EUROPEAN
COMMISSION

Brussels, 5.5.2014
COM(2014) 247 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on a new EU approach to the detection and mitigation of CBRN-E risks

I. CONTEXT

The EU, its Member States and other key partners have undertaken numerous activities to improve the ability to prevent chemical, biological, radiological, nuclear (CBRN) and explosives incidents and protect citizens, institutions and infrastructure against such incidents.

More needs to be done however. Following the progress reports[1] under the EU CBRN Action Plan[2] and under the Action Plan on Enhancing the Security of Explosives in 2012[3], extensive consultation took place with Member States and other stakeholders on how best to address these issues. A new CBRN-E Agenda was set out to focus on key priorities to be addressed at EU level.

The Council in its conclusions adopted on 11 December 2012 "underlines the need to identify areas with insufficient security arrangements and to focus on and prioritise further common efforts to enhance the security of production, storage, handling and transportation of high-risk CBRN and E materials. Furthermore the Council encourages the Commission "to use the EU Chemical, Biological, Radiological and Nuclear Action Plan, and the Action Plan on Enhancing the Security of Explosives, as a foundation for creating a revised policy."[4]

This communication is a first step in implementing the new CBRN-E Agenda. It aims to bring about progress in the area of detection of CBRN-E threats, and put effective measures in place for detecting and mitigating these threats and risks at EU level.

II. BACKGROUND AND OBJECTIVES

II.1 A changing threat and risk environment

Protecting citizens, institutions, infrastructures and assets is one of the four key pillars of the EU's Counter-Terrorism Strategy[5]. An EU approach to CBRN-E threats must also take into account the EU's Internal Security Strategy[6], with detecting and mitigating CBRN-E risks among its key objectives.

Recent developments – as evidenced by reports from INTCEN[7] or Interpol – give good reasons to believe that the **threat from CBRN materials and explosives remains high and is evolving**. Events such as the terrorist attacks in Madrid, London and Moscow, and the bombings during the Boston Marathon last year, as well as recent advice to jihadists to target crowded places[8], have shown how innovative and opportunistic attackers can be and that threats to public events and urban security must be better detected. Even though terrorists have tended to use commercial or homemade explosives, CBRN agents such as sarin, ricin or

[1] Progress Report on the implementation of the EU CBRN Action Plan, May 2012 (public version): http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/securing-dangerous-material/docs/eu_cbrn_action_plan_progress_report_en.pdf
Progress Report on the implementation of the EU Action Plan on enhancing the security of Explosives (public version): http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/explosives/docs/progress_report_on_explosives_security_2012_en.pdf

[2] Council document 15505/1/09 REV 1

[3] Council document Doc. 8109/08

[4] Council document 16980/12

[5] Council document 14469/4/05 REV 4

[6] COM(2010) 673 final

[7] EU Intelligence Analysis Centre

[8] The 12th (Spring 2014) issue of the Al-Quaeda in the Arabian Peninsula on-line magazine "Inspire" advices jihadists to target crowded places such as sports events, tourist hotspots, election rallies, and festivals using vehicle borne improvised explosive devices

anthrax also represent a serious threat. Ever since the Tokyo metro **chemical** agent (sarin) attack in 1995 and the **biological** agent (salmonella) attack in Oregon in 1984[9], terrorist groups have attempted to acquire capabilities to handle and operate CBRN materials. The recent use of sarin gas in Syria has also brought this issue to the fore.

Thefts and misplacements of CBRN materials occur on hundreds of occasions each year. Recent seizures of highly enriched uranium (in Georgia in 2010 and Moldova in 2011) show that the trafficking of radiological and nuclear materials continues to be a serious problem. More than 150 such cases are reported annually to the International Atomic Energy Agency's (IAEA) Incident and Trafficking Database (ITDB). The many examples of illicit trafficking cases highlight the need to develop effective countermeasures that are not merely based on preventing traffickers from gaining access to such materials, but also on effective detection strategy.

Threats can also emanate from **highly qualified individuals** who have access to sensitive information and materials, such as the senior bio-defence researcher carrying out medical research for the US military who allegedly perpetrated the 2001 anthrax attacks, or the French scientist from CERN[10] who was convicted of helping Al-Qaeda carry out attacks in France.

The EU debate on radicalisation recently intensified. Latest reports suggest that of particular concern are returnees from Syria. Some of these and other **radicalised individuals,** having access to and working in sensitive areas might use their insider knowledge to strike against critical infrastructures, such as a water purification plant, or they may disable railways electrical power supplies. Such insider threats may have transnational impacts and therefore also pose threats to EU security.

A recent example of a **soft target attack** is the 2013 Boston Marathon bombing, where the young attackers, utilised an old bomb making method. This example as well as the earlier metro and rail attacks highlight the need to enhance the detection of threats.

While work at national level continues to play a vital role in the fight against terrorism, a **robust, better designed, and proportionate strategy to anticipate and deter future CBRN-E risks at EU level** is needed, including tackling illegal methods of production, handling, concealing and storing these materials.

It is therefore important to adopt a proactive approach and to put effective, proportional safeguards in place, including **prevention**, **preparedness** and **response** measures at EU level, while respecting fundamental rights.

II.2 Achievements and ongoing work at EU level

The EU and its Member States have already done a lot to address CBRN-E priorities. For instance, the establishment of database tools such as the European Bomb Data System (EBDS) and the Early Warning System (EWS), as well as the activities of the European Explosive Ordinance Disposal network (EEODN). Another example is the new Regulation (98/2013) on the marketing and use of Explosives precursors, which aims to restrict access to dangerous precursors for members of the public.

[9] 1984 religious cult Rajneeshee bioterror attack was the largest biological attack in the US history poisoning more than 750 persons.
[10] The European Organisation for Nuclear Research

In addition to research, training and awareness raising, a number of practical activities have been carried out to identify and share best practices, test and trial new equipment, develop guidance for practitioners, etc.

Progress has been made in all areas, but the recent evaluations of the two CBRNE action plans showed that there is a **need to do more, to prioritise and better focus on key areas of EU added value**.

II.3 Need to address CBRN-E risks at EU level

Several post-attack investigations have shown that explosive materials and precursors to make explosives had been **purchased in one Member State** and transferred **to another Member State** where the attacks took place. Interpol's monthly CBRN-E intelligence reports also show numerous examples of attempts to acquire, smuggle or use CBRN-E materials. Attacks using CBRN substances, such as the case of the Litvinenko radiological poisoning , have shown that CBRN threat substances have been carried undetected in and out of the European Union. Serious radiological or nuclear incidents, or the intentional dissemination of bio-agents (such as SARS, H1N1 or foot-and-mouth disease virus), could severely affect people and economies across Europe.

The *2012 EU Gap Analysis on Detection of Explosives*, carried out as part of the explosives action plan, highlights numerous shortcomings in the detection of explosive threats, despite technological advances, and pinpointing an urgent need to strengthen the EU's detection capability. The report, based on a review of security measures, equipment and processes using state-of-the-art technology, urges further review and stresses the need to strengthen measures in the different areas of public security. On the basis of this gap analysis, the Commission also launched in 2013 an *EU Gap Analysis on Detection of CBRN threat agents*.

CBRN-E threats and risks are common to all EU Member States. The **EU is therefore well placed to play a central role by helping** to detect and mitigate such threats and by ensuring that: i) priority is given to the most serious threat areas, ii) these problems are tackled collectively, iii) there is no duplication and iv) economies of scale and synergies are maximised.

The EU can add value by **developing practical and effective tools for practitioners,** ranging from workshops, guidance materials, training and awareness raising to supporting research and testing activities. One example is the support provided for the collaboration — under the auspices of the ATLAS network — of the EU police special intervention forces which train and operate together.

III. A NEW APPROACH TO THE DETECTION AND MITIGATION OF CBRN-E RISKS

The **objectives** of this Communication are to better assess the risks, to develop countermeasures, to share knowledge and best practices, test and validate new safeguards with the ultimate goal of adopting new security standards.

The following issues need to be addressed in any effective mitigation strategy:

- The *effectiveness and performance* of existing equipment and processes;

- *New threat substances*;

- *New modus operandi* for attacks;

- *New concealment methods* to attempt to by-pass security controls;

- *New attack targets* (soft targets, critical infrastructures, public areas, non-aviation areas)

The new approach will be put into practice **step by step, taking into account each type of threat and environment,** with the aim to:

- improve the detection of risks;

- improve the usage of results of research, testing and validation;

- promote awareness raising, training sessions and exercises;

- promote Lead Country initiatives and engage with industry and other stakeholders in security;

- take into account the external dimension, when appropriate.

Throughout the process it is important to involve all stakeholders, such as academia, private sector or civil protection authorities, in the work and to provide sufficient financial support to ensure that the activities and policies in this area are properly implemented. Under each of the five aspects listed above, actions to which work done by the EU will add value will be identified.

III.1 Better detection

In the past, our threat prevention strategy has typically been based on historical data relating to attacks. Protection measures have often been introduced after the perpetration of attacks or the discovery of plots, and we have not been proactive enough in developing an effective threat detection and mitigation strategy.

An effective threat detection strategy can be achieved only if the threat substances and the environment (aviation, public sports areas, etc.) are taken into account during its development and review.

The approaches used in the past, whereby we try to adjust a security technology or process to the specific threat, do not work. S**pecific risk-based approaches must be considered for each protection mission**, including a range of different activities designed to effectively detect the different threats. Each environment we intend to protect should be carefully analysed and the measures considered should not only take into account historical data, but also ways of mitigating emerging threats.

Any EU detection strategy should build on identified gaps such as highlighted in the 2012 *EU Gap Analysis on the Detection of Explosives.* A recent assessment also indicates that, in spite of significant progress in recent years, a lot of work still needs to be done to efficiently **address shortcomings in detection** technology in the different areas of public security, including transport. The activities need therefore to tackle the weaknesses identified and develop realistic solutions for the risks that we mitigate.

"Insiders" can pose a specific challenge regarding the CBRN-E threat and **more measures against insider CBRN threats** are needed. For instance, one of the actions under the CBRN action plan asks the Commission and Member States to look at how to improve the **security vetting of personnel.** The proper vetting of personnel involved in the whole life-cycle of explosives and CBRN materials is crucial for addressing the issue of insider threats. A study has been done on the subject, which recommends taking steps to harmonise vetting procedures for CBRN-E industries, starting with adopting best practices for background checks and security vetting. Since security check processes are the competence of Member States, the Commission will work closely with them to tackle these issues.

The Commission has been **working with end-users** such as private entities and the law enforcement community to create better awareness of technology capacity. It has done so through workshop-based activities in which law enforcement and other officials have received classified information about the limitations of security technology and processes. We must however do more to involve the end-user and practitioners in the detection design process in the future. Lessons learned during the UK Olympics and the 2012 European football championship in Poland highlighted this key message from the law enforcement community: one detection tool is not always enough, and the combination of tools, such as behaviour detection analyses in combination with explosive detection dogs, can make the system perform better. The detection mission needs to dictate what tool to use, and not the other way round.

The Commission, together with practitioners, is also carrying out various **practical trials** in areas which laboratory environments cannot reproduce. The aim is to evaluate and test technology, products and processes considering different detection objectives in order to make detection more effective. An example of such a trial is 'the testing of CBRN-E detection equipment in conjunction with the Polish authorities during the 2012 European football championship'. Building on this, the Commission teamed up with the Belgian police to test CBRN-E detection equipment during the EU-Africa summit in early April 2014. The trial involved detection activities on the site of the summit and in the Belgian metro, high-speed train and airport environment.

The Commission will

- support further short-term trials for practitioners in order to improve detection during future sport, cultural and other large-scale events, such as the 2016 European football championship; ultimately leading to creation of an EU approach to public events security

- review and build on the gap analysis on the detection of explosives

- carry out a gap analysis on the detection of CBRN materials

- prepare analytical papers and overviews of CBRN and explosives threats and risks in different areas of public security, including transport to support policy

- organize and support more actions dealing with the issue of insider threats, such as workshops, awareness-raising activities and providing guidance on the subject.

- include CBRN risks in the 'cross-sectoral overview of natural and man-made risks the Union may face' that the Commission must establish and update

- build on existing EU networks, and explore together with Member States the establishment of a civil-military cooperation group in the areas of a) detection technologies, and b) methods to counter improvised explosive devices, man-portable air defence systems (MANPADs) and other relevant threats, such as CBRNE threats[11]

III. 2 Using better research, testing and validation

Member States, academia, industry and other stakeholders should work together to pinpoint and **define the needs** that CBRN-E research should meet. The Commission has funded many research activities under the Seventh Framework Programme (FP7). The results need to be

[11] As also stated in COM(2013)542 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a more competitive and efficient defence and security sector

better disseminated and turned into useful commercial products. The new research programme Horizon 2020 should respond better to policy needs and the needs of end-users. The Commission will play a key role in this regard.

1. So far, around €200 million of funding has been allocated to 60 CBRN-related projects under **FP7**. Apart from that, over €67 million was allocated to more than 15 projects focusing on explosives. Examples of these are PREVAIL (*PRecursors of ExplosiVes: Additives to Inhibit their use including Liquids*)[12] and the large-scale demonstration project EDEN[13], highly relevant to the policy and practical work on CBRN-E.

2. The Commission's **Joint Research Centre (JRC)** also provides scientific support for CBRN-E policy needs.

For instance, it has long-standing experience on nuclear safety, safeguards and security, has participated in many research projects and collaborated with key partners. For example, in cooperation with US partners, it implemented the ITRAP+10 project (Illicit Trafficking Radiation Detection Assessment Programme), which aimed to test and evaluate the performance of different radiation detection equipment. The results could help Member State authorities identify detection equipment which best corresponds to their needs. The manufacturers have also received recommendations on how to improve the equipment's performance, reliability and user-friendliness. This work will continue to be supported by the Commission.

JRC is also implementing a project aiming at improving of the IAEA's Incident and Trafficking Database (ITDB). Together with Member States, JRC has prepared a set of best practices on how to improve the ITDB's reporting culture and hence the quality of data available to the IAEA. Moreover, JRC is developing a secure protocol in order to make on-line reporting to the ITDB possible.

3. The Commission has also put in place **cooperation between several law enforcement networks**. The aim is for the networks to better articulate their needs for new technology, and to see if ENLETS (European Network of Law Enforcement Technology Services) could be used as a hub for the law enforcement networks to inform researchers and industry of them.

4. To complement FP7 research activities and support certification and standardisation efforts in different areas, the Commission has been doing **trials and tests** on new equipment. Trials with existing state-of-the-art technology are being launched to find out how it can be best adapted to each sector's needs. Airport experiences should serve as examples of best practices which could be applied to other sectors.

---

[12] PREVAIL, supported by FP7 with an amount of € 4.3 million, was the first project in the 'prevent' strand of the EU CBRN Action Plan. It addressed the security problem posed by chemicals that are available to the public because of their everyday legitimate uses, but that can be misused towards the manufacturing of home-made explosives. A first goal of PREVAIL was to limit the usefulness of these everyday chemicals as explosives or explosives precursors, by identifying inhibitors which can be added to them. A second goal of PREVAIL was to improve the detectability of fertiliser-based homemade explosives, by finding markers that can be added to fertilisers and developing detectors for those markers. PREVAIL thus directly supported EU policy by inhibiting the precursor potential of certain everyday chemicals, limiting the availability of explosive precursors, and improving their detectability and tracking

[13] The flagship FP7 project on CBRN is the large scale demonstration project *EDEN* (with 39 partners, € 24 million EU contribution). The EDEN project will leverage the added-value of tools and systems from previous R&D efforts and improve CBRNE resilience through their adaptation and integration. The concept of the EDEN project is to provide a "toolbox of toolboxes" EDEN Store to give stakeholders access to interoperable capabilities they deem important, or affordable, from a certified set of applications. It will share the burden of development and allows for lessons to be learned and applications to be enhanced.

The trials focus on setting out in detail how the practitioners should use different equipment and processes in different environments (transport, public security, sports events, etc.). They will also give practitioners and Member States input for further refining the tools used to detect threats in their countries.

5. The Commission is also carrying out numerous activities in this area to ensure the harmonised development of standards and testing procedures. Appropriate threat- and risk-based detection standards need to be developed and applied across the EU, so that all its citizens have the same level of protection. Such standards would also help the technology suppliers to better understand specific law enforcement requirements.

Detection standards for responding to known attacks are well developed. However, military technology, practices and experiences should also be considered and adapted – where appropriate - to civilian applications. Law enforcement should work together with military in order to exchange experience and find best solutions to common problems.

The Commission will

- continue to ensure that research takes security policy needs into account, and help develop the programming so that the research priorities reflect law enforcement and other end-user needs, as well as policy needs.

- further support CBRN-E research, testing and validation activities, and progress towards appropriate detection standards adapted to each type of environment, including projects such as ERNCIP (European Reference Network for Critical Infrastructure Protection)

- continue to support ITRAP Phase 2, the follow-up project that will for the first time assess the feasibility of integrating radiological and nuclear risks and explosives detection in the same device. It also helps Member States' laboratories obtain accreditation in the detection of radiological and nuclear risks, evaluate new equipment for detecting radiological and nuclear risks and enabling the definition, in close collaboration with the various standardisation organisations, European or international standards.

III.3. Training, awareness and capacity building

Effective training and awareness raising among the security community is essential for properly implementing security measures. The Commission therefore needs to provide more funding for and **improve training initiatives** that provide the law enforcement community and private industry with the appropriate training support. Below are some examples:

- support the *European Explosives Ordnance Disposal Network (EEODN),* which offers Member States' explosives experts an operational forum to share best practices and train in the areas of explosives and CBRN threats.

- *Improve training facilities for law enforcement practitioners* in order to help Member States deal with CBRN-E risks, for instance through different EU law enforcement networks (Atlas, Airpol, Railpol, Aquapol, etc).

- to help develop a *common approach for dealing with future soft target attacks,* such as after the Burgas airport attack, the Commission is, together with Member States, developing an airport soft target guidance handbook.

- improve civil-military cooperation, such as the joint *European Defence Agency and Commission training* (in spring 2014) on *man portable air defence systems* (MANPAD)

vulnerability guidance and assessment methodology, which will take place in the context of the airport police network (Airpol).

- the *EU Customs Detection Technology Expert Group* that share information and best practices, with the aim of improving detection capability of CBRNE threats and performance standards of existing and new detection equipment.

- training opportunities at the *European Nuclear Security Training Centre* (EUSECTRA) in the areas of nuclear detection, response and nuclear forensics. This will complement national training and be conducted in cooperation with partners from Member States and international organizations. Training programs will comprise multi-disciplinary aspects including law enforcement, radiation protection, and material analysis.

Efforts to **improve awareness and capacity building** should also be stepped up. It should include more work on sharing best practices and developing guidance. Example sof such activities are:

1) *ATLAS, the network of special intervention police units*, is an excellent example of how the EU builds capacity and trust among these units, deployed when other measures fail. Support for such networks help the EU build its capacity to be prepared for crises, create synergies and eliminate duplication among Member States in protecting EU citizens.

2) The *explosives detection dogs working group*, a forum for practitioners, which has successfully promoted the sharing of best practices on training, deployment and certification including guidance materials and handbooks. It consists of Commission and Member States experts, as well as observers from Canada and the US.

3) Home-made explosives and the relative ease with which materials for making bombs can be obtained, highlight the need to do more in this area and to *swiftly implement the provisions of Regulation No 98/2013* on limiting illicit access to explosives precursors that can be used to make bombs.

4) The *human factor* is also important to consider. Besides selection and basic training, processes such as alarm resolution, need to be optimized and fine-tuned in order to ensure that we have skilled operators behind the equipment, well trained and motivated to enhance the person's performance, while making full use of the technology at hand.

5) The recently adopted legislation on the *EU Civil Protection Mechanism*[14] paves the way for the creation of a European Emergency Response Capacity in the form of a voluntary pool of pre-committed response capacities. This includes specific capacities dealing with CBRN incidents (e.g. CBRN detection and sampling modules and Urban Search and Rescue teams for CBRN conditions).

The Commission will

- further develop training tools, encourage the sharing of best practices and develop guidance materials to support practitioners with state-of-the-art training, in particular helping law enforcement practitioners improve their detection practices, for instance through the EEODN activities

[14] Decision of the European Parliament and of the Council No 1313/2013/EU on a Union Civil Protection Mechanism, OJ L 347, 20.12.2013, p. 924.

- continue to raise awareness of the limitations of explosives detection equipment

- publish the EU airport soft target guidance handbook in mid-2014, which will be available to every police officer at EU airports who is a member of the airport police network, Airpol.

- develop model quality control programmes for testing the effectiveness of explosives detection dogs (e.g. Belgium, Hungary, Italy);

- provide MANPAD airport assessments training for members of Airpol;

- help Member States develop explosives detection dog certification protocols, recognised as top global models;

- improve its guidelines on implementing Regulation No 98/2013 on the marketing and use of explosives precursors;

- address the human factor risks by promoting a programme to ensure that those who operate detection equipment are well trained and motivated, and improve communication between industry, security service providers and Member States through workshops and tools and improve the level of security.

- ensure CBRN risks are taken properly into account in the development of the European Emergency Response Capacity

- Closer links with training and exercises provided in the framework of the EU Civil Protection Mechanism should be explored

- expand the portfolio of nuclear security related training courses at the European Nuclear Security Training Centre (*EUSECTRA)*

III. 4. Promote more lead country initiatives and work with industry

The aim of the *lead country initiatives* the Commission launched in 2012 is to get the Member States to implement the CBRN and explosives action plans more actively. The Commission invited them to sign up as lead countries for actions they considered a priority and could coordinate their implementation at the EU level. So far five initiatives have been launched or are about to be launched[15].

Lead country initiatives should be seen as a way of speeding up the start-up phase of a major project. The initiatives cover a wide range of topics. The first one resulted in a project on the security of sales of high-risk chemicals for which the Commission provided funding. Others tackle issues such as security arrangements in facilities handling and possessing high-risk biological agents and toxins, or better spread of research results.

The Commission will enhance the dialogue with the private sector – such as operators of facilities handling CBRN-E materials, equipment manufacturers, and security services providers – to better understand its needs and concerns. The goal is to create an *effective public-private dialogue* on CBRN-E threats and risks, similar to what has been done with

[15] Initiatives officially started:
1. Actions C7 and C11 of the EU CBRN Action Plan; led by the Netherlands and the United Kingdom.
2. Actions B2 led by France
3. Action H29 led by the United Kingdom
4. Action H63 led by Sweden in close cooperation with the Netherlands and the United Kingdom

regard to explosives precursors, with the setting up the Standing Committee on Precursors. This committee includes both Member State authorities and industrial associations.

The Commission will

- proactively engage with stakeholders and organise meetings with Member States' representatives on CBRN-E affairs to better handle prevention, preparedness and response measures;

- set up a platform for the exchange of information between the Commission, Member States and other stakeholders, and organise regular workshops on the research needs of end-users;

- continue to help Member States put forward lead country actions under one or more of the actions in the CBRN or explosives action plans. The Commission will in particular encourage initiatives that address detection issues.

III. 5. The external dimension

CBRN-E threats know no borders, as shown by the SARS and bird-flu (H1N1) viruses. Although the result of the unintended distribution of the virus, the consequences were of global proportions. Threats from commercial and homemade explosives, such as the 2010 Yemen cargo bombs, are another example of external threats that go beyond EU borders.

For this reason, we need to build relationships with, and support preparedness and detection measures, in third countries to ensure that we can adequately protect the EU.

The Commission therefore proposes to *consolidate the implementation of the EU CBRN Risk Mitigation Centres of Excellence initiative*[16], which currently involves more than 44 countries in 8 regions worldwide. This EU initiative provides support and expertise (e.g. assessment of national CBRN needs; drafting of national action plans; regional CBRN projects) to partner countries based on a voluntary and bottom up approach.

It is also important to *continue to cooperate with key international partners*. One example is the EU-US explosives expert forum, which held its fifth EU-US meeting in November 2013. The three working groups on detection, information sharing and training noted good progress in these areas. The forum gives Member States' experts the opportunity to be involved in frequent training exchanges, share information on various bomb-making devices and on CBRN agents using existing mechanisms such as Interpol notices, Europol and the US TRIP*wire* system.

Another example of such cooperation is the third countries' authorities' interest in the explosives detection dogs working group and in EU practices and standards for explosives detection dogs and their potential implementation in Canada.

The Commission also actively participates in international gatherings of experts such as the Nuclear Forensics International Technical Working Group or the Global Initiative to Combat Illicit Trafficking, which serve as a resource for developing good practices and guidance documents.

The Commission will:

[16] Initiated since 2010 under the Instrument for Stability (IfS) and now continued under the new Instrument contributing to Stability and Peace (IcSP 2014-2020).

- work towards deliverables in the EU-US explosives experts context, including by sharing lessons learned from implementing the relevant chemical precursors regulations and other control measures; look at new ways of sharing information and best practices regarding informing members of the public and private sector of improvised explosive device incident indicators and protective measures;

- organise pilot projects providing technical assistance and training in third countries, for instance on vulnerability assessments with a view to help build their capacity. The first training could build on the EU's Airport Soft Target guidance material.

- develop explosives detection dog programmes with the US, using the explosives detection dogs working group's resources;

- support the sharing of EU best practices and information on explosives detection dog programmes with third countries who are interested in such an exchange (Canada, the US and others).

- work with Member States to support the work of international expert groups in Nuclear Security

The Commission will also look into ways to provide **financial support** for the activities proposed.

So far, the current Commission funding programme, the *Prevention of and Fight against Crime programme* (2007–13), has provided more than €20 million of funding for almost 30 CBRN projects and more than 20 projects focusing on explosives. They cover a wide range of activities, from training sessions and activities (such as those of the EEODN) and the development of new detection screening methods, to IT tools for exchanging information, such as the European Bomb Data System (EBDS).

The next funding programme — the *Internal Security Fund — Police* (2014–20) — is being prepared. During the policy dialogues with each Member State, the Commission has emphasised the need for better CBRN-E response capacity, the need to use the systems and databases currently in place for exchanging information (such as SCEPYLT[17], the Early Warning System and the Europol-based EBDS) and the importance of raising awareness of the new regulation on the marketing and use of explosives precursors.

The Commission will better target the use of resources available under the Internal Security Fund and make better use of funding under the new research programme Horizon 2020, so that EU-financed activities better respond to users' needs and are more in line with CBRN-E policies at EU level.

IV. CONCLUSIONS

With the innovation and opportunism shown by terrorists seeking to inflict damages using CBRN-E materials, the EU needs to adopt a more proactive approach to detecting CBRN-E materials. This new step by step approach includes considering each threat and environment, using better research, testing and validation, promoting awareness building, training and

[17] SCEPYLT - Pan European Information System of Explosives Control to Prevent Fight against Terrorism. The system is used for exchange of information on intercommunity transfers of explosives

exercises while engaging all stakeholders. With this approach, the Commission believes it can play an active role at EU level in helping Member States and other important actors to make Europe a safer place for its citizens.

Work is now starting on implementing the initiatives proposed in this communication, which forms the first element of the new CBRN-E Agenda. The first year will be devoted to addressing the most urgent needs with regard to detecting and mitigating CBRN-E risks. At the same time, work will continue with Member States and stakeholders on all other key areas identified in the Agenda. The aim is to propose actions in other areas also to effectively prevent and respond to CBRN-E threats and risks at EU level.