



Council of the
European Union

Brussels, 16 March 2015
(OR. en)

7272/15

LIMITE

**JAI 180
COSI 34
ENFOPOL 68
CYBER 18
COTER 50
DAPIX 41**

NOTE

From: Europol
To: Standing Committee on operational cooperation on internal security
Subject: Proposals from Europol: Improving information and intelligence exchange
in the area of counter terrorism across the EU

Delegations will find in Annex Europol proposals on improving information and intelligence exchange in the area of counter terrorism across the EU.

Proposals from Europol

Improving information and intelligence exchange

in the area of counter terrorism across the EU

1 Aim

This document summarises Europol's proposals regarding the Presidency's outline on the way forward, presented to the Justice and Home Affairs (JHA) Council of 12 March 2015. Section 4 of that paper "Step up information sharing and operational cooperation" invites Europol to "submit proposals on how existing platforms and services can be better used for information exchange, which will be considered by COSI as a matter of priority with a view to reporting to the Council in June."¹

2 Current situation

The Paris and Riga statements as well as the European Council declaration giving political direction on enhanced information sharing and operational cooperation are the most recent of many such calls stretching back to 2001².

¹ doc. 6891/15 JAI 160 COSI 31 ENFOPOL 57 SIRIS 15 FRONT 51

² The European Council Declaration on Combating Terrorism concluded on 25 March 2004, after the terrorist attacks in Madrid, stated that it is the political objective to "... improve mechanisms for co-operation and the promotion of effective systematic collaboration between police, security and intelligence services. The flow of intelligence in relation to all aspects of terrorism to Europol should be improved. The further development of the relationship between Europol and intelligence services will also be taken forward...". Earlier on, the European Council of 21 September 2001 called for "Member States will share with Europol, systematically and without delay, all useful data regarding terrorism". The Justice and Home Affairs (JHA) Council of 20 September 2001 concluded "The Council would reiterate how important it is for the quality of Europol analyses that the police authorities and also the intelligence services of the Member States should quickly pass on any relevant information on terrorism ..."

In 2005, Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences introduced a legal requirement for Member States to ensure that information on criminal investigations in respect of terrorist offences is sent to Europol.

Europol's experience, supported by the figures below, is that the expectations generated by these political decisions have not been generally met, with the potentials for the full and proper use of Europol's information management capabilities not realised in the area of counter terrorism.

2.1 Use of Europol's secure information and intelligence platform (SIENA)

- **Only 14 Member States have connected a counter terrorism unit/authority to SIENA.**
- **In 2014, terrorism crime** related information and intelligence exchange accounted for **4% of the overall volume of messages exchanged** (605.000) between EU Member States, Europol and third parties through SIENA. This ratio has been at comparable levels since 2010.
- This figure showed a **significant increase to 8% in January 2015** but by the **end of February 2015** had already returned to the **average level of 4%**.

Resulting from the above SIENA statistics, it emerges that there is still an urgent need to **facilitate awareness and access, as well as engender greater trust in the counter terrorism environment for sharing information and intelligence at EU level.**

2.2 Use of the Europol Information System (EIS) at Europol

- **By December 2014, 18 foreign terrorist fighters** had been inserted into the EIS by **2 Member States**. By the beginning of **March 2015** this had increased to **233** submitted by **8 Member States**.
- Overall, by the end of **December 2014**, there had been **1125 objects** (incl. around **350 person** entities) linked to terrorism inserted in the EIS. By the beginning of **March 2015** there were **1694 objects** (including around **580 person** entities) related to terrorism.

2.3 Exploiting Focal Point (FP) Travellers at Europol

- All **28 EU Member States participate in FP Travellers**. Australia, Norway, Switzerland and, since the end of February 2015, the US Custom and Border Protection Service (CBP) are associated to FP Travellers. The association of Eurojust, the Former Yugoslav Republic of Macedonia (FYROM), Albania and Interpol is currently being considered by Member States.
- Member States have increasingly provided information on foreign terrorist fighters to Europol since January 2013. The **total number of contributions** was close to **620** by the end of **February 2015**, with over **3.600 person entities** stored in FP Traveller.
- However, **60%** of these contributions **originate from 5 Member States and one associated third country**.
- Recent reporting suggests that Member States believe there are over 10,000 persons of interest in the EU with links to foreign terrorist fighters. Despite the positive developments, **there is still a considerable shortfall between the information available to counter terrorist services and that which is shared with or through Europol**.

2.4 Use of Terrorist Finance Tracking Programme (TFTP) through Europol

- Between the entry into force of the TFTP agreement in **August 2010** and **December 2014**, **69 contributions** (information provided directly by the US) occurred, resulting in **1000 intelligence leads**. 240 requests were sent by Europol and Member States, leading to **6335 intelligence leads**. Overall, **more than 7300 intelligence leads** have been generated by TFTP since it went into force.
- In 2014 (from the overall figures), there was also a significantly growing number of requests related to the phenomenon of travelling fighters (Syria/Iraq/IS). **35 requests were sent by Europol and Member States**, generating **937 intelligence leads of relevance to 11 Member States**.

- Over **January and February 2015**, 23 contributions were submitted by the US authorities and 26 requests were sent by EU Member States and Europol, with a total to date of **1983 intelligence leads in 2015** of relevance to **17 Member States**. This included **25 exchanges** within TFTP concerning travelling fighters (Syria/Iraq/IS), leading to **818 leads** specific to this phenomenon.

2.5 Use of Check the Web (CtW)

- All Member States are part of the Check the Web (CtW) portal at Europol which contains **1538 entities** (statements, publications, videos, audios) that were **published in 2014**. In addition, Switzerland and Australia are associated third parties.
- Europol has observed that terrorist propaganda material now focuses on videos and audio material, given the expected higher impact on potential supporters and volunteers through social media.
- Since 2007 (when CtW was established at Europol), close to **11500 publication items** have been incorporated onto the portal. The vast majority of propaganda items available on Check the Web were provided by Europol through own monitoring activities: In **2014, 1 Member State provided 2 contributions while Australia submitted 8 dedicated analysis reports to CtW**.

2.6 Exploiting Focal Point (FP) Firearms

- **21 Member States** are members of FP Firearms, which was opened **in January 2014**. **6 third parties** are associated to FP Firearms (Eurojust, Switzerland, Australia, the US (ATF), Albania and Interpol).
- FP Firearms has so far received **1780 contributions**, relating to around **300 investigative cases**, about **60.000 firearms and close to 1800 suspected companies** involved. Since January 2015 to today, FP Firearms has received **415 contributions**. This shows an **increase of contributions** if compared with the same period last year (164 contributions received in the same period in 2014).
- The **Paris and Copenhagen terror attacks in 2015** highlight that the terrorists obtained the firearms from the criminal markets. It is therefore **crucial to identify supply opportunities for terrorist**, thus Europol has re-enforced its operational activities to close this intelligence gap.

3 Proposals

3.1 Information sharing and operational cooperation

To step-up information sharing and operational cooperation action is required both at Europol and at the level of national authorities. Focusing on existing platforms and services still allows scope for considering new and innovative approaches without reinventing the wheel. The answer lies more in exploring how existing platforms and services might be better used rather than identifying whether new platforms and services are needed.

3.1.1 Actions by Europol

- Building on the Europol experience of establishing the European Cybercrime Centre (EC3) where internal restructuring and reallocation of resources and priorities delivered an effective response Europol intends to follow a similar model in addressing the current challenge. Establishing an **EU Counter Terrorism Centre (ECTC)** within the existing organisational structure of Europol ensures the existing platforms and services (listed in Annex 1) are utilised to maximum effect.
- Europol shall provide **sealed off, high security office space** (including Faraday compartments for classified information and intelligence handling) to house ECTC.
- Europol shall prioritise the work required to facilitate the exchange of information and intelligence at the level of **EU CONFIDENTIAL through SIENA** (currently EU RESTRICTED).
- Europol shall exploit the opportunities afforded by the **cross-matching of data between law enforcement authorities and intelligence authorities through the use of pseudonymization tools**.
- Europol shall implement a **”three-tier intelligence sharing approach“** ensuring synergies on data stored on SIS II, EIS and in FP Travellers.
- Europol builds an **Internet Referral Unit (IRU)** as per the guidance of the Justice and Home Affairs Council of 12 March 2015 (see doc. 7266/15).
- Europol will continue its efforts to **engage with counter terrorism units and their heads** in order to step up information and intelligence sharing with or through Europol and by providing a **platform at EU level**.

3.1.2 Actions by Member States

- Counter terrorism units in **all Member States should start using the secure exchange system of Europol (SIENA) to share information and intelligence**. This can be realised by establishing a secure connection through the Europol National Unit (ENU), or by opting for a direct connection towards Europol (subject to agreement with the ENU).³ Counter terrorism units connected to SIENA use a Point-To-Point (P2P) connection, allowing counter terrorism units to send and receive SIENA messages directly with other counter terrorism units. While Europol's FPs can be part of the P2P network they need to be addressed by counter terrorism units directly.
- Member States should **maximise their use of the other Europol platforms and services** (listed in Annex 1).
- Member States should **improve the mechanism at the national level for sharing relevant information** between the law enforcement including Europol and intelligence services.
- Member States should improve their information sharing and operational cooperation in respect of the **terrorist acquisition and use of firearms** (see doc. 6739/15).
- **Member States**, in particular in the formation of COSI, consider promoting **Europol as the channel of first choice** for information and intelligence sharing across EU Member States.

3.1.3 Actions by Commission

- The Commission, in the context of the development of the **EU Security Agenda**, could consider promoting **Europol as the channel of first choice for information and intelligence sharing across EU Member States**.
- The Commission could promote the use of **Europol's key tools and core systems**, e.g. SIENA, EIS and EAS as EU solutions to information sharing requirements.

³ Article 7 (2) of the Europol Council Decision (ECD) defines: "The national unit shall be the only liaison body between Europol and the competent authorities of the Member States. Member States, however, may allow direct contacts between designated competent authorities and Europol subject to conditions determined by the Member State in question, including prior involvement of the national unit."

3.2 Closing intelligence gaps

The absence of real time intelligence at Europol leads to **key intelligence gaps** which require to be addressed at the EU level. The following are additional proposals to that end.

- Coordination through **Europol** of **risk indicators to support targeted checks at the borders of the EU and among EU Member States** (travel patterns). On this basis, relevant follow-on information and intelligence being shared with Europol's key tools and core systems (e.g. individual profiling).
- Making **full use of the capabilities of EC3**, Europol will **assess the cyber related terrorist threat scenarios**, focusing on intent and capability.
- Close integration of the **FIU network through Europol (ongoing)** to complement the **fight against the financing of terrorism beyond TFTP** (e.g. payment card fraud, means and modi operandi of terrorists to obtain funds).
- Sharing of relevant **Passenger Name Record (PNR) data with Europol** to complement the analysis of travel routes etc. and to enrich counter terrorism FPs. To this end, SIENA should be adopted as the communication system linking the proposed Passenger Information Units (PIUs) in Member States.
- Ensuring that all possible **links between terrorism and organised crime** (serious organised crime related profile of radicalised individuals posing a terrorist threat; firearms and explosives supply channels as well as illegal immigration are key areas linked to terrorism) **are identified** with a view to initiating relevant operational action and a consistent and integral response with all relevant authorities.
- **Information exchange between law enforcement and intelligence services** (within the given regulatory framework of concerned actors – see also Section 3.1.1 above).

Existing platforms and services provided by Europol in the area of counter-terrorism

- **Information/intelligence capabilities in respect of terrorism**
 - **Secure Information Exchange Network Application (SIENA)** – As a **central tool to enable connectivity**, SIENA is used to manage the exchange of operational and strategic crime-related information amongst Member States, Europol and third party cooperation partners.
 - **Analysis Work File (AWF) Terrorism** is a distinct and self-contained component of the Europol Analysis System (EAS), with individual Focal Points (FPs) to reflect current priorities in the fight against terrorism⁴ thus improving operational analysis, cross-matching, case and phenomena analysis and coordinated responses incorporating input from:
 - **FP Travellers** (foreign terrorist fighters travelling to and from conflict zones);
 - **Terrorism Financing Tracking Program – TFTP** (targeted searches on data provided by MS's);
 - **Check the Web** (analysis of terrorist propaganda material available on the internet including threat analysis);
 - (Planned) **Internet Referral Unit** (identification and take down of extremist internet material).

⁴ Europol's AWF Terrorism also contains the following 3 additional FPs: Hydra (Islamic terrorism beyond the phenomenon of so called travelling foreign fighters), Piracy (East of Africa and Gulf of Aden maritime piracy), Dolphin (all other terrorist activities, i.e. right-wing terrorism)

- The **Europol Information System (EIS)** is Europol’s central criminal information and intelligence database covering all of Europol’s mandated crime areas. It contains serious international crime-related information on suspects, convicts and ‘potential future criminals’⁵, criminal structures, and offences and means used to commit them. It is a reference system which provides **Europol and Member States** with a rapid means to verify whether information on a **certain person or another object of interest is available beyond national or organisational jurisdictions**.

All new data inserted in the EIS is automatically compared with all information already stored in the EIS and in the AWFs (e.g. names, telephone numbers, emails, DNA, firearms, open source intelligence etc.) The purpose is to look for matches with a view to enhancing intelligence and providing new leads for further investigations. A distinctive feature of EIS is that it is directly accessible in all Member States on the level of the ENU. This access can be further widened to include national counter terrorism units.

- **Provision of counter terrorism expertise within a secure environment supported by strong logistical arrangements**
 - **Senior counter terrorism investigators and analytical staff with language expertise** relevant for counter terrorism (security cleared, with background in all relevant competent authorities across the EU, including the intelligence service community)
 - **Utilising established CT networks and services at EU level: Europol National Contact Points for counter terrorism** (informal information exchange, meeting facilities at Europol etc.) and **Working Group Dumas**: Based on the initiative of the former Presidency in October 2014: EU wide approach to address foreign terrorist fighter phenomenon
 - **EU Bomb Data System (EBDS)**: Application for the timely sharing of relevant information and intelligence on incidents involving explosives, incendiary and explosive devices, as well as chemical, biological, radiological and nuclear (CBRN) materials

⁵ Art. 12 of Europol Council Decision (ECD), OJ L 121,15.5.2009, p. 37.

- **European Explosive Ordinance Disposal Network (EEODN):** Information sharing and capacity building including training
 - **Option of Europol and Member States coordinating high impact operations** aimed at terrorist logistics, e.g. travel or financing.
 - **Robust security and confidentiality framework**
 - **Guarantee of data ownership for counter terrorism authorities (legal provisions and operating arrangements, e.g. handling codes)**
 - **Information and intelligence sharing in a controlled environment, based on the requirements of the data originator.**
 - **Direct and immediate on-the-spot support**
 - **Mobile office:** Deployment of staff with full access to Europol's databases
 - **First Response Network (FRN)** at Europol: In case of a major terrorist incident, the FRN can be established at Europol to provide the best possible support to the competent authorities in charge of the investigation
 - **24/7 capabilities to connect terrorism with organised crime activities – Horizontal information and intelligence sharing and data matching**
 - **Liaison Bureaux Network at Europol (over 150 liaison officers seconded to Europol by EU Member States and Europol's non-EU partners)**
-