Council of the European Union

Brussels, 31 May 2016
(OR. en)

9201/16

LIMITE

JAI 441
COSI 90
FRONT 220
ASIM 78
DAPIX 78
ENFOPOL 155
SIRIS 86
DATAPROTECT 56
VISA 158
FAUXDOC 21
COPEN 165

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Information sharing in the counter-terrorism context: Use of Europol and Eurojust

There is great political momentum to improve information sharing:

The Netherlands Presidency has presented the "Draft Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area"[1] to the JHA Council for adoption. It contains the political commitment to feed and use the information systems to the maximum extent and highlights the importance to identify lessons learned and support continuous improvement. Full implementation of the roadmap, in particular the actions contained in the CT Action Plan, will be important moving forward.

[1] Doc. 9368/16

In April 2016, the Commission issued a Communication on Stronger and Smarter Information Systems for Borders and Security. Interoperability of systems could substantially improve sharing and access to information. There are several IT improvements that could be beneficial in terms of efficienty, speed and interoperability, e.g. common data exchange standards as a prerequisite of interoperability, a single search interface, the use of semi or fully-automated data loaders allowing the insertion of bulk data. There is the need to explore how to make best out of all these, as indicated in the Communication on Stronger and Smarter Information Systems and the Presidency Roadmap. The High Level Group of Experts could come up with proposals for interoperability solutions closing the intelligence gaps in information sharing.

At previous meetings of the Council, the EU Counter-Terrorism Coordinator (EU CTC) informed Member States of the state of the use of Europol, SIS II, Interpol and other relevant databases in the context of the fight against terrorism.[2] This note is based on the assessment of the figures provided at the April 2016 JHA Council as well as consultations with a number of Member States most affected by the foreign fighters phenomenon and sets out examples of operational added value of Europol and Eurojust, a number of recommendations and questions for discussion.

Annex 1 sets out good practices and areas for further improvement identified from Member States. In Annex 2 the potential use of the various Europol tools is explained. In addition, several Member States that have made a strong political commitment and particular operational efforts to use the tools at EU level for information sharing describe their good practices (Annexes to follow).

Information sharing to counter terrorism is high on the political agenda of Member States. This is also reflected at operational level by the strong increase of information exchanged via the different mechanisms over the last year. Moreover, a number of Ministers of the Interior got personally involved in boosting their Member State's information sharing at EU level which is making a real quantitative and qualitative difference. This is based on a recognition of the importance of using EU information sharing channels in support of operational success.

[2] The analysis is based on data provided at the April 2016 JHA Council (figures reflect state of play mid April 2016 and the year of 2015.)

However, the use of EU systems, tools and services by Member State services varies greatly. Some, including those who have recently been supported by Europol in the aftermath of attacks, report great operational benefit from using the tools on a systematic basis. Others, remain unconvinced of the operational benefit provided by Europol, believing that the risk posed to sensitive operations outweighs what they have thus far deemed to be limited operational gains.

I. QUESTIONS FOR DISCUSSION AT THE JHA COUNCIL

The following points can be detected for which political steer from ministers is necessary:

1. Generally, consultations showed that successful improvement of use of Europol and Eurojust tools heavily depends on political will and/or recognition of operational added value by the relevant services/investigators rather than on financial or technical constraints. Good cooperation of the various actors (law enforcement, security services) at national level is also crucial for effective information sharing at EU level. A virtuous circle can be identified: Those Member States that closely involve Europol (and Eurojust) in their CT investigations see the added value and engage even more. It is an iterative process: the more information is being shared, the more operational value the cooperation with Europol tends to have. Initially, it can be a leap of faith.

Based on the success stories provided by Europol and Eurojust from recent months, Ministers are invited to consider how they can get greater value from the information and services available to them in support of their investigations. Those Member States who have judged that Europol has not been able to articulate it's added value are also invited to share their experiences.

Given the commitment in the draft Roadmap to share by default, can ministers agree on the need for a political steer to encourage services to share more systematically with Europol and engage more with Europol on CT? How best could Europol help Member States in CT?

2. A lot of information in CT is classified as 'secret' or above. This requires an update at Europol. Europol's information sharing system SIENA will be upgraded to "confidential" in the autumn of 2016. Handling codes and IT solutions allow a lot of protection.

Do Ministers agree that it would be indispensable to integrate the information sharing network of the Police Working Group on Terrorism (level 'secret') into Europol to also provide an information sharing environment at the level 'secret' and avoid creating of parallel structures as well as to provide training on handling codes?

3. Procedures for sharing and with regard to IT, sufficient amount of terminals, batch upload systems are necessary.

Do Ministers agree on the necessity to put these procedures and IT tools in place as a matter of priority?

4. Do Ministers agree to the proposed recommendations?

II. ADDED VALUE OF THE USE OF EUROPOL AND EUROJUST TOOLS FOR COUNTER-TERRORISM

At the core of the political and operational decisions about feeding and use of Europol and Eurojust in the context of CT is the perceived (lack of) added value, in particular at operational level. For some Member States, in-depth experience with Europol, such as in the aftermath of the Paris and Brussels attacks, has shifted perceptions and increased significantly the perceived usefulness. Moving forward, it will be key for Europol and Eurojust to provide clear examples of added value, in order to help Member States understand the operational benefits Europol and Eurojust have to offer them for CT. As a first step, a few examples are set out below:

1. Europol

Information sharing in the area of counter terrorism advances significantly in quantity and quality, requiring continuous commitment by all stakeholders in order to keep pace with the terrorist threat. Given that all Member States are now connected to the counter terrorism space in SIENA, the function of the ECTC as a hub to exchange information, conduct analysis and coordinate operational support can be fully exploited by Member States and relevant third parties.

The main added value of making use of Europol is to establish links between counter terrorism and organised crime activities, providing key opportunities to identify new lines of investigation. Comparing the situation with bilateral and multilateral cooperation arrangements prior to Europol's structural involvement, information is now exchanged faster, in a more efficient and effective way. Continuing support to the Joint Liaison Team (JLT) is key to effectively address the wider European and international dimensions of the current terrorist threat affecting Member States. Concerning secondary security checks, it can be expected that an increased on-the-spot presence in the hotspots (Greece, as well as in Italy) will, over time, increase opportunities to identify new lines of investigation in the area of counter terrorism.

In the context of Taskforce Fraternité established at Europol in December 2015 to support the investigations into the Paris attacks and, subsequently, the Brussels attacks, frequent operational meetings were organised between Europol, France, Belgium, and other Member States, bringing together investigators, analysts and prosecutors. The Joint Investigation Team (JIT) 'Vendredi' was set up through Eurojust, in which France, Belgium, Europol and Eurojust participate. As a follow-up to the Brussels attacks, the ECTC served as a support platform for the concerned counter-terrorism authorities in Member States. Examples of added value generated by cooperation through, and support by, Europol, are:

– Unprecedented levels of information (of over 16,7 TB) have been shared with the Taskforce Fraternité by the investigative authorities.

– Phone data analysis in relation to the Paris terror attacks.

– Financial investigations: 24,428 intelligence leads have been provided by the TFTP since 2010, of which 17,500 leads were generated in 2015 and 2016 (up to May 2016). A significant amount of exchanges within TFTP concern the phenomenon of travelling fighters (Syria/Iraq/IS), 8.251 leads (34% of the overall number of leads) are specific to this phenomenon (of relevance to 27 EU MS); in addition, more than 3,000 money transfer leads were established with support of US authorities (US Immigrations and Customs Enforcement (ICE)) in Fraternité.

– The Internet Referral Unit (IRU) provides a core internet investigation and social media analysis support capability (e.g. to establish (historic) whereabouts and contacts of the Paris terror attackers). In 2016, internet investigative support was provided to in total 29 operational cases, including Fraternité. In addition, 47 operational reports were delivered.

– Analysis in relation to the geographical whereabouts of the Paris terrorists, prior to the attacks, especially in two Member States, resulting in further investigative leads (locations, contacts, possible facilitators). Operational analysis of a list of individuals, suspected to have used same travel routes as the Paris attackers, generating leads including financial intelligence regarding the location of these individuals (for follow-on investigative activities at national level).

– In the context of the arrests of two terror suspects in Austria in December 2015 (suspected to have travelled from Syria via Turkey and Greece with two of the Paris attackers, among migrants to the EU), eight Member States joined forces at Europol (travel patterns, communication data, information on facilitators for travelling to the EU). Operational analysis through Europol identified additional links to the recruitment of fighters and collection of money to support jihadist activities in Eurasia.

– In February 2016, checks were performed against Europol's databases, in relation to the arrest of an EU national in France (suspected to be a member of IS and responsible for activating terrorist sleeper cells in two Member States). On this basis a match was established concerning one of the main suspects' contacts, an individual in another Member State, arrested as part of a case against facilitation of illegal immigrants (Syrian nationals); furthermore, communication data established links to an investigation against an Organised Criminal Group (OCG) of facilitators in the context of the smuggling of migrants to the EU.

– Since the beginning of March 2016, Europol has deployed its own staff to Greece (EU Regional Task Force – RTF in Piraeus, as well as to the islands of Lesvos, Chios, Samos and Leros), to help coordinate investigations regarding migrant smuggling as well as trafficking in human beings in support of the national authorities, and to carry out secondary security checks (on the islands) as re-affirmed by the JHA Council following the Brussels terror attacks. The common risk indicators developed by the Commission in cooperation with Member States and EU agencies are used to support secondary security check activities. From the overall activities performed to date, there are 70 hits against Europol databases. 4 cases indicate counter terrorism investigative leads, of which one case also suggests organised crime links: illegal immigration facilitators in Mersin/Turkey and Idlib/Syria. Greece has meanwhile submitted further information which is being analysed.

– At the end of March 2016, in the context of an arrest of a terror suspect in France, analysis of hits against data provided (generating links to counter terrorism and organised crime cases in other MS).

– In the context of the investigations into the Brussels attacks, four specific operational analysis reports were generated regarding two members of the concerned terror cell, identifying links to a Member State, including social media and connected financial intelligence leads. That country contributed its list of foreign fighters, sharing the full profiles (including ID document information, aliases, photos, fingerprints, DNA etc.), setting a best practice example concerning the range and quality of data for cross-matching and analysis at EU level.

– More recently, identification of links, making use of JIT 'Vendredi', to an on-going investigation into a network involved in facilitation of illegal immigration in a Member States, with multiple links to other Member States.

– From an overall perspective, the information analysed by Europol corroborates the suspected connection of the Brussels and Paris terror attackers, underlining a profile of terrorist attackers which is related to (organised) criminal activities and networks across multiple Member States and beyond (e.g. illegal immigration, counterfeit travel documents, drug trafficking (cannabis, heroin), aggravated thefts, robberies etc.): all of the six Brussels attackers and six out of the ten perpetrators of the Paris attacks in November 2015 had an organised crime/criminal background.

– The Joint Liaison Team (JLT) is key to effectively address the wider European and international dimensions of the current terrorist threat affecting EU Member States. Germany acts as the driver in relation to one of the JLT's work strands which aims at working towards a consolidated baseline list of foreign fighters.

2. Eurojust

Eurojust underlines the crucial importance of information sharing between Member States and with the relevant EU agencies and calls for a better compliance with the obligations stemming from Council Decision 2005/671/JHA on the exchange of information on terrorist offences. Further to information on convictions, Member States should also provide Eurojust, in a timely and systematic manner, with information on all prosecutions, links with other relevant cases, as well as requests for judicial assistance, including letters rogatory and European Arrest Warrants, addressed to or by another Member State and the relevant responses, as required by the Council Decision 2005/671/JHA.

Eurojust also calls for a better compliance with the obligations stemming from Article 13 of the Eurojust Decision, in particular the exchange of information with Eurojust on cases of illicit trafficking in firearms, illegal immigrant smuggling, drug trafficking and cybercrime.

An increased, timely and systematic information sharing with Eurojust would bring important benefits for the Member States' security. In particular:

1. It could give Member States' competent authorities the possibility to immediately be notified by Eurojust in case **links between cases and, where appropriate, criminal networks** are detected as a result of cross-checking by Eurojust of the information it receives.

2. It would give Member States' competent authorities the possibility to regularly receive **enriched Eurojust analyses of the judicial responses to terrorism** coming from prosecutions and convictions for terrorist offences (via the *Terrorism Convictions Monitor*, the *Eurojust's Reports on Foreign Terrorist Fighters* (FTFs) and the Eurojust tactical meetings on terrorism).

   – Through these analyses, Member States could identify similarities with cases in other countries that could serve as inspiration, could consult the **challenges and best practice** identified in different Member States in terrorist prosecutions and convictions, including court arguments on relevant topics. Where appropriate, the EU legislator could also consider the challenges and best practice when drafting relevant laws. For example:

   – Eurojust's analysis of a judgment from one Member State has been assessed as very useful to identify similarities with a case under trial in another Member State. Furthermore, Eurojust has been consulted in a couple of cases when the prosecution has brought (or is to bring) charges in order to identify similar cases in other Member States and explore the sentencing level.

   – Eurojust has identified that Member States encounter difficulties in determining whether the conduct of women and girls travelling to conflict zones and supporting the FTFs in various way is a crime. It signalled that the nature of the conduct of women and girls in the context of an armed conflict has been interpreted differently by the courts of two Member States, leading to a conviction in one Member State and to an acquittal in the other.

   – Eurojust highlighted certain arguments of the courts on the terrorist nature of the groups FTFs join in Syria/Iraq, emphasising, for example, that in some Member States, the court heard testimonies of (counter-)terrorism experts or considered the origin of the group and the degree to which it met the criteria defining a terrorist group, as set out by national law or that the United Nations' listing of groups, such as ISIL and Jabhat al-Nusrah, has been used by courts in some Member States in cases in which FTFs joined any of them.

– Eurojust highlighted certain arguments of the courts in relation to the acts committed by FTFs, emphasising that courts may sometimes be confronted with a wide diversity of criminal acts that the defendants have (allegedly) committed while in the conflict zone or while preparing to leave. Depending on national laws, the scope of acts constituting a terrorist offence may vary.

– Eurojust highlighted certain arguments of the courts on the applicability of international humanitarian law (IHL), emphasising that despite the fact that IHL has often been used by the defence to question the jurisdiction of the court or the applicability of national criminal law provisions, the analysis of judgements shows that courts in the Member States do not appear to be facing major challenges in addressing that issue.

– Eurojust highlighted certain arguments of the courts on procedural issues, emphasising for example, differences between the legal systems of the Member States in rendering judgements *in absentia* in FTF cases, the arguments of some courts in placing aspiring FTFs in psychiatric institutions, or the approaches to juvenile FTFs.

– As a follow-up to the Council Conclusions on the **criminal justice response to radicalisation** leading to terrorism of 20 November 2015, Eurojust would be in a better position to share with the Member States:

– trends and developments of relevant case law in the Member States, including the use of alternatives to prosecution and detention in terrorism cases, and thus contribute to the further development of criminal policy with regard to foreign terrorist fighters.

– existing national practices and the lessons learnt thereof, in particular the risk assessment tools for assessing the level of threat posed by foreign terrorist fighters and returnees, rehabilitation programs both in and outside prisons and the use of Internet and social platforms.

3. If requested, Eurojust could facilitate cooperation among Member States on **convictions of third-country nationals** in relation to terrorist offences and share this information with the Member States. This is particularly important until ECRIS will be further developed to support information on convictions of third country nationals.

Member States are encouraged to involve Eurojust in an early stage of investigations and prosecutions and in particular, to make use of Eurojust's coordination meetings and coordination centres to exchange information and discuss investigation and prosecution strategies.

Coordination meetings are unique and effective tools in judicial cooperation, bringing together judicial and law enforcement authorities from Member States and third countries, and allowing for informed and targeted operations in cross-border crime cases. During coordination meetings, legal and practical difficulties resulting from differences among the 30 existing legal systems in the European Union can be resolved. Coordination centres play a highly relevant role in operations, fostering real-time support during joint action days, coordination and immediate follow-up of seizures, arrests, house/company searches, freezing orders and witness interviews.

An example of the added value for Member States in making use of the Eurojust coordination meetings and centres is presented in the case study below.

Case Study: Operation JWEB

In November 2015, Eurojust coordinated a Joint action against radical Islamist terrorist group in a complex trans-border case. The case concerned suspected leaders and members of a terrorist organisation (Rawti Shax), with a structure active in Germany, Switzerland, the UK, Finland, Italy, Greece, Sweden, Norway, Iraq, Iran and Syria and with cells communicating and operating via the Internet. The organisation provided logistical and financial support to recruiting FTFs to be sent to Syria and Iraq, also with the intent of training them for the future conflict in Kurdistan. The joint action was agreed following several coordination meetings that took place at Eurojust and allowing to identify all judicial and practical issues to be addressed. A coordination centre was set up at Eurojust to facilitate the joint action. As a result, 13 suspected leaders and members of Rawti Shax were arrested in Italy, Norway and the UK and charged with international terrorism. In addition, the Italian, German, Finnish, Norwegian, Swiss and UK authorities conducted searches of 26 premises and seized several items, including electronic devices and documents.

Some suspects could not be located, as they are believed to have travelled to the Middle East (Syria and Iraq) to join jihadist organisations as FTFs. The level of cooperation provided by all the authorities involved in this case was exceptional. The efficient and continuous collaboration between the magistrates dealing with this case, at national level and through their Eurojust Desks and liaison magistrates, secured this positive outcome.

III. RECOMMENDATIONS

1. Europol and Eurojust should be invited to provide additional detailed examples and arguments for their operational added value on CT to those Member States (in particular at operational level) which do not yet fully exploit cooperation tools at EU level. Member States more deeply involved with Europol and Eurojust could also contribute to providing examples of the added value for their investigations and prosecutions. This could be done by regular reports to COSI.

2. On this stronger basis of information, Member States are invited to **further evaluate the operational benefits they could gain by enhanced use of the systems and tools available to them at Europol and Eurojust**. In this context, it may be helpful for Member States to start engagement as a test, to see the outcomes for themselves. Unprecedented levels of information (of over 16.7 TB) have been shared with the Taskforce Fraternité, established at Europol in support of the investigations into the terror attacks in France and Belgium. CT cooperation requires trust and data ownership control. Member States reported that information is handled well by Europol, respecting handling codes and the protection of information, with no reported examples of data security breaches. This has also been confirmed through the EU-US reviews on Europol's implementation of the EU-US TFTP Agreement.

3. The **separate communication network of EU law enforcement authorities in the Police Working Group on Terrorism (PWGT)**[3] **should be integrated in due course into the ECTC at Europol**, thus providing for a full range of CT information exchange, including 'EU Confidential' (through SIENA at Europol in 2016) and 'EU Secret' (current communication network of the PWGT).

4. High **quality analysis contributions to the relevant Focal Points (FPs),** especially contextual information on terrorist suspects and their associates, need to increase further, in order to further support Member State investigations through providing them with as rich a picture as possible of the terrorist threat. This includes further verification activities to validate personal data on travelling fighters in FP Travellers, on the basis of contributions by Member States.

5. As **Eurojust** is underused with regard to counter-terrorism, it may be useful to do the exercise on contributions to and use of Eurojust tools with the Ministers of Justice.

6. Given similar IT challenges in several Member States related to **EIS feeding**, **automatic data loaders** developed by some Member States should serve as a best practice example. Europol is available to help Member States identify the best solution for data feeding.

7. Based on the opportunities the new Europol Regulation will bring when it enters into force on 1 May 2017, Europol is preparing an **integrated data management model**. The core principle is that one unified data set will hold all different data types, ensuring at the same time robust security and handling controls concerning the data across relevant Focal Points (FPs) and other applications. The underlying maxim is to provide information (with handling codes) once only, with data processing being based on conditions by the data owner.

8. To ensure a wide range of information sharing on FTF, the reference document with criteria to be developed according to the Presidency Roadmap (action 17) to create a **common understanding** will be helpful.

---

[3] Including Iceland, Norway and Switzerland

9. Given that the profile of the terrorists involved in the Paris and Brussels attacks is related to (organised) criminal activities and networks across multiple Member States and beyond (e.g. illegal immigration, counterfeit travel documents, drug trafficking etc.), the Council could consider confirming that an effective counter terrorism response requires, with the remit of national regulatory frameworks, the **development of a link between the ECTC at Europol and the CTG** platform. This is in particular relevant considering that the overall volume concerning organised crime related information in the analysis repository of Europol comprises over 27.5 Million data entities.

10. Europol and Eurojust should be invited to **anticipate the take-up of EU funded security research** results by involving themselves in the follow-up of relevant research projects, on the dissemination of their results and, where appropriate, on hosting the tools developed by these projects for testing by the Member States.

ANNEX I

Good practices and areas for further improvement identified from Member States

I. GOOD PRACTICES IDENTIFIED FROM MEMBER STATES

1. Contributions to Europol

The **political decision to feed the databases** is a very important factor which precedes procedures and IT tools. In one Member State where this is seen as a political priority, the Minister of Home Affairs gets himself involved regularly to review progress and is tasking his administration to address obstacles. The importance for the operational services to see added value was also highlighted as a basis for engagement.

A number of good practices could be identified from Member States contributing a lot to Europol databases:

Step-by-step approach

– Some Member States have **taken the political decision more recently to intensify their work with Europol,** in particular the feeding of databases on CT, but want to progress step by step and start with one database/tool which may be enlarged later on. This means that still not all databases are being fed, but that the Member State is progressing towards more active involvement. One Member State which has taken the decision recently to feed and use the EIS, plans to send a dedicated counter terrorism liaison officer to Europol to strengthen cooperation and trust and identify the added value, which may lead to (and increased) feeding of the FP Traveller later on.

Inter-agency cooperation

– One Member State currently assesses options of how Europol can be used by the security service and what added value it can bring.

– One Member State has created a **platform including all relevant services to feed the databases 24/7 and to respond to requests/inquiries**, including all the relevant databases. This is linked to the Europol National Unit and the SIS/SIRENE Bureau. Another Member State has a task force in which all agencies participate and where a consolidated list of FTFs is established, which is then shared with Europol by the police.

– In some Member States, where police and security services are double-hatted or where the security service is a police service, files are directly shared with Europol (sometimes only as soon as there are enough elements to bring the file to the judicial system).This leads to strong sharing in some but not all of these Member States.

– Another Member State also has intense sharing between the security service and the police (and other services in the context of the fusion centre). As soon as a file on a person is established and verified on a person by the police (which can be based on information received from the security service), it is shared with Europol.

– Another Member State has meetings every two weeks between the security service, the police and justice to review files. As soon as there are enough elements that a person is engaged in criminal conduct, a file is given by the security service to the police, which is then shared with Europol. These file reports are done in a way that they protect sources and methods, hence there are no concerns as far as sharing is concerned and providing action options to the police is regarded by the security service as one way to reduce the threat. In addition, this Member State has the possibility for joint work on targets among the various services. Only information about identified persons is shared with Europol, not those where the identity is still unclear.

– One Member State has a Focal Point committee consisting of the police and the judiciary. Whenever a new Focal Point is created at Europol, the Committee ensures that legally and organizationally the necessary measures are taken so that the Member State can start feeding the Focal Point.

Moment of sharing

– Information not shared with Europol among the Member States feeding a lot are unidentified persons and persons that are watched early on but have not yet fulfilled the elements of a terrorist crime. Conduct at an early stage, including preparing to travel to Syria, can already constitute a terrorist crime. Hence for those Member States that share with Europol as soon as the person's conduct constitutes a terrorist crime, the numbers of sharing are very high and more or less reflect the foreign fighters figures of those Member States.

– The political decision to share with Europol needs to be supported in terms of **procedures**, so that sharing is embedded into the regular routine of police officers. One Member State is translating the political willingness to work with the European databases into an effort to **systematize and automatize the IT** in addition to **human investment** which remains necessary. To become more effective, standardized procedures for information sharing are needed. In this regard, **training of officers** to feed and use the databases, as well as an **efficient system for authorization and control of access to databases**, is regarded as important.

– The importance to **share and analyse high quality information** was highlighted: it was regarded as more useful to share fully developed files on individuals rather than just give raw data to Europol. This may mean less quantity of data but more quality.

– Member States that feed the EIS a lot have **batch upload systems**. Several Member State that recently took the political decision to systematically feed the EIS (in addition to FP Traveller) are now developing the necessary software solutions that allow automatic upload and update with regard to the EIS.

2. Queries of Europol tools

– Queries of the EIS and the TFTP are frequent when the **operational added value is being recognized** by the Member State. The TFTP is regarded by some Member States as very valuable, producing lots of leads which are useful for further analysis and includes the weight of the US system. For other Member States, following the financial links is a priority and in this context the TFTP is regarded as an important tool.

– A Member State that recently decided politically to carry out regular queries of the EIS is now **rolling out the necessary IT terminals** across the relevant services to facilitate access.

– **IT tools, standard operating procedures, a single interface and training** are important for officers on the ground. **Technology** such as tablets and smartphones which can scan passports and check databases should be provided to field officers.

3. Information sharing with Eurojust

– The Member State where the prosecutor shares information about all ongoing CT investigations and prosecutions with Eurojust does so because of the **political decision** to do so and has the procedures and information exchange channel in place: The **TESTA NG network is used as secure channel**.

– Several Member States have the political decision and practice to share all **convictions** with Eurojust. Several other Member States mentioned good cooperation with Eurojust.

4. Interpol

– Member States sharing a lot of FTF with Interpol have an efficient way of using the **Interpol fusion system** (they can control which other States get the information) so that there are no operational data protection or other human rights concerns.

– There are very high figures for **SLTD checks at external borders** when done **systematically for all external border crossings,** but much less when it is done based on common risk indicators. However, a Member State relying on common risk indicators is additionally using Advanced Passenger Information (API).

II. AREAS FOR FURTHER IMPROVEMENT IDENTIFIED BY MEMBER STATES

1. Contributions to Europol in CT

– **Some Member States where the added value of working with Europol on CT has not been recognized** (this can concern Europol as a whole on CT or a specific database) feed and/or use the databases less for CT. Several Member States have excellent experience to work among security services in the Counter-Terrorism Group (CTG) context, where the classification level is higher (majority at the level of 'secret' but also above). Therefore, the argument is being advanced that there is no need to change something that works well (e.g. through the CTG) and brings the results. Sharing only in the CTG context is regarded as problematic when the security service of the other Member State which receives the information does not share with the police.

– One Member State where the security service carries out the initial CT investigations, stressed that the **operational risk to share outweighed the operational value for CT**: CT information was classified secret and above. To share it with Europol was perceived as not possible at that classification level given that this also meant that police agencies at the national level would receive/transmit the information which would normally not have access.

– One Member State is very much convinced of the added value of Europol in organized crime and contributes and uses among the most in that area but is of the view that Europol has not made the case of its usefulness in CT.

– Several Member States stressed the **importance for Europol to make the case and provide specific operational examples** of the added value of working with Europol and the various databases. If they had a clearer picture of the added value, it would help future considerations and assist operational colleagues to identify when and at what stage of investigations these tools should be deployed.

– Several Member States also asked **why they needed to contribute the data to several systems** (such as EIS, FP Travellers, FP Hydra) instead of having Europol connecting the dots and enter the data where necessary (which however is impaired by Europol's current legal framework which does not allow Europol to act as an independent information broker on behalf of Member States across databases)? The value of hits was also questioned, as was the difference between hits in the Focal Point and the EIS.

– Several Member States that have taken recently the decision to feed the EIS are facing **IT obstacles**, as their systems and infrastructure at national level do not yet allow for automated uploads. Europol is available to help Member States identify the best solution for data feeding. The automatic data loaders developed by some Member States should serve as a best practice example.

– One Member State informed that only confirmed FTF were shared with FP Traveller, but that all others (facilitators etc.) were shared with **FP Hydra**. Therefore, the figures could also be misleading, as the Member State shared all information on FTF in the hands of the criminal police with Europol as soon as the personal files were verified. The question was raised how the information of both focal points was cross-matched by Europol.

– A definition**, or at least a common understanding of FTF** is lacking for the various databases, so it may be not clear at national level what category of persons should be contributed (those who are currently in Syria/Iraq, those who are on their way to and back; those who have returned: those allegedly killed etc.). This may explain some differences in numbers according to some Member States. To ensure efficient sharing of information, Europol promotes a wide application of the term FTF, in line with the definition given in the UN Security Council Resolution 2178 (2014)[4] on foreign terrorist fighters, complemented with national specific arrangements (thus covering the entire cycle: fighters being currently in a conflict zone or training site, those intending/preparing to do so as a result of radicalisation, being on their way to a conflict zone/training site or also returnees/killed jihadists).

[4] See also: Implementation reports to the Security Council: S/2015/338, 14 May 2015 and S/2015/683, 2 September 2015; S/2015/975, 29 December 2015

– One Member State requires the **authorization of a special CT prosecutor** to share information with Europol and the SIS II, which leads to delays and which may result in denial of the possibility to share.

– One key issue is still the consistent use of the ECTC at Europol. The Police Working Group on Terrorism (PWGT) which was established by EU Member States in the mid 1970ies[5] as a response to the then terrorist threat, has just prepared the procurement of a separate communication tool at the level of 'EU Secret' which is expected to become operational in Q3 2016, next to SIENA (at the level of 'EU Confidential'). Europol has still to be connected to that network as a full user. In order to maximise the political direction made by the Council regarding a central information sharing through the ECTC, it is therefore advisable that the communication network is integrated into the ECTC at Europol in due course, in particular as the concerned third countries of the PWGT network all have an operational cooperation agreement with Europol. It has been confirmed that the ECTC has offered to host the communication network moving forward.

2. Queries of Europol tools

– Several Member States that have low levels of queries of the EIS are not certain of the added value. While one Member States automatically queries the EIS for organized and serious crime and trafficking, where it was part of the standard operating procedure, this was not done for CT, because there the risk/benefit analysis was quite different: the operational risk of queries is regarded as higher and greater benefits were to be found elsewhere. Other parties nationally and in other Member States would know that a query for a certain name had been made, which could be problematic.

3. Information sharing with Eurojust

– Most Member States questioned the **usefulness (i.e. added value) of systematically transmitting information about investigations and prosecutions to Eurojust**.

[5] Including Iceland, Norway and Switzerland,

– The particular **sensitivity of investigations** was highlighted which made information of Eurojust difficult. However, distinctions between investigations and prosecutions (more advanced stage, public) do not seem to be made with regard to sharing.

4. Interpol

– Member States that do not share or share few FTF with Interpol have **concerns with regard to data protection and human rights** (what may happen to a terrorist suspects in a third country with a less advanced track record on human rights).

ANNEX II

The use of tools available through the ECTC at Europol

1. **Making information available to counter terrorism authorities and front-line investigators – Europol Information System (EIS)**

– Covering Europol's entire mandate, the EIS is designed to make key information on Foreign Terrorist Fighters directly available in EU Member States.

– The EIS is a database for real-time queries by Member States, in order to check data on offenders, convicts and suspected individuals, as well as key information to support investigations (personal data, related objects, places, vehicles, communication means such as phone numbers, email addresses, websites, contacts etc.). Cross-matches are identified directly on insertion of data objects. A hidden hit functionality can be applied in the EIS, allowing the data owner to be notified about searches against the concerned data, while the requesting party is notified about a potential hit (without disclosing the data owner).

– 4,129 foreign travelling terrorist fighters (including supporters) are now shared by 27 contributing parties in the EIS (19 MS, 8 third parties) - of which 1,700 are contributed by EU MS (in May 2015, there were 1,163 entries overall (17 contributing parties overall, 13 MS, 4 third parties), compared to 4,129 now).

– An overall increase of terrorism-related objects in the EIS is noticed: 25% increase noted in May 2016, compared to the status at the end of 2015.

– The range of contributing entities expands, now including also intelligence authorities in some MS, as well as the key third party authorities, for instance, the US Federal Bureau of Investigation (FBI) and the US Department of Homeland Security (DHS).

– The key added value for EU Member States is that Europol, on behalf of third parties, makes relevant data entries on foreign fighters available to all EU Member States through the EIS.

– The SIS II is designed for Member States to share alerts on wanted persons and objects, as well as the exchange of related supplementary information matters, thus, in essence, a tool first line end-users on the field, including border guards, police officers and immigration authorities to identify wanted persons and objects ('for a concrete action', e.g. arrest, check, seize). The EIS and the SIS are complementary to each other and in combination create opportunities to enrich information but they follow different objectives.

2. Cross-matching and analysis sensitive data for counter terrorism authorities

– Focal Point Travellers (FP), established in April 2014, is a dedicated analysis data repository operated by the ECTC at Europol, for in-depth analysis and resulting operational support/coordination.

– The purpose is to share sensitive live information and intelligence for cross-matching and analysis purposes, with a view to identifying new lines of investigation that are communicated and subsequently operationalised at national level by all relevant (including border control) authorities. Member States and associated law enforcement authorities of third parties feed FP Travellers which compiles information and intelligence on individuals, associates and contacts (logistical and financial support networks), in relation to travel activities across international borders to terrorist hotspots (e.g. conflict zones and training venues), in order to engage in terrorist activities, thus posing in particular a threat to the security of Member States upon their eventual return to the EU.

– 25,353 person entities overall (in May 2015, 6,044 person entities).

– 5,769 verified foreign travelling fighters (from the overall number of person entities), which includes 3,303 fighters contributed by EU Member States (in May 2015, 1,789 overall foreign travelling fighters were noted, 1,522 by EU Member States).

– Given that sensitive information and intelligence is shared, access is limited to Europol staff and representatives of Member States, in the latter case, through an index function which preserves data ownership and access to information in a controlled environment. Beyond Focal Point (FP) Travellers, FP Hydra compiles data on Islamic religiously inspired terrorist (support) activities.