EUROPEAN
COMMISSION

Brussels, 18.10.2017
COM(2017) 610 final

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

Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks

INTRODUCTION: THE EVOLVING THREAT

The EU is currently facing a range of terrorist threats and attacks of a violent nature, from both networked groups and lone actors. Both terrorist groups and radicalised individuals have sought to carry out mass-casualty attacks in the EU with the aim of maximising both the number of victims and the psychological and economic impact on society.

Terrorist organisations have not used chemical, biological, radiological and nuclear ("CBRN") agents in Europe. Still, there are credible indications suggesting that terrorist groups might have the intention of acquiring CBRN materials or weapons and are developing the knowledge and capacity to use them.[1] Daesh has used chemical weapons in Syria and Iraq and is assessed as being able[2] to produce and use these weapons. Smaller incidents have shown Daesh's interest in innovating and in developing biological and radiological weapons.[3] It should be noted that whilst the term CBRN is used throughout the document, the likelihood of a nuclear weapon attack by any non-State actor is considered lower than that of chemical, biological or radiological attacks.

This should be seen against the backdrop of technological developments which might be exploited by terrorists for malicious purposes. Daesh has made use of unmanned aerial systems (UAS), either for surveillance and command or for carrying out attacks with explosives.[4]

The potential of CBRN attacks features prominently in terrorist propaganda, with Jihadist media expressing intentions to commit CBRN attacks and sharing – on various social media platforms – possible tactics for attacks and targets.[5] The CBRN threats have been acknowledged by the United Nations Security Council[6], which expressed concern over the evolving risk of proliferation, including the use by non-State actors.

This underlines the need for the European Union to enhance its resilience and step up its preparedness to deal with the CBRN threat in the coming years.

THE NEED FOR INCREASED EU COOPERATION

This evolving threat requires taking a look at vulnerabilities and our defences against possible terrorist attacks involving CBRN material. CBRN threats so far are considered as low probability but with high impact risks. Even at a small scale, a CBRN attack may have a considerable impact on the societies and economies against which they are used, resulting in significant and lasting disruption, widespread fear and uncertainty. Both the human and

1 Europol, Terrorism Situation and Trend report (TE-SAT) 2017, p. 16, available at: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. See also the statements by the Director-General of the OPCW: www.globaltimes.cn/content/1044644.shtml.

2 Interpol – Assessment of ISIL chemical weapons threats outside of Iraq and Syria, 7 February 2017.

3 In 2016, a Daesh cell preparing an attack with a rudimentary biological weapon was intercepted in Morocco. Interpol - Biological Threats and Incidents Pose Increasing Threat to Critical Infrastructure and Public Health; 24 October 2016. Furthermore, a senior nuclear official in Europe was found to be under surveillance by terrorists linked to the Paris and Brussels attacks. Europol, TE-SAT 2016; page 14. Secrétariat général de la défense et de la sécurité nationale (France), Chocs futurs - Etude prospective à l'horizon 2030, May 2017, p.88: http://www.sgdsn.gouv.fr/

4 The threat of terrorist attacks with the usage of UAS is addressed by the Action Plan to improve the protection of public spaces – COM(2017)xxx.

5 Europol, TE-SAT 2017; page 16.

6 United Nations Security Council, Resolution S/RES/2325 (2016), 14 December 2016.

financial costs associated with attacks, involving for instance a radioactive dispersal device (also known as dirty bomb)[7] or an anthrax attack using unmanned aerial systems, could be extremely high.

Reinforcing resilience against CBRN threats in terms of prevention, preparedness and response, requires significant investments on the part of Member States. It therefore calls for closer cooperation at EU level with a view to learning from each other, pooling expertise and assets and exploiting synergies across borders. The Comprehensive Assessment of EU Security Policy[8] points to the need for increased cooperation at the EU level, based on better understanding of the CBRN threat and pooling of resources with a view to achieve better preparedness for possible CBRN attacks.

The Directive on Combating Terrorism[9] includes for the first time provisions on all strands of CBRN terrorism. It imposes obligations on Member States when it comes to the response to a terrorist attack, including an obligation to provide medical assistance to all victims. The initiatives proposed in this Communication will help Member States to meet their obligations to assist victims when it comes to an attack conducted with the CBRN materials.

This Action Plan aims to increase the European cooperation to strengthen CBRN security with a focus on preventing, preparing for, and responding to CBRN threat and terrorism attacks. Actions set out in this Communication will support Member States to protect citizens and infrastructures. Many of the proposed actions pursue an all-hazards approach and will also contribute to improving preparedness for any large scale CBRN incidents unconnected to terrorism.

BUILDING UPON THE 2010-2015 CBRN ACTION PLAN

This Action Plan builds upon the work launched in the EU with the 2010-2015 CBRN Action Plan.[10] It addresses the gaps identified in its implementation and takes into account emerging threats. At EU level, the 2010-2015 Action Plan has led to a better understanding of the threat, more information sharing (development of a CBRN-E Glossary and inclusion of CBRN incidents in the European Bomb Data System), and achievements such as the development of an EU training infrastructure (European Nuclear Security Training Centre – EUSECTRA). The biological area has also seen an important legislative development with the adoption of Decision 1082/2013/EU on serious cross-border threats to health, which sets up provisions to strengthen preparedness and response planning in the EU.

Member States consulted on the implementation of the 2010-2015 Action Plan reported a large number of activities taking place at national level, including trainings and exercises. They reported also some difficulties in ensuring coordination of different actors. Stakeholders emphasised for instance the need to further deepen knowledge on CBRN risks, promote cross-

7 See for instance von Winterfeldt, Detlof and Rosoff, Heather, "A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach" (2007). Published Articles & Papers. Paper 39. http://research.create.usc.edu/published_papers/39. The authors assessed the consequences of a dirty bomb attack at the port of Los Angeles. Apart from decontamination costs, for instance the impact of shutdown of the port and related businesses would cost up to 100 billion EUR. https://pdfs.semanticscholar.org/5cc0/3b4436d06165aac72041315c824fbef44d5b.pdf.

8 COM(2017) 407, SWD(2017) 278 final. 26.7.2017.

9 OJ L88 of 31/3/2017, p. 6.

10 Council of the European Union, document 15505/1/09 REV 1, adopted in December 2009 by the Council with the aim of strengthening CBRN security throughout the EU.

sector cooperation and investing further in trainings and exercises.[11] Providing cross-border/cross-sectoral trainings and exercises – ideally organised in a structured way and following pre-agreed curricula – was identified as one of the areas where the EU can add value. Member States also pointed at insufficient information exchange on CBRN incidents, threats, equipment and technologies developed to tackle these threats. They underlined also the need to develop cooperation with other partners not covered by the previous CBRN Action Plan, such as military and key third countries.

SETTING OUT A MORE FOCUSED AND COORDINATED APPROACH

Building on these achievements, this new Action Plan takes a targeted approach, in line with the 2012 EU CBRN-E Agenda, in which the Council asked the Commission to develop a more focused policy, addressing a selected number of key priorities with clear EU added value and tangible outcomes.

The Action Plan provides an opportunity for Member States to strengthen their preparedness capacity against the evolving threats through voluntary participation in a series of initiatives proposed under the Action Plan.

This Action Plan is rooted in the firm belief that tackling CBRN risks requires a horizontal approach, cutting across diverse areas and actors such as law enforcement, emergency management, protection of critical infrastructure and public spaces, public health, and the private sector. Some of the actions proposed will also contribute to an increased resilience of critical infrastructures in the EU, especially as regards nuclear plants and chemical facilities.

There is also a clear need to increase internal-external security actions, focusing efforts in particular through the EU CBRN Centres of Excellence initiative. One key priority will be to ensure border security and detection capacity against illicit entry of CBRN materials. Customs officials play a key role in ensuring external border and supply chain security. Adapting cargo information systems is essential to strengthening monitoring and risk based controls of international supply chains in order to ensure that CBRN material are not illicitly entering into the EU. Measures to strengthen dual-use trade controls at export are also required. Cooperation and coordination with EU strategic and regional partners is essential, and synergies will be sought with all relevant stakeholders, including military actors, the EDA and NATO, as well as the private sector.

The Action Plan therefore pursues the following four objectives:

(1) Reducing the accessibility of CBRN materials,

(2) Ensuring a more robust preparedness for and response to CBRN security incidents,

(3) Building stronger internal-external links in CBRN security with key regional and international EU partners, and

(4) Enhancing our knowledge of CBRN risks.

11 As part of the review, Member States were also asked specific questions regarding future priority areas for cooperation.

By pursuing work across these pillars, the EU can provide a more robust framework for reducing the threat of CBRN attacks, strengthening security measures, increasing resilience and preparing for an effective response in case of attack.

The proposed actions will be supported by mobilising funding under the different existing instruments of the Commission, including Horizon 2020, ISF-Police and the Union Civil Protection Mechanism (UCPM) or the wide range of external financing instruments (e.g. Development Cooperation Instrument, European Neighbourhood Instrument, Instrument contributing to Stability and Peace).

OBJECTIVE 1: REDUCING THE ACCESSIBILITY OF CBRN MATERIALS

The capability of terrorists to carry out CBRN attacks depends on the accessibility of agents, substances and materials needed for CBRN weapons. Similar to the work already done for explosives and firearms, the EU needs to better control access to high risk CBRN materials and to optimise our ability to detect such materials at the earliest stage possible, restricting or controlling access. The significant issue of insider threats to critical infrastructure and facilities possessing CBRN materials also needs to be addressed. Moreover, there is a clear need, acknowledged by EU Member States, to further improve the exchange of information on CBRN materials, including threats and security incidents such as thefts or trafficking thereof. This can be achieved by maximising the use of existing tools and information sharing systems.

The Commission therefore sets out the following priority actions that need to be taken in close cooperation with Member States and other stakeholders.

Commitment		Action	Deliverable and Timeframe
1.1	Optimise the exchange of information on CBRN	Member States to more systematically include technical information on CBRN weapons and incidents in the European Bomb Data System (EBDS)[12] managed by Europol. Consideration should be given to the feasibility to establish a reporting system mirroring what is in place in the field of explosives precursors.	Europol to regularly report to the EU CBRN Security Advisory Group on the use of the EBDS (starting as of 2018). Commission to work with EU Member States to improve information sharing through EBDS.

12 European Bomb Data System (EBDS) is an IT platform which allows Member States to share timely and relevant information and intelligence on explosives and CBRN materials and related incidents. Since it requires a higher level of secure connection, Europol created a complementary on-line-based Europol Platform for Experts, where users can interact and collaborate with each other via virtual communities.

		Better use of other information sharing tools such as the Incident and Trafficking Database[13] at IAEA[14]. Explore links with other information systems – such as DUeS, the Dual-Use Electronic System[15], with information on items and persons are suspected of "harmful" trade.	Europol to conduct a mapping of information systems, needs and possible shortcomings in terms of information exchange by mid-2018).
1.2	Strengthen risk-based customs controls to intercept dangerous CBRN materials at the border	Improve cargo information from trade and enhance detection capacities for customs in cooperation with other agencies to monitor international supply chains in order to detect and control illicit entry of CBRN materials. Raise awareness of CBRN threat among customs and law enforcement, improve inter-agency cooperation and information-sharing between customs and other authorities, in line with the EU Strategy and Action Plan for customs risk management (COM (2014) 527)	Agreement with Member States (mid-2018) to establish common repository of cargo information. Customs Detection Technology Project Group to explore detection capability for Biological and Chemical materials in international supply chains. Report by Mid 2018 Extend the Radiological/Nuclear training for law enforcement, customs officers and other front line agents at EUSECTRA[16] training facility
1.3	Strengthen EU export controls	Preventing external actors (state and non-state) to access dual-use / CBRN items through trade	Update the EU lists of CBRN high risk materials in 2018 and assess the scope and nature of

13 Incident and Trafficking Database (ITDB) is the IAEA's information system on incidents of illicit trafficking and other unauthorized activities and events involving nuclear and other radioactive material outside of regulatory control.

14 International Atomic Energy Agency.

15 Dual-use e-System (DUeS) is a secure electronic system hosted by the Commission for exchanging information among Member States. It has been fully operational since 2012 and it aims to improve the exchanges of denials of dual-use items between EU Member States. The main information processed covers the description of the goods under denial and the parties involved in the denials such as the Member States, the exporter, broker, consignee and end-user.

16 The European Nuclear Security Training Centre has been established to address concerns of theft of radioactive materials that could be associated with crime and acts of terrorism. It provides hands-on-training using real nuclear material to front line officers, trainers and other experts in the field. The centre is located at the European Commission Joint Research Centre in Karlsruhe and Ispra.

			technical interactions between "CBRN" and "dual-use" items
1.4	Address insider threats	Exchange best practices on vetting and background checks in facilities holding CBRN materials such as biological laboratories or nuclear facilities.	A mapping of existing vetting practices to be finalised by end 2017.

OBJECTIVE 2: ENSURING A MORE ROBUST PREPAREDNESS FOR AND RESPONSE TO CBRN SECURITY INCIDENTS

Operational preparedness is crucial in order to effectively mitigate the impact of a CBRN attack or incident. Given the inherently cross-border and transnational nature of the CBRN threat, EU cooperation can add value by encouraging capacity building activities in the EU, such as cross-border cooperation in training, exercises and response, facilitating mutual assistance, providing guidance, promoting minimum standards across the Union, and where needed, funding for trans-national projects in this area.

The Commission has already organised numerous training sessions and exercises at the EU level focusing on cross-sectoral cooperation in case of CBRN attacks. For instance, the 2014 ARETE exercise focused on cooperation between law enforcement and civil protection in case of a complex chemical and terrorism situation including hostage-taking. Moreover the Commission funded a series of training courses organised in cooperation with the Member States' authorities on cross-sectoral response to a radiological dirty bomb attack. These initiatives were complemented by exercises organised in the civil protection area and trainings organised by Europol and CEPOL.

Further actions will build on these experiences and bring the various preparedness and response initiatives together in a coherent programme, maximising the training and exercise opportunities for Member States and enhancing consistency in Member States' approaches.

Additional actions facilitating multi-agency cooperation will be identified following the EU workshop on cooperation of first responders at the disaster scene following terrorist attacks, held in October 2017. In case of a major CBRN incident, the response will require the involvement of various stakeholders, including private actors, e.g. when it comes to ensuring that medical countermeasures are available.

The Commission therefore sets out the following priority actions that need to be taken in close cooperation with Member States and other stakeholders.

Commitment		Action	Deliverable and Timeframe
2.1	Strengthen EU CBRN preparedness and response through cross-	The Commission in cooperation with Member States will strengthen training and exercises for first responders from the law enforcement, civil protection, health structures and, where relevant, borders and	A mapping of existing EU training activities by January 2018

	sectorial training and exercises	customs authorities and military partners. Training and exercises will be carried out through existing financial instruments and operational tools, in particular the Union's Civil Protection Mechanism (UCPM), CEPOL and the ISF-Police. The development of a common EU CBRN training curriculum will be promoted in close cooperation with EU Member States' experts.	EU Advisory Group to consider additional needs by Q2 2018 Roll-out of new training and exercises starting in Q4 2018 Conduct further exercises at EU level (similar to the ARETE exercise in 2014) in 2019
2.2	Strengthen the EU's response capacity for CBRN incidents under the EU civil protection mechanism	In order to provide better support to Member States in the event of a major CBRN incident, Member States and the Commission will continue strengthening the existing European Emergency Response Capacity (EERC) of the UCPM, including the EU Medical Corps. Encourage Member States to continue committing new CBRN capacities to the EERC. Support Member States in the process of registering and certifying CBRN modules and other capacities into the EERC. Review the initial capacity goals in the field of CBRN disasters. Test cross-sectorial preparedness and response to pandemics.	Assess gaps in the field of CBRN disasters response in 2018. Adaptation grants for registration/ certification of modules Cross-sectorial table top exercises on business continuity planning during a pandemic (2018) Workshops on preparedness and International Health Regulations implementation and on best practices regarding entry and exit screening. Planned for 2017-2018.
2.3	Conduct a gap analysis on the detection of CBRN materials	In close cooperation with the CBRN Advisory Group, the Commission will examine the extent to which existing detection equipment can detect CBRN materials. Results will feed into detection pool activities and work on standardisation.	Initial gap analysis report with recommendations by Q3-2018
2.4	Improve early warning and response as well as information exchange regarding	Re-engineer the Early Warning and Response System (EWRS) with a view to improving situational awareness and incident management for serious cross border threats to health as well as to link EWRS to other EU rapid alert and information systems.	New platform to be ready by mid-2018

	serious cross-border threats to health[17]		
2.5	Strengthen preparedness of laboratories in the EU against serious cross-border threats to health	Ensure rapid identification and characterization and rapid sample sharing mechanisms; provide support to less equipped Member States.	2015-2018 Implementation by Member States with Commission support in the framework of the EMERGE Joint Action[18] on Efficient response to highly dangerous and emerging pathogens at EU level.
2.6	Increase preparedness of Member States for cross-border threats to health	Increase preparedness of Member States for cross-border threats to health via joint procurement of medical countermeasures (based on Article 5 of Decision 1082/2013/EU on serious cross-border threats to health). Strengthen preparedness as well as actions at points of entry (air, maritime and ground crossing. Member States and the Commission to develop a shared vision at EU level on how to improving vaccine coverage in the EU, and start actions to strengthen vaccine supply and stock management, enhance the interoperability and interaction of immunisation information systems, improve vaccine confidence and tackle hesitancy, and increase the effectiveness of vaccine research and development at EU level.	Joint procurement of vaccines together with the Member States concerned; 2018 (preparations ongoing) 2017-2020 (Joint Action in preparation) 2017-2020 (Joint Action in preparation)
2.7	Improving awareness, preparedness and response to bio-risks, including emerging	Strengthen EU's cross-sectoral awareness on bio-risks arising from accidental or voluntary releases through training, such as the joint European Centre for Disease Prevention and Control (ECDC)/Europol course on "*Cross-sectoral biorisk awareness and mitigation training*" for health	Next edition of the course in Q2-2018 (further sessions to be arranged as needed)

17 As defined in the Article 2 of the Decision 1082/2013/EU on serious cross-border threats to health: 1. threats of biological origin (communicable diseases; antimicrobial resistance and healthcare-associated infections related to communicable diseases (hereinafter 'related special health issues'); biotoxins or other harmful biological agents not related to communicable diseases; 2. threats of chemical origin; 3. threats of environmental origin; 4. threats of unknown origin; 5. events which may constitute public health emergencies of international concern under the IHR, provided that they fall under one of the categories of threats set out in points (a) to (d).

18 http://www.emerge.rki.eu/Emerge/EN/Home/Homepage_node.html.

	threats	emergency services, law enforcement and civil protection. Support Member States in their fight against bioterrorism, including elaboration of national preparedness strategies for bioterrorism issues via development – in collaboration with network of experts from Member States – of an EU focussed handbook on bioterrorism threats. ECDC will help Member States raise awareness and exchange best practices as regards "Do it yourself" (DIY) biology, including amateur experimentation, use of biological agents and genetic engineering techniques outside laboratory environments and by non-trained individuals and risks for biosafety and biosecurity[19].	Development of the handbook by Q3 2018 Awareness raising material on risks related to emerging biotechnologies The activity will start in Q3 2017 and will continue in Q4 2017 – Q1 2018
2.8	CBRN detection pool of Member States' experts	Extend the explosives detection pool[20] to CBRN experts with a view to assist Member States with e.g. securing large scale events. Activities of the detection pool will be based – among others - on the guidance material developed for the protection of public spaces.	Training for detection pool experts – Q3-2018 with a view to be operational in 2019.
2.9	Reinforce nuclear security capacities and networks	Promote full use of European Nuclear Security Training Centre (EUSECTRA) for joint trainings in radiological and nuclear detection.	Customs Training campaign phase-2 at EUSECTRA to be launched in Q4 - 2017
2.10	Enhance cooperation in the area of nuclear forensics	The scope and comprehensiveness of nuclear forensic capabilities vary significantly with only a few Member States being able to perform in-depth examination of nuclear and radioactive material. Most Member States rely only on core capabilities, which are complemented by the more advanced ones offered i.a. by the Commission's Joint Research Centre.	Develop legal framework for using the Commission services capability in the nuclear forensics domain – by the end of 2018

19 Commercially available "do-it-yourself" bio-kits make it possible for a user to produce genetically modified microorganisms. Progress in this area may lead to intentional attack or accidental contamination with modified viruses or bacteria. See also: European Centre for Disease Control, Rapid Risk Assessment: Risk related to the use of 'do-it-yourself' CRISPR-associated gene engineering kit contaminated with pathogenic bacteria, https://ecdc.europa.eu/en/publications-data/rapid-risk-assessment-risk-related-use-do-it-yourself-crispr-associated-gene.

20 The pool was introduced in the 2015 EU action plan against illicit trafficking in and use of firearms and explosives (COM(2015) 624 final) with an aim to provide Member States operational support in the area of detection of explosives.

		The Commission will further develop the legal framework (agreements with Member States) for using these Commission services and to provide - both general and advanced - training to Member States in this area.	

OBJECTIVE 3: BUILDING STRONGER INTERNAL-EXTERNAL LINKS AND ENGAGEMENT IN CBRN SECURITY WITH KEY REGIONAL AND INTERNATIONAL EU PARTNERS

CBRN threats can arise from both inside and outside the Union. Working beyond the Union as well as building stronger partnerships and closer internal-external security links are an inherent part of the EU's strategy to counter-terrorism and CBRN risks. The call for a more "joined-up Union" between the internal and external dimensions of security policies is a key priority in the EU Global Strategy[21]and in the context of the 2016 EU-NATO Joint Declaration .

CBRN security needs to be mainstreamed in the EU's external action, through the development of capacities in third countries (notably in neighbouring countries), enhancing cooperation with strategic partners as well as specialised international organisations, such as Interpol, IAEA, OPCW building on the renewed commitment of the UN Security Council to prevent terrorists from acquiring weapons of mass destruction. There is also a need to develop closer links between activities undertaken within the framework of EU CBRN Centres of Excellence. In this regard, priority should be given to the EU Neighbourhood countries.

The Commission therefore sets out the following priority actions that need to be taken in close cooperation with Member States and other stakeholders.

Commitment		Action	Deliverable and Timeframe
3.1	Develop CBRN security cooperation with key international partners, including in the context of the CT/Security dialogues	Deepen cooperation with strategic partners experienced with CBRN: (1) sharing of information on CBRN threat and risks; (2) exchange of best practices; (3) joint trainings or exercises. Discuss on a regular basis CBRN security in the CT/Security dialogues with relevant third countries, with a view to identify possible cooperation and capacity-building actions.	In the context of the existing CBRN dialogue, hold a workshop on security of radioactive sources with the United States – Q2-2018 EU-US workshop on joint criminal-epidemiological investigations – Q4-

22 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy. http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

			2018 Invite strategic partners to dedicated sessions of the CBRN Security Advisory Group, where appropriate.
3.2	Develop cooperation with NATO on CBRN related issues	Work towards closer cooperation with NATO in relation to third countries, notably in the fields of: (1) information exchange; (2) capacity building; (3) training; (4) exercises. Develop synergies with NATO on how counter-terrorism may benefit from defence capability development inter alia in the areas of Unmanned Airborne Vehicles (UAVs), and Chemical Biological, Radiological and Nuclear (CBRN) weapons. In cooperation with the NATO-accredited CBRN Centre of Excellence design tailor made training modules for EU CBRN Centre of Excellence partners.	EU-NATO workshop – Q1/2-2018. Common trainings, e.g. in NATO-accredited CBRN CoE (Q4 2017) and envisaged for 2018/ 2019/2020 2018, based on lessons learned from first rounds of common trainings.
3.	Develop cooperation with specialised international organisations	The EEAS and Commission will engage with specialised multilateral organisations (Interpol, IAEA, OPCW[22], BWC ISU[23], UNODA[24]) to share best practices and look for synergies notably in the field of information sharing and capacity-building in third countries.	Regularly invite these organisations to the CBRN Security Advisory group as well as trainings and exercises

OBJECTIVE 4: ENHANCING OUR KNOWLEDGE OF CBRN RISKS

CBRN is a technically complex and rapidly developing area which needs close monitoring. At present, CBRN expertise is distributed unevenly within the European Union and spread across many different governmental, academic and private actors. An EU-wide framework is needed to bring relevant actors together, to build partnerships across these sectors, collectively identify further needs and harness the benefits of EU Research.

4.1 Creation of an EU CBRN security network

22 Organisation for the Prohibition of Chemical Weapon.
23 Biological Weapons Convention – Implementation Support Unit.
24 United Nations Office for Disarmament Affairs.

To improve coordination at EU level, an EU CBRN security network will pool together all CBRN actors at both strategic (policy-making) and operational levels to overcome the fragmentation of efforts. It will bring together Member States, EU institutions and relevant agencies, and where appropriate key international partners and the private sector. The network will rely on three pillars: 1) an advisory group bringing together all CBRN security coordinators of the MS, 2) a support network composed of existing CBRN centres across the EU and 3) a CBRN knowledge hub set up in the European Counter-Terrorism Centre (ECTC) in Europol.

Its objectives will be to (1) maintain a comprehensive and updated understanding of CBRN risks coming from inside and outside EU and to support the formulation of policies and initiatives to address identified gaps; (2) develop cooperation and coordination at operational level (e.g. information exchange, exchange of best practices); and (3) facilitate civil-military cooperation in areas which are mutually beneficial.

Commitment		Action	Deliverable and Timeframe
4.1.1	Set up a dedicated Advisory Group on EU CBRN Security	Member States to appoint national CBRN Security Coordinators, as primary points of contact in Member States for the implementation of the EU CBRN Security Action Plan. Building upon the previous CBRN advisory group, which was created under the 2010-2015 Action Plan with the mandate of overseeing its implementation, the Commission will set up a new dedicated Advisory Group on EU CBRN Security for the purposes of the present Action Plan, bringing together Member States CBRN Security Coordinators, the Commission and relevant EU agencies, the European External Action Service and other relevant public and private CBRN stakeholders, which will: (1) regularly review and analyse the evolving CBRN threats and risks (in cooperation with INTCEN and Europol); (2) identify gaps in CBRN prevention, detection, preparedness and response measures, and advise on new policy initiatives to address those gaps; (3) map existing centres of expertise and identify collaborative arrangements to encourage synergies and complementarity.	A list of coordinators in all Member States by December 2017. A first meeting of the Advisory Group by January 2018 and periodically (2-3 meetings /year) afterwards A first gap analysis by April 2018 and to be reviewed periodically A regular and systematic exchange of good practices on identified risks and gaps A first mapping of existing centres of expertise by May 2018.
4.1.2	Creation of an EU CBRN	At operational level, an EU CBRN Support Network composed of existing CBRN centres	Commission to publish a call for

	Support Network	of expertise and networks will feed into the CBRN Security Advisory Group in: (1) developing a EU expert support structure (in close cooperation with Europol) which can provide guidance and advice also on technical and scientific issues to Member States and EU institutions on CBRN security, including during incidents; (2) facilitating the identification and dissemination of good practices and lessons learned; (3) sharing expertise and liaising with existing CBRN centres of excellence in Europe and outside. Interested Member States will be asked to identify by December 2017 structures which could feed into an EU CBRN Support Network.	CBRN project proposals under ISF-Police by October 2017[25] A fully operational Network by summer 2018
4.1.3	Europol (ECTC) to develop a knowledge hub on CBRN	Europol (ECTC) to develop its existing CBRN team into a knowledge hub to support law enforcement authorities on CBRN security, including weapons and threats: (1) supplying analytical products on CBRN threats and incidents; (2) facilitating cooperation and exchange of information (notably via EBDS, and networks such as EEODN[26]) between law enforcement and other actors (including military), as well as with its network of international partners; (3) organising training (in cooperation with CEPOL); (4) providing operational support and deploying CBRN expertise to support investigation of CBRN incidents	Optimise the use of existing Europol capabilities to enhance collective knowledge on CBRN threats Systematic sharing of CBRN-relevant information via EBDS Deploy CBRN expertise to assist investigations

4.2 Harnessing the benefits of EU security research

Exploiting better EU security research via dissemination activities for research results, as well as via ensuring that research activities respond to the operational needs in the area of CBRN.

25 The call for proposals will support implementation of this Action Plan as well as the EU Action Plan on the protection of public spaces as well as the Commission Recommendation on the implementation of Regulation 98/2013. The call can support – among others - developing an EU expert support structure or regional networks, which will later be part of the Support Network.

26 European Explosive Ordnance Disposal Network (EEODN) is a network of bomb technicians and CBRN experts managed by Europol. The network allows its members sharing of best practices and lessons learned as well as common trainings. EEODN organises yearly conferences combined with trainings.

The Commission will extend the testing of equipment, encourage harmonisation of standards and support the development of shared capacities via its extended detection pool of experts.

Commitment		Action	Deliverable and Timeframe
4.2.1	Support the dissemination and take-up of research results	Further develop the Platform of the Community of Users on Secure, Safe and Resilient Societies (CoU), which gathers researchers, policy makers, industry/SME representatives and practitioners including first responders, to translate research outcomes into practical action. Increase the dissemination of research results and promote information exchanges to enhance the dialogue among different actors, in the CBRN area, and provide regular update about research outputs also in the context of the EU CBRN Security Advisory group and its support network	2018 CoU planning to be presented in November 2017, covering 18 thematic workshops, including 6 CBRN-related topics like chemical hazards or water safety and security. The workshops will provide an annual update on ongoing research and capacity building activities and identify future priorities Mapping report of H2020 projects covering the 2014-2016 calls to be finalised by December 2017 Regularly publish results from CBRN research projects via the EU CBRN security network
4.2.2	Identify further research needs and address emerging CBRN threats	Ensure that research projects focus on the needs of end-users in the CBRN area Prioritise research efforts to: (1) provide solutions on how to mitigate emerging CBRN threats, such as UAS or bio-hacking; (2) enhance Member States' disaster risk reduction capacities, from preparation/preparedness, monitoring to response and recovery.	Continuous dialogue in the various EU fora, such as the CBRN advisory group, New actions under the Horizon 2020 2017 call New CBRN projects selected from the call 2017 starting in Q1-2018 A CBRN security call for proposals in Q2-2018
4.2.3	Encourage	Extend the current testing of CBRN detection	Enhance the capacity

	harmonisation through standardisation and certification for CBRN security products and systems	equipment with a view to propose areas for standardisation. This work will also help inform practitioners on equipment performance and provide training to the detection pool experts. Continue pre-normative research activities within the framework of the Commission's European Reference Network for Critical Infrastructure Protection[27] with an aim to develop CEN[28] Workshop Agreements; identify CBRN areas in which mandates to CEN can be launched and launch new calls in support of CBRN standardisation under Horizon 2020.	of performance testing of CBRN detection equipment in MS and identify standardisation needs prone to mandates to CEN by the end of 2018. Calls for standardisation-related research in Q2-2018 and Q2-2019

CONCLUSIONS

In light of the evolving threats, Europe needs to pool resources and expertise to develop innovative, sustainable and effective solutions. Cooperation efforts across the EU along the lines set out in this Action Plan can result in significant security gains and lead to tangible results.

The proposals set out in this Communication will pave the way for a more effective and focused EU cooperation in the protection, preparedness and response against chemical, biological, radiological and nuclear threats. The Commission encourages Member States to take advantage of the various opportunities set out in this Communication, and invites the European Parliament and the Council to endorse this action plan and to actively engage in its implementation, in close cooperation with all relevant stakeholders. The Commission will review progress at the latest after two years.

27 The European Reference Network for Critical Infrastructure Protection (ERNCIP) is the Commission co-financed project coordinated by Joint Research Centre aiming at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards and to the creation of a single market for security solutions. Three of the working groups deal with CBRN threats: chemical and biological risks to drinking water; detection of indoor airborne chemical-biological agents and radiological and nuclear threats to critical infrastructure.

28 European Committee for Standardisation.