Council of the European Union

Brussels, 7 June 2016
(OR. en)

9795/16

LIMITE

JAI 519
COSI 95
FRONT 237
ASIM 85
DAPIX 92
ENFOPOL 174
SIRIS 95
DATAPROTECT 60
VISA 190
FAUXDOC 24
COPEN 186

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Permanent Representatives Committee/Council
No. prev. doc.:	9201/16
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 of identifying lessons learned and supporting continuous improvement. Full implementation of the roadmap, in particular the actions contained in the CT Action Plan, will be important moving forward.

[1] Doc. 9368/1/16 REV 1

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. Various IT improvements could enhance efficiency, speed and interoperability, e.g. common data exchange standards as a prerequisite of interoperability, a single search interface, and the use of semi or fully automated data loaders allowing the insertion of bulk data. There is a need to explore how to make the most of these developments, as indicated in the Communication on Stronger and Smarter Information Systems and the Presidency Roadmap. The High Level Expert Group could come up with proposals for interoperability solutions to close 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 the Member States most affected by the phenomenon of foreign fighters. It sets out examples of the operational added value of Europol and Eurojust, a number of recommendations, and questions for discussion.

Annex I sets out good practices and areas for further improvement identified by Member States. In Annex II, the potential use of the various Europol tools is explained. In addition, several Member States that have made strong political commitments and engaged particular operational efforts to use EU-level tools for information sharing describe their good practices (Annex III).

Sharing information to counter terrorism is high on Member States' political agendas. This is also reflected at operational level by the significant increase in information exchanged via the different mechanisms over the last year. Moreover, a number of Ministers of the Interior have become personally involved in boosting their Member States' 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 to support operational success.

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

However, the use of EU systems, tools and services by Member State services varies greatly. Some, including those who have recently received support from Europol in the aftermath of attacks, report great operational benefit from using the tools systematically. Others remain unconvinced of the operational benefit Europol provides, 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 have been identified as requiring political guidance from ministers:

1. Generally, consultations have shown that successful improvement in the use of Europol and Eurojust tools depends heavily on political will and/or recognition of operational added value by the relevant services/investigators rather than on financial or technical constraints. Good cooperation between 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: 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 shared, the more operational value cooperation with Europol tends to have. Initially, it can be a leap of faith.

Based on the success stories provided by Europol and Eurojust in 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. Member States which do not have experienced that cooperation through Europol adds value for CT are also invited to share their experiences.

Given that the endorsement of the Roadmap expresses the political commitment to share all relevant information unless there are legal or operational reasons not to do so, can Ministers agree to take the necessary measures to translate this political guidance into the necessary procedures and IT tools and to encourage services to share more systematically with Europol and engage more with Europol on CT?

How best could Europol help Member States in the area of CT? Europol has offered to hold an operational workshop at its headquarters, in order to demonstrate with practical case examples how all relevant Member State services can exploit the tools of the ECTC.

2. Ministers are invited to comment on the proposed recommendations.

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

At the core of the political and operational decisions about feeding and using 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 significantly increased its 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 for CT. As a first step, a few examples are set out below:

1. Europol

Information sharing in the area of counter-terrorism is advancing significantly in both quantity and quality, requiring continuous commitment by all stakeholders in order to keep pace with the terrorist threat. Now that all Member States are connected to the counter-terrorism space in SIENA, the function of the ECTC as a hub for exchanging information, conducting analysis and coordinating 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 addressing 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 (in 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. Joint Investigation Team (JIT) 'Vendredi', in which France, Belgium, Europol and Eurojust participate, was set up through Eurojust. In the follow-up to the Brussels attacks, the ECTC served as a support platform for the counter-terrorism authorities concerned 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 Taskforce Fraternité by the investigative authorities.

– Phone data analysis in connection with the Paris terror attacks.

– Financial investigations: 24 428 intelligence leads have been provided by the TFTP since 2010, of which 17 500 were generated in 2015 and 2016 (up to May 2016). A significant amount of exchanges within TFTP concern travelling fighters (Syria/Iraq/IS): 8 251 leads (34% of the total) are specific to this phenomenon (of relevance to 27 EU MS). In addition, more than 3 000 money transfer leads were established by Fraternité with the support of US authorities (US Immigrations and Customs Enforcement (ICE)).

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

– Analysis in connection with the geographical whereabouts of the Paris terrorists prior to the attacks, especially in two Member States, resulting in further investigative leads (locations, contacts and possible facilitators). Operational analysis of a list of individuals suspected to have used the same travel routes as the Paris attackers, generating leads including financial intelligence on 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 the 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, who was arrested as part of a case against the 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 Lesbos, Chios, Samos and Leros) to help coordinate investigations regarding migrant smuggling and trafficking in human beings in support of the national authorities, and to carry out secondary security checks (on the islands) as reaffirmed 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. The work performed to date has turned up a total of 70 hits against Europol databases. Four 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 the arrest of a terror suspect in France, analysis was carried out 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 terror cell in question, 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, the identification of links, through JIT 'Vendredi', to an ongoing investigation into a network involved in the facilitation of illegal immigration in one Member State, 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 for 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 theft, robbery, etc.): all six of the Brussels attackers and six of the ten perpetrators of the Paris attacks in November 2015 had a background in organised or other crime.

– The Joint Liaison Team (JLT) is key to effectively addressing the wider European and international dimensions of the current terrorist threat affecting EU Member States. Germany acts as the driving force behind 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 better compliance with the obligations stemming from Council Decision 2005/671/JHA on the exchange of information on terrorist offences. As well as information on convictions, Member States should provide Eurojust, in a timely and systematic manner, with information on all prosecutions, links with other relevant cases, and 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 Council Decision 2005/671/JHA.

Eurojust also calls for 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.

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

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

2. It would allow Member States' competent authorities to regularly receive **enriched Eurojust analyses of the judicial responses to terrorism** based on prosecutions and convictions for terrorist offences (via the *Terrorism Convictions Monitor*, *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 examples, consult the **challenges and best practice** identified in different Member States <u>for terrorist prosecutions and convictions</u>, 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 for identifying similarities with a case under trial in another Member State. Furthermore, Eurojust has been consulted in a couple of cases in which 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 ways is a crime. It has highlighted the fact 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 has 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 examined the origins of the group and the degree to which it met the criteria defining a terrorist group as set out by national law, and 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 where FTFs joined such groups.

– Eurojust has 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 a conflict zone or while preparing to leave. Depending on national laws, the scope of acts constituting a terrorist offence may vary.

– Eurojust has 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 judgments shows that courts in the Member States do not appear to be facing major challenges in addressing that issue.

– Eurojust has highlighted certain arguments of the courts on procedural issues, emphasising, for example, differences between the legal systems of the Member States as regards rendering judgements *in absentia* in FTF cases, placing aspiring FTFs in psychiatric institutions, and defining an approach to juvenile FTFs.

– Following up on 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 in 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 FTFs.

– existing national practices and the lessons learnt from them, in particular the risk assessment tools for assessing the level of threat posed by FTFs and returnees, rehabilitation programmes 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 will be particularly important until ECRIS is further developed in order to support information on convictions of third-country nationals.

   Member States are encouraged to involve Eurojust at an early stage of investigations and prosecutions and, in particular, to make use of Eurojust's coordination meetings and 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 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 a radical Islamist terrorist group in a complex cross-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 for 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 at Eurojust, at which all the judicial and practical issues to be addressed were identified. 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 the 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 by 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 initiate their engagement as a test, to see the outcomes for themselves. Unprecedented levels of information (of over 16.7 TB) have been shared with 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 have reported that information is handled well by Europol, in compliance with handling codes and the protection of information, with no reported examples of data security breaches. This has also been confirmed by EU-US reviews of Europol's implementation of the EU-US TFTP Agreement.

3. The November Conclusions of the JHA Council on counter-terrorism include the setting up of the ECTC and the political commitment of Member States to make maximum use of these capabilities to improve the overall level of information exchange between CT authorities in the EU. This, as well as the interoperability agenda, call for harmonization of information sources. Resulting from this, it is important that in the future Europol is in a position to provide information sharing support to the **communication network of EU law enforcement authorities in the Police Working Group on Terrorism (PWGT)**[3] (level 'EU Secret'), in the same manner as this has happened concerning other law enforcement information related exchange initiatives (such as FIU.net which has been gradually integrated into Europol).

[3] Including Iceland, Norway and Switzerland

Europol and the German Federal Criminal Police (BKA) which is in the lead of the development of the new PWGT system are working on a joint proposal in this context, with a view to maximising the support the ECTC can offer to the PWGT network.

4. **High-quality analytical 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 by 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 for counter-terrorism purposes, it may be useful to carry out 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 could serve as a best practice example. Europol is available to help Member States identify the best solution for data feeding. It would be useful to further discuss this at expert level.

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 the different data types, ensuring both robust security and handling controls for the data across relevant FPs and other applications. The underlying maxim is to provide information (with handling codes) once only, with data processing being based on conditions set by the data owner.

8. The reference document with criteria to be developed according to the Presidency Roadmap (action 17) to create a **common understanding** will be helpful in ensuring a wide range of information sharing on FTFs.

9. The Paris and Brussels attacks have shown an increasing relationship between serious and organized crime and terrorism. At European level opportunities for better addressing the terrorism/crime nexus are increasing considering the overall volume of organised crime-related information in the analysis repository of Europol with over 27.5 million data entities, the rapid development of the ECTC and of the CTG platform. A fact finding visit of the CTG (platform) to the ECTC is forthcoming to explore options for further modalities of interaction.

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, the dissemination of their results and, where appropriate, hosting the tools developed by these projects for testing by the Member States.

ANNEX I

Good practices and areas for further improvement identified by Member States

I. GOOD PRACTICES IDENTIFIED BY 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 is regularly involved, reviewing progress and tasking his administration to address obstacles. The importance for the operational services of seeing added value was also highlighted as a basis for engagement.

A number of good practices can be identified by Member States which contribute a lot to Europol databases:

Step-by-step approach

– Some Member States have **taken the political decision to intensify their work with Europol more recently,** in particular the feeding of CT databases, 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 recently took the decision 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 increase) feeding of FP Traveller later on.

Inter-agency cooperation

– One Member State is currently assessing options on 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 the 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. It establishes a consolidated list of FTFs, 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 also a police service, files are shared with Europol directly (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 demonstrates 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 by the police (sometimes based on information received from the security service), it is shared with Europol.

– Another Member State has meetings every two weeks between the security, police and justice services to review files. As soon as there are enough elements to show that a person is engaged in criminal conduct, the security service gives a file to the police and then shares it with Europol. These file reports are created in such a way as to protect sources and methods, hence no sharing concerns are raised 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 makes joint work on targets by the various services possible. Only information about identified persons is shared with Europol, not those whose 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 the necessary legal and organisational measures are taken so that the Member State can start feeding the Focal Point.

Moment of sharing

– Information not shared with Europol by the Member States that feed the systems a lot are unidentified persons and persons under early surveillance who 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. This means that, for Member States that share with Europol as soon as a person's conduct constitutes a terrorist crime, the rate of sharing is very high and more or less reflects those Member States' FTF figures.

– The political decision to share with Europol needs to be supported by **procedures**, so that sharing is embedded into the police officers' regular routine. One Member State is translating its political willingness to work with the European databases into an effort to **systematise and automatise the IT** involved, in addition to the **human investment** which remains necessary. Standardised procedures for information sharing are needed for improved effectiveness. In this regard, **training officers** to feed and use the databases and an **efficient system for authorisation and control of access to databases** are regarded as important.

– The importance of **sharing and analysing high-quality information** has been highlighted: it is regarded as more useful to share fully developed files on individuals than simply to give raw data to Europol. This may mean a lower quantity of data, but higher quality.

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

2. Queries of Europol tools

– Querying the EIS and the TFTP is frequent when the **operational added value is recognised** by the Member State. The TFTP is regarded by some Member States as very valuable as it produces lots of leads which are useful for further analysis and includes the benefits of the US system. For other Member States, following 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 in 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 whose prosecutor shares information about all ongoing CT investigations and prosecutions with Eurojust does so because of the **political decision** to do so and the fact that the procedures and information exchange channel are in place: the **TESTA NG network is used as secure channel**.

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

4. Interpol

– Member States which share a lot of FTFs with Interpol have an efficient way of using the **Interpol fusion system** (whereby they can control which other States receive the information) to avoid operational data protection and other human rights concerns.

– There are very high figures for **SLTD checks at external borders** when carried out **systematically for all external border crossings**, but far fewer when they are carried out based on common risk indicators. However, one Member State which relies on common risk indicators also uses Advanced Passenger Information (API).

II. AREAS FOR FURTHER IMPROVEMENT IDENTIFIED BY MEMBER STATES

1. Contributions to Europol in CT

– **Some Member States which have not recognised the added value of working with Europol on CT** (be it with 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 working with other security services within the Counter-Terrorism Group (CTG), where the classification level is higher (mostly at 'secret' level but also above). It is therefore being argued that there is no need to change a system that works well (e.g. through the CTG) and creates results. Only sharing within the context of the CTG is regarded as problematic when the security service of the other Member State which receives the information does not share it with the police.

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

– One Member State is very much convinced of the added value of Europol in organised crime and is among the most active contributing and using it in that area but is of the view that Europol has not made the case for its usefulness in CT.

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

– Several Member States also asked **why they needed to contribute data to several systems** (such as EIS, FP Travellers and FP Hydra) instead of having Europol connect the dots and enter the data where necessary (a process which is impaired by Europol's current legal framework, which does not allow it 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 recently taken 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 reported that only confirmed FTFs were shared with FP Traveller, but that all others (facilitators, etc.) were shared with **FP Hydra**. Therefore, the figures could be misleading, as the Member State shared all the information on FTFs in the hands of the criminal police with Europol as soon as the personal files were verified. This raised the question of how information from the two Focal Points was cross-matched by Europol.

– A definition**, or at least a common understanding of FTFs** is lacking for the various databases, so it may not be clear at national level what category of persons should be added (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 of the 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 UN Security Council Resolution 2178 (2014)[4] on foreign terrorist fighters, in combination with national specific arrangements (thus covering the entire cycle: fighters currently in a conflict zone or on a training site, those intending/preparing to leave as a result of radicalisation, those on their way to a conflict zone/training site and 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 **authorisation of a special CT prosecutor** to share information with Europol and the SIS II, which leads to delays and may result in denial of the possibility to share.

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 State automatically queries the EIS for organised 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 was 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**.

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

4. Interpol

– Member States that do not share or share few FTFs with Interpol are **concerned about data protection and human rights** (what may happen to 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 to EU Member States.

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

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

– An overall increase in terrorism-related objects in the EIS has been observed: a 25% increase was noted in May 2016, compared to the status at the end of 2015.

– The range of contributing entities is expanding, now also including the 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 to exchange related supplementary information. It is therefore essentially a tool that allows 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 complement one another and, when combined, create opportunities to enrich information, but they follow different objectives.

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

– Focal Point (FP) Travellers, established in April 2014, is a dedicated data repository operated by the ECTC at Europol, for in-depth analysis and the 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 the relevant authorities (including border control). Member States and the 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 across international borders to terrorist hotspots (e.g. conflict zones and training venues) in order to engage in terrorist activities, thus posing a particular threat to the security of Member States upon their eventual return to the EU.

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

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

ANNEX III

Good practices contributed by Member States

Contribution from Germany

In Germany, the security authorities at federal and Land level work together in a Joint Counter-Terrorism Centre (GTAZ) to combat Islamist terrorism.

Within that Centre, a total of 40 German security authorities – in particular the Federal Criminal Police Office and the Land criminal police offices, the Federal and Land offices for the protection of the Constitution, the Federal Police, the Federal Office for Migration and Refugees and the Federal Prosecutor-General – share real-time information in accordance with their respective legal frameworks, making use of all available information sources.

Unless, in exceptional circumstances, there are overriding intelligence-related reasons for not doing so, intelligence is communicated to the police authorities where the facts suggest that sharing such information is necessary in order to prevent or prosecute offences against state security or other serious crimes. Criminal intelligence is communicated to the Federal and Land offices for the protection of the Constitution in particular where there are factual indications of violent extremism and terrorism.

In practice, cooperation at the GTAZ takes place in various working groups at daily briefings, or in briefings on individual cases, where appropriate. In the course of the routine cooperation, intelligence and police information is compared, pooled and acted upon.

As the national central body for the exchange of police information with other countries and the Europol National Unit, the Federal Criminal Police Office communicates all relevant information to Europol directly and without delay. To remedy possible security concerns, the information transmitted is subject to handling restrictions.

The GTAZ has proven its worth for Germany's federal structures. At European level, however, there is a need for a customised model which fits into the existing structures.

Contribution from Belgium

Information sharing between the Belgian authorities and Europol concerning terrorist offences and relating to the participation to an AWF/Focal Point (FP)

In Belgium there is a specific procedure to decide on the participation of a Focal Point (FP). This procedure is described in the Common Circular Letter of the Minister of Justice and the College of Attorneys-General with regard to the international judicial police cooperation of September 2011 (COL 09/2011). Different steps are foreseen in that procedure:

– Creation of a FP advisory commission within the Federal Police: responsible for providing an advice to the Federal Prosecutor and the Attorney-General responsible for international cooperation containing elements on what information will be shared, how, by whom and the feasibility of sharing specific information. This is being described in a national data collection plan also as a part of the abovementioned advice.

– Advice of the Federal Prosecutor and the responsible Attorney - General: if this is a positive advice, this will be regarded as a duty to share information with the relevant FP for all concerned police services. Once this positive advice has been given there is no need any more for the police services to ask permission to the magistrates whether or not information can be shared with the relevant Focal Point.

– In general, the FP expert responsible for the feeding of the FP, will be part of the federal judicial police and will assemble useful contributions from within the Belgian integrated police.

– Next to the specific FP contributions, Belgium is applying already for several years a sharing policy with Europol. This means that SIENA messages are being copied (the local level ("arrondissement") is able to draft SIENA messages - those drafts are formally sent by our National Unit) to Europol and that Europol is given the opportunity to use this information in the relevant Focal Point.

– Belgium's philosophy is to feed the EIS to the maximum extent in order to be able to detect international links so that the FP can be used for proper analysis of ongoing live investigations.

Information sharing between the Belgian judicial authorities and Eurojust concerning terrorist offences

Implementation by Belgium of the obligation to exchange information by virtue of article 2 of Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences

All terrorism cases in Belgium are de facto dealt with by the anti-terrorism division of the federal prosecutor's office.

In accordance with the provisions of Council Framework Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, the Eurojust national correspondent for terrorism matters, i.e. the head of the anti-terrorism division of the federal prosecutor's office, provides the Belgian Eurojust member, in a centralized way, with all relevant information from the federal criminal case files involving terrorism (violation of articles 137 to 141 of the Penal Code), in the context of which:

– an international request for judicial assistance is drafted;

– a European arrest warrant or an international arrest warrant is issued by default;

– there are, from the beginning (initial written record), serious indications of terrorist offences, as referred to in articles 137 to 141 of the Penal Code, which affect or may affect two or more member states of the European Union;

– there are, in the course of the investigation, serious indications of terrorist offences, as referred to in articles 137 to 141 of the Penal Code, which affect or may affect two or more member states of the European Union.

This information is transmitted in a secured automated way (S-Testa), using the template drawn up by Eurojust.

In order to allow for the efficient management of the fact sheets, every fact sheet that is drafted in the context of a case mentions the file reference number of the federal prosecutor's office, followed by 'Eurojust fact sheet', followed by 1 (first fact sheet in the case), 2 (second fact sheet in the case), etc., given the evolving nature of the fact sheets. These will indeed have to be further completed in the light of the further investigation, new identities, the drafting of international requests for legal assistance and European arrest warrants, the resolution of the proceedings, the summons, the judgment, the decision, etc.

It has been agreed with the Belgian Eurojust member that the text of the sixth recital of Council Framework Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences fully applies.

This recital provides as follows:

"In the execution of the exchange of information, this Decision is without prejudice to essential national security interests, and it should not jeopardise the safety of individuals or the success of a current investigation or specific intelligence activities in the field of State security."

In order to draw the attention of the Belgian Eurojust member to this, a special section with the title 'handling codes' will be added to the templates ('Eurojust' fact sheets). In this special section, it should be clearly mentioned whether essential national security interests, current investigations or the safety of individuals are at risk.

This will certainly be the case if the federal criminal investigation on terrorism is put under judicial embargo in Belgium (article 11 of the law of 10 July 2006 concerning threat analysis, article 44/5 of the law of 5 August 1992 on the Police Service and article 44/8 of the law of 5 August 1992 on the Police Service).

The Belgian Eurojust member will observe this handling code in the context of the exchange of the 'Eurojust' fact sheets she receives with Eurojust.

Since August 13th of 2012, the National Correspondent of the terrorism Section of the federal Public Prosecutor's Office has provided 292 filing cards to Eurojust concerning requests of mutual assistance and conviction sentences. This high number of filing cards is obviously caused by the increasing number of files and sentences in relation with the issue of Foreign Terrorist Fighters.

Recent enhanced cooperation between the Belgian judicial authorities and Eurojust concerning terrorist offences

The cooperation of the terrorism Section and Eurojust was further reinforced since Belgium was confronted with the presence of networks preparing or committing attacks on Belgian and European soil. In the wake of the intervention in Verviers, the Paris attacks on 13 November 2015 and the recent assaults in Brussels and Zaventem on 22 March 2016, among other things, intensive contacts were established between the Belgian Judicial Authorities (Examining Judges specialized in terrorism and the Terrorism Section of the Federal Public Prosecutor's Office) and Eurojust, resulting in the handing over of several urgent requests of mutual judicial assistance to the European colleagues through Eurojust.

Eurojust is moreover the technical expert in several terrorism files, quote in evidence thereof the recent Joint Investigation Team constituted between Belgium and France in the aftermath of the Paris attacks of 13 November 2015.

The cooperation has recently further been stepped up:

– In response to various anti-terror operations carried out in the aftermath of the Zaventem and Brussels assaults, intercession by Eurojust in real time established contacts between Magistrates and Police services with a view to exchanging operational information having an immediate impact on the current operations.

– The Federal Public Prosecutor's Office, finally, deemed it useful and appropriate to invite the Belgian member of Eurojust to assist the coordination meetings in the wake of the 22 March 2016 attacks with a view to efficaciously exchanging information about the current judicial inquiry and, more specifically, about the links to other European countries.

Contribution from The Netherlands

On Counter Terrorism (CT) in The Netherlands the national CT coordinator, the national police, the prosecutor's office and both intelligence and security services, the civil AIVD and military MIVD are the main actors. Via official reports of the AIVD (or MIVD) to the national prosecutor on CT, the prosecutor's office can start a criminal investigation executed by the police. The legal basis for these reports is the national law on the intelligence and security services.

This practice of official reporting by the AIVD is in place already for decades, the system is refined as a result of (the nature of) the current terrorist threat: The amount of targets increased dramatically in the last couple of years. Every 2 weeks, when necessary ad hoc, there is a meeting of the national prosecutor(s) on CT (president), the AIVD and the national police to exchange information on CT investigations. Via the aforementioned practice of reporting, information on targets can officially be transferred from the AIVD to the police. Targets can become suspects in the legal sense, meeting the criteria set by the Netherlands (criminal) law. These people have to be identified of course (on a lot of targets nowadays only identifiers such phone number, IP address, account on social media are known).

Via the usual way (HENU channel) dossiers on suspects handled by the prosecutor on CT/police can be notified to Europol. This is done regularly, The Netherlands has brought more dossiers under the attention of Europol than the number of the people that left The Netherlands for Syria or Iraq.

Secondly the so-called CT-infobox in the Netherlands is an important tool to combat terrorism, in place already for more than 10 years and improved over the years. Trust increased amongst partners. All important operational actors that are able to contribute to CT, e.g. the Financial Intelligence Unit and the Immigration and Naturalization Service, are in the box. The basic idea behind the box is sharing information on cases/targets as well as establishing the most effective way to act when necessary (by the partner or the network of the partner that is best placed or best equipped to do so). Action can vary from disruption by the AIVD or arrest by the police to financial actions or using national alien's laws etc. Multidisciplinary expertise and analyses is available on one location, the premises of the AIVD.

Access to all relevant data and information is available: access to more than 100 databases. Every partner has its own digital connection to his own organization, nowadays it is possible to work on dossiers in the box via the internal ICT-network in the box. The sharing of information by partners is done under the guarantee of ownership of information. Nothing leaves the box without the approval of the owners of the information. The cooperation - typically Dutch - is based on equality, though some partners of course are more important than others in CT investigations. The competences and responsibility of each partner are being recognized, no transfer of respective responsibilities to the box. Located in the building of the AIVD the box provides for a secure environment to store classified data. The CT infobox is a flexible organization with the ability to respond to new developments.