measure is the least intrusive one for the purpose of collecting the targeted information 3. **Proportionality:** When invading personal privacy, the surveillance must be proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties by the authorising body 4. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance

Palestine		
SIT	**National Legislation**	**Comments**
		5. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for surveillance than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 6. **Review:** A process to justify the continued use of surveillance and to extend where appropriate 7. Urgency: Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner surveillance is obtained retrospectively without prior consent from the authorisation body or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 8. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 9. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to conduct surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 10. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 11. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Palestine		
SIT	**National Legislation**	**Comments**
Interception of communications (computer)	**Decree Law No. 20 of 2015 on Combating Money Laundering and the Financing of Terrorism** **Article 33** The Attorney General may, upon a decision of the competent court, 1. Control of bank accounts and other similar accounts. 2. Access to computer systems and networks and main computers 3. Subject to surveillance or tracking of communications. 4. Audio and visual recording or portraying acts, behavior or conversations. 5. Intercepting and booking correspondence. **Law No.16 of 2017 on Electronic Crimes** **Article 35(2)** The Public Prosecution may order the immediate collection and supply of any data including traffic, electronic information, traffic data or content information that it deems necessary for the benefit of the investigations, using the appropriate technical means and, where appropriate, using the service providers according to the type of service it provides.	**Legal Analysis** This power is essential for national legislation to compel CSPs cooperation to collect or record content data in real-time in Palestine. Article 33 Decree Law No. 20 of 2015 relates only for money laundering and financing of terrorism investigations. Article 35 of Law No. 16 of 2017 will be more wide-ranging and applies to the cybercrime offences it criminalizes.

Palestine		
SIT	**National Legislation**	**Comments**
Interception of Communications	The Palestinian Penal Procedures Law No. 3 of 2001 Article 51 1. The Attorney General or one of his assistants may control letters, letters, newspapers, publications, parcels and telegrams relating to the crime and the perpetrator of the crime. 2. He may also monitor wiretapping and conduct recordings of conversations in a private place on the authorization of the magistrate when it is useful to show the truth in a felony or misdemeanor punishable by imprisonment for a period not less than one year. 3. The order of seizure or control or registration warrant shall be reasoned, and for a period not exceeding fifteen days renewable for one time	**Legal Analysis** Article 51 allows the Attorney General to "*monitor*" interception authorized by a magistrate. Article 51 is subject to the provisions of the Code of Criminal Procedure and a specific period of control and the requirement for court authorization. It is unclear what the standards required when the magistrate authorizes – other than it must be "*reasoned*" The authority to monitor communications and correspondence is limited to the narrowest ranges and is surrounded by guarantees and limitations as it may affect the privacy of the person. Therefore, the law limits the power to the Attorney General or one of his assistants (only two). This jurisdiction is not subject to other provisions of the law and is limited by a clear period (15 days renewable) and provided that the suspicions are serious and the demand is caused by the magistrate of the peace within a narrow range. The investigation body implements the Code of Criminal Procedure, which is the law that balances the right of the state to punishment and the right of the person to liberty. The freedom or privacy of the person cannot be attacked except for serious reasons and after exhausting all other means of investigation. The technology used in the monitoring is clear and specific and targets specific information without intruding on other information. Those intercepting have undergone in-depth training in this area and are doing their work under the scrutiny of the legal section. Therefore, they will not disclose any confidential information. Monitoring communications includes conversations and their content and everything related to the case, not just a record of contacts or numbers. There is no specific legal material that prevents the taking of evidence derived from the control of communications. On the contrary, this is often the main evidence, provided it is obtained consistent with the law and within the limits of the investigation. There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor interception **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations.

Palestine		
SIT	**National Legislation**	**Comments**
		The following further standards for authorisation are suggested 1. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize interception. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of interception. 2. **Review:** A process to justify the continued use of interception and to extend where appropriate 3. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner interception is obtained retrospectively without prior consent from the authorisation body or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 4. **Disclosure:** A mechanism to ensure consistent protection of the methods used and any intelligence sources is required at trial (i.e. not just to prevent those intercepting disclosing use of this SIT) – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 5. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to conduct interception domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 6. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 7. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Palestine		
SIT	**National Legislation**	**Comments**
Covert audio or visual devices	**Decree Law No. 20 of 2015 on Combating Money Laundering and the Financing of Terrorism** **Article 33** The Attorney General may, upon a decision of the competent court, 4. Audio and visual recording or portraying acts, behavior or conversations.	**Legal Analysis** This SIT is available for money laundering and terrorism financing offences. **Gap Analysis** **Recommendations:** Provision should be made to allow this SIT for a wider range of serious offences; and safeguards should be incorporated to ensure the collection by way of covert devices is legal, necessary, reasonable and proportionate in the circumstances. Harmonization of legislation in the SPCs and developing a SPC wide instruments for use of covert devices - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for legislation are suggested 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a covert device 2. **Necessity:** The legislation must establish the proposed covert device is necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** A public prosecutor or examining magistrate should be satisfied that the covert device is the least intrusive one for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize the use of covert devices. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for deploying covert devices 6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for covert devices than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of covert devices and to extend where appropriate

Palestine		
SIT	**National Legislation**	**Comments**
		8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Tracking devices	**No legislation**	**Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested for the domestic legislation 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a tracker 2. **Necessity:** A public prosecutor or examining magistrate should be satisfied the proposed tracker is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** A public prosecutor or examining magistrate should be satisfied that the tracker is the least intrusive one for the purpose of collecting the targeted information

Palestine		
SIT	**National Legislation**	**Comments**
		4. **Proportionality:** When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** A public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** A practical issue is what happens when a requesting state has a longer timeframe for a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to deploy a tracker domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information can be used evidentially in Jordan or form part of the prosecution file in the other state requiring an MLA request and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy

Palestine		
SIT	**National Legislation**	**Comments**
Controlled deliveries	**The Palestinian Penal Procedures Law No. 3 of 2001** **Article 43** The Minister of the Interior may, on the basis of a presentation by the Director General of the Police, authorize the Attorney General and inform the Director of Customs that a consignment of narcotic substances in the territory of the State shall be allowed in writing to another State in accordance with the controlled delivery regime if he considers that this will contribute to the disclosure of persons Who cooperate in the transport of the shipment and the consignee. **Article 45** "Free zones shall be subject to the same control and supervision measures as other parts of the State 2. The competent authorities shall prevent the traffic in or trafficking in narcotic drugs or psychotropic substances in accordance with the laws in force or in fulfillment of the obligations contained in the conventions to which the State is a party.	**Legal Analysis** Article 43 does not provide any information on what the "*controlled delivery regime*" is. There is a definition of controlled delivery in Article 1 of Decree Law No. (20) of the year 2015 on Combating Money Laundering and the Financing of Terrorism, which states: "*Controlled Delivery: The method by which smuggling offenses can be verified and proven by all means of proof. The basis for this shall be the seizure of goods within or outside the customs zone. It shall not preclude the investigation of smuggling offenses in respect of the goods for which customs data have been submitted, to be disclosed and cleared without any notice or reservation from the Chamber referring to the crime of smuggling.*" Pursuant to Article 5 of Decree Law No. (13) for the year 2016 on Amending the AML / CFT Law No. 20 of the year 2015, the Customs Department has the authority to carry out the supervised delivery regarding the combating of smuggling crimes and their detection. Controlled delivery is an exceptional method that can be approved only when it is expected to achieve a clear and sure benefit of detecting and controlling smuggling groups, traffickers, regulators, financiers, leaders and planners. The implementation of this method at the international level requires a high degree of security cooperation between the implementing agencies in Palestine and the state of destination, with the necessary financial resources, but Unfortunately, Palestine does not have powers over the crossings and borders that Israel is unique in managing, which makes the internationally controlled delivery process very difficult. Article 43 does not allow the full or partial substitution of smuggled goods – Article 20(4) UNTOC states that controlled delivery methods that may be applied at the international level include the interdiction or permitting of goods to proceed intact, or to intercept and replace the goods in whole or in part, leaving the choice of method to the state party concerned. The method applied may depend on the circumstances of the case in question. Therefore, it is possible to have a controlled delivery in accordance with a specific agreement with the countries concerned, applying UNTOC or in application of the principle of reciprocity. It is not clear what contraband the Palestinian law relates to and whether it includes laundered proceeds of crime. There are no standard operating procedures

Palestine		
SIT	**National Legislation**	**Comments**
		Gap Analysis **Recommendations:** 1. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to determine if a controlled delivery is appropriate if drugs or other contraband are being transmitted in their state – this may lead to them commencing their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 2. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 3. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 4. **Substitution:** This should be considered appropriate in legislation on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue 5. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 6. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 7. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[42]

42. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412

Palestine		
SIT	**National Legislation**	**Comments**
Informants	**No legislation**	**Legal Analysis** Palestinian law does not allow for infiltration measures to be carried out by informants or a legal framework for the management of informants. **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. A legislative basis for such a procedure will ensure consistency The following minimum standards for legislation are suggested 1. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or examining magistrate should decide the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or examining magistrate should decide infiltration is the least intrusive method for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate must decide that the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of infiltration and to extend where appropriate

Palestine		
SIT	**National Legislation**	**Comments**
		g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or examining magistrate – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or examining magistrate or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.
Undercover Agents	**No legislation**	The law does not allow for the use of domestic or foreign agents to carry out infiltration on Palestinian territory. **Gap Analysis** **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. Entrapment: Ensuring there are SOPs and specific instructions for a case (or tasking instructions) will reduce the impact of entrapment 3. **Legislation should consider the following:** a. Necessity: The public prosecutor or examining magistrate is satisfied the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. Reasonable: The public prosecutor or examining magistrate is satisfied the infiltration is the least intrusive method for the purpose of collecting the targeted information c. Proportionality: When invading personal privacy, the measure must be proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties d. Threshold: The public prosecutor or examining magistrate should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an undercover officer. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an undercover officer. e. Disclosure: A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial

Palestine		
SIT	**National Legislation**	**Comments**
		f. Witness anonymity: When an undercover agent is required to give evidence, it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise. 7. Immunity: Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents 'are allowed to acquire, possess, transport, dispense or deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and telecommunications.'[43] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations h. Urgency: Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization. i. Time limit: Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 4. International cooperation: The lack of a common definition of an, 'undercover agent', and the inclusion of 'citizens' and 'informants' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There maybe a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state 5. Cybercrime: Consider process for authorizing an undercover agent online

43. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Tunisia		
SIT	**National Legislation**	**Comments**
Surveillance	**Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching** **Article 61** The decision of the public prosecutor or investigating judge shall include, as applicable, authorisation to access private places, premises or vehicles, even outside the hours envisaged by the Code of Criminal Procedure, unbeknownst and without the consent of the owner or any person having the right to use the vehicle or place. The above decision shall include all elements allowing for the identification of personal affairs, public or private places, premises or vehicles concerned by the audiovisual surveillance, acts justifying it and the duration	**Legal Analysis** Article 61 is cited as the applicable law allowing for surveillance. There are no provisions confirming how a justified decision is determined or if evidence can be adduced There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor surveillance There are no provisions allowing hot-pursuit and cross-border surveillance. **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instrument for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. Consideration of a mechanism to enable cross-border surveillance and hot-pursuit - using the following as a guide: 1. Convention implementing the Schengen Agreement of 19 June 1990 (CISA, Schengen Convention – Title 3 Police and Security), amended by Council Decision 2003/725/JHA of 2.10.2003 **or** 2. Council of Europe: The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters refers to cross-border observations Article17), The following minimum standards for legislation are suggested 3. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or investigating judge should decide the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. **Reasonable:** The public prosecutor or investigating judge should decide surveillance is the least intrusive method for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or investigating judge must decide that the surveillance is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties

Tunisia		
SIT	**National Legislation**	**Comments**
		d. **Threshold:** The public prosecutor or investigating judge should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize surveillance. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for application of surveillance e. **Timeframe:** The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. **Review:** Ensure there is a process to justify the continued use of surveillance and to extend where appropriate g. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or investigating judge - surveillance is obtained retrospectively without prior consent from the public prosecutor or investigating judge or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. h. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial. i. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to conduct surveillance domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused j. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for surveillance as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. k. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of surveillance domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Tunisia		
SIT	**National Legislation**	**Comments**
Interception of communications (computer)	**Organic Law No. 2016-61, dated on 3 August 2016, pertaining to the prevention and countering of human trafficking (trafficking in persons).** **Article 42** Any person, except those authorized by law, who intentionally intercepts communications and correspondence or audiovisual surveillance disregarding legal provisions, shall punished by five years' imprisonment and a fine of five thousand dinars. The attempt shall be punishable. **Organic Law No. 2015-26 of 7 August 2015 on the fight against terrorism and the repression of money laundering.** **Article 64** Any person, except those authorized by law, who intentionally intercepts communications and correspondence or audiovisual surveillance disregarding legal provisions, shall punished by five years' imprisonment and a fine of five thousand dinars. The attempt shall be punishable.	**Legal Analysis** This power is essential for national legislation – and there must be safeguards and requirement/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Tunisia. The national legislation does not contain explicit provisions concerning a real-time collection of data. Although the restriction on the use of interception technique criminalized in Article 42 of Organic Law No. 2016-61 and Article 64 of Organic Law No. 2015-26 **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Tunisia to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 21 BC and section 26 HIPCAR and incorporating language in national legislation. Further there should be legal provision to collect real-time traffic data. Article 20 BC and section 25 HIPCAR are applicable precedents: **Article 20 BC -** **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

Tunisia		
SIT	**National Legislation**	**Comments**
		4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. 3. A country may decide not to implement section 25.
Interception of communications	**Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching** **Article 54** If the investigation so demands, the public prosecutor or investigating judge can intercept the defendants' communications, upon written, grounded decision **Organic Law No. 2016-61 of 3 August 2016 related to the Prevention and Combating of Trafficking in Persons** **Article 32** If the investigation so demands, the public prosecutor or investigating judge can intercept the defendants' communications, upon written, grounded decision	**Legal Analysis** Interception is authorized by a public prosecutor or the judge of instruction only for terrorist and trafficking in persons offences. The decision by the public prosecutor or the judge of instruction will determine: 1. The identification of the communications 2. Object of the request for interception 3. Acts which justify the use of the interception Interception cannot exceed 4 months and is renewable only once for the same period. The authority responsible for conducting the interception must inform the public prosecutor or the judge of instruction of arrangements taken to achieve the mission and the conduct of the interception operation. After the end of the interception, the responsible agency shall draft a report, confirming the operations carried out and the data collected, reproduced or recorded. It is unclear what the legal thresholds or justification for interception are for a "*grounded decision*" This raises the following questions: 1. Does the public prosecutor or investigating judge consider proportionality between the effects of an SIT – namely an evaluation in the light of the seriousness of the offence and taking account of the intrusive nature of interception?

Tunisia		
SIT	**National Legislation**	**Comments**
		2. Does a public prosecutor or investigating judge need to consider less intrusive SITs before ordering interception? 3. Are there any safeguards on the use of interception as evidence – for example privileged material is inadmissible? 4. Are there appropriate measures to ensure that the technology required for interception of communications, meets minimum requirements of confidentiality, integrity and availability? 5. Is there any procedure for protecting sensitive techniques, methodology and sources? This is a different process to the offence contrary to Articles 62-63 of Organic Law No. 2015-26 of 7 August 2015. Article 43 of Organic Law No. 2016-61 of 3 August 2016 prevents the disclosure of how the evidence was collected – but there is not a similar provision for terrorist or money laundering prosecutions/ trial 6. Is it interception of a subject (which could increase collateral intrusion) or a telephone number? There are no standard operating procedures (SOPs) for law enforcement to apply, use and monitor interception Article 65 confirms the evidence collected can be adduced in evidence. **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for interception - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested 1. **Necessity:** The public prosecutor or judge of instruction should decide the proposed interception is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 2. **Reasonable:** The public prosecutor or judge of instruction should decide interception is the least intrusive method for the purpose of collecting the targeted information – this includes consideration whether the interception will be of the subject or a specific telephone number 3. **Proportionality:** When invading personal privacy, the public prosecutor or judge of instruction should decide the proposed interception is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 4. **Timeframe:** A practical issue for international co-operation is what happens when a requesting state has a longer timeframe for interception than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 5. **Renewal:** Is there a standard procedure for renewal to justify the continued use of interception.

Tunisia		
SIT	**National Legislation**	**Comments**
		6. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner interception is obtained retrospectively without prior consent from the public prosecutor or judge of instruction or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 7. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required for all offences – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 8. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to intercept domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 9. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order for interception as if an order from within its jurisdiction (e.g. EIO) - is highly recommended. 10. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of interception domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Covert audio or visual devices	**Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching** **Article 61** When the investigation so requires, the public prosecutor or investigating judge may, as applicable, order, on the basis of a written, grounded decision, that the legal police officers appointed to report terrorist offences envisaged by this law, shall place a technical device amongst the personal affairs of defendants, in public or private places, premises or vehicles,	**Legal Analysis** Use of an audiovisual covert device is authorized by a public prosecutor or the judge of instruction only for terrorist or trafficking in persons offences. The covert device is used to capture, fix, transmit and discretely record the words and photos and locate an accused or suspect, in places, premises or private vehicles, or public. Use of an audiovisual device cannot exceed 2 months and is renewable only once for the same period. It is unclear what the legal thresholds or justification for a covert device are for a "*grounded decision*" The authority responsible for conducting the installation of the audiovisual must inform the public prosecutor or the judge of instruction of arrangements taken to achieve the mission and the conduct of the interception operation.

Tunisia		
SIT	**National Legislation**	**Comments**
	so as to discreetly capture, fix, transmit and record their words and photographs and locate them. The decision of the public prosecutor or investigating judge shall include, as applicable, authorisation to access private places, premises or vehicles, even outside the hours envisaged by the Code of Criminal Procedure, unbeknownst and without the consent of the owner or any person having the right to use the vehicle or place. The above decision shall include all elements allowing for the identification of personal affairs, public or private places, premises or vehicles concerned by the audiovisual surveillance, acts justifying it and the duration. The duration of audiovisual surveillance may not exceed two months from the date of the decision, which can be renewed just once for the same terms and on grounded decision **Organic Law No. 2016-61 of 3 August 2016 related to the Prevention and Combating of Trafficking in Persons** **Article 39** When the investigation so requires, the public prosecutor or investigating judge may, as applicable, order, on the basis of a written, grounded decision, that legal police officers shall place a technical device amongst the personal affairs of defendants,	After the use of the covert device, the responsible agency shall draft a report, confirming the operations carried out, their place, date, timetable and result – with the audiovisual recordings must be attached. There is not a defined procedure for protecting sensitive techniques, methodology and sources This is a different process to the offence contrary to Articles 62-63 of Organic Law No. 2015-26 of 7 August 2015. Article 43 of Organic Law No. 2016-61 of 3 August 2016 prevents the disclosure of how the evidence was collected – but there is not a similar provision for terrorist or money laundering prosecutions/trial **Gap Analysis** **Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments for cross- border surveillance and hot-pursuit - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a covert device 2. **Necessity:** The public prosecutor or judge of instruction must demonstrate the covert device is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** The public prosecutor or judge of instruction should be satisfied that the covert device is the least intrusive method for the purpose of collecting the targeted information 4. **Proportionality:** When invading personal privacy, the public prosecutor or judge of instruction should decide use of the covert device is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** The public prosecutor or judge of instruction should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize the use of covert devices. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for deploying covert devices 6. **Timeframe:** A practical issue for international co-operation is what happens when a requesting state has a longer timeframe for interception than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes

Tunisia		
SIT	**National Legislation**	**Comments**
	in public or private places, premises or vehicles, so as to discreetly capture, fix, transmit and record their words and photographs and locate them. The decision of the public prosecutor or investigating judge shall include, as applicable, authorisation to access private places, premises or vehicles, even outside the hours envisaged by the Code of Criminal Procedure, unbeknownst and without the consent of the owner of the vehicle or property or any person having the right to use the vehicle or place. This decision shall include all elements allowing for the identification of personal affairs, public or private places, premises or vehicles concerned by the audiovisual surveillance, acts justifying it and the duration. The duration of audiovisual surveillance may not exceed two months from the date of the decision, which can be renewed just once for the same terms and on grounded decision	7. **Review:** Ensure there is a process to justify the continued use of covert devices and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or judge of instruction or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required for all offences – this sensitive information should be withheld from the accused unless to do so would prevent a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert devices domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross-border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of covert devices domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.
Tracking devices	**No legislation**	**Recommendations:** Harmonization of legislation in the SPCs and developing a SPC wide instruments - with common definitions, authorization process, timeframes and monitoring will advance investigations. The following minimum standards for application are suggested for the domestic legislation 1. **Legal:** There must be provision to enable lawful entry on private premises or property (i.e. vehicle) covertly install a tracker 2. **Necessity:** The public prosecutor or judge of instruction should be satisfied the proposed tracker is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. 3. **Reasonable:** The public prosecutor or judge of instruction should be satisfied that that the tracker is the least intrusive one for the purpose of collecting the targeted information

Tunisia		
SIT	**National Legislation**	**Comments**
		4. **Proportionality:** When invading personal privacy, the public prosecutor or judge of instruction should be satisfied the tracking device is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties 5. **Threshold:** The public prosecutor or judge of instruction should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize a tracker. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of a tracker 6. **Timeframe:** A practical issue for international co-operation is what happens when a requesting state has a longer timeframe for use of a tracker than the requested state. The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes 7. **Review:** Ensure there is a process to justify the continued use of a tracker and to extend where appropriate 8. **Urgency:** Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner, it is obtained retrospectively without prior consent from the public prosecutor or judge of instruction or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests. 9. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial 10. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to use covert probes domestically and commence their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 11. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 12. **SOPs:** SOPs should be considered to ensure consistent practice by officers applying, using and monitoring the continued use of trackers domestically. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy.

Tunisia		
SIT	**National Legislation**	**Comments**
Controlled deliveries		**Legal Analysis** There is no national law for controlled deliveries, therefore, UNTOC, Vienna Convention and UNCAC will be the basis for any ad hoc arrangement with another state. **Gap Analysis** **Recommendations:** 1. **Spontaneous Information:** Consider the application of Article 18(4) UNTOC to allow for information to be shared with another state to allow them to determine if a controlled delivery is appropriate if drugs or other contraband are being transmitted in their state – this may lead to them commencing their own investigation – this maybe quicker than the use of MLA. Although consideration should be given to whether the information will be evidential or form part of the prosecution file in the other state and ensuring that any sensitive material is protected from disclosure to the accused 2. **Cross border:** Due to the fast-paced nature of cross-border operations - moves towards a system of mutuality, where the executing central authority executes a requesting states' domestic order as if an order from within its jurisdiction (e.g. EIO) - is highly recommended 3. **SOPs:** SOPs should be considered to ensure consistent practice by officers using controlled deliveries. This will also provide some assurance to the public of appropriate safeguards being in place to protect against beaches of privacy. 4. **Substitution:** This should be considered appropriate in legislation on a case-by-case basis to reduce the risks associated with allowing an intact controlled delivery to continue – further it should consider all types of contraband and not just drugs (i.e. money, firearms etc) 5. **Urgency:** There should be a process to allow for oral authority to be granted with a written authority to be provided within a short time frame. The identification of the relevant competent authority in another jurisdiction to enable quick and effective authorization for controlled deliveries – this could be by a 24/7 network or single points of contact (SPOCs) that provides practical and legal advice on the execution of controlled deliveries 6. **Controlled deliveries will require monitoring by another SIT:** Informants, undercover agents, interception, trackers or surveillance maybe used and the authorizations will need to be obtained quickly – to reduce bureaucracy a SPOC will assist to ensure the correct information is provided to enable these authorizations to be secured 7. **Harmonization:** Creating a common set of rules for the transmission and execution of international requests[44]

44. See the form in Annex II Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412

Tunisia		
SIT	**National Legislation**	**Comments**
Informants	**Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching** **Article 57** If the investigation so requires, infiltration may take place through a police officer taking on a false identity or an informant known to the legal police officers, qualified to note terrorist offences.	**Legal Analysis** Article 57 allows for infiltration by an informant – but only for terrorist offences. The authorization process is unclear and the standards for any decision Where an accused provides information to assist investigations consideration is given to immunity from prosecution and/or reduction in sentence. Articles 9 and 10 of Organic Law 2015-26 apply. **Gap Analysis** **Recommendations:** Consideration is given to the handling of information from informants to ensure confidentiality of sources to enable effective investigations for all offences. The following minimum standards for legislation are suggested: 1. **Legislation should consider the following:** a. Necessity: The public prosecutor or judge of instruction should decide the proposed infiltration is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable. b. Reasonable: The public prosecutor or judge of instruction should decide that the sought-after infiltration is the least intrusive method for the purpose of collecting the targeted information c. Proportionality: When invading personal privacy, the public prosecutor or judge of instruction must decide the infiltration is proportionate to the seriousness of the crime - this includes consideration of collateral intrusion and minimizing harm on third parties d. Threshold: The public prosecutor or judge of instruction should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an informant. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an informant e. Timeframe: The requesting state should apply for the maximum period for the requesting state domestically and then renew according to the requested state's timeframes f. Review: Ensure there is a process to justify the continued use of infiltration and to extend where appropriate

Tunisia		
SIT	**National Legislation**	**Comments**
		g. Urgency: Where there is an imminent threat, immediate danger or other exigent circumstances and it is not possible to obtain authorisation in the legally prescribed manner from the public prosecutor or investigating judge – informant infiltration is obtained retrospectively without prior consent from the public prosecutor or judge of instruction or with a simple verbal approval. For MLA diminish delay by providing for electronic transmission – and not just for urgent requests.
Undercover Agents	**Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching** **Article 57** Infiltration is carried out by written, grounded decision of the public prosecutor or investigating judge, and under its control, for up to four months, which can be renewed for the same duration by grounded decision If the investigation so requires, infiltration may take place through a police officer taking on a false identity or an informant known to the legal police officers, qualified to note terrorist offences. **Article 60** The legal police officer in charge must supervise the infiltration operation and submit reports to the public prosecutor or investigating judge as necessary, or when asked to do so and upon conclusion of the infiltration operation. Only the final report is put on file.	**Legal Analysis** The use of undercover agents is authorized by a public prosecutor or the judge of instruction only for terrorist or trafficking in persons offences – for a period of 4 months The public prosecutor or the judge of instruction will receive a fingerprint and the identity of the undercover agent. It is forbidden to reveal the real identity of the agent, for whatever reason to any other party.The officer of the judicial police in charge must supervise the undercover operation and submit reports to the public prosecutor or the judge of instruction (Article 60) There are no SOPs or procedures to manage the handling of undercover agents. It is unclear what the legal thresholds or justification for infiltration are for a "*grounded decision*" There is not a defined procedure for protecting sensitive techniques, methodology and sources This is a different process to the offence contrary to Articles 62-63 of Organic Law No. 2015-26 of 7 August 2015. Article 43 of Organic Law No. 2016-61 of 3 August 2016 prevents the disclosure of how the evidence was collected – but there is not a similar provision for terrorist or money laundering prosecutions/trial **Gap Analysis** **Recommendations:** 1. A SPC wide agreement or MOUs between SPCs could allow cross border deployment and management of undercover agents – e.g. the European Cooperation Group on Undercover Activities is an informal police network for the MS that facilitates co-ordination and exchange of undercover officers across Europe and could be a model for the SPCs 2. Entrapment: Ensuring there are SOPs and specific instructions for a case (or tasking instructions) will reduce the impact of entrapment 3. **Legislation should consider the following:** a. **Necessity:** The public prosecutor or judge of instruction should be satisfied the proposed undercover agent is absolutely necessary for the purposes of the investigation by demonstrating all other means have either been exhausted or are inapplicable.

Tunisia		
SIT	**National Legislation**	**Comments**
	Organic Law No. 2016-61 of 3 August 2016 related to the Prevention and Combating of Trafficking in Persons **Article 35** Infiltration is carried out by written, grounded decision of the public prosecutor or investigating judge, and under its control, for up to four months, which can be renewed for the same duration by grounded decision	b. **Reasonable:** The public prosecutor or judge of instruction should be satisfied that the undercover agent is the least intrusive method for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or judge of instruction should be satisfied that the use of an undercover agent is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties d. **Threshold:** The public prosecutor or judge of instruction should be satisfied of reasonable suspicion of a serious crime being or having been committed, in order to authorize an undercover officer. As a priority, there should be a consistent penalty limit, as confusion can arise if the requesting state has a lower penalty threshold than the requested state. Consideration should be given to an all crimes approach or a penalty limit such as definition of serious crime in UNTOC (Article 2(b)) of more than 4 years imprisonment – this could avoid any uncertainty about the relevant offences for use of an undercover officer. e. **Witness anonymity:** When an undercover agent is required to give evidence, it is essential that his identity is protected to allow deployment in future investigations and to reduce the risk of harm to them and their families. Witness protections could be used such as video conferencing and anonymising a witness through voice distortion, pseudonym and disguise. f. **Immunity:** Officers may need to be party to the commission of crimes, for example test purchase of drugs. The undercover agent should have immunity from certain criminality that can be included in a tasking document or a procedure is included in the SOPs. In a MS (Luxembourg) for instance, it is specifically stated that undercover agents '*are allowed to acquire, possess, transport, dispense or deliver any substances, goods, products, documents or information resulting from the commission of any offences or used for the commission of these offences, as well as use or make available to those persons carrying out these offences legal or financial help, and also means of transport, storage, lodging, safe-keeping and telecommunications.*'[45] Any legislation should ensure as a minimum that undercover agents are not criminally responsible for an offence committed in the implementation of a covert investigation; the definition of the limit of undercover agents' powers and the definition of offences that are permissible as part of undercover operations

45. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf page 273

Tunisia		
SIT	**National Legislation**	**Comments**
		g. **Disclosure:** A mechanism to ensure protection of the methods used and any intelligence sources is required – this sensitive information should be withheld from the accused unless to do so would prevent the accused having a fair trial h. **Urgency:** Legislation needs to allow for the emergency authorisation or when opportunities for operations suddenly arise. This could include verbal authorization, followed by a written authorization. By the public prosecutor or judge of instruction i. **Timeframe:** Consideration of the appropriate time limit to allow for an effective investigation. There should be consistent monitoring and oversight to ensure the principles of necessity, reasonableness and proportionality are protected 4. **International cooperation:** The lack of a common definition of an, 'undercover agent', and the inclusion of '*citizens*' and '*informants*' as undercover agents in some SPC legislation may create situations where immunity and hosting of such agents will be difficult. There may be a limited scope to deploy or host foreign undercover agents as SPC legislation may state that an undercover agent needs to be an officer of the national police or intelligence services. Consideration should be given to provisions that allow the possibility for the acceptance of a foreign law enforcement officer as an agent in that other state 5. **Cybercrime:** Consideration should be given to allowing an undercover agent online

Conclusion

The use of SITs is an essential element of an investigation to identify perpetrators and to prevent serious crime. The different legal frameworks in the SPCs can inhibit the efficient deployment of SITs, thereby reducing their operational impact. The following recommendations, to enhance the use of SITs, are recommended:

1. Legislation regulating the minimum punishable offence for which a SIT may be authorized can present jurisdictional challenges. For example, when a requesting state with a lower authorization threshold wishes to cooperate with authorities in a requested state with a higher authorization threshold for the same SIT. A consistent application of SITs for serious crime, such as UNTOC (Article 2(b)) of more than 4 years imprisonment, would resolve this issue. Realistically legislation will not be enacted to remedy this immediate issue. **It is recommended** that SPOCs are deployed in competent authorities to enable quick-time co-ordination to deploy SITs in cross-border operations. The SPOCs can liaise with counterparts in the SPCs and MSs to determine which state is best placed to use SITs efficiently and effectively.
2. Definition of SITs may differ from one state to another – for example informer and undercover agent. **It is recommended** that processes are in place for requesting states to ensure that an SIT is appropriate in the circumstances according to domestic law. Again, this could be through SPOCs.
3. Dual criminality issues can prevent execution of requests – **it is recommended** that dual criminality is not a specific requirement for requesting SITs.
4. Where there are no reciprocal provisions this could hamper investigations – **it is recommended (where there is no SIT legislation this is enacted with safeguards to protect individual privacy.**
5. A mutual recognition system (such as the EIO) **is recommended** as a long-term objective to enable SITs to be used more efficiently.

Bibliography

- AMOC Report 2015 Part 3 Legal and Investigative tools
- EuroMed Fiche 2014
- Transnational Controlled Deliveries in Drug Trafficking Investigations Manual JUST/2013/ISEC/DRUGS/AG/6412
- The Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions

Acknowledgements

Special thanks to the commitment and dedication of the scientific consultants whose contribution was essential to the production of this paper.