Council of the European Union

Brussels, 11 July 2017
(OR. en)

10880/17

LIMITE

CT 68
ENFOPOL 342
COTER 59
JAI 654
COSI 163

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Strengthening military, law enforcement and judicial information exchange in counter-terrorism

As a follow up to the Joint Home Affairs and Defence Council Lunch on 18 May 2017, the EU Counter-Terrorism Coordinator was invited to present proposals on strengthening military and law enforcement information exchange in counter-terrorism to the July TWP/COTER meeting in view of discussion of PSC/COSI in September 2017 (cf. COREU CFSP/SEC/0288/17).

According to the European Council conclusions of 22-23 June 2017 "*We need to accelerate our collective efforts to share knowledge on foreign terrorist fighters … and take forward policy and legal measures to manage the threat*".

The issue of foreign terrorist fighters was also addressed in the conclusions of the Foreign Affairs Council of 19 June 2017, which emphasized among other things the role of Europol, Eurojust and Interpol, and which stated: "*Without prejudice to Member States' sole responsibility for national security the Council welcomes ongoing efforts to strengthen EU action on counter-terrorism by enhancing law enforcement and military cooperation, within a rule-based order, including through exchange of information among relevant national actors, which form a key part of the rule-of-law response. The Council stresses the importance of supporting Interpol, by sharing appropriate information where appropriate and legally possible…*"

The note does not cover issues related to information sharing between CSDP operations and JHA actors in CT, as this will be covered separately by the EEAS. Not all information shared between CSDP operations and JHA actors will be battlefield information.

The discussion in COTER/TWP is meant to prepare the discussion in COSI/PSC on 26 September 2017 and will guide further work over the summer. The issues should also be discussed by the Military Committee.

Quick wins: priorities

This note focuses on measures that could be put in place quickly to improve access to battlefield information of European law enforcement, judicial and border authorities, in particular in view of investigation and prosecution of FTF returnees from Syria, Iraq and Libya and border checks. As returning FTFs are an immediate threat to the EU, urgent and concerted action is required. In essence, all activities should aim at ensuring that information which is collected on the battlefield reaches law enforcement, judicial, border and any other affected competent authorities of Member States in a timely manner.

1. Quick wins, priorities which could make a significant difference immediately:

- revival of INTERPOL/VENNLIG in Iraq with active participation of the EU Member States present on the ground
- deployment of Europol to the law enforcement part of Operation Gallant Phoenix in the context of the anti-ISIL coalition

2. Additional measures which could add value in the short term

- revival of the INTERPOL/HAMAH project in Afghanistan with active participation of the EU Member States present on the ground
- increased use of INTERPOL Black, Blue and Purple Notices
- Europol access to the Secure Real-Time Platform (SRTP) of the US Department of Homeland Security

– Europol access to NATO's Biometric Enhanced Watch list and Network analysis information

– increased use of the evidence collected by Commission for International Justice and Accountability (CIJA)

– ensure collection and preservation of forensic evidence from the (improvised explosive devices) IEDs in Iraq

– access of Europol and Eurojust to evidence collected by the International Criminal Court (ICC)

– Eurojust mapping of challenges and best practice in using information collected by military for investigations and prosecutions.

3. In the medium term, the following measures would be useful

– capacity building in Iraq in view of collection of battlefield information and sharing with INTERPOL (to ensure sustainability of VENNLIG after departure of the international coalition).

With regard to the Member States, what could have the greatest impact would be the decision to use battlefield information to the greatest possible extent for law enforcement. This would include avoidance of over-classification and systematic sharing with Europol and INTERPOL, and putting in place the relevant procedures, similar to what the US has done since 9/11, especially in Iraq, but also other conflict zones such as in Afghanistan. It would be important to discuss potential challenges.

The suggestions are set out in greater detail in ST 10880/17 ADD 1.

Importance of sharing battlefield information

Battlefield information is of significant value to support operational or tactical analysis, related investigations, as well as the ordering of coercive or surveillance measures (e.g. the interception of telecommunications) or measures taken by border guards. Although battlefield information, due to the nature and circumstances of its sourcing and collection, may not always be admissible as evidence in criminal proceedings before a court of law competent for prosecution, battlefield information should be exploited for law enforcement purposes as much as possible.

Against this background, battlefield information which is particularly relevant for investigations and prosecutions includes data collected from FTFs' cell phones, documents (such as Daesh sign-up sheets, forms/questionnaires or passports, lists of FTF), files contained on FTFs' computers found in house searches after liberation from Daesh as well as forensic information (such as fingerprints recovered from explosives devices or documents in Daesh controlled territory or fingerprints or DNA of deceased or captured foreign terrorist fighters).

Key to an efficient and prompt sharing of battlefield information with law enforcement and, subsequently, judicial authorities where applicable, is to ensure a classification level regarding the collected data which allows the information to be used for law enforcement purposes. What is not always self-evident for those in possession of this information but absolutely necessary is to ensure that those with a “need to know” are able to have access to relevant information, while determining at the same time whether and to which extent the corresponding information can be used for subsequent judicial proceedings or as evidence in court. In addition, sharing with law enforcement would allow the military to indicate objectives important to them. Battlefield information can serve to identify the FTFs and returnees, to learn more about the networks sending fighters to combat areas or to develop cases for prosecution etc.

It is important to ensure horizontal information sharing across the military, law enforcement and judicial authorities, with the appropriate level of access, which will allow the military to protect data that require heightened protection but at the same time enhance the situational awareness of those agencies engaged in efforts to degrade the networks: an intended effect of the military of Member States or allies sharing data from the battlefield with law enforcement agencies is to enable to target the same network from the "point of origin" (i.e. city or town of origin, sources of financing for travel to conflict zones, the routes selected to evade border control measures). Such a unity of effort of law enforcement, the judiciary and the military would make it more difficult for the terrorist networks to access the battlefield. Hence, the efforts of law enforcement and judicial authorities to dismantle FTF networks can contribute to prevent FTFs from travelling and to arrest them upon return, not only protecting the security of EU Member States, but also amounting to a "force protection issue", which is very relevant and important to the military on the ground. It is also important to ensure effective international judicial cooperation and the systematic and timely transmission of information on prosecutions and convictions to Eurojust.[1]

Law enforcement authorities can protect information. As an example, Article 19 of the Europol Regulation[2] gives the provider of information to Europol the right to determine the modalities of access and transfer of information to other parties. Europol's information handling codes therefore ensure a controlled and predictable handling of information, with a view to respecting the needs of the data owner. For instance, by applying a dedicated handling code, the provider may determine, at the moment when supplying information, approval by the data owner prior to disclosing information in judicial proceedings or to any other third party. This mechanism - which has been an integral part of Europol's working processes from its beginning - ensures that Europol can process information for analysis purposes in line with its mandate under the Europol Regulation.

---

1 Based on Council Decision 2005/671/JHA.

2 REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA,

Battlefield information could be used, if national legal systems permit, as evidence for both terrorism and/or core international crimes. Europol's new war crimes' responsibility and Eurojust and the European Network of contact points in respect of persons responsible for genocide, crimes against humanity and war crimes (the Genocide network) could be associated to the further development of a number of these measures.

Europol and Eurojust war crimes contributions

An initiative to establish a related Europol Analysis Project (AP) on Core International Crimes (CIC) was launched in February 2017, with strong support from the respective competent authorities in Germany and the Netherlands. Meanwhile, the Heads of Europol National Units (ENUs) have expressed their support, with eight Member States having indicated their readiness to take a leading role. An opening order for the AP CIC is under preparation at Europol. Battlefield information could be of interest to law enforcement stakeholders who investigate and prosecute perpetrators of war crimes (genocide, crimes against humanity and war crimes). Depending on the start of the AP CIC, an assessment of the required resources should be conducted.

Eurojust and the Genocide Network could be asked to identify challenges and best practice in using information collected by the military as evidence in criminal proceedings and/or as the basis for opening criminal investigations or prosecutions, as well as for ordering coercive and surveillance measures (such as the interception of a suspect's telecommunications). This should be done in consultation with specialised prosecutors in countering terrorism and core international crimes, Already in 2016, Eurojust started mapping the practices of the Member States in using intelligence as evidence in criminal proceedings which raise similar issues.

Delegations are invited to :

- ✓ *provide information on who has the authority over the classification process/classification level of information collected on the battlefield*

- ✓ *share the practices that are followed for sharing and exploiting of information collected by the national armed forces on the battlefield; describe the current procedures in place and give examples for law enforcement/military information sharing at national level (for example through involvement of military police or gendarmerie type services) and internationally; national examples of use of the "law enforcement sensitive" or something similar, which could pave the way for a closer cooperation;*

- ✓ *indicate whether, if present on the ground in Syria/Iraq or Afghanistan, participation in the revival of Vennlig / Hamah would be an option, including potential challenges*

- ✓ *indicate which of the suggested avenues they consider as most viable to ensure that battlefield evidence be made available to law enforcement and which actions should be taken forward as a priority.*