Council of the European Union

Brussels, 14 April 2016
(OR. en)

7726/16

LIMITE

JAI 266
COSI 55
FRONT 170
ASIM 52
DAPIX 51
ENFOPOL 93
SIRIS 65
DATAPROTECT 25
VISA 95
FAUXDOC 12
COPEN 101

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Council
Subject:	Systematic feeding and consistent use of European and international Databases - information sharing in the counter-terrorism context

EU Heads of State or Government and the JHA Council have called repeatedly for strengthening information sharing and maximum use of EU tools in this context. While this is a political priority and while some progress has been made, the current implementation at Member State level remains uneven and information sharing still does not reflect the threat.

This paper sets out a number of issues to focus the discussion at the JHA Council.

1. Feeding of the EU databases and exchange of information

Europol

There are still significant gaps with regard to feeding **Europol**: As per 11 April 2016, Europol's **Focal Point Travellers** database still contained only 2,956 verified foreign terrorist fighters (FTF) entered by EU Member States (overall FTF number, including third parties: 5,353). The **European Information System** (EIS) contained only 1,615 FTF entered by Member States (overall FTF number in EIS, including contributions from third parties: 4,044). This despite well-founded estimates that around 5,000 EU citizens have travelled to Syria and Iraq to join DAESH and other extremist groups. It should also be noted that more than 90% of the contributions by Member States regarding verified FTFs in FP Travellers in 2015 originate from just 5 Member States. (By contrast, at least three quarters of Member States put alerts on FTFs in SIS.) To date, since the TFTP Agreement came into force, more than 22,000 intelligence leads have been provided by the TFTP. This includes a significant amount of exchanges within TFTP concerning travelling fighters (Syria/Iraq/IS), leading to 5,416 leads specific to this phenomenon (of relevance to 27 Member States).

The SIENA system will be updated to confidential in Q 3, the information sharing network of the police working group on terrorism (PWGT level secret) will be integrated into Europol. Cooperation through Europol allows establishing matches and subsequent sharing of information with full data ownership control (handling codes for contributed information).

The need to feed Europol with full data on FTFs is all the more compelling in the light of the evolving criminalization of terrorist behaviour. It covers the preparatory phases and membership in a terrorist group, preparing travel to a conflict zone as well as the early stages of behaviour and preparation. As the recent attacks indicate, a number of the terrorist suspects involved have a criminal past and criminal networks are used for procurement of weapons and false documents and other logistical support. All this calls for the strongest possible involvement of Europol and cross-matching with information available at Europol on other types of criminality, such as on firearms and drugs. It also calls for a better compliance of the Member States 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, on drug trafficking, illegal immigrant smuggling, cybercrime, and other serious crimes, to allow the identification of links with terrorism cases and, where appropriate, detection of criminal networks.

In this context it could be worth while to have an exercise in each Member State to look at how security services share information with law enforcement nationally and how this can then be shared with Europol.

It would be interesting to learn from the 5 Member States contributing most to FP Travellers (re verified travelling fighters): What are the national procedures, decisions and instructions in place that allow the effective contribution to Europol? How have obstacles been overcome? What are the experiences with sharing comprehensively with Europol? Are there good practices of effective operational cooperation between security services and law enforcement in Member States, of secondments from the security services to the national Liaison Bureaux at Europol or in the Europol national unit in the home country or of the connection of the security service to SIENA?

SIS II

While there has been a substantial increase in 2015 in the number of FTF alerts in SIS II, not all FTFs are systematically entered into the **SIS II** or the information is not complete. It is up to Member States at national level tackle this including by removing obstacles for security services to enter information into the SIS II and to get access to the database. An efficient way of course are effective digital connections on operational level but also may be a secondment into the SIRENE bureau which would then allow full access to the service for cross-checking and which may facilitate feeding the database.

Interpol's SLTD and FTF databases

Feeding the **Interpol's Stolen and Lost Travel Documents (SLTD) and FTF databases** also remains uneven, some Member States don't have automatic uploading functions for the SLTD, for example. The diffusion mechanism (FTF names only shared with countries indicated by the MS) can address concerns that may exist about notices.

Eurojust

There is little justification why information about all prosecutions, convictions, links with other relevant cases, as well as requests for judicial assistance, including letters rogatory and European Arrest Warrants, and the relevant responses are not being transmitted to Eurojust in a timely and systematic manner, as legally required by Council Decision 2005/671/JHA.

FADO

Feeding the Expert FADO (False and Authentic Documents Online) data base likewise needs to be improved.

Member States are invited to indicate:

– *what is being done at national level to ensure systematic feeding of the EIS, SIS II, Interpol databases, FADO and to comply with the Eurojust information sharing legislation, in particular with regard to instructions and procedures;*

– *what is being done at national level to address the obstacles to systematic feeding of the SIS II*

– *with regard to the 5 Member States contributing most to FP Traveller: which are the national procedures, decisions and instructions in place that allow the effective contribution to Europol.*

– *how the (23) Member States that contribute less to FP Traveller intend to increase their contributions, of course recognizing the FTF-phenomena varies per Member State.*

2. Use of the EU tools and analysis of the information

It is very much welcome that France and Belgium have asked **Europol** and **Eurojust** to support the investigations after the Paris and Brussels attacks (November 2015 and March 2016). This allows to identify links to other Member States and to cross-check with information and expertise available at Europol. It also allows the coordination of investigations and prosecutions with support from Eurojust. It is welcome that the Commission has amended the budget to include the posts asked by Europol to support the ECTC and Task Force Fraternité, it is now important for the budgetary authority to approve this. On the way forward, further resources for the ECTC should be considered, based on the continuous assessment of the terrorist threat, data sharing and resulting analysis needs.

The Paris and Brussels attacks seem to indicate that some if not most of the attackers were known to the police, some as criminals, some as a former generation of jihadis, some FTFs, there also seem to be links to several other Member States. This shows the importance not only of feeding the data, but also the importance of quality of data on one hand and of assessing threats individual targets pose, based on proper analysis, on the other hand. After the Brussels attacks, Ministers decided to put in place at Europol a Joint Liaison Team (JLT) to analyse the networks across Europe with a view to identifying new lines of investigation. To date, six Member States have provided an expert and two other Member States and three third countries have committed to do so. In total, Europol estimates that it is necessary, as an immediate measure, to have a team of 10 to 12 full time counter-terrorism expert staff drawn from the Member States most affected by the current threat and therefore with the strongest related investigative links from on-going operational activities. The other Member States should have a dedicated counter terrorism expert in the respective Liaison Bureau at Europol to support the functioning of the JLT as required.

It is also welcome that Joint Investigation Teams (JITs) have been established after the attacks in France and Belgium as well as in other recent terrorism cases. In November 2015, the first coordination center on CT at Eurojust took place, leading to several arrests in several MS.

However, the possibilities for Eurojust's legal, operational and financial support in the setting up and functioning of JITS and the use of Eurojust's coordination meetings and coordination centres to exchange information and discuss investigation and prosecution strategies, as well as requests to the Terrorist Financing Tracking Programme remain heavily underused.

Common analysis Europol – EU INTCEN, especially the CT-unit within INTCEN, of the Paris and Brussels attacks including lessons learned could also be of help. One of these lessons is that, while all the perpetrators were all subject of a SIS alert, sufficient information had not been inserted in the alert and therefore it was not shown in SIS that the person was wanted for terrorism. This could be dealt with by making it obligatory to specify "terrorism related activity" in the alert. Now it is not mandatory. Another problem was that the persons were traveling under a false identity and SIS could not capture them on the basis of an alphanumeric search. The SIS AFIS, announced in the recent Commission Communication, will solve such problems.

Member States are invited to indicate

– *their intention to provide an expert to Europol's JLT*

– *What would need to happen for Europol and Eurojust operational tools to be truly mainstreamed into counter-terrorism work by Member States?*

– *their willingness to actively contribute to an INTCEN/Europol lessons learned exercise after the Paris and Brussels attacks.*

3. Consultation of databases

There is a variety of quantitative use of systems/checks in systems by Member States.

In November 2015, the Council highlighted the importance of border security in the CT context. However, progress is mixed. There are still Member States that don't have electronic connection to the SLTD at external border crossing points, which does not allow systematic checks of the SLTD database at external borders, although systematic checks of the validity of travel documents of all travelers is obligatory under the Schengen Border Code of 2006 and the November Council had requested that such systematic checks be done by the end of March 2016. The targeted amendment of the Schengen Borders Code will require systematic checks of databases of all travelers at external borders.

Systematic checks of the SIS II and Interpol databases are carried out for each irregular migrant arriving in the Greek hotspots. In Italian hotspots, they take place on the basis of risk profiles, although systematic checks are obligatory under the Schengen Border Code.

Europol still needs 50 secondments for the second line checks in the hotspots, with, according to current estimates, an overall pool of at least 150 officers to be available for deployment in order to ensure rotation. Administrative arrangements to prepare the secondment of staff from Member States are currently being finalized with the involvement of the Europol Management Board.

Member States could use the Advance Passenger Information ("API, Directive 2004/82) much more intensely and systematically and check all the passenger information against the relevant EU and Interpol databases before arrival.

iFADO should in principle be available at all external border crossing points, at all visa issuing consulates and where appropriate at other authorities relevant to counter terrorism. It should be ensured that the relevant authorities are also made aware of the potential benefits of actually consulting the system.

Member States are invited to indicate what is being done at national level to address compliance with these commitments.