European Commission - Fact Sheet

European Agenda on Security - State of Play

Brussels, 17 November 2015

European Agenda on Security - State of Play

What is the European Agenda on Security?

The Commission adopted the European Agenda on Security on 28 April 2015, setting out the main actions envisaged by the Commission to ensure an effective EU response to terrorism and security threats in the European Union over the period 2015-2020. The Agenda identified three priorities: tackling terrorism and preventing radicalisation, disrupting organised crime, and fighting cybercrime.

The Agenda fulfilled a commitment made in the Political Guidelines of European Commission President Jean-Claude Juncker and replaces the previous strategy adopted in 2010 (the Internal Security Strategy 2010-2014). Recent incidents show how relevant the priorities identified in the Agenda are and illustrate the need to step-up action, and speed up the implementation of concrete measures.

The Agenda foresees action in a number of different fields to complement the actions of Member State authorities, who have primary responsibility in the field of security. The Commission's role is to tackle cross border aspects of the fight against terrorism and organised crime and to facilitate cooperation among Member States.

Since then progress has been made notably on:

- Legal and technical improvements to the Schengen Information System database;
- Common Risk Indicators concerning foreign terrorist fighters;
- Establishment of an EU Internet Referral Unit in Europol;
- EU Internet Forum to be launched on 3 December 2015;
- Establishment of a Radicalisation Awareness Network (RAN) Centre of Excellence, operational since 1 October 2015;
- Establishment of a platform bringing together Financial Intelligence Units from the Member States;
- Development of practical tools and guidance material such as handbooks to assist practitioners, first respondents and law enforcement specialists.

How can the EU help Member States in the area of internal security?

Member States remain primarily responsible for ensuring internal security. However, the threats to Europe's citizens are becoming more varied and increasingly cross-border in nature. Member States have the frontline responsibility for security, but can no longer succeed fully on their own.

Combatting organised crime and terrorism is a common European responsibility. The Agenda on Security identified three pillars of the EU action, where it can bring clear added-value: (1) ensuring better information exchange between national law enforcement authorities and EU Agencies, (2) increasing operational cooperation, and (3) through supporting actions such as training and co-funding.

The European Agenda on Security will help police and other law enforcement services in different Member States to share data more effectively and better cooperate against cross-border crime. Member States can rely on support by EU Agencies.

The European Agenda on Security is a major building block of the renewed Internal Security Strategy that was adopted by the Council on 16 June 2015. Importantly, and as advocated by the Commission, the Council clearly stated that developing and securing the internal security of the EU is a shared agenda of the Council, the European Commission and the European Parliament.

Coherent action at EU level, involving all three institutions, can help strengthen the EU security framework, thus allowing the EU and the Member States to address today's threats and challenges in the field of internal security.

Crime and terrorist activities are not confined within the borders of the EU nor to neighbouring regions. EU internal security and global security are mutually dependent and interlinked. The Union's security is

highly dependent on cooperation with international partners and neighbouring countries.

Border Management and Information Exchange

What is the Schengen Information System (SIS)?

The **Schengen Information System** (SIS) is used by law enforcement authorities to consult alerts on wanted or missing persons and objects. The Commission will further encourage Member States to make full use of the SIS together with Interpol's database on **Stolen and Lost Travel Documents (SLTD)** at the external borders**.** Today there are more than 66 400 alerts for discreet and specific checks, which is a 300% increase compared to the situation in June 2013.

On 1 February 2015, the Commission made **legal and technical improvements to SIS** to provide for real-time communication from the ground to the competent services in other Member States. The Commission also distributed an explanatory document to Member States at the beginning of October 2015 to help border guards seizing invalidated documents.

In the context of the revision of the SIS announced for 2016 to enforce return and entry bans, the Commission will also look into possible needs to enhance the law enforcement aspect of the SIS. In the meantime, the Commission is urging Member States to make full use of the possibilities to enter into the SIS alerts relating to all measures involving expulsion, refusal of entry or removal from the territory of a Member State.

The Commission together with the current Luxembourgish Council Presidency will assess the progress made since the Informal meeting of the Heads of State and Government of 12 February 2015 February and the Special meeting of the European Council on 23 April on Security. The Commission will identify areas where Member States need to make greater efforts, and present recommendations ahead of the December Justice and Home Affairs Council.

On 15 June 2015 the Commission revised the **Schengen Handbook for Border Guards** in line with the Commission's interpretation of the so-called "non-systematic checks".

What verifications does the SIS allow for?

All persons, upon entry and exit to the territory of the EU, must undergo a check to establish their identity by the verification of their travel documents. This check should be carried out against the relevant databases and use the necessary technical devices to verify if the travel document is lost, stolen, misappropriated or invalidated.

At the external borders third country nationals must be subject to a thorough entry check, including a control in SIS. This control applies to the person as well as to the travel document. Upon exit, a control in SIS of third country nationals is not mandatory, although border control authorities should verify whether the person is considered as a threat to public security.

Persons enjoying the right of free movement (EU citizens and their third country national family members) are subject to a minimum check at the external borders. They should not be subject to a systematic control in SIS, unless there is considered to be a risk. Member States determine whether there is a risk or not. If for example, a country considers that all flights arriving from a particular third country or all flights into a particular EU country pose a risk, then systematic controls including against the SIS database can be carried out on all persons, including EU nationals.

For this reason, the Commission proposed a set of Common Risk Indicators concerning foreign terrorist fighters which assist border control authorities by providing further criteria on persons who can be a threat to public security.

The Commission has recommended on several occasions to intensify the checks on EU citizens against the databases at the external border. Currently the number of EU citizens checked against the databases remains low (between 1.5-17%, depending on the Member State and border crossing point). In some Member States the thorough checks required on third country nationals are not always carried out as required in the Schengen Borders Code.

Is there a security check in the context of asylum applications?

When processing an asylum request some Member States carry out security verifications on the person seeking international protection, including a check in SIS. The asylum process is a national responsibility, therefore Member States are entitled to carry out security checks in accordance with their national legislation.

What is EURODAC?

The "Eurodac" database, established in 2003, is an EU asylum fingerprint database. When someone applies for asylum or is apprehended having crossed an external border irregularly having come from a third country, no matter where they are in the EU, their fingerprints are transmitted to the Eurodac

central system. The recast "Eurodac" (Regulation (EU) No 603/2013) entered into force on 20 July 2015 and introduced updates to the system, in particular, to ensure data is transmitted within 72 hours to the Central System, to address data protection concerns and to help combat terrorism and serious crime. Currently 27 out of the 28 Member States have implemented this Regulation; the Commission is taking action against Cyprus, who has not yet implemented it.

How does EURODAC interact with SIS?

The Eurodac and SIS databases are two separate databases without any interconnection as they follow different objectives, i.e. SIS is a security database and Eurodac is an immigration database. Of course, it is possible that there is an alert in SIS on a person whose fingerprints are also stored in Eurodac.

Can EU law enforcement authorities have access to the asylum fingerprint database Eurodac?

The Recast Eurodac Regulation allows, inter alia, for the consultation of Eurodac by law enforcement authorities for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences. The aim is to enable law enforcement authorities to request the comparison of fingerprint data with those stored in the Eurodac central database when they seek to establish the exact identity of, or get further information concerning, a person who is suspected of a serious crime or terrorism or concerning a victim.

Prior to making a law enforcement access request to Eurodac, Member States must first check fingerprint databases available under national law; compare the fingerprint dataset with the Automated Fingerprint Databases of other Member States under the "Prüm" Decision; where applicable, compare the fingerprint data set with the Visa Information System; determine that a comparison with Eurodac data is necessary in a specific case and determine that there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. There must also be a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls in a category covered by the Eurodac Regulation.

What is the European Criminal Records Information System (ECRIS)?

The **European Criminal Records Information System** (ECRIS) supports crucial information exchange between EU law enforcement authorities. To date, 26 Member States are using ECRIS and its increased use means over 100,000 messages are exchanged between national authorities each month.

However, it does not cover non-EU nationals.

In 2016, the Commission **will propose to amend** the EU system for the exchange of information of criminal convictions to render it more effective for the exchange of criminal records of Third Country Nationals.

How is the Commission helping to detect terrorist travel?

The Commission finalised in May, in close cooperation with national experts, the EEAS, EU Agencies and Interpol, a first set of **common risk indicators**, concerning foreign terrorist fighters, with a view to detect terrorist travel. Common risk indicators support the work of national border authorities when conducting checks on persons. To make the common risk indicators an effective operational tool, the Commission has invited FRONTEX to support Member States in the field of training and awareness-raising.

What is the Prüm Decision? How does it work?

The **Prüm Decision** introduced procedures for fast and efficient data exchange in specific areas. The core of the Prüm framework lays down provisions under which EU Member States allow each other searches in the DNA analysis files, fingerprint identification systems and vehicle registration data bases. DNA and fingerprint searches take place based on a "hit/no-hit" approach, which means that DNA or fingerprint profiles can be compared with profiles held in the databases of other EU Member States. The automated reply reveals whether this profile exists in the requested Member State. Additional personal information needs to be requested separately.

The Prüm Decision should have been implemented fully by Member States by August 2011. Member States received financial and technical support from the EU to implement it. However, a number of Member States have not yet implemented the Prüm Decision, in particular with respect to the automated searches. So far, 22 Member States have implemented the DNA data exchange, 18 Member States have implemented the fingerprint data category and 19 have implemented the vehicle registration data category.

Prüm does not regulate the conditions under which Member States take and store fingerprints or DNA profiles of suspects or convicted persons. This is up to the Member States. Once a profile is stored in

the police database and under the condition that a Member State has implemented the relevant provisions (i.e. it is connected to the Prüm system for this data type) the data would be available according to the mentioned "hit/no-hit" approach to all other connected Member States. DNA searches under Prüm are permitted only for the investigation of criminal offences; searches with fingerprint profiles are permitted for the prevention and investigation of criminal offences.

Operational Cooperation

How is the European Commission increasing operational police cooperation?

Example 1: Joint Investigation Teams (JITs) gather police officers from several Member States for a fixed period to investigate specific cross-border cases. The European Commission will promote more regular use of JITs by Member States and will make sure that third countries are involved in JIT in cases with an international dimension.

Example 2: EU agencies, and in particular Europol and Eurojust, play **a crucial role in facilitating cross-border cooperation and investigations.** Operation Archimedes, coordinated by Europol in September 2014 to address a variety of serious crimes across 34 Member States and third countries, resulted in over 1000 arrests made across Europe. The European Commission will improve coordination of the work of EU agencies to make sure that their potential to support Member States is used to the full.

Can you give concrete examples of how EU coordination in the area of security has made a difference?

The European Arrest Warrant is an important tool to catch criminals and render our criminal justice systems more effective, ensuring the swift return of numerous suspects who may not otherwise have faced justice. It now takes on average around 16 days to hand over a wanted person who consents to his/her surrender, and 48 days when he/she does not. It was notably thanks to this tool that one of the 2005 "London bombers" could be extradited back to the UK from Italy in a matter of weeks. Thanks to the same mechanism, in 2014, the Belgian authorities were able to apprehend the main suspect in the Brussels Jewish museum attack, who had fled to France.

Terrorism in Europe feeds on extremist ideologies. In pooling our knowledge and expertise, we are stronger in tackling radicalisation. On 30 January 2014, the Radicalisation Awareness Network (RAN) hosted the Cities Conference on Foreign Fighters to Syria in The Hague. This conference brought together 120 local practitioners from 23 affected cities across different Member States as well as 50 representatives from the national authorities from most EU Member States and RAN experts to discuss the issue of "foreign fighters" and exchange knowledge and best practices. Today more than 2000 experts and practitioners are involved in the RAN.

The Schengen Information System is the largest law enforcement exchange platform in Europe, containing over 62 million alerts on wanted persons and objects which led to over 128,000 police actions in 28 Schengen States in 2014.

What is the EU doing to go after terrorism financing?

The **anti-money laundering package** adopted in May 2015, once in place, will help strengthen and improve cooperation between Financial Intelligence Units; improve awareness of and responsiveness to any weaknesses and money laundering and terrorist financing risks; bring about a coordinated European policy to deal with non-EU countries which have inefficient Anti-Money Laundering/Combating the financing of terrorism (AML/CFT) regimes; and ensure full traceability of fund transfers both within the European Union and to and from the EU.

As part of this new AML framework, the European Commission has already started work on the overall assessment of the money laundering and terrorism financing risks that can affect the Internal market because of their supranational and cross-border dimensions. Through this analysis, the European Commission will provide a clear picture of the threats and vulnerabilities of the financial system that can lead to terrorist financing risks including the methods and the sources of funds for the terrorists. In line with the 4th AMLD, the outcomes of this risk assessment will be available by June 2017, and will be accompanied by recommendations to Member States on the measures suitable to address the risks identified. Member States will have to comply with such measures or explain the reasons why they ask for derogations. Both the supranational risk assessment and the recommendations aim to bring about a greater improvement of the understanding and the mitigation of the terrorism financing risks at EU level. Among the sectors under assessment, the use of virtual currencies will be subject to particular attention, as requested by the European Council of 26 January 2015.

In addition, the EU will put in place a **coordinated European action towards high risk third countries,** through the publication by the European Commission, of a list of countries which present some deficiencies in their anti-money laundering and terrorist financing regimes ("black list"). Once

identified, the financial flows entering the EU from these identified countries will have to be closely monitored by the Member States and the entities in charge of the anti-money laundering and terrorist financing policy (such as financial institutions) in order to ensure that they do not present any risks for the Internal market. Member States will have to apply enhanced controls on these transactions and will be able to decide to limit or prohibit the financial relationships with these high risk third countries.

The 4th AMLD already reinforced the powers and resources of the Financial Intelligence Units (FIUs), as well as their cooperation obligation through the secured channel of communication FIU.net. The Commission will continue to support this initiative which is a key tool to effectively cut networks that facilitate terrorist activities from financing.

The European Agenda on Security aims to put in place effective measures to "follow the money", by reinforcing the powers of **financial intelligence units** (FIU) to better track the financial dealings of organised crime networks and enhance the powers of competent national authorities to freeze and confiscate illicit assets.

A platform bringing together Financial Intelligence Units from the Member States is now fully in place. Its purpose is to detect and disrupt terrorist finance and money laundering activities. It meets on a regular basis with the Commission services with a view to enhance cooperation, develop common tools and better identify suspicious financial transactions. Effective IT tools have been developed for direct information exchange among FIU's. FIU's closely cooperate with EUROPOL.

The EU concluded with the U.S. an agreement on access to transfer of financial data in the framework of the US Terrorist Finance Tracking Program (**'TFTP Agreement'**) which is in force since August 2010. The Terrorist Finance Tracking System enables identification and tracking of terrorists and their support networks through targeted searches run on the financial data provided by the Designated Provider (SWIFT).

Reciprocity is a basic principle underlying the Agreement and two provisions (Articles 9 and 10) are the basis for Member States as well as, where appropriate, Europol and Eurojust to benefit from TFTP data. Under the EU rules, National Treasuries must ensure the availability to law enforcement, public security, or counter-terrorism authorities of concerned Member States, and, as appropriate, to Europol and Eurojust, of information obtained through the TFTP. Since the Agreement entered into force in 2010, more than 7300 investigative leads were generated by the TFTP for the EU.

There is a significantly growing number of requests related to the phenomenon of travelling fighters (Syria/Iraq/IS). In 2014, there were 35 TFTP (Article 10) requests generating 937 intelligence leads of relevance to 11 EU Member States. The TFTP was used, through Europol, to support the investigations of the French authorities related to the Paris attacks in January 2015.

What about the external dimension of security?

Many security challenges originate outside the EU, and collaborating with third countries is an essential element of the European Agenda on Security. The EU has set up a Western Balkan Counter-Terrorism initiative to improve regional cooperation and information sharing on the fight against terrorism and jihadism in the European neighbourhood. Progress on the implementation of this initiative will be discussed at the EU-Western Balkans Ministerial on 7 December 2015.

External aspects of security will be more comprehensively developed in the framework of the Strategic Review that the High Representative for Foreign Affairs and Security Policy/Vice-President of the Commission has initiated, as well as in the ongoing review of the European Neighbourhood Policy.

Fighting Radicalisation

What does the EU do to tackle the phenomenon of radicalisation among young people in Europe?

Education has a crucial role to play in building open, tolerant societies. Classrooms are the first place where we support the potential of most vulnerable students, and promote democratic, non-discrimination as well as active citizenship values.

By signing the joint "Paris Declaration" on 17 March 2015, the European Commission and EU Education Ministers agreed to do more 1) to ensure that children and young people acquire social, civic and intercultural competences, 2) to enhance critical thinking and media literacy, particularly in the use of the Internet and social media, 3) to foster the education of disadvantaged children and young people and 4) to promote intercultural dialogues.

The EU has, for example, funded projects such as "The Hesse Advice Centre" in Germany, which provides prevention, intervention and de-radicalisation measures to deal with religious extremism. The EU has also helped the French Association of Victims of Terrorism to initiate dialogues between victims of terrorism and citizens by organising conferences in schools and local associations. Here, the main objectives are to make victims more visible to youth, to promote a sense of citizenship through the

victims of terrorism and to involve teachers and pupils in the prevention of radicalisation.

The new Education and Training Report (ET2020), which was proposed by the Commission in August 2015, calls on Members States to make European education and training systems more socially inclusive. The report proposes to set six priorities for the next five years, including improving people's skills and employment prospects, creating open, innovative and digital learning environments, while at the same time cultivating fundamental values.

Overall, the Commission can help Member States in tackling radicalisation by mobilising policy and funding instruments, notably Erasmus+, to strengthen peer learning and mutual exchanges, pool knowledge and disseminate good practices.

The Commission will soon launch a call for proposals for projects worth up to €8 million aimed at disseminating inclusive and preventive practices in education to reach out to the grass-root level and encourage networking among organisations and associations active in the field. .

What is being done to address terrorists' use of the internet?

The Commission is increasingly concerned at how terrorists exploit the internet to radicalise and recruit, facilitate and direct terrorist activity, and then glorify in their atrocities.

Whilst it is perhaps impossible to rid the internet of all terrorist material, we must do more to reduce the immense volume of material that is online and so easily accessible to our citizens. The Commission is organising an EU Internet Forum on 3 December with Ministers and Internet companies to address these themes.

An EU Internet Referral Unit was set up at Europol in July 2015 to support Member States in identifying terrorist material on the internet, and then referring it to the internet companies where Europol assesses it to have breached their terms and conditions. This is a voluntary arrangement in order to alert the companies when their sites are being abused by terrorist organisations.

The e-Commerce Directive already foresees that when illegal content is identified, internet service providers should take effective action to remove it. In practice, the removal of illegal content can be slow and complicated; this is why the Commission aims at making this process more efficient under the Digital Single Market Strategy.

Should there be 'backdoors' for governments to bypass encryption?

There are no simple means to enable lawful access to secured communications. This is not only a question of technology: checks and balances need to be put in place in order to have proportionate measures. Encryption is widely recognised as an essential tool for security and trust in open networks. It can play a crucial role, together with other measures, to protect information, including personal data, hence reducing the impact of data breaches and security incidents. However, the use of encryption should not prevent competent authorities from safeguarding important public interests in accordance with the procedures, conditions and safeguards set forth by law.

What financing is made available to prevent radicalisation?

The European Agenda on Security calls on focusing on the prevention of radicalisation in prisons, and developing effective disengagement/de-radicalisation programmes**.**

The European Commission organised on 19 October a **Ministerial Conference on the criminal justice response to radicalisation** leading to terrorism (see press release). This point will be further discussed at the next Justice and Home Affairs Council meeting on 3 December and will be followed up by the concrete actions.

As regards funding, the draft conclusions mention that while the above actions should be done within the financial resources set out in the Multiannual Financial Framework, these questions have to be integrated into the mid-term review of this Framework. In addition to available amounts for 2015, for 2016, the following amounts will be available:

- Call for proposals to support transnational projects to promote judicial cooperation in criminal matters, including instruments directly linked with fight against terrorism: €3 400 000
- Call for proposals to support transnational projects on judicial training covering civil law, criminal law or fundamental rights, including Criminal law instruments allowing to fight terrorism and radicalisation: €5 700 000.

What is the EU doing to prevent radicalisation and violent extremism via the Radicalisation Awareness Network (RAN)?

The EU supports Member States' efforts **in countering radicalisation on the ground** through the work of the Radicalisation Awareness Network (RAN). It is at a local level – in schools, prisons, the health care sector – where preventive work can most effectively be delivered. In recognition of this

fact, in 2011, the Commission set up a Radicalisation Awareness Network to support practitioners across the EU who come into contact with individuals who have been radicalised or those deemed vulnerable to radicalisation. The RAN is a network of networks, bringing practitioners together to discuss emerging trends and exchange and develop best practices.

Within dedicated RAN working groups, different aspects of radicalisation and different approaches to preventive action are discussed and tested. For instance, the Communication and Narratives Working Group focuses on the delivery of online and offline communication that counters or challenges violent extremist narratives. There is the Education Working Group which supports those working in education to identify warning signs, safeguard pupils and challenge extremist behaviour. The Exit Working Group looks at how best to support those who are turning their backs on violent extremism and want to reintegrate back into society. The Youth, Families and Communities Working Group looks at how best to engage with youngsters who are considered vulnerable to radicalisation and how best to support their families and the local community. The Local Authorities Working Group looks at the important co-ordinating role local authorities play in bringing together practitioners in the local area. The Prison and Probation Working Group considers how best to tackle radicalisation post-conviction and the RAN POL group looks at the important role local police officers can play in supporting local communities to deal with violent extremism. Finally, the Remembrance of Victims of Terrorism Working Group ensures victims of terrorist atrocities are not forgotten, and considers the powerful effect that their stories can have on deterring individuals from engaging in violent extremism.

More specifically as regards the foreign terrorist fighter phenomenon, the RAN issued a RAN Declaration of good practices for Engagement with Foreign Fighters for Prevention, Outreach, Rehabilitation and Reintegration. Practices and recommendations have been updated and tested in several events and conferences dedicated to the foreign terrorist fighter phenomenon (the last one in June 2015). Good practices concern in particular different forms of family support programmes including helplines (prior to departure) and tailor made exit-programmes (upon return). To further support Member States' efforts in this field, RAN offers expertise and hands-on advice in dedicated workshops for instance on the development of helplines, the multi-agency follow up and aftercare.

Whilst the RAN has brought together over 2000 practitioners from across the Union, more needs to be done. The Commission has therefore bolstered the RAN, turned it into a Centre of Excellence and committed €25 million for the next 5 years. The new RAN Centre of Excellence is operational since 1 October 2015.

What is the RAN Centre of Excellence?

The Radicalisation Awareness Network (RAN) Centre of Excellence allows experts and practitioners to exchange best practice; the aim is:

(i) to facilitate and enhance the exchange of experiences and cooperation between the relevant stakeholders (inside and outside the EU), in particular through the RAN;

(ii) to support the EU and the Member States in their prevent efforts through different support services, practical tools and policy contributions;

and (iii) to consolidate, disseminate and share expertise, best practices and targeted research in the field of preventing radicalisation.

What is the EU Internet Referral Unit? How can it contribute to prevent terrorism?

The establishment of the EU Internet Referral Unit (IRU) at Europol aims to help reduce the volume of terrorist material online. It was launched on 1 July 2015 (pilot phase). In its first three months, it has made over 550 referrals. The Commission intends to support the IRU in reaching out to more internet companies, as well as encouraging the companies to have adequate arrangements in place to receive referrals from the EU IRU.

What is the aim of the EU Internet Forum with Internet companies? When will it take place?

The Commission is finalising the preparations for the launch of the EU Internet Forum, which will take place on 3 December 2015, with Ministers and CEOs of major internet companies and smaller internet actors. It will provide a framework for more efficient cooperation with the industry. The aim is to contribute to:

(i) reducing accessibility to terrorist material online (removal of content),

(ii) making better use of the internet to challenge the terrorist narrative (development and dissemination of counter narratives),

and (iii) exploring the concerns of law enforcement on new encryption technologies. Communication between terrorists is increasingly taking place using highly sophisticated encryption techniques and this needs to be addressed.

What are the main actions to prevent and fight cybercrime?

Investigating **cybercrime** raises many challenges. The Agenda proposes to reinforce the capacity of law enforcement authorities, in particular through **Europol's European Cybercrime Centre**, and to address the obstacles to criminal investigations on cybercrime, notably in relation to **access to evidence**. In parallel, the implementation of existing legislation on attacks against information systems and on combatting child sexual exploitation will be prioritised.

Furthermore, the Commission is considering proposing updated rules on non-cash payment fraud in 2016. These frauds play an increasingly important role in the financing of organised crime and terrorism, for example enabling offenders to purchase travel and other services with stolen payment credentials.

Risk management and fighting against weapons and explosives

How can the EU help mitigating the risks related to the terrorism threat?

In its European Agenda on Security, the Commission advocated the development of a risk based approach in the field of security, as support to risk mitigation related to the terrorism threat.

The Commission has consolidated and expanded the risk assessment based approach to different domains of security, both in the area of justice and home affairs, and in support of other policy domains (aviation, money laundering and financing terrorism, customs, etc.).

For instance, the Commission is currently working on a number of aviation security risk assessments, which are particularly relevant as support to risk mitigation in view of the severe terrorism threat the EU is facing; They relate to air cargo, passenger-related risks to aviation security, risks from conflict zones and the development of risk criteria for the analysis of pre-loading advance cargo information.

When will the Passenger Name Record (PNR) proposal be adopted?

Tracking the movements of offenders is key to disrupting terrorist and criminal networks. The Commission hopes that the establishment of an EU Passenger Name Record (PNR) system for airline passengers can be adopted by the co-legislators swiftly. Analysis of PNR information provided at the time of booking and check-in helps to identify high risk travellers previously unknown to law enforcement authorities.

With the recent terrorist attacks in Paris, the Commission believes it is of crucial importance to finalise the work on the EU PNR Directive. The Commission will work together with the co-legislators to swiftly achieve a legal instrument which is effective and fully in line with fundamental rights.

The Commission is also considering a horizontal approach for cooperation with third countries on the use of PNR data. In the meantime, the Commission is waiting for an opinion of the European Court of Justice on the draft revised PNR agreement with Canada, and its compliance with the EU Treaties.

Equally importantly, the co-legislators are working on the Commission's proposals on data protection legislation that would offer a more effective protection to citizens and further facilitate the work of law enforcement authorities.

How does the European Commission intend to fight illegal weapons possession and trafficking?

The legal framework on **firearms** will be revised to reduce access to weapons by criminals and terrorists. The Commission intends to propose on Wednesday 18 November a full revision of Directive 477/91 which sets out the legal framework on firearms. The revision will aim at strengthening rules and reducing the legal uncertainty caused by national divergences, thus facilitating the role of national police and investigation authorities.

In addition, if the Member States Committee which is meeting on 18 November 2015 adopts a positive opinion, the Commission will adopt on the same day the implementing regulation on common firearms deactivation standards. It will ensure that deactivated firearms are rendered irreversibly inoperable and cover both domestic and cross-border situations in order to fulfil the security objectives.

The Commission will also adopt on 18 November an Implementation report analysing the current Firearms Directive, to identify existing obstacles to tracing firearms, law enforcement, categorisation and registration of firearms and the treatment of essential parts and components.

In addition, the Commission will also announce new plans to develop an action plan against the illegal trafficking of weapons and explosives. Issues to be tackled in this future action plan could include: the illegal purchase of weapons on the black market; the control of illegal weapons and explosives in the internal market and especially their entry/import into the single market (especially from the Balkan countries or ex-war zones); the fight against organised crime.

What is being done to help detect explosives?

The Commission has started developing practical tools and guidance material such as handbooks to assist practitioners, first respondents and law enforcement specialists; this work is developed in the framework of law enforcement and practitioners networks such as AIRPOL (Airport Police) RAILPOL (Railways Police), the European Explosives Ordinance Disposal Network (EEODN), and the European Dog Detection Group.

The aim is to share experiences, develop best practices and common operational procedures in areas such as new detection technologies, disposal of explosives devices, securing public space and critical infrastructures (including for example the Thalys network). A first classified handbook on aviation soft targets was published last summer, and other such materials are being finalised and will be presented soon to Ministers of Interior.

What is next?

The European Agenda on Security is a shared agenda. It will achieve results in the fight against terrorism and cross-border crime only if all actors concerned do more to work better together, including EU institutions, Member States, EU agencies and relevant civil society actors.

In addition to the ongoing actions mentioned above, the Commission will give priority to the following actions:

Framework decision on terrorism: following the adoption of the additional protocol to the Council of Europe convention of terrorism, the Commission will propose a directive harmonising the criminalisation of offences linked to terrorist travel, passive training, financing and facilitation of such travel.

Freezing of terrorist assets: the Commission intends to finalise its assessment of possible benefits of additional measures in the area of terrorism financing, including measures relating to the freezing of terrorist assets under Article 75 TFEU, to illicit trade in cultural goods, to the control of forms of payment such as internet transfers and pre-paid cards, to illicit cash movements and to the strengthening of the Cash Controls Regulation.

Prüm framework: this is an information exchange tool that is yet to be used to its full potential. It can offer automated comparison of DNA profiles, fingerprint data and vehicle registration data – which are key to detecting crime and building an effective case for prosecutions. The system is falling short of its potential because at this stage only a limited number of Member States have implemented their legal obligations and integrated the network with their own systems. The Commission will continue to prioritise the enforcement of the existing Prüm framework as a matter of urgency and is exploring in parallel the need for and possible benefits to propose a directive to improve cross-border law enforcement information exchange.

Border Package and Smart Borders: Common high standards of border management are essential to fighting terrorism. The Border Package to be presented before the end of the year will create a European Border Guard with much stronger obligations in terms of cooperation. The Smart Borders initiative – planned for 2016 – will provide for a much more effective EU entry/exit system permitting to trace the movements of third country nationals across the EU's external border. This information could be highly valuable for law enforcement.

MEMO/15/6115

Press contacts:

Natasha BERTAUD (+32 2 296 74 56)
Tove ERNST (+32 2 298 67 64)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email