Council of the European Union
General Secretariat

Brussels, 17 January 2015
(OR. en)

DS 1035/15

LIMITE

MEETING DOCUMENT

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015

This is a first paper for discussion in COSI on 20 January 2015. It does not yet include the Commission's proposals which will be discussed in the College on 21 January, nor the contributions from the Member States. The document which will be submitted to the informal meeting of JHA ministers in Riga on 29/30 January will be shorter, include the outcome of the COSI discussions as well as contributions from the Member States and the Commission.

Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took place in Paris between 7 and 9 January 2015 were followed by an unprecedented show of unity by millions of citizens in France and across Europe as well as a show of solidarity and political will by many EU and world leaders. In addition to action from the national governments, citizens are looking to the European Union to provide an ambitious response. Core European values have been attacked, in particular freedom of speech. The EU has to respond with meaningful action. Failure to do so could result in disillusionment of citizens with the EU.

At the EU level, work is already well on track and a lot is in the pipeline. However, as was the consensus in COREPER on 15 January 2015, now we need to mobilize the political will to amplify and accelerate implementation of measures which have already been decided by the Council since June 2013 and make better use of existing EU mechanisms, including the EU's revised Strategy for Combating Radicalisation and Recruitment to Terrorism and its guidelines.

We need to focus on sustainable and long term policies that increase the overall resilience of our societies in dealing with radicalisation and terrorism. In order to build this resilience, we need to not only target the response to terrorism but also have a strong focus on long term prevention of radicalisation. Past and current events have shown us the importance of including a strong cooperation and exchange with civil society in these policies.

The declaration adopted by the Ministers of Interior present in Paris on 11 January 2015[1] is an excellent basis for the EU's further work and should be endorsed and implemented by the EU.

On this basis and following, the discussion in COREPER on 15 January 2015 as well as further consultations with Member States, the current note sets out priorities which should be taken forward urgently. They should be examined at the informal meeting of JHA ministers in Riga on 29 January, with a few to submitting a meaningful package of measures to the meeting of Heads of States and Government on 12 February.

Coherence between the internal and external work is crucial. Given the parallel work of the FAC where suggestions for action will also be developed, this note does not include suggestions for the external side. This external aspects of JHA will be included in the note prepared for the informal JHA ministerial meeting in Riga on 29 January (after the FAC).

1. Prevention of radicalization

a) Internet

The EU and its Member States have developed several initiatives related to countering radicalisation and terrorism on the internet, ranging from developing and promoting counter narratives to engaging in high-level dialogue with the industry and several Member States, led by the Netherlands, have started to develop informal joint policies on social media and the legal framework related to internet and counter-terrorism. It is important to draw on these initiatives and identify what actions can be stepped-up to increase the EUs effectiveness.

[1] doc 5322/15

The Commission should deepen the **engagement with the internet companies.** The **Forum** with representatives from the EU institutions, Member States and industry counterparts to discuss terrorism in full compliance with human rights should be set up quickly. The Forum could also explore joint training and workshops for representatives of the law enforcement authorities, internet industry and civil society. A dialogue with the internet companies is necessary at both EU and at international level. In this context, further cooperation with the US could be explored.

Working with the **main players in the internet industry** is the best way to limit the circulation of terrorist material online. We should build on the existing relationships between the major platforms, Member States and the EU institutions in order to develop a stronger joint response.

We should build on the positive industry response, of which the UK Counter-Terrorism Internet Referral Unit (CTIRU) work[2] is an excellent example, and also on the successful models in some other Member States. There are options to take this forward at a national level and/or to work together with other states and industry partners to further limit the use of the internet by terrorist groups:

- Member States should consider establishing similar units to the UK CTIRU and replicate relationships with the main social media companies to refer terrorist and extremist content which breaches the platforms' own terms and conditions (and not necessarily national legislation).

- Member States should also consider what role the EU can play. For those Member States which do not yet have a national capability, EU involvement in referring terrorist and extremist content to social media platforms for removal could make a difference. Consideration should be given to a **role for Europol in either flagging or facilitating the flagging of content which breaches the platforms' own terms and conditions.** These often go further than national legislation and can therefore help to reduce the amount of radicalising material available online.' In this context, Europol's Check the Web project could be beefed up to allow for monitoring and analysis of social media communication on the internet.

[2] **CTIRU** continues to work with social media platforms to flag terrorist and extremist content to them which breaches their own terms and conditions. Since February 2010, social media platforms and other parts of the internet industry have voluntarily removed 72,000 pieces of terrorist content following referrals from CTIRU because they have agreed that the content represents a breach of their rules. The main players have started to improve their response and held a training event for the smaller platforms on this issue in December. The UK is committed to sharing its experience across the EU.

The Commission should examine the **legal and technical possibilities to remove illegal content** and make proposals for a common approach, in full compliance with fundamental rights.

In the law enforcement and judicial context, cross-border information about owners of **IP addresses** can take very long to obtain, given the need to use MLAE tools. The Commission should be invited to consider ways to speed up the process. In the meantime, existing best practices in the Member States to deal with this issue could be collected and shared. Eurojust could facilitate this process, as discussed at the Eurojust Strategic Meeting on Cybercrime held on 19-20 November 2014 in The Hague.

As proposed in the EU Strategy for Combating Radicalisation and Recruitment to Terrorism, **internet safety education in schools** should be improved to ensure that the dangers of online activity and potential to radicalisation and recruitment are highlighted and addressed appropriately and consistently. In this context, Sweden could be invited to share its experience with training to strengthen the critical thinking skills of young people with regard to the internet.

b) Strategic Communications

Member States and EU institutions are encouraged to develop **strategic communications and counter-narrative** policies, making maximum use of the already existing Syria Strategic Communications Advisory Team (**SSCAT**). Member States should develop positive, targeted and easily accessible messages.

The Commission, in cooperation with Belgium, could convene urgently a meeting of the SSCAT network and Member States to brainstorm proposals for **national/pan-European/cross-border communications** efforts in the coming weeks, building on the unprecedented public response to the Paris attacks and the mobilization of civil society. Proposals should be refined in time for the informal JHA Ministerial meeting. The Commission might consider emergency funding in support to this end.

With regard to counter-narratives, **training to civil society organisations to exploit their online potential** is important. The RAN Center of Excellence in cooperation with industry could explore to provide this.

Drawing on the experience of the EU's Fundamental Rights Agency (FRA), the EU should develop and implement a **communication and outreach strategy with regard to fundamental rights and values**. It is therefore important to also step-up our efforts to counter all kinds of extremism, including the anti-Islamism and right-wing extremism, and continue to **promote tolerance and solidarity** throughout the EU. We can build on the positive message that was echoed by the majority of EU citizens in response to the Paris attacks.

It is important to engage in dialogue with Muslim communities in Europe. The Commission could be tasked to draw on the expertise of the RAN Centre of Excellence and the BEPA to facilitate this. The Commission, drawing on the experience of the FRA, could be tasked to develop **dialogue with Muslim communities on freedom of speech and expression** and assist the Member States to do so. The FRA could be invited to present suggestions for **integration and non-discrimination of Muslims**.

c) Underlying factors of radicalization

The Commission should be invited to mobilize all relevant departments and resources to develop a comprehensive package to assist Member States to address the **underlying factors of radicalization** and support initiatives across the EU with regard to education, vocational training, job opportunities, integration.

d) Dis-engagement, rehabilitation, de-radicalization

As discussed at the December 2014 JHA Council**, de-radicalization, disengagement and rehabilitation programmes**, including in prison and as alternative to prison in the judicial context, should be developed. The Commission should be asked to examine how best such judicial rehabilitation and disengagement programmes could be set up and facilitate the sharing of best practices and consider support to such projects, including financial, drawing on the experience of the RAN Centre of excellence and Eurojust.

The Commission should speed up the establishment, amplify and project also to third countries the **RAN Centre of Excellence**. The RAN Centre of Excellence should be in a position as soon as possible to provide expert advice to Member States to set up programmes. Member States are encouraged to develop at national level similar multidisciplinary networks which allow to exchange good practices and coordinate efforts.

2. Border controls

Schengen is part of the solution, not the problem. The free movement inside the Schengen area is one of the major achievements and values of the EU. To maintain Schengen and at the same time a high level of security, controls at the Schengen external borders have to be strengthened.

Work engaged under the auspices of the Commission to step up the detection and screening of travel movements by European nationals crossing the Schengen external borders should be swiftly finalized. To that end, Member States will more extensively detect and monitor certain passengers based on objective, concrete criteria which respect smooth border crossings, fundamental liberties and security requirements. Common risk indicators and criteria will systematically be implemented across the Schengen area.

In addition, the Commission could be invited to present a proposal in a timely fashion to **amend the rules of the Schengen Borders Code** to allow for broader consultation of the Schengen Information System during the crossing of external borders by individuals enjoying the right to free movement. At the same time, technical solutions should be developed so that there is no impact on passenger waiting times at passport controls.

The recommendations of the SIS/Sirene Working Party of December 2014 (doc 14523/3/14 Rev 3) should be implemented as a matter of priority and urgency.

The Commission could support, as appropriate, Member States' initiatives to establish appropriate technological and procedural requirements to reinforce systematic controls of the validity of travel documents against the relevant databases such as Interpol's SLTD as well as the document section of the SIS. Member States should establish such solutions as a matter of priority.

Common criteria to enter foreign fighters information into the SIS II should be developed.

3. Information sharing

Member States should implement all measures that may be helpful with respect to the sharing of information on the different forms of the threat, notably foreign terrorist fighters, on knowledge of their movements, and the support they receive, wherever they are, with a view to improving the effectiveness of the fight against these phenomena. To that end, Member States should use fully the resources of Europol, Eurojust and Interpol, as well as consider other measures.

The UK should be admitted to the SIS II as soon as the legal, technical and procedural requirements are completed.

a) PNR

There is a crucial and urgent need to move toward a European Passenger Name Record (PNR) framework, including intra-EU PNR. The Council is prepared to move forward, adopting a constructive approach with the European Parliament without however jeopardizing the effectiveness of the system. Member States and EU institutions are committed to engage MEPs as a matter of priority.

b) Europol

The amount of information transmitted to Europol doesn't match the threat. Political will is needed to increase the use of Europol - the biggest shortcoming has been the lack of information provided by national CT authorities[3].

Member States should contribute to the maximum extent to the Europol Focal Point Travellers. The situation that so far four Member States contribute 80 % of the data is not yet sufficient. and participate in the working groups related to foreign fighters set up by Europol, which might need to intensify their work.

Adopting some measures similar to those employed in the EU Policy Cycle against Serious and Organised Crime, such as assigning driver roles to lead Member States, multilateral strategic and operational planning and dedicated Commission funding, could add impact to EU CT work.

The creation of a **European Counter-terrorism Centre** at Europol, like the European Cybercrime Centre (EC3), would allow Europol to translate existing capabilities into operational impact quickly. The EU Counter-terrorism Centre could focus on five main pillars of work:

(1) Focus on Foreign Fighters, with complementary levels of intelligence sharing (SIS II, EIS, Focal Point Travellers) and synergies with EU PNR;

[3] While the overall number of cases supported by Europol increased by 52 % from 2011 to 2014, the increase in CT cases was only 2 %.

In addition to better use of Focal Point Travellers, multinational ad-hoc working group Dumas and the Network of CT contact points, Europol could establish a resident CT task force drawn from the appropriate national agencies and hosted by Europol. This would follow the successful model of J-CAT in the cybercrime sphere. The CT task force would identify suitable networks to be reviewed jointly, starting with less sensitive cases in order to build confidence. It would act as a fusion centre for law enforcement and intelligence service data and would allow CT practitioners to interact with their CT peers without the many interfaces which usually separate them from Europol at national level.

As the repository for more detailed intelligence in prioritised operations, Focal Point Travellers should be seen as part of a three-tier intelligence sharing strategy, along with the **Europol Information System** (EIS) and the **Schengen Information System** (SIS II). The EIS should be used by investigators to share basic information about all suspected foreign fighters. It already has the capability to store data on terrorists, but less than 2 % of current records are terrorism related. Only minimal details need to be shared as a basis for follow-up inquiries, handling codes and "hidden hits" can be used to restrict access (same model already successfully used in organized crime).

In order to extract maximum value of an EU PNR, the national Passenger Information Units (PIUs) should use SIENA for their cross-border communications, and should systematically cross-check their PNR data against Europol's databases. Europol should work with PIUs to establish common European methods for trend and travel pattern analysis, suspect identification etc. A central PIU located at Europol could be established to work alongside those at the national level.

(2) Unique financial intelligence capabilities (EU-US TFTP, FIU.net integration);

Investigative leads of EU-US Terrorist Financing Tracking Programme are cross-checked with Europol's main CT database. Over 60 leads have already been provided following the Paris attacks. As well as bringing the European FIU and CT communities into closer proximity, the FIU.net (European network of Financial Intelligence Units) integration into Europol will also give Europol the opportunity to use **ma3tch techniques** currently used by FIU.net for counter-terrorism purposes. This would allow the identification of ‘need-to-know’ information in real time without information being transmitted to Europol. This could be a key factor in convincing reluctant CT units to make use of Europol channels.

(3) Support services to tackle firearms, explosives and CBRN threats

(4) Cyber capabilities to identify online terrorist activity and help to prevent acts of cyber-terrorism

Europol and MS should commit multidisciplinary resources to identifying, disrupting and prosecuting terrorist activity online.

(5) Improved strategic intelligence (improving the TESAT, providing advice to Member States on national terrorist threat levels and strengthening ties with INTCEN).

c) ECRIS

There is a threat posed to the security of our citizens from those who travel within the EU, and into the EU, with **criminal records indicating a violent or terrorism-related past**. We have in place a system, **ECRIS**, to ensure that each Member States holds a central record of its own nationals' criminal history (wherever offences were committed within the EU) which can be shared with other Member States when those individuals come to the attention of their law enforcement authorities. However, the scope of ECRIS is limited. The problem is that the existing system for exchange of criminal records at EU level (ECRIS) is reactive, case-by-case, in practice limited to EU citizens (it does not work well with regard to third country nationals as it is not clear which Member State should be requested for these criminal records) and limited primarily for specific criminal investigations**. We should explore how we can provide for a more systematic and proactive exchange of such data within the EU, in particular on terrorist related convictions.** This would help to strengthen our ability to protect the public including against the insider threat. This may involve strengthening the ECRIS framework, a greater role for Europol or other approaches. The Commission could be invited to present proposals. There is already work underway to be able to capture and share data on non-EU nationals who are convicted in the EU, which should now be accelerated.

d) Data retention

The Commission could be invited to present as soon as possible a new legislative proposal for data retention.

e) API data

The existing API directive should be implemented fully and used to the maximum extent. The Commission could be invited to make suggestions in this regard.

f) Encryption/interception

Since the Snowden revelations, internet and telecommunications companies have started to use often de-centralized encryption which increasingly makes lawful interception by the relevant national authorities technically difficult or even impossible. The Commission should be invited to explore rules obliging internet and telecommunications companies operating in the EU to provide under certain conditions as set out in the relevant national laws and in full compliance with fundamental rights access of the relevant national authorities to communications (i.e. share encryption keys).

g) European Terrorist Financing Tracking System (TFTS)

It should be explored whether to relaunch the discussion started under the previous Commission on the feasibility of a European TFTS.

4. Judicial response

There is a need to step up international judicial cooperation in terrorism cases, in particular cases of foreign fighters.

a) Judicial information sharing

Member States should be encouraged to make optimal use of the possibilities for **exchange of information on prosecutions and convictions with Eurojust**, as set out in Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences.

Member States should be also encouraged to increase the exchange of information with Eurojust, in accordance with Article 13 of the Eurojust Decision, in cases of trafficking in firearms and cybercrime.

The use of the Eurojust national coordination system should be enhanced to facilitate the carrying out of the tasks of Eurojust. The well-functioning network of national correspondents for Eurojust for terrorism matters should continue to be fully used to foster the exchange of judicial information and best practices in terrorism cases.

b) Strategic aspects

Coordination at EU level in addressing the **legal challenges in the gathering and admissibility of e-evidence in terrorism cases** would be beneficial. Such challenges were discussed at the Eurojust Strategic Meeting on Cybercrime in November 2014, where the need for a cybercrime judicial network supported by Eurojust was strongly advocated. The possibility of creating a platform of cyberterrorism prosecutors inside this cybercrime judicial network could also be explored. Eurojust could be invited to further facilitate systematic exchanges of experience by national judicial authorities and collection of good practices with regard to the gathering and admissibility of evidence, in particular internet related, as well as investigation and adjudication of foreign fighters cases.

Eurojust should continue to analyse relevant case law on terrorism in its Terrorism Convictions Monitor (TCM) to further consolidate a common understanding of terrorist phenomena and identify reoccurring legal challenges and best practice.

Where appropriate, Member States should be encouraged to use Eurojust's assistance in terrorism cases involving third States and share relevant experience and best practice during tactical and strategic meetings.

c) Operational aspects

Member States should make **maximum use of Eurojust tools, in particular its coordination meetings and coordination centres. Member States should explore the setting up of Joint Investigation Teams in terrorism cases with the assistance of Eurojust, including legal advice, as well as financial support.** Member States should be encouraged to refer to Eurojust European Arrest Warrants concerning terrorist offences to ensure their proper and timely execution. In the future, Member States should also make use of Eurojust's assistance in the execution of European Investigation Orders.

d) Rehabilitation programs in the judicial context should be developed as a priority.

e) Implementation of UN Security Council Resolution 2178

The Commission could be asked to present a legislative proposal to update the Council Framework Decision on Combating Terrorism to collectively implement UNSCR 2178.

The Commission could also be asked to establish an overview of implementation of UNSCR 2178 by EU Member States, which is relevant also in the context of the US Visa Waiver Programme.

5. Firearms

The EU has a comprehensive set of measures in place and fighting illicit firearms trafficking is one of the EU's crime priorities for the 2014-2017 period, as decided by the Council. However, only 13 Member States are participating in the **Operational Action Plan firearms** adopted by COSI. Therefore, increased participation by Member States and acceleration of the implementation of the various measures should be a priority notably to improve information sharing among Member States and with Europol and to increase the number of join firearms operations across Europe. These operations should also target firearms trafficking on the internet and the Darknet.

Europol could be invited to present state of play on the use by Member States of Europol's firearms database at the informal meeting of JHA ministers, in particular contribution of information, and its activities in this context, to better identify and dismantle trafficking networks.

The **Commission** could be invited to make proposals to improve information exchange mechanisms and the collection and destruction of prohibited weapons.

The rules across Europe for the **de-militarization of firearms** are not harmonized, which means that in some Member States it is easier to re-activate de-militarized weapons. The Commission could be invited to examine possibilities for harmonization.

The **traceability of firearms** only lasts 20 years. It should be explored to make this indefinite.

The Commission could also be invited to make suggestions to better address the **trade of firearms via internet**.

More information on terrorist acquisition of firearms needs to be shared with Europol. Synergies between CT and organized crime work must be sought.

6. Information sharing about measures at national level

a) National measures

Member States are invited to share unclassified measures they have adopted or are planning to adopt at the national level by sending contributions in writing to the General Secretariat of the Council so that an inventory can be established and shared with all Member States. The COSI meeting on 20 January is aimed at determining the measures to be taken by the EU and not at analyzing measures taken or contemplated by Member States at national level.

b) Threat level

In 2010, the Council had agreed a system of notification of change of alert levels through INTCEN, which has never really functioned. Overall, as suggested by Spain, a discussion is desirable.

As suggested by the Spanish Minister of the Interior[4], it could be explored to harmonize the designation of terrorist threat levels across Member States and to design a common mechanism covering the EU with different levels of alert. In addition, the remit and purpose of TE-SAT could be boosted to make it a viable threat assessment rather than a trend report. An even more ambitious way forward would come with a closer alignment of the functions of Europol and INTCEN, to make a genuine EU CT threat assessment centre with a dedicated task to inform threat levels in MS.

c) EU Integrated Political Crisis Response (IPCR)

In order to support communication efforts in relation to the current events, it is important for the EU Member States and institutions to have an overview of messages released. In addition, sharing information on communication monitoring (i.e. public/media/social media reaction to those messages) may help crisis communication preparedness efforts. The **EU Integrated Political Crisis Response (IPCR) web platform** is readily available and includes features built for that purpose, such as the opening of a dedicated page for "monitoring on-going complex situations". Such a page acts as an information-exchange forum and a repository where all communication-related data may be easily found. Such an initiative may also rely on the recently established IPCR communication correspondents network.

[4] doc. 5216/15

This informal network is constituted of crisis communication officials from the Member States and institutions who act as points of contact and reference for crisis communication issues. A dedicated section of the IPCR Web Platform has been also set-up to allow crisis communication specialists to interact for preparedness purposes.

7. Internal/external link: Projecting JHA tools externally

Concrete proposals will be developed after the meeting of the FAC on 19 January 2015.

Interpol

Member States should use Interpol to a maximum extent (diffusion system) to share information with third countries. In order to maximise the use of these databases, experts should study and deliver methods to harmonise the national practices for inserting national information on foreign fighters in such a way that they are better exploitable by relevant third countries but also limited in their distribution to the concerned partners.