



Council of the
European Union

Brussels, 20 December 2016
(OR. en)

14260/16
EXT 1

JAI 924
CT 1
CFSP/PESC 914
COSI 183
COPS 333
ENFOPOL 400
COTER 111
SIRIS 155
FRONT 436
CATS 87
EDUC 360

NOTE

From: EU Counter-Terrorism Coordinator
To: Council

Subject: Implementation of the counter-terrorism agenda set by the European Council

This report covers progress against the conclusions on counter-terrorism (CT) agreed by the Members of the European Council on 12 February 2015. It takes into account the CT related conclusions of the European Council of 17 and 18 December 2015 and the JHA Council of 20 November 2015 and the Joint statement on the terrorist attacks in Brussels on 22 March 2016. This report - drafted in consultation with Commission services, the EEAS, Europol, Eurojust, Frontex, the EU Fundamental Rights Agency, eu-LISA and Interpol - is complementary to the Commission's "First progress report towards an effective and genuine Security Union" (Commission Communication COM(2016) 670 of 12 October 2016).

The EU Counter-Terrorism Coordinator draws the following recommendations from the report:

Roadmap

1. Implementation of the Roadmap on information sharing adopted under the Netherlands Presidency should progress as a matter of priority. This is particularly relevant with regard to the use of the Schengen Information System (SIS II) for CT purposes.

PNR

2. Member States should progress on the implementation of the Passenger Name Record (PNR) directive as a matter of priority and urgency.

Europol

3. Member States should maintain a high volume and quality of contributions provided to Europol, while increasing the data quality, e.g. by contextual information for analysis purposes.

4. Those Member States particularly affected by the terrorist threat may wish to consider dedicating additional staff to the Joint Liaison Team (JLT) at Europol.

5. Member States' contributions to the EU Internet Referral Unit at Europol (both in terms of staff seconded and in relation to the volume of referrals) remain low and should be increased.

Participation of Member States in the Referral Action Days (RAD) should also be increased, alongside the use of the capabilities of the EU Internet Referral Unit.

6. Further progress on cooperation between the European Counter-Terrorism Centre (ECTC) and the Counter-Terrorism Group (CTG) is needed while fully respecting Member States sole responsibility for national security. Some positive developments have been recorded recently in this respect.

7. Europol should receive budgetary support for second-line security checks in the hotspots as well as overall staffing levels as authorized by the Management Board.

8. Following the integration of Financial Intelligence Units Network (FIU.net) into Europol, steps should be taken by the Member States and Europol to strengthen the operational cooperation between the FIUs and law enforcement authorities. Member States should allow and encourage their FIUs to participate in Europol's project. Legal obstacles at national level for FIUs to work directly with Europol should be addressed as a matter of priority.

Eurojust

9. Member States should continue to increase the exchange of information concerning terrorist offences with Eurojust and to transmit all such information on a regular basis in a timely and systematic manner.

10. Member States should further increase their use of Eurojust tools for operational coordination in counter-terrorism cases.

11. Eurojust should receive budgetary support to effectively deal with the increase in the number of terrorism cases, coordination meetings, Joint Investigation Teams (JITs) and processing and analysing information on prosecutions and convictions of terrorist offences. Eurojust's staffing levels should be reinforced to enhance Eurojust's involvement in the ECTC at Europol to improve coordination of investigations and prosecutions.

Legislative measures

12. The planned legal revision of the SIS framework should take into account interoperability as well as the business needs of Europol and facilitate the systematic cross-matching of biographic and - once the Automated Fingerprint Identification System (AFIS) for SIS II is operational - biometric data against Europol systems.

13. Law enforcement needs should be adequately reflected in the expected legislative review of the Visa Information System (VIS) framework and in the negotiations of the Eurodac regulation.

14. Frontex should use its possibilities of information exchange under the recently adopted regulation and should be given access to the relevant databases, including the Entry-Exit System, which needs to be taken into account in the legislation on the databases.

Checks at external borders

15. Member States are invited to upgrade technology relevant for systematic checks against relevant databases, where necessary.

16. The consultation of Interpol databases should be further increased as searches remain uneven across the Member States.

17. Member States are invited to ensure adequate feeding, deployment and consultation of FADO (False and Authentic Documents Online). The legal basis of the system, including its hosting and future development should be overhauled in order to ensure full integration with the developing EU information management architecture.

Security checks at hotspots

18. A complete capacity for proper registration, including the security checks of the relevant databases in the hotspots, should be finalised as a matter of priority (interoperability of databases, staffing, processes, infrastructure).

19. Following agreement by Italy in September 2016 regarding secondary security checks involving Europol, guest officers from Europol for second-line security checks in Italy should be deployed as soon as possible, and the corresponding operational plan should be concluded. Progress needs to be made on the systematic checking of all relevant databases for all migrants, including the process for relocation, based on adequate security checks.

20. Referrals to Europol for second-line security checks should be made in all cases where persons need to be further checked, making full use of the deployment of Europol guest officers (in Greece, 1,490 persons were checked by Europol guest officers in October 2016, compared with 782 persons referred for checks up to September 2016).

Terrorist financing

21. Listings should take place as soon as possible using the new CFSP autonomous listing system, in particular related to Daesh.

EU Internet Forum

22. The next meeting of the Internet Forum at Ministerial level of 8 December 2016 should explore together with the industry the possibility of voluntary implementation of automated detection mechanisms to facilitate removals, co-financing of relevant initiatives and solutions for timely voluntary cooperation on e-evidence (subscriber and transaction data). The key threats characterising the internet governance landscape, as identified in Europol's recent Internet – Organised Crime Threat Assessment (I-OCTA) 2016, should be addressed as a priority, in order to ensure efficient and effective investigations, especially also in the area of counter-terrorism.

E-evidence

23. The Commission is invited to accelerate efforts to propose a long-term solution for speedy and efficient access of investigators and judicial authorities to e-evidence, including strengthening the legal obligations to cooperate irrespective of where internet service providers are based.

Encryption

24. The issue of encryption should be addressed, as requested by the German and French Ministers of the Interior in their joint letter of 28 October 2016.

Returnees

25. The EU should as soon as possible define a common approach with regard to foreign terrorist fighter returnees.

External aspects

26. Development and implementation of CT packages with priority partners in the Middle East and North Africa (MENA) region, Turkey and the Western Balkans should proceed as quickly and ambitiously as possible, with additional funding as appropriate. Follow-up for projects launched under the Instrument contributing to Stability and Peace (IcSP) short term needs to be ensured. The EU Justice and Home Affairs agencies should remain closely involved. As per the Commission Communication of 14 September 2016, there is a need to progress enhanced cooperation especially with MENA region third countries for cross-checking data against Europol's databases. The EEAS could help promote relevant transmission of information by third countries to Europol (either through Member States law enforcement officers posted abroad or through Interpol as an intermediary). The involvement of third countries has already generated tangible results, by contributing data to the Europol Information System (EIS).

Overview

Developments with regard to the **European Counter-Terrorism Centre (ECTC) at Europol** have been positive. While still not reflecting the full extent of the threat, information sharing in the context of Europol has improved considerably¹: 3 979 FTFs have been contributed by EU Member States to the Analytical Work File Focal Point Travellers (up from 2 421 in 2015), 3 291 FTFs (up from 1 493 in 2015) have been contributed by EU member States to the Europol Information System (EIS) and 6 400 individuals have been contributed by EU Member States to Focal Point Hydra (up from 4 398 in 2015). Queries of the EIS have increased to 954 375 in 2016 (up from 598 652 in 2015). 79 TFTP requests so far in 2016 (85 in 2015).

¹ Europol data as of 23 September 2016

Task Force Fraternité has continued to provide support to the investigations after the Brussels and Paris attacks and the Joint Liaison Team has started to identify new lines of investigations. The ECTC's staff is being increased, CT authorities of all EU Member States are now connected to the Secure Information Exchange Network Application (SIENA). Europol is developing a batch search mechanism for the SIS II and is preparing connection to the Visa Information System (VIS) and Eurodac. On 14 September 2016, the Commission presented new initiatives to reinforce the ECTC, notably as regards upgraded access to EU databases, strengthened internal governance, cooperation with third countries, as well as financial and human resources. The Communication², also highlighted the importance of finding a practical solution for cooperation between law enforcement and intelligence communities whilst fully respecting Member States sole responsibility for national security.

By October 2016, the **EU Internet Referral Unit (IRU)** has made 15 421 referrals to internet service providers (88,9 % which resulted in removals by the companies), while referrals by Member States to the EU IRU remain low (1 203 items by 8 Member States, out of the 15 421 in total). Additional joint referral action days will be organized in November 2016, aimed also at the initiation of investigative measures.

There is a positive trend towards making better use of **Eurojust** in the fight against terrorism, however, this starts from a low level. Several Member States have requested Eurojust support in counter-terrorism cases, including major complex cases of cross-border nature such as the terrorist attacks in Paris and Brussels (47 cases registered so far in 2016 compared to 41 cases in 2015). Only one Eurojust Coordination Centre on counter-terrorism has ever been organized (in 2015). Member States have provided little information on criminal investigations and prosecutions for terrorist offences so far in 2016. Some Member States only share information about concluded court proceedings and not about ongoing prosecutions. Few Member States have submitted to Eurojust information on concluded counter-terrorism court proceedings. However, overall, information submitted to Eurojust has increased (113 ongoing CT prosecutions in 2016 compared to 100 in 2015 and 30 in 2014; 65 concluded CT court proceedings in 2016, 218 in 2015 and 180 in 2014).

² Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders, COM(2016) 602 final

Use of **SIS II** in the context of the fight against terrorism has increased significantly. In 2016, 78 015 alerts have been entered under Art. 36 (2) (up from 61 575 in 2015) and 9 516 alerts have been entered under Art. 36 (3) (up from 7 945 in 2015)³. Work is underway to further improve the use of the SIS II for counter-terrorism, particularly in relation to foreign terrorist fighters, in order to implement fully the Roadmap on information sharing adopted under the Netherlands Presidency. It will be important to fully cover interoperability in the update of the SIS II (Commission proposal expected in the near future). The SIS II Automated Fingerprint Identification system is being developed by eu-LISA, with the test phase starting in 2017 and full capability available in 2018.

Searches in the relevant **Interpol databases** have increased considerably, but remain uneven among Member States.

Implementation of **security aspects in the hotspots** has improved.

Further progress needs to be made with regard to systematic checks of the migrants against all relevant databases and the development of integrated system interface for simultaneous checks of the relevant databases in a single search (national AFIS database, Eurodac and SIS II).

In Greece, where Europol has been present in the hotspots for second line checks, few refugees have been referred to Europol for second line checks against Europol databases (782 persons between March and September 2016, there have already been hits in databases). In October, 1 490 persons were checked when the Europol guest officers had taken up full work. The number of second line checks should be proportionate to Europol capacity (26 guest officers from Member States at the moment). Europol guest officers should be used as effectively as possible in Greece.

³ Reference date for 2015 numbers is 31 December 2015; reference date for 2016 numbers is September 2016.

There has been significant progress with regard to operational cooperation between **Frontex and Europol**, including the sharing of personal data. Efforts are being made to address the issue of **forged documents**, including the Commission's intention to present an action plan shortly and the deployment of Frontex advanced-level document experts in all hotspots. At the end of October 2016, Europol received confirmation from the Commission that the additional budget to cover the costs related to the deployment of guest officers for second-line security checks will be provided (1,5 Million Euro for the period March 2016 to February 2017).

FADO (False and Authentic Documents Online) currently contains about 3.000 specimen of genuine documents and of anonymised examples of false documents, including known forgery techniques, as well as about 2.000 national false document alerts. Proper feeding, as well as adequate deployment and consultation at all border crossings points (including hotspots), at immigration services, at embassies and consulates, as well as with police forces remains uneven throughout the Union. In a mid-term perspective, FADO needs an overhaul of its communication technologies, in particular with a view of ensuring a better integration into the EU's information management architecture. Also, the legal basis of FADO⁴ is outdated and needs revision.

Frontex is supporting the Member States to implement the **Common Risk Indicators** and has integrated them into all operations. Operational activity against **firearms trafficking**, included related to the Western Balkans, has increased. Europol and Frontex are very involved.

The **integration of the FIU.net into Europol** has so far not resulted in significantly enhanced cooperation between FIUs and Europol on counter-terrorism, although it would be beneficial to systematically cross-check information from the FIUs via the FIU.net. Europol has launched pilots to strengthen such cooperation.

A new **anti-terrorism Common Foreign and Security Policy (CFSP) regime** (allowing for autonomous EU listings for assets freezing and entry bans also for EU nationals) has been adopted, but listings on this basis have not taking place yet.

⁴ Council Joint Action of 3 December 1998, 98/700/JHA

In the context of the **EU Internet Forum**, the Commission has focused on removal of content (preparation of the establishment of an industry-wide Joint Referrals Platform) and counter-narratives (Commission will launch a 10 Million Euro Civil Society Empowerment Programme). The successful work of the Syria Strategic Communications Advisory Team will be continued with Commission support and has as of 1 October 2016 been transformed into the **European Strategic Communications Network**, continuing to provide consultancy services to interested Member States and increase common understanding through the network. Europol's recent Internet – Organised Crime Threat Assessment (I-OCTA) 2016 has highlighted key threats emerging from the internet governance landscape. In particular, the so called Carrier Grade Network (CGN) modalities undermine the ability of law enforcement authorities to associate and link a particular cyber criminal's activity back to a particular IP address, requiring further action as highlighted in the I-OCTA.

Council Conclusions **on e-evidence** were adopted in June 2016. On this basis, the Commission is working closely with Member States, Eurojust and Europol and has launched a process of experts meetings with a view to provide a report at the JHA Council in December 2016 on the progress made so far to explore a common EU approach. In a joint letter of 28 October 2016, the German and French Ministers of the Interior highlighted the need to find in this context also solutions for **encryption**, based on strengthening the legal obligation of electronic communication service providers, including those based outside of the EU, to directly cooperate with the competent authorities of the Member States with regard to criminal investigations.

The European Commission is offering financial support to Member States to set up **rehabilitation programmes and risk assessments of foreign terrorist fighters** and has involved the European Judicial Training Network, Europris and the European Confederation for Probation in training activities for judicial staff related to radicalization inside and outside prison.

The Commission will organise the **Radicalisation Awareness Network (RAN) High Level Conference** on 9 November to discuss effective ways to tackle radicalisation, in particular in relation to returning foreign terrorist fighters, children and the challenges of polarisation in society. The conference does not only aim at feeding back practitioners' insights and recommendations to policy makers but also to pave the way for increased exchanges of experiences and expertise on prevention strategies and approaches among Member States.

In line with its Communication on supporting the prevention of radicalisation leading to violent extremism of 14 June 2016, the Commission is mobilizing **education and youth policies** to support prevention of radicalization and inclusion and has launched a number of initiatives, in particular moderated virtual exchanges to connect young people from the EU and countries in North Africa and the Middle East (MENA) with the aim of reaching 200 000 young people by 2019. The Education Council will adopt Conclusions on prevention of radicalization in November 2016.

Externally, the EU (EEAS, Commission services, EU CTC) has focused on and progressed with regard to the development of CT packages for priority partners in the **MENA region, Turkey and the Western Balkans**. Europol, Eurojust, the EU Agency for Law Enforcement Training (CEPOL) and as appropriate Frontex are playing an active role in these efforts. The comprehensive package for Tunisia is most advanced and serves as a model for engagement with other partners. The CT/security experts deployed in EU delegations are playing an important role to facilitate a stronger engagement. A number of CT capacity building projects are under way, new projects are under preparation. The EEAS is also stepping up and improving communication with the Arab World.