



Brussels, 11 July 2017
(OR. en)

10880/17
ADD 1

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

1. Measures in the context of the anti-ISIS coalition

The anti-ISIL coalition has highlighted the importance of sharing of battlefield information and evidence via law enforcement channels: "*Coalition members are actively disrupting ISIS networks that move individuals, material and funds to enable external attacks. Information sharing, enhanced traveller screening and law enforcement cooperation – including collection of evidence admissible in courts of law – are essential to this effort, as is the ability to prosecute and penalize foreign terrorist fighters and others providing material support to ISIS. We encourage information sharing through INTERPOL and other collective law enforcement channels, such as EUROPOL, as well as through financial intelligence unit (FIU) channels.*"¹

It is urgent now to operationalize this in practice.

¹ Statement by Ministers of the Global Coalition: Meeting on the Defeat of ISIS, 22 March 2017

a) Europol deployment to Operation Gallant Phoenix

Europol is on stand-by to deploy a liaison officer to the law enforcement part of to the US-led Operation Gallant Phoenix (OGP) in Jordan, which is aimed at pooling and analyzing information from the battlefield in Syria and Iraq, as soon as the US side has finalized the terms of reference, which are still under inter-agency consultation in the US. The issue was raised at the EU-US JHA Ministerial in on 15-16 June 2017. Europol deployment would allow cross-checking with Europol information and integration of battlefield information shared via OGP into Europol databases. It could also be explored how Europol could contribute relevant information to SIS II. If Daesh financial information was shared via OGP, Europol could feed this into its operational analysis processes, including other capabilities such as the FIU.net or TFTP.

For example data of a number of FTF entities was seized, transmitted to INTERPOL and resulted in five FTF returnee arrests in a Member State and the flagging of four previously unknown entities.

b) Vennlig revival

In the context of the VENNLIG project created in the context of the first Iraq war in 2006, as well as the corresponding project HAMAH for Afghanistan, battlefield information was collected by the US military and shared with the global law enforcement community via US law enforcement agencies, such as the FBI and the National Central Bureau in Washington (i.e. INTERPOL Washington), which then forwarded the information to the INTERPOL General Secretariat in Lyon for dissemination to approved member countries through INTERPOL Notices and Diffusions.

A procedure for this was jointly developed by the US military and law enforcement communities. As a first step, it is important not to overclassify such information, for example related to cell phones or documents, collected by the military forces, but rather classify it as "law enforcement sensitive", which would allow for the broadest sharing of information and increasing the chance of those with a "need to know" to have access to such information for appropriate use. The US military shared the information with law enforcement nationally (US Department of Justice (DoJ), FBI). An inter-agency authorization process was developed in the US, which after green light from all stakeholders, including the intelligence community, allowed the DoJ via the US INTERPOL National Central Bureau (NCB) to share the information with the INTERPOL General Secretariat.

It was then shared worldwide via INTERPOL and FBI Legal Attaches posted in EU capitals with their counterterrorism counterparts, which included law enforcement, investigating judges and prosecutors, depending on the host country. The project was presented to counter-terrorism prosecutors and criminal investigators from the EU and US in April 2008 at a tactical meeting organized by Eurojust on “Exchanging and sharing of information on returning Jihadists”. During this tactical meeting, the participants discussed possibilities to “judicialise” information collected from the battlefield in view of its admissibility in court. It was underlined during the meeting that successful prosecutions based on battlefield information took place and that the use of such information as evidence must respect the particularities of each case, as well as the legal requirements of each country. The project ended after withdrawal of the US forces from Iraq, as Iraqi authorities did not continue the practice of collecting information on foreign fighters and sharing it with the global law enforcement community.

One example from the VENNLIG project in the past is the sharing of data from the battlefield to prosecute members of the network that sent Belgian national Muriel Degogue and her husband to Iraq to conduct a suicide attack against coalition forces. Evidence originally overclassified by the US military was later declassified through the intervention of the US Department of Justice and sent to Belgian prosecutors within 24 hours to defend an appeal by a convicted terrorist (That information was obtained from Iraq with the understanding that the Platoon leader targeted by Degogue would not have to testify in person at a court proceeding in Belgium as his identity needed to be protected for fear of retaliation).

Another example involved information passed from the US military on the activities of Nizar Trabelsi in Afghanistan and a “Martyrs List” compiled in Afghanistan identifying multiple key targets for Trabelsi to attack, including an Air Force base and an Embassy in a Member State, among other targets in Europe.

Another example was the US military sharing information with France on a French national and FTF, Peter Cherif, who had engaged in terrorist attacks against Coalition forces and was apprehended in Iraq. The information also revealed the existence of a Scandinavian Facilitation Network sending foreign fighters from Scandinavian countries to Iraq via Syria.

Given the presence of Global anti-ISIS coalition forces on the ground, a systematic revival of the VENNLIG project would be important and timely. The US government has taken affirmative steps to revive VENNLIG more systematically and should be encouraged to do so as soon as possible. There has been revival of the VENNLIG approach on an ad hoc basis. INTERPOL is ready and has staff on the ground but there is no operational information exchange yet via VENNLIG, green light from the US is awaited in the coming weeks.

The process of publishing notices and diffusions is often time consuming and resource intensive. Furthermore, INTERPOL has to review each notice and diffusion for compliance with its Constitution and Rules for Processing of Information, consistent with human rights concerns and privacy rights. Additional resources to INTERPOL for processing and analyzing the battlefield data could be considered.

In order to prevent attacks in the EU and elsewhere, sharing of the information with Europol at the same time as with INTERPOL should be considered, given that the information is often time-sensitive. In addition to passing information to Europol, INTERPOL has the option of passing information directly to all 28 Member States. The information could also be passed directly from DoJ via FBI LEGATT channels to the specialized units. If there is a VENNLIG revival, it needs to be considered, in the long-term, to receive the information from NCB Baghdad to INTERPOL Lyon to Europol/EU Member States. The CT expert in the EU delegation could be helpful for Europol in this context.

A number of Member States have military forces present in Iraq and Syria. Hence VENNLIG concerns not only the US, but also Member States. In the context of battlefield evidence, information collected by regular military forces on the ground (not special forces or intelligence agencies that operate in a classified way) are particularly relevant. While the US is very advanced in military/law enforcement cooperation (for example, they have embedded investigators and prosecutors in military units), Member States could consider to introduce procedures similar to the US of classifications like "law enforcement sensitive" and share with their own law enforcement authorities, enabling them to further enrich the information and share it with Europol, SIS II and INTERPOL, as appropriate and as quickly as possible.

Consultations could take place with the US DoJ and INTERPOL to learn from the US experience of military law enforcement cooperation and explore whether interested Member States present in Syria, Iraq or other conflict zones relevant to CT such as Afghanistan could introduce similar procedures. In view of the ongoing battle of Mosul, where a lot of documents and other materials related to FTF have been recovered, it will be urgent to progress to put the relevant procedures in place.

2. INTERPOL notices

a) INTERPOL Black Notices

An INTERPOL Black Notice serves to seek information on unidentified bodies. DNA and fingerprints of dead/captured FTF can be shared with INTERPOL. This allows Member States to confirm/cross-check deaths of their FTF. INTERPOL has launched an initiative with a few Member States, with good results, to compare DNA evidence collected in the battlefield on FTFs and comparing it to DNA databases in Member States for the purpose of confirming the death of EU FTFs believed to be fighting in Syria and Iraq. Only a few Member States are using this tool at the moment. Others could also avail themselves of this capability.

b) INTERPOL Purple Notices / Operation Crosstalk

An INTERPOL Purple Notice serves to seek or provide information on *modus operandi*, objects, devices and concealment methods used by criminals. Operation Crosstalk is an INTERPOL Washington Initiative (hence by the US), supported by INTERPOL HQ, to fill the gap between military and law enforcement on information sharing linked to improvised explosive devices (IEDs). The objective is to share with INTERPOL Member States' law enforcement community, information on IEDs being used in the battlefield and conflict zones, with the understanding that terrorists are using knowledge on bomb manufacturing gained in the theatres of war and exporting it to European and Western capitals. Via the US INTERPOL National Central Bureau the US Department of Defense (DoD) will compile and share information on devices to enhance awareness of IEDs, emerging trends, and associated tactics worldwide, relying on battlefield information. It would be interesting for Member States and Europol to consider feeding and using this INTERPOL system.

c) INTERPOL Blue Notices

An INTERPOL Blue Notice serves to collect additional information about a person's identity, location or activities in relation to a crime. It will be important to use INTERPOL Blue Notices to share biometrics collected in conflict zones to identify bomb makers and IED networks.

3. Europol access to the Secure Real-Time Platform (SRTP) of the US Department of Homeland Security and the Terrorist Screening Centre (TSC) of the Federal Bureau of Investigation (FBI)

Europol has started to explore with the US Department of Homeland Security (DHS) the possibility of getting access to SRTP, which supports, inter alia large-scale, automated biographical and fingerprint comparison against databases held by the U.S., including terrorism or national security records including (with overall over 300,000 records). These fingerprints include those collected in conflict zones from IEDs or other locations. The process for utilizing relevant data in an automated manner is being identified (given the amount of data available through the SRTP). These data are assessed to be relevant in the context of Europol's support to Member State CT investigations, but also for example for the second line security checks at the hotspots. It would allow Member States, in particular those that don't have SRTP access bilaterally, and Europol to identify relevant data from cross-matching SRTP data against Europol's databases. The required (ICT) resources still need to be scoped on both sides.

The FBI Terrorist Screening Centre (TSC) hosts a database on foreign terrorist fighters and their facilitators and associates, consisting of data gathered from US agencies and their operational partners. Data were supplied to Europol which are now fully inserted into the Europol Information System (EIS). The data consist of approximately 26,000 person entities and their associated aliases and identity documents. It is now available for searching directly in the EIS for MS and Europol.

4. Cooperation with NATO

The EU and NATO have decided to strengthen their cooperation, including on CT. On 22/23 June the European Council concluded: "The transatlantic relationship and EU-NATO cooperation remain key to our overall security, allowing us to respond to evolving security threats, including cyber, hybrid and terrorism."

Battlefield information is relevant also in this context, in particular in areas where NATO has missions, such as in Afghanistan or off the Horn of Africa. The EU is also looking at funding a project with NATO and INTERPOL on collecting evidence from the battlefield in Iraq. It would be interesting for Europol to get access to NATO's Biometric Enhanced Watch list and Network analysis information with regard to counter-terrorism relevant information.

Under the new Europol Regulation which applied from 1 May 2017, Europol will be able to receive operational and strategic information directly from NATO missions, including personal data subject to certain conditions (Article 23(5) of the Europol Regulation). It will also be able to enter into working arrangements to exchange strategic information (i.e. excluding personal data) with NATO. For Europol to transfer personal data to NATO, the conditions of Article 25 of the Europol regulation need to be fulfilled.

It could be explored to put in place more structured cooperation between NATO missions and Europol, in particular with regard to sharing of information. It could be explored whether and if so how to add INTERPOL to this cooperation.

5. Evidence collected by the Commission for International Justice and Accountability (CIJA)

CIJA² is a private organization consisting of investigators and prosecutors, working with local partners on the ground in Syria and Iraq to collect non-forensic (mainly documents, exploitation of computers and cell-phones, internet) evidence on regime crimes and Daesh. Its efforts to establish accountability of those committing crimes in the warzone have been supported financially by the EU in 2015-16 (1.5 million Euros). CIJA is working to an evidentiary standard, it is not a human rights organization. It analyzes, contextualizes and cross-checks the information and builds case files, in particular on high and mid-level operatives. It also has a huge database of Syrian regime officials.

² CIJA is a non-profit foundation registered in the Netherlands, in accordance with Dutch law. The executive director is Dr. Bill Wiley. CIJA is currently funded by the EU (through FPI/IFS), the UK, Canada, Denmark, Norway and Germany. Switzerland and the United States have supported the CIJA in the past. CIJA's current (i.e., 2017) budget for Syria and Iraq is roughly EUR 6.5 million which enables them to employ roughly 150 personnel, most of them deployed in Syria and Iraq, in operations vis-à-vis the Islamic State and the Syrian regime. CIJA's Board of Commissioners (i.e., governors) is chaired by Stephen Rapp, who was the United States Ambassador for War Crimes Issues during the Obama Administration.

The EU CTC, the President of Eurojust and the Head of Europol's ECTC visited CIJA in early 2017. CIJA presented its work also to COTER and the Eurojust tactical meeting on terrorism. At the Eurojust tactical meeting, counter-terrorism prosecutors from the Member States started reflecting on whether and if so under which conditions their legal systems would allow the use of information collected by a non-governmental organization (CIJA) as evidence in terrorism and/or war crimes proceedings. Europol is exploring access to CIJA's databases. A Member State has offered to act as intermediary for CIJA to provide relevant information for analysis purposes at Europol (Analysis Project Travellers). The receipt of 40 FTF profiles from CIJA is envisaged to arrive at Europol in due course.

CIJA is open to share its information and evidence with interested national authorities or EU JHA agencies. It is open to visits and adapting the form of the cooperation to the needs of the relevant authorities. It is also open to receive feedback on evidentiary requirements of Member States. Battlefield information collected by CIJA has already supported a number of investigations and prosecutions in Member States. CIJA can also be asked to collect information on a specific FTF if the location and other characteristics are precise enough. CIJA may also be in a position to testify in national court proceedings.

6. Evidence collected by the International Criminal Court (ICC)

The ICC is carrying out investigations on the ground in a number of conflict areas which are relevant to CT. Not all of these investigations lead to criminal procedures at the ICC, given its complementary role. The ICC investigation team is ready to explore whether and if so how best to share relevant information with Europol, Eurojust and Member States. Consultations could take place in view of operationalizing this. Eurojust already invited in 2016 and 2017 the ICC representatives to begin discussions. Links between core international crimes and terrorism are sometimes encountered on the ground by the ICC investigators. The ICC can share, including on request, CT information that could assist national prosecutors from the EU Member States. Eurojust is encouraged to continue consultations with the ICC.

The importance of involving the ICC is that its mandate is limited to serious international crimes. It does not have a mandate to investigate organized crime, which often finances and fuels war crimes and genocide, and does not have the mandate to investigate terrorism matters. It does, however, collect data - collateral or otherwise - that could be relevant to European CT officials because of the potential links between counter-terrorism, organized crime and serious international crimes.

7. Information collected through EU projects/capacity building

Given the vast extent of EU involvement in capacity building and humanitarian projects in priority countries, it should be explored whether information collected in this context could be made available for law enforcement and judicial use as well. This might entail asking the partner States for their generalized consent to such a procedure.

A prime example for opportunities existing in this field would be the IED project in Iraq. In addition to an EU-funded project (iTRACE) that is effectively tracing the illicit movement of weapons, ammunition and related material, the supply chain of components being utilised by Da'esh to make IEDs; the weaponising of drones, the EU is supporting the clearance of explosive hazards from areas recovered from Da'esh in Iraq with a humanitarian project. The EU is also chairing the Coalition's committee responsible for coordinating international support in this domain. It has devised an effective "Blended Solution" which has recently been recognised by the UN Security Council as a model for future cooperation in other high risk conflict and post-conflict scenarios. Owing to humanitarian principles on the need for "neutrality", the opportunity to **expedite the effective collection and exploitation of forensic evidence and battlefield DNA** relating to the hazards and, in particular, **IEDs** is not meaningfully taking place before their removal and destruction.

The EEAS and the Commission, together with Member States, could be asked to examine a possible solution to leverage off the work of humanitarian mine action to reinforce due process through the **collection and preservation of forensic evidence from the IEDs in Iraq** as soon as possible, respecting the Chain of Evidence.

In the medium term, the EU could also explore capacity building of the law enforcement and military forces on the ground to support collection of battlefield information and sharing via INTERPOL.

8. UN mechanism for Syria

In December 2016, the UN General Assembly set up a mechanism for Syria "to collect, consolidate, preserve and analyse evidence of violations of international humanitarian law and human rights violations and abuses and to prepare files and to facilitate and expedite fair and independent criminal proceedings"³. This includes Daesh crimes. It will be important to follow closely the implementation of this mechanism. In case it assembles CT relevant information from the battlefield, it will be important to explore the possibility of sharing with Europol and Eurojust.

9. Frontex/border security related aspects

In principle, as a possible recipient and end-user, Frontex does not regard terrorism-related battlefield information as specific or different from other operational terrorism-related information. Such information can and certainly should be used, whenever appropriate, in support of border control activities with a view to disrupting FTFs' travel movements. In the context of joint operations, Frontex' access to such information remains dependent on permissible consultation of relevant databases as described in the operational plans. Therefore, **a proper processing of terrorism-related battlefield information and a subsequent proper populating of relevant databases are key to effective border control activities aiming at countering terrorism.**

³ International, Impartial and Independent Mechanism to assist in the Investigation and Prosecution of Those Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011. A/RES/71/248. The French magistrate Catherine Marchi-Uhel was nominated as head of the mechanism and will take up her functions in August 2017 in Geneva.

In the context of joint operations, Frontex staff can come into possession of terrorism-related battlefield information that might for instance originate in accounts issued by migrants coming from conflict zones. Such information including possible supporting information (pictures, messages, files, documents, etc.) may facilitate the selection of ‘‘subjects of interest’’ for second-line checks. It is in any case to be conveyed, depending on the circumstances, to Europol / Eurojust / MS authorities for further investigations.
