European Commission

A Community of Users on Secure, Safe and Resilient Societies

Mapping Horizon 2020 and EU-funded Capacity-Building Projects under 2016-2018 Programmes

October 2019

Migration and Home Affairs

Printed by Bietlot in Belgium

Manuscript completed in 2019

1st edition

Luxembourg: Publications Office of the European Union, 2019

Print	ISBN 978-92-76-12419-1	doi: 10.2837/51066	DR-03-19-812-EN-C
PDF	ISBN 978-92-76-12420-7	doi: 10.2837/89145	DR-03-19-812-EN-N

Responsible Editor: Philippe Quevauviller (European Commission, DG HOME.B4). This document has been prepared by the Secure Societies Programme (Horizon2020). It does not reflect a formal position of the European Commission nor does it represent an exhaustive list of all projects related to security research.

This document has been prepared by Ecorys Research and Consulting for the European Commission.

A Community of Users on Secure, Safe and Resilient Societies

Mapping Horizon 2020 and EU-funded Capacity-Building Projects under 2016-2018 Programmes

October 2019

Contents

1. EXECUTIVE SUMMARY

In a world facing a growing risk of man-made and natural disasters resulting from increasingly frequent and severe natural, industrial and man-made hazards, the security of citizens, infrastructure and assets and the environment protection have become a high priority in the European Union. Strengthening capacities in disaster risk / crisis management and improving resilience in the fields of CBRN-E (Chemical, Biological, Radiological, Nuclear and Explosive) and natural and man-made disaster management, as well as in the areas of border security and the fight against crime and terrorism, represent key EU policy and research challenges.

The overall EU security policy framework covers many different sectors, which require coordination among various communities. In this respect, policy development and implementation rely on effective interactions among policy-makers, research, industry (including SMEs) and operational actors (first responders, civil protection units, police forces etc.) in the EU Member States. This requires a proper exchange of information and communication about either policy updates or (research) project results, which should be tailor-made to different sectors concerned with the goal of enhancing the transfer of research solutions or new policy recommendations to users in a timely and relevant fashion. Such exchanges are also needed to identify and address users' needs regarding research, technologies and policies, in order to better design funding programmes at an EU level. Finally, a proper transfer of knowledge from research to policy and operational sectors may have a positive impact on policy formulation and review.

However, the policy complexity, the high number of research projects, the difficulties associated with bringing innovative tools to the market and the lack of "interfacing" mechanisms make it difficult to efficiently reach these goals. In order to improve this situation, the European Commission is funding various types of projects, including large-scale demonstration projects. These projects, along with different policy committees and think-tanks, develop networks with users' groups in the Member States which have great potential but are currently too fragmented. In this respect, the need to build a "Community of Users" in the EU based on existing users' communities has been expressed in various fora. Discussions with different actors have hence taken place over the past months and a mapping of policies and research projects has been carried out in light of operational features regarding the overall risk management cycle (from preparedness / prevention, detection / surveillance, response / recovery) and the need to ensure a proper transfer (and implementation) of research outputs to users.

This working paper is built on the mapping exercises carried out in 2016 and 2018 of H2020 and FP7 projects which presented the reasoning for the development of a Community of Users on Secure, Safe and Resilient Societies[1]. The iteration of the mapping document at hand focuses on mapping H2020 projects funded under the 2018 calls for proposals. It will be complemented by projects resulting from the 2016-2018 calls for proposals and capacity-building projects funded by different EU instruments (ISF, ECHO, LIFE+, INTERREG) and projects funded through the Marie Skłodowska-Curie Actions and the Erasmus+ programme[2].

This document does not reflect a formal position of the European Commission nor does it represent an exhaustive list of all projects related to security research.

1 A Community of Users on Secure, Safe and Resilient Societies (CoU) – Mapping EU Policies and FP7 research for enhancing partnerships in H2020 and A Community of Users on Secure, Safe and Resilient Societies (CoU) - Mapping Horizon 2020 and EU-funded Capacity-Building Projects

2 For the Erasmus+ programme the following funds have been included in this mapping: Jean Monet Chairs programme and Innovative Actions.

2. OVERVIEW OF TASKS AND OBJECTIVES

2.1 Background

The management of disaster risks and crises of different kinds (unintentional or intentional man-made disasters, natural hazards) as well as other security / safety issues in the areas of border control, supply chains and crime are ruled by a number of international, EU and national policies covering various sectors and operational features such as preparedness, prevention, detection, surveillance, response, and recovery. A wide range of research and technological developments, as well as capacity-building and training projects, are striving to support the implementation of these policies. However, the complexity of the policy framework and the wide variety of research, capacity-building and training initiatives often leads to a lack of awareness about policies and/or project outputs by the among users, namely policy-makers, scientists, industry/SMEs and practitioners, e.g. civil protection units, medical emergency services and police departments. Highly fragmented information often leads to poor awareness of policy requirements by research and industry communities and poor transfer of research results to policy and stakeholders communities.

2.2 Objectives

In the light of the above, there is a strong need to establish a mechanism enabling better information exchanges with regular updates for all possibly interested organisations and effective interactions among projects and different communities. To better understand the type of information that should be considered and how it fits to a larger "architecture", a mapping exercise was carried out to highlight the scientific and technological challenges of key related policies and their possible matching by research projects funded by the 7th Framework Programme. A first step is to build up the framework of science-policy-industry-practitioner's interactions and to figure out how an efficient mechanism of information transfer could be made operational at EU and national levels in the light of Horizon 2020 developments. This is the core objective and mission of the **Community of Users on Secure, Safe and Resilient Societies**. More specifically, five key objectives are defined, namely:

1. Ensuring that research programming (particularly H2020) takes account practitioners' needs, thereby promoting research results that are relevant to them;
2. Identifying the most promising tools, methods, guidelines (including those developed in FP7 and H2020 projects) that have the potential to be taken up by practitioners;
3. Support the competitiveness of EU industry by enhancing the market for research results;
4. Ensuring that the expertise of practitioners is available to policy makers, thereby facilitating the policy-making process;
5. Facilitating the implementation of policy.

2.3 Logistics

The agenda and organisation of the Community of Users is under the responsibility of DG HOME.B4 in close coordination with various DGs and Agencies, as well as with REA and relevant projects.

In its first phase (2014-2015), the development of the Community of Users has been closely linked to two demonstration projects (EDEN[3] and DRIVER[4]) in terms of logistics, i.e. CoU meetings were organised under the umbrella of these two projects, while all other tasks were coordinated with other services. From 2016 to date, logistics are now carried out under a service contract with the development of a dedicated website. The first phase of the CoU development has focused on disaster risk and crisis management. The scope of the mapping has been enlarged to encompass all the areas covered by research on secure, safe and resilient societies.

2.4 Knowledge transfer

The knowledge transfer has to be established in the lights of the different interactions among different categories of actors, linking research, industry, policy sectors and practitioners.

In this respect, several levels need to be considered: (1) a "horizontal" level in the framework of which interactions among research, industry, policy-makers and practitioners are established in a coordinated way at different scales, i.e. EU, national and regional; (2) a "vertical" level which establishes operational links among the EU, national and regional levels through appropriate information relays, synergies and demonstration activities.

a. Horizontal transfer

- **Science to science**: sharing information and developing interactions among H2020 projects (via the Research DGs) dealing with specific themes to develop a critical mass and reduce fragmentation, and bring tools/technologies to the market through links with industrial stakeholders. EU-funded projects respond to topics which are generally based on well-defined policy hooks. We might hence expect that projects supporting common policy goals will establish synergies, which is rarely the case without a push from the Commission owing to various considerations (IPR and classified information in particular). Here again, sharing information and developing interactions on a regular basis should become a practice that the Commission asks of projects.
- **Policy to policy**: policy interactions in the light of policy implementation needs, including the respective DGs, and establishing links with Member States through formal committees (e.g. CBRN-E Advisory Group, Civil Protection Committee, Seveso Committee etc.). While International and EU policies are developed in close consultation among different sectors, in practice few interactions take place at the implementation level among sectors within the Member States. This is partly due to insufficient sharing of information and joint actions.

3 https://www.eden-security-fp7.eu/

4 http://driver-project.eu/

- **Science to policy**: formatting/translation of research information in a way which is tailor-made to policy-makers and ultimately user's needs, responding to well specified technical challenges. This is obviously directly linked to the above, with the requirement for the scientific community to format/translate research information in a way which is tailor-made to policy applications, basically responding to well specified technical challenges. This is the subject of the mapping described in this document.
- **Policy to science**: identification of research needs from policy-makers, stakeholders and practitioners on the short to long term and communication of these needs to be taken into account in research programming, development and implementation. An essential component of the policy to science interaction is the capacity for policy-makers to identify research needs on the short to long term and communicate these needs in anticipation to the research community so that programming, research development and implementation can match the policy timeline (e.g. access to the scientific state-of-the-art, short-term research / capacity building, longer term research goals, pre- and co-normative research).

b. Vertical transfer

- **International/EU to National**: in the research sector, interactions through H2020 consortia; in the policy sector, interactions through Committees representing Member States and stakeholders, working out appropriate relays to national authorities and stakeholders based on well-formatted information. At international/EU level, policies are elaborated by relevant organisations (e.g. UN for various conventions and European Commission for security-related EU policies). The links to the National level take place through Committees in which Member States are represented. There is a need to ensure that these Committees be informed on similar grounds about science & policy developments.
- **National to Regional/Local**: information relays through interactions with regional research partners and regional authorities as well as practitioner's networks and associations. Once representatives of the Member State's Committee are duly informed, it is to be expected that appropriate relays with regional / local implementers will then take place under the MS responsibility. This also requires a level of coordination which depends upon the willingness and capacity of each Member State. This level of interaction is less well defined than the EU level because of different settings within the Member States.
- **Regional to National/EU**: return of experiences from either practitioners involved in EU-funded projects or practitioners informed via national channels to the EU level.

2.5 Who are the users?

Fields concerned by security, safety and resilience for societies are themselves scattered into many different disciplines and sectors. To simplify, we will distinguish five main categories of users: (a) Policy–makers; (b) Scientists; (c) Industry (including SMEs); (d) Training and Operational units; and (e) NGOs and general public:

a. Policy-makers and stakeholders

- At the international level, UN bodies are closely working with the EU in the fight against crime and terrorism (UNICRI), disaster risk reduction (UN-ISDR), transboundary industrial accidents (UNECE), environment protection (UNEP) etc.
- At EU level, the main policy DGs concerned with Crisis Management are DGs HOME (migration and home affairs), ECHO (civil protection), SANTE (health), GROW (enterprise), ENV (environment), CLIMA (climate action), ENER (energy), MOVE (transport), TAXUD (customs), TRADE (export, trade), EEAS/FPI (external security, foreign policy instrument) and the SG (Secretariat General), as well as the Joint Research Centre (JRC) as supporting DG, see section 5
- At the Member State's level, Ministries of Defence, Interior, Foreign Affairs, Civil Protection, Environment, Research and Industry, as well as Agencies and Regional Authorities, are concerned
- Often working at the interface between policy and science, various stakeholders are involved in bridging interests of different communities, e.g. consultancy companies

b. Scientists

- Security research involves a wide range of scientific disciplines which have to interact, ensure complementarity and build interdisciplinary networks
- Different types of scientists are to be considered (universities, research institutes, research units linked to Defence/Interior ministries or agencies)

c. Industry (including SMEs)

- Many industry branches and stakeholders are involved in the areas of defence, forensics, civil protection etc. Research results can benefit most first responders
- Different communication approaches to be followed towards large industries and SMEs often disconnected from discussions at EU level

d. Practitioners

- First responders, i.e. fire brigades, emergency services, police forces, civil protection units, military units, laboratories, water/flood management etc. as well as Decision-makers (at national or regional levels)
- Training centres for first responders, command control centres

e. NGOs and general public

- NGOs, Civil Society Organisations, public at large, education (schools) and training

While some of the above actors in categories a, b and c are used to participate in international meetings, this is less frequent for SMEs (in category c) and even less for actors in categories d and e. New ways must be found to ensure that information may freely circulate "horizontally" as well as "vertically" (see p. 7) in order to fertilize all project deliverables while, at the same time, maturing them to the final operational phase (also called "usefulness & use") by end-users, and integrating them into appropriate policy implementation and development.

3. POLICY BACKGROUND

3.1 General framework

A large span of sectors and policies cover secure, safe and resilient society's issues in a direct or indirect way, either by providing legally-binding frameworks of actions by EU Member States in the form of Directives, general frameworks in the form of Communications or technical specifications in the form of Decisions, for example.

Crisis Management policies follow an integrated approach for the management of natural and man-made hazards focusing on disaster risk reduction (prevention and preparedness) and disaster response. The policy is mainly represented by the EU Civil Protection Mechanism (UCPM)[5] , and the operational dimension is coordinated by the Emergency Response Coordination Centre (ERCC). Disaster risk management is also addressed through the EU Renewed Internal Security Strategy[6] and the European Agenda on Security adopted in April 2015[7] (DG HOME) and Consumer Health Protection policies (DG SANCO)[8]. In addition, climate-related disasters are covered by environmental and climate policies (DG ENV, in particular the Flood Directive[9] and DG CLIMA through the EU climate change adaptation strategy[10]). Finally, intergovernmental agencies are also involved in security policies, namely the European External Action Service (EEAS) – which implements the EU Common Foreign and Security Policy – and Europol – which is the EU Law Enforcement Agency. Both agencies assist EU Member States. There are also links with the Council Decision 2014/415/EU on the arrangements for the implementation by the Union of the solidarity clause, which covers response, situational awareness and analysis and threat assessment at Union level.

Other key EU policies concern industrial competitiveness and innovation, namely the Renewed EU Industrial Policy Strategy[11] which aims to boost industrial competitiveness and innovation (thus the access to market of developed technologies) and the EU research policy represented by Horizon2020.[12]

With regards to CBRN-E, the key EU policy is represented by the Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks[13] (DG HOME) and the EU Action Plan on Enhancing the Security of Explosives[14] which expired at the end of 2015 and which is now under revision; the Regulation 98/2013 on the Marketing and Use of Explosives Precursors[15] is directly applicable to all MS and is currently under revision (COM(2018) 209 final). Other EU policies include CBRN as a focal point, namely in the sectors of Civil Protection and Consumer Health Protection (see above), as well as Energy Infrastructure and Transport

5 Decision 1313/2013, most recently amended by Decision 2019/420 (“RescEU”) which strengthened the UCPM in various ways

6 EU Internal Security Strategy for period 2015-2020 (also called "renewed internal security strategy"), Council Conclusions 10 June 2015, 9798/15.

7 The European Agenda on Security, COM(2015) 185 final 8 Decision 1082/2013

8 Decision 1082/2013

9 Directive 2007/60/EC

10 COM (2013) 216 final

11 COM(2017) 479 final

12 http://ec.europa.eu/programmes/horizon2020/en/

13 COM(2017) 610 final.

14 Doc.8311/08/Council of the European Union, EU Action Plan on Enhancing the Security of Explosives

15 Regulation 98/2013

Networks[16] (DGs ENER and MOVE), Customs[17] (DG TAXUD), Environment and Industrial Risks[18] (DG ENV) and International Cooperation, e.g. CBRN-E Centres of Excellence (DG DEVCO).

Complementary to EU policies, international policies are also active in Disaster Risk and Crisis Management. In the case of CBRN-E, various conventions exist, namely the United Nations Security Council Resolution 1540, the Chemical Weapon Convention (CWC controlled by the Organisation for the Prohibition of Chemical Weapons, OPCW), the Biological and Toxin Weapon Convention (BTWC without control mechanisms), and the Nuclear Non- proliferation Treaty (NPT controlled by the International Atomic Energy Agency, IAEA). In the field of Disaster Risk Management, Disaster Risk Reduction has been the core action line of the United Nations Hyogo Framework for Action on how to mitigate the impact of natural and man-made disasters, now continued by the Sendai Framework for Action setting priorities for the 2015-2025 period, among which the promotion of a better understanding of disaster risk management through the building, sharing and development of knowledge and the strengthening of the policy-science interface at local, national, regional and global levels.

The implementation of these policies represents a complex and ambitious challenge as they involve a wide variety of players whereas each Member State often follows specific national approaches (national action plans) for dealing with crises and are also differently organised in terms of disaster risk management capabilities. The EU framework represents a means and a real opportunity to discuss possible ways to improve coordination among the various national approaches and develop a common EU vision strengthened by a joint strategy in this field. The development of a Community of Users is, in this respect, an essential component to bring together key scientific, policy and industry actors, as well as other stakeholders (e.g. first responders, police representatives, fire fighters, civil protection units) around this common vision and strategy. This is closely linked to the EU industrial policy[19] under the responsibility of DG GROW, the EU research policy[20] coordinated by DG R&I and involving DG HOME (Secure Societies Programme), DG CNECT and JRC, the EU civil protection policy managed by DG ECHO, as well as the EU environmental and climate policies coordinated by DG ENV and CLIMA respectively.

3.2 EU Civil Protection Mechanism and related international policies

The **UCPM**[21] aims to facilitate reinforced cooperation between the EU and the Member States and to facilitate coordination in the field of civil protection, in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters. It supports and complements the efforts of the Member States for the protection, primarily of people but also of the environment and property, including cultural heritage, in the event of natural and man-made disasters, acts of terrorism and technological, radiological or environmental accidents, including marine pollution. Built upon these policy instruments, the UCPM is about developing an integrated approach to disaster management. The EU action is based on the principles of solidarity. The overall mechanism takes due consideration of laws and international commitments, and exploit synergies with relevant Union initiatives such as the European Earth Observation Programmes (Copernicus), the European Programme for Critical Infrastructure Protection (EPCIP) and the Common Information Sharing Environment (CISE). The mechanism is based on the Emergency Response Coordination Centre (ERCC) and the European Civil Protection Pool in the form of voluntary pool of pre-committed capacities from the Member States, trained experts, a Common Emergency

16 Regulation 347/2013 and Decision 661/2010

17 COM(2012) 793 final

18 Directive 2012/18/EU

19 COM (2010) 2020 final

20 COM (2011) 152 final

21 Council Decision 2007/779/EC, OJ L 314, 1.12.2007, most recently amended by Decision 2019/420 (“RescEU”).

Communication and Information System (CECIS) managed by the Commission and contact points in the MS. It also recognises the role of regional and local authorities in disaster management. Outside the Union, disaster response is coordinated with the United Nations and other relevant international actors with reference to Council Regulation No 1257/96 concerning humanitarian aid.[22] Finally, the use of military means under civilian leads as a last resort may constitute an important contribution to disaster response.

On technical grounds, the UCPM is working towards a general policy framework on disaster risk prevention aimed at achieving a higher level of protection and resilience against disasters by preventing or reducing their effects and by fostering a culture of prevention. From this perspective, it promotes the review of risk assessment, risk management planning conducted at national/regional level and the development of an integrated approach, linking risk prevention, preparedness and response actions. On the basis of information received from the EU Member States, the European Commission establishes and regularly updates a cross-sectoral risk overview. Among its priorities is the action to 'improve the knowledge base on disaster risks and facilitate the sharing of knowledge, best practices and information.[23]

The UCPM is closely related to the **Sendai Framework for Action 2015-2025**[24] "Building the resilience of nations and communities to disasters" which is the successor of the Hyogo Framework for Action adopted by 168 UN Member States that voluntarily committed to work towards achieving its objectives, in particular improving disaster resilience and disaster risk reduction as a necessary ingredient for the achievement of poverty reduction and sustainable development. The Sendai Framework for Action sets out an ambitious set of priorities to place disaster risk reduction as a key element of sustainable development efforts, to define further steps to reduce existing and emerging risks and foster disaster resilience. As stressed in Council Conclusions on this matter, the EU supports a framework which strengthens the contribution of disaster risk management to smart, sustainable and inclusive growth by promoting the use and development of innovative technologies and encouraging a more systematic and reinforced science-policy interface in disaster risk management. These objectives are supported among others by IPCC recommendations expressed in the special report on extreme events.[25]

The UCPM is also financing actions related to preventing, preparing for and responding to disasters. These include: an important EU Civil protection training programme, regular large-scale exercises and modules exercises, exchange of experts, prevention and preparedness projects (through annual calls for applications)[26], logistical and transport support for response missions, deployment of coordination, assessment or advisory missions, adaptation and certification of assets to be included in the Voluntary Pool, the availability of buffer capacities under the Voluntary Pool (additional assets than those made available by the Member States). In the area of marine pollution these actions are coordinated with the European Maritime Safety Agency and the regional sea conventions.

22 Council Regulation No 1257/96, OJ L 163, 2.7.1996

23 Art.5.1(a), Council Decision No. 1313/2013/EU, Official Journal of the European Union, L347, 20.12.2013

24 http://www.unisdr.org/we/coordinate/sendai-framework

25 Special Report on Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation (SREX), http://ipcc-wg2.gov/SREX/report/

26 http://ec.europa.eu/echo/en/funding-evaluations/financing-civil-protection-europe/selected-projects 27 SWD(2013) 318 final

3.3 Critical Infrastructure Protection

The **new approach to the European Programme for Critical Infrastructure Protection**[27] (EPCIP) is built on a review of the 2006 programme and the Council Directive 2008/114/EC[28] on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. It aims to ensure a high degree of protection of EU infrastructures and increase their resilience (against all threats and hazards). It looks at interdependencies between critical infrastructures, industry and state actors, taking account of the cross border dimension and interdependencies between sectors (e.g. European high-voltage electricity grid). The EPCIP established (1) procedures for the identification and designation of European critical infrastructures and assessment of the need to improve their protection (Directive 2008/114/EC); (2) measures to facilitate its implementation, including an action plan, CIWIN, CIP expert groups at EU level and information sharing process; (3) funding for CIP-related measures and projects focussing on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks' such as ERNCIP (see 6.9.2); and (4) an external dimension for engagement with third countries on CIP. At the time of publication of the revised approach (2013), less than 20 European Critical Infrastructures had been designated and hence very few Operator Security Plans had been produced; the number of ECI designated has since increased substantially. The Directive 2008/114/EC has mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation – the sector-focused approach of the directive represents a challenge to a number of MS as in practice the analysis of criticalities is not confined to sectoral boundaries and follows rather a 'system' or 'service' approach (e.g. hospitals, financial services). There is a need for a cross-sectoral approach development. In practical terms, development of preparedness strategies are based around contingency planning, stress tests, awareness raising, training, joint courses, exercises and staff exchange. The programme also promotes the dialogue between the operators of the critical infrastructures and those who rely upon them in order to better prepare responses to events affecting European critical infrastructures. The gaps identified in the review of the EPCIP led the Commission to present its new approach to the implementation of the EPCIP in 2013, with a greater focus on interdependencies and proposing practical work with four critical infrastructures of a European dimension (Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network).

The guidelines for trans-European energy infrastructure[29] are built upon the Communication of 28 February 2011 entitled 'Energy infrastructure priorities for 2020 and beyond – A blueprint for an integrated European energy network'; it stipulates that the Union's energy infrastructure should be upgraded in order to prevent technical failure and to increase its resilience against such failure, natural or man-made disasters, adverse effects of climate change and threats to its security, in particular as regards European Critical Infrastructures and the assessment of the need to improve their protection.

Creating the environment for safe transport is essential for European citizens. **EU transport policies**[30] cover a wide range of security and safety policies in the air, road, maritime and rail areas which all relate to technical standards for preventing / detection risks and responding to major threats, including terrorist attacks, crimes and accidents. In order to maintain proper security levels cooperation with third countries is paramount and the Commission consolidates and strengthens security by working together with major international partners, exchanging experiences and best practices. Security in transport also relies on new technologies that can really assist in developing smooth high-security systems for the future but without making the security checks too long and intense.

27 SWD(2013) 318 final

28 Council Directive 2008/114/EC, OL L345/75

29 Regulation (EU) no 347/2013 of 17 April 2013, OJ L115/39 of 25.04.2013

30 http://ec.europa.eu/transport/home_en

3.4 CBRN and Explosives

From the above, it is clear that Chemical, Biological, Radiological, Nuclear and Explosive (CBRN-E) threats are covered by a range of policies. In views of improving coordination of actions related to CBRN-E risk management, the European Commission has issued strategic documents which main features are described below regarding technical challenges.

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

The Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks aimed to ensure that unauthorised access to CBRN materials of concern is as difficult as possible. Prevention is based on robust risk-assessment processes, which include the prioritisation, security and control of high-risk CBRN materials and facilities, developing a high-security culture of staff, improving the security of transport, information exchange, import and export regimes, and strengthening cooperation on the security of nuclear materials. Key Actions defined in the Plan are designed to reduce threat and damage from CBRN incidents of accidental, natural and intentional origin, including terrorist threats. It is a political commitment which may be seen as a roadmap of intentions guided by principles of EU solidarity (the responsibility of protecting populations against CBRN incidents lays with the Member States), EU added value (respecting principles of subsidiarity and proportionality), based on existing regulations and instruments, and in close consultation with national authorities. Actions are based on risk- and threat assessments and cost- effective assessments. Confidentiality of certain types of information is taken into account. Actions have been financially supported by expired and existing Union programmes and fund.[31] [32]

The plan aimed to efficiently respond to incidents involving CBRN materials and recover from them as quickly as possible. Specific attention is made to CBRN emergency planning, strengthening countermeasure capacity, reinforcing information flows, developing better modelling tools and improving criminal investigation capacity. The plan focuses on the required capability to detect CBRN materials in order to prevent or respond to CBRN incidents. This is related to the development of minimum detection standards to be applied across the entire EU, establishing trialling, testing and certification schemes for CBRN detection and improving the exchange of good practices on the detection of CBRN materials. The Plan promotes a scenario-based/modelling approach at EU level to identify work priorities in the detection field (identification of CBRN material and detection technologies), wide risk assessment (including events with cross-border effects) built on existing scenarios and national experience, and gap analysis; it supports the exchange of methods and procedures for developing scenarios and modelling, interconnecting detectors at national levels where feasible including data on incidents, coordination of exercises and lessons learnt. It also promotes a mechanism of information exchange among Member States on methodologies of scenario development related to sampling and detection, taking appropriate confidentiality into account. In the specific area of biological pathogens and toxins, the Plan promotes the development of detection models, considering distribution, possible vectors, infectious dose and stability.

The CBRN Action Plan is complemented by the **new EU approach to the detection and mitigation of CBRN-E** risks which adopts a proactive approach to the detection of threats, and proposes among others to put effective, proportional safeguards in place, including prevention, preparedness and response measures at EU level with the objective 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 response mechanisms within the CBRN Action Plan are linked to various EU policy instruments such as the EU Mechanism for Civil Protection (see section 5.2), the EU Integrated Political Crisis Response Arrangements (IPCR), the implementation of the Solidarity Clause, the ARGUS crisis management system allowing for an

31 http://ec.europa.eu/transport/home_en

32 OJ L 58, 24.2.2007, p.1-6 - Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks

immediate exchange of information among Commission rapid alert systems such as the ECURIE system for radiological emergencies, the Early Warning and Response System (EWRS) for communicable diseases, and the RAS-BICHAT for biological and chemical health threat.

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

The enhancement of the security of explosives has been identified as a priority issue for the European Commission in its efforts in the field of combating terrorism. Home-made explosives can be fabricated from certain easily accessible chemical precursors and can be misused by terrorists to inflict casualties and damage. In order to mitigate the risk of such misuse, in 2008 the Justice and Home Affairs Council approved the **EU Action Plan on Enhancing the Security of Explosives**. The Action Plan thus contributes to the implementation of the EU Counter Terrorism Strategy (2005) and is in line with the Renewed Internal Security Strategy (2015).

The EU Explosives Action Plan contains 48 measures related to the prevention, detection, and preparedness and response to explosives-related incidents. The recommendations for action address a comprehensive range of relevant aspects, such as precursors, storage, transport, traceability, detection, research, information exchange, and inter-agency coordination.

A first set of horizontal measures aims at improving the exchange of timely information and best practices, and supporting and promoting research, including research into inhibitors to precursors. A second set of measures focuses on prevention around explosives precursors, by raising staff awareness, increasing control over substances and explosives available on the market (including pyrotechnics), and establishing a mechanism for reporting suspicious transactions. Other prevention measures cover the security of explosives facilities and transport, as well as the security vetting of personnel at any stage in the supply chain. The action plan calls, in addition, for increased efforts to reduce the presence of bomb-making information over the internet. A third set of actions focuses on the detection of explosives threats. The plan has as a priority to establish a scenario-based approach to identifying priorities in the detection field, notably to identify detection technology requirements, current equipment that is available, and common minimum detection standards which should be applied. In the area of detection, the action plan recognises that there is an urgent need for improved exchange of information between authorities, researchers, and end-users, particularly in order to establish an EU-wide certification, testing and trialling scheme for the detection of explosives, and to continuously reassess the use of detection technologies in specific locations. Finally, a set of preparedness and response measures call on the creation of a network which improves the exchange of information and best practices among explosives ordnance disposal units in Europe, and also supports the development of threat assessments on explosives and on specific threats.

The actions contained in the EU Explosives Action Plan are implemented through a joint effort of the European Commission, Member States, Europol, research institutions as well as private sector stakeholders. DG HOME aimed at fully achieving implementation by the end of 2015.

One of the key actions of the EU Explosives Action Plan called on the Commission to consider measures to regulate the availability of explosives precursors on the market. As a result of the work done to implement this action, **Regulation (EU) 98/2013 on the marketing and use of explosives precursors** was adopted with a view to enhancing the protection of citizens from the threat of homemade explosives. Regulation 98/2013 came into force on 2 September 2014 and an update is currently under revision (COM(2018) 209 final). It restricts availability, possession and use, by members of the general public, of seven dangerous substances ('restricted explosives precursors,' listed in Annex I). Member States may decide to grant access by the public to these substances only through a system of licenses and registration. In addition, the Regulation introduces obligations for economic operators who place such substances on the market. Operators must ensure the appropriate labelling of restricted explosives precursors, and must also report any suspicious transactions involving both the seven restricted substances and eight other non-restricted substances which are also considered of concern (listed in Annex II).

3.4.3 International Conventions

At international level, the **EU strategy against Proliferation of Weapons of Mass Destruction** (WMD strategy), together with relevant Community Instruments, in particular the Instrument for Stability (supporting third countries to develop training and assistance on CBRN risk mitigation and preparedness), reinforces actions on reducing the risks from CBRN materials. This is linked to nuclear non-proliferation for strengthening nuclear security.[33] Furthermore, the Implementation of the UN Security Council Resolution 1540 will be further strengthened by supporting the International Atomic Energy Agency (IAEA), in particular contributing to more efficient export control and border monitoring systems. Regional Centres of Excellence will be instrumental in order to exchange best practices, support capacity building and share experiences gathered at EU level with key regions. Issues related to the threat of CBRN materials are also discussed by international organisations such as the Organisation for the Prevention of Chemical Weapons (OPCW), the BTWC Conference, Interpol and the Global Health Security Initiative (GHSI).

3.5 Major accident hazards

Major accidents can have consequences beyond the limits of industrial establishments and the potentially significant human, ecological and economic costs of an accident are borne not only by the establishment affected, but also by the society concerned. It is therefore necessary to establish and apply safety and risk-reduction measures to prevent major accidents, and to minimise their effects if they nevertheless occur, thereby ensuring a high level of protection throughout the Union as well as supporting sustainable economic growth.

The **Directive 2012/18/EU (on major-accidents hazards involving dangerous substances)**[34], better known as Seveso-III-Directive, sets a risk management framework: a) by obliging operators to take all necessary measures to prevent major accidents and to limit their consequences for human health or the environment and b) by requesting competent authorities to establish supporting policies (e.g. emergency or land-use planning). Different sets of requirements are set depending on the amount of dangerous substances present in the establishment. The Directive excludes military establishments, pipelines, as well as the transportation of dangerous substances outside establishments. Risk assessments should consider operational causes, natural causes (e.g floods, earthquakes) and other external causes of accidents. The latter would, where appropriate, also include malicious acts even if those are not explicitely mentioned. While the Directive does not distinct between causes of accidents (e.g. unintentional or intentional) and is rather impact-oriented, traditionally it is rather a safety measure and implementation focusses on unintentional events. However, there is an increasing awareness in the community towards malicious causes of major accidents and the relevance of Seveso establishments for national security, which requires a cross-sectorial coordination as stipulated in the new CIP approach (see § 5.3). The Directive is complemented by CIP regulations for attack-prone installations.

At international level, the EU is actively engaging in the **Convention on the Transboundary Effects of Industrial Accidents** (TEIA)[35] of UNECE (UN Economic Commission for Europe) which is designed to protect people and the environment against industrial accidents, aiming to prevent accidents from occurring, or reducing their frequency and severity and mitigating their effects if required. The Convention promotes active international cooperation between countries before, during and after an industrial accident. The TEIA has also close links with the Sendai Framework for Action (see section 5.2) and is increasingly aware of cross-links with CBRN-E issues, thus offering an additional cooperation channel. A number of other agencies (e.g. OECD, OPCW) are also active in the area of industrial accidents and cooperate with the EU and UNECE on the issue.

33 COM(2009) 143 final, 26.03.2009

34 Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on major-accidents hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, Official Jornal of the EU, No. L 197/1, 24.7.2012.

35 http://www.unece.org/env/teia.html

3.6 Serious cross-border threats to health

The protection of human health is a matter which has a cross-cutting dimension and is relevant to numerous Union policies and activities. The Commission should ensure, in liaison with the Member States, the coordination and exchange of information between the mechanisms and structures established under the **Decision 1082/2013/EU on serious cross-border threats to health**[36] as well as activities which are relevant to the preparedness and response planning, monitoring, early warning of, and combating serious cross-border threats to health. Pursuant to Decision 2119/98/EC a network for the epidemiological surveillance and control of communicable diseases in the Community has been set up. Apart from communicable diseases, a number of other sources of danger to health, in particular related to other biological or chemical agents or environmental events, which include hazards related to climate change, could by reason of their scale or severity, endanger the health of citizens in the entire Union, lead to the malfunctioning of critical sectors of society and the economy and jeopardise an individual Member State's capacity to react. The legal framework set up under the above Decision should, therefore, be extended to cover other threats and provide for a coordinated wider approach to health security at Union level. In the context of this Decision, an important role in the coordination of recent crises of Union relevance has been played by an informal group composed of high-level representatives from Member States, referred to as the Health Security Committee, and established on the basis of the Presidency Conclusions of 15 November 2001 on bioterrorism. The Decision promotes preparedness and response planning through consultation among the Member States and the Commission in order to share best practice and experience, as well as interoperability of national preparedness planning and addressing the intersectoral dimension of preparedness and response planning at Union level.

The Health Security Committee plays an important role in responding to health threats (notably in terms of crisis preparation, exercises on CBRN events and the listing of pathogens and chemicals which pose a health threat) whilst the European Centre for Disease and Control (ECDC) provides risk assessments for communicable diseases and biological incidents.

3.7 EU Adaptation to Climate Change

The **EU Adaptation Strategy to Climate Change** highlights the consequences of climate change and the need for adaptation measures. It focuses on early, planned and coordinated action rather than reactive adaptation. The communication highlights the need for systematic exchanges of best practice on how to best adapt to climate change. The strategy takes account of global climate change impacts such as disruptions to supply chains or impaired access to raw materials, energy and food supplies. The overall aim is to contribute to a more climate resilient Europe by enhancing the preparedness and capacity to respond to the impacts of climate change at local, regional, national and EU levels, developing a coherent approach and improving coordination. This strategy is closely linked to national adaptation strategies which are considered as recommended instruments by the UN Framework Convention on Climate Change. A close coordination between climate change adaptation and disaster risk management / policies is also required. Development is foreseen of guidelines on minimum standards for disaster prevention based on good practices.

The requirement for "climate-proofing" and mainstreaming of adaption measures in various sectors also calls for strengthened preparedness and science-policy links. The strategy makes reference, in particular, to the Marine Framework Directive (Directive 2008/56/EC)[37] and various environmental policies, related to e.g. Forestry (EC Regulation 2152/2003), Water (Directives listed in the COM(2012)673 on the Blueprint to Safeguard Europe's Water Resources[38]), as well as other sectors such as Transport (Decision 661/2010/EC),

36 DECISION No 1082/2013/EU

37 Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive), OJ L 164/19.

38 COM(2012) 673 final

Energy (COM(2011)665/3), and the above described Disaster Risk Prevention (within the Union Civil Protection mechanism) and Health (Decision 1082/2013).

3.8 Water and marine policies

Linked to the above, specific policy instruments are in place in the water sector related to extreme hydrometeorological events such as floods and droughts. In the first place, complementing the Water Framework Directive (WFD)[39] (and its daughter Directives, namely the Priority Substances Directive[40] and the Groundwater Directive[41]), flood prevention and management are tackled by the Flood Directive which requires EU Member States to assess and manage flood risks, with the aim of reducing adverse consequences for human health, the environment, cultural heritage and economic activity associated with floods in Europe. This directive has to be coordinated with the implementation of the WFD from the second river basin management plan onward (which will take place from 2015 to 2021). It therefore provides a comprehensive mechanism for assessing and monitoring increased risks of flooding, taking into account the possible impacts of climate change, and for developing appropriate adaptation approaches. Water scarcity and droughts are also considered in the policy context.[42] In particular, a European assessment of water scarcity and droughts has been conducted by the European Commission in the framework of the Water Scarcity and Drought Communication to monitor changes across Europe and to identify where further action is needed in response to climate change. Recommendations have been taken on board in the Blueprint to Safeguard Europe's Water Resources. It may, therefore, be considered that the successive steps of the WFD River Basin Management Planning (RBMP) and the related flood and drought policy framework may conveniently incorporate adaptation to climate-related water risks through risk assessment, monitoring, environmental objective setting, economic analysis and action programmes to achieve well defined environmental objective.

The Drinking Water Directive (DWD)[43] regulates the quality of water intended for human consumption. The Directive is currently under evaluation as a follow-up of the European Citizens' Initiative (ECI) Right2Water.[44] The policy concerns the quality of drinking water from around 100,000 water supplies. It aims to protect human health by ensuring that drinking water at the consumer tap is wholesome and clean. It lays down essential quality standards at EU level, for which monitoring programmes have to be performed. For any failure remedial action has to be taken. Its intervention logic was to address all possible contamination causes, including from treatment and distribution, by setting strict minimum parametric values to be complied with at the consumer tap. It thus implicitely includes deliberate poisoiningpoisoning risks. The abstraction of drinking water and the protection of water bodies for this aim is, however, not regulated in the DWD, but in Article 7 of the above mentioned Water Framework Directive (WFD), which requires Member States to identify bodies of water for the abstraction of drinking water and to protect them, so that the resulting water will meet the DWD requirements under the water treatment regime applied.

39 Directive 2000/60/EC

40 Directive 2013/39/EU of the European Parliament and of the Council of 12 August 2013 amending Directives 2000/60/EC and 2008/105/EC as regards priority substances in the field of water policy, OJ L 226/1

41 Directive 2006/118/EC of the European Parliament and of the Council of 12 December 2006 on the protection of groundwater against pollution and deterioration, OJ L 372.

42 COM(2007) 414 final

43 Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption, OJ L 330, 5.12.1998, p. 32

44 Communication from the Commission on the European Citizens' Initiative "Water and sanitation are a human right! Water is a public good, not a commodity!" COM/2014/0177 final

Finally, while the protection of the (coastal) marine environment is covered by the WFD, EU environmental policymakers considered there was a lack of strategy underpinning the policies to protect the marine environment. A strategy was thus developed in the sixth Environmental Action Programme (2002-2012) which resulted in setting up environmental objectives for the marine environment. The related protection regime is regulated under the EU Marine Strategy which was adopted in 2008.[45]

3.9 Control of export and Union Custom Code

The Council Regulation (EC) no 428/2009 on a Community regime for the control of exports, transfer, brokering and transit of dual-use items (Recast)[46] is setting rules that Member States have to apply to control the transfer of certain dual-use items within the Community in order to safeguard public policy or public security. This includes the effectiveness of controls on exports from the Community and those items which only pass through the territory of the Community (i.e. not assigned to a customs-approved treatment or use other than the external transit procedure or placed in a free zone or warehouse with no record of them).

The Union Customs code (UCC) is part of the modernisation of customs and serves as the new framework regulation on the rules and procedures for customs throughout the EU. Its substantive provisions have entered into force on 1 May 2016.[47] With the increase in global threats, EU customs holds a key role in ensuring external border and supply chain security and thus contributing to the security of the European Union. The use of detection technology and control equipment, together with the mandatory data submission (Entry Summary declarations) and the EU risk management system, are important elements of the overall customs control and supervision process.

Detection technologies have long played an important part in customs border controls by assisting in the detection of dutiable, prohibited and controlled goods and materials. However, as the volume of international trade continues to expand and an increasing emphasis is placed on supply chain security and trade facilitation, the role of Customs is evolving. For instance, the use of data analysis has become as important as the use of detection technologies in dealing with existing and emerging threats. **This continuous drive for more efficient and more effective customs processes calls for the integrated application of innovative information and detection technologies.**

Adapting cargo information systems is essential to strentening monitoring and risk based controls of international supply chains in order to ensure that CBRN material are not illicitly entering in to the European Union.

3.10 Border security

In the framework of the Communication "Examining the creation of a European Border Surveillance System (EUROSUR)[48], support needed in the area of border security targeted the development of technologies and capabilities which are required to enhance systems, equipment, tools, processes, and methods for rapid identification to improve border security, whilst respecting human rights and privacy. This includes both control and surveillance issues, contributing to the further development of the EUROSUR and promoting an enhanced use of new technology for border checks; also in relation to the Smart Borders legislative initiative (for both EUROSUR and the Smart Borders, the Commission published the initial relevant communications on 13 February 2008).

45 EU Marine Strategy Framework Directive, 2008/56/EC 45 OJ L 134/1 of 29.05.2009, recast in 2018.

46 OJ L 134/1 of 29.05.2009, recast in 2018..

47 Regulation (EU) no 952/2013.

48 COM(2008) 68 final

At sea, the main technical challenge was identified in the detection and identification of small non cooperative vessels (and of their anomalous behaviour). At the system level the identified priority was to improve the sharing of information amongst actors active in maritime surveillance. A close interactive dialogue has taken place with other Commission DGs (DG HOME, DG MARE, DG JRC, DG MOVE) as well as with EU agencies (EBCGA/'Frontex', EMSA and EDA). This helps the setting by the European Border and Coast Guard Agency of CONOPS (concepts of operations) as related to the detection of small boats.

3.11 Fight against Crime and Terrorism

Regarding the fight against crime and terrorism, the European Commission is not in charge of operational activities but supports and facilitates the activities of the security practitioners at the EU level.

The main policy framework for this action is provided by the **European Agenda on Security (COM(2015) 185 final)** adopted on 28th April 2015, which provides strategic focus for the EU and Member States for the overall goal of strengthening the Union's security framework. The three pillars of the Union's action to obtain this goal are: to strengthen the information exchange; to increase the operational cooperation; and to provide support in training, funding, research and innovation. The main thematic priorities listed in the Agenda are: terrorism, organised crime and cybercrime.

A Communication on the delivery of the Agenda on Security (COM(2016) 230 final) has been adopted in April 2016. It acknowledges the common position of the European Parliament, the EU Ministers for Justice and Home Affairs and the Commission to press ahead with the measures foreseen and to deepen the fight against terrorism. For this reason, the Communication, one year on from the presentation of the Agenda, takes stock of the progress that has been made in its implementation as concerns the EU contribution to counter-terrorism.

In addition to the Agenda, a number of more specific EU legislative and policy documents apply in the area of fight against crime and terrorism. Two of the most relevant ones are the **Regulation (EU) No 98/2013** of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors (currently under revision), and the **Communication COM(2016) 379 final** on supporting the prevention of radicalisation leading to violent extremism.

Also, on 13 and 14 December 2011, the Council approved conclusions (17537/11 ENFOPOL 413 COPEN 342) on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe. Their aim was to foster cooperation between police and judicial authorities across the European. An action plan has been developed under the Dutch presidency which should be adopted as Council conclusions in June 2016.

Furthermore, the Commission assists EU Member States in the implementation of existing legal instruments such as e.g. the Data Retention Directive, the Decision on access for consultation of the Visa Information System etc.[1]. The EC also participates in specialised working groups of the Council such as COSI, and agencies such as Europol and CEPOL.

Finally support to security practitioners is also granted via the financing of national and multi-national projects that enhance police cooperation, including among police networks

4. EU-FUNDING INSTRUMENTS - RESEARCH AND CAPACITY-BUILDING

4.1 Introduction

As highlighted in section 4.1, EU research funding is orchestrated by different "research families", namely various programmes of DG RTD, DG CNECT and DG HOME, as well as research actions undertaken by the Joint Research Centre (JRC). Other funding instruments focus on capacity-building and training (e.g. prevention, preparedness and response projects in disaster risk management funded by DG ECHO, security-related projects funded by DG HOME) but they will not be developed in this document. Linked to EU research actions, the European Defense Agency (EDA) funds research projects with interactions with DG HOME funded projects under the so-called European Framework Cooperation (EFC).

While research programming and policy responsibilities lay with the respective General-Directorates of the European Commission, the management of projects is increasingly delegated to "sister" agencies, namely the Research Executive Agency (REA) and the Executive Agency for SMEs (EASME).

4.2 Horizon 2020

Horizon 2020 is the biggest EU Research and Innovation programme ever with nearly €80 billion of funding available over 7 years (2014 to 2020) – in addition to the private investment that this money will attract. It promises more breakthroughs, discoveries and world-firsts by taking great ideas from the lab to the market. Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. By coupling research and innovation, Horizon 2020 is helping to achieve this with its emphasis on excellent science, industrial leadership and tackling societal challenges. The goal is to ensure Europe produces world-class science, removes barriers to innovation and makes it easier for the public and private sectors to work together in delivering innovation. In the Security area, Horizon 2020 will contribute to the implementation of the policy goals of the Europe 2020 strategy, the Security Industrial Policy, the Internal Security Strategy, the Cyber Security Strategy[49], the Union Civil Protection Mechanism, as well as supporting the various above-mentioned thematic policies. The primary aim of the Work Programme on "Secure societies – Protecting freedom and security of Europe and its citizens" is to enhance the awareness, preparedness and resilience of our society against natural and man-made disasters. Crisis Management (including CBRN-E, natural and man-made disaster risk management) related research will be considered in various topics focusing on new crisis management tools, novel solutions for the protection of critical infrastructure, and new forensic tools for fighting crime and terrorism.

49 COM (2013) 48 final

The current EU Framework Programme for Research and Innovation is built up upon achievements of the 7th Framework Programme, which mapping is focused upon and which embedded serveral programmes of direct or indirect relevance to secure, safe and resilient societies, namely:

- Health, demographic change and wellbeing;
- Food security, sustainable agriculture and forestry, marine and maritime and inland water research, and the Bioeconomy;
- Secure, clean and efficient energy;
- Smart, green and integrated transport;
- Climate action, environment, resource efficiency and raw materials;
- Europe in a changing world - inclusive, innovative and reflective societies;
- Secure societies - protecting freedom and security of Europe and its citizens;
- Security for smart and safe cities, including for public spaces.

4.3 DG ECHO

The overall rationale of the DG ECHO's Programme for Capacity Building is that such investments into the global humanitarian system lead to more rapid and more cost-effective humanitarian responses, allowing a better and broader humanitarian coverage. EU Member States and the European Commission's partners agreed that: "supporting the development of the collective global capacity to respond to humanitarian crises is one of the fundamental tenants of our [EU] approach".[50] The principal objective of the programme is to strengthen the global humanitarian preparedness and response capacity. Specific objectives are:

- To increase the effectiveness and reinforce the capacity of international humanitarian organisations and stakeholders to assess, analyse, prepare and respond to humanitarian needs during man-made and /or natural disasters and their immediate aftermath in a coordinated and inclusive manner.
- To reinforce the capacity of international humanitarian organisations and stakeholders to deliver more varied and appropriate forms of food assistance, during emergencies and their immediate aftermath.

4.4 DG HOME / ISF

The goal of the Internal Security Fund, managed by DG HOME, is to contribute to ensuring a high level of security in the EU. One of two general objectives is enhancing the capacity of EU States and the Union for managing effectively security-related risk and crisis, and preparing for protecting people and critical infrastructure against terrorist attacks and other security related incidents. In this context the Fund co-finances projects in the areas of CBRN-E, critical infrastructure protection as well as crisis management. The projects are supposed to be much more operational than those funded under the Horizon 2020. The majority of the funds are implemented via the shared management, nevertheless the Commission directly manages – as union actions – around 1/3 of the total budget (which for the 2014-20 period, slightly over EUR 1 billion). These funds will have to cover however all security-related priorities, i.e. apart from above-mentioned areas, also fight against organized crime and police cooperation mechanisms.

50 As adopted by the Council, EP and Commission on 18 December, (OJ 2008/C/ 25/01 of 30.01.2008).

4.5 DG DEVCO - CoE

As a matter of new international priority, the European Union decided in 2010 to launch and fund a new concept called "CBRN Risk Mitigation Centers of Excellence (CoE)", based on a voluntary, cross border, local ownership and, last but not least, bottom up approach. As of today, 52 partner countries joined the initiative, coordinated around 8 regional secretariats based Georgia, Jordan, Algeria, Morocco, Kenya, United Arab Emirates, Uzbekistan and The Philippines launched its chemical, biological, radiological and nuclear (CBRN) Centres of Excellence (CoE) initiative (hereinafter the initiative) in May 2010. The initiative is designed to strengthen the institutional capacity of non-EU countries to mitigate CBRN risks which, if not countered, may constitute a threat to the EU. The origin of these risks can be criminal (proliferation, theft, sabotage and illicit trafficking), accidental (industrial catastrophes, in particular chemical or nuclear, waste treatment and transport) or natural (pandemics but also consequence of natural hazards on CBRN material and facilities).

With a budget of 250 million euro for the 2010–2020 period, the initiative is the single biggest measure of the long-term component of the Instrument contributing to Stability and Peace (IcSP). The IcSP was designed to provide the European Union with a new strategic tool to address a number of global security and development challenges. The IcSP provides non-EU partner countries with technical and financial assistance for risk mitigation and preparedness relating to chemical, biological, radiological and nuclear material or agents. According to the European Parliament and the Council, the measures adopted through the IcSP should be complementary and consistent with measures adopted in pursuit of the EU's common foreign and security policy.

The main objectives of the EU CBRN Centres of Excellence initiative are to strengthen the long-term national and regional CBRN governance and capabilities of responsible authorities and administrative infrastructure. The CoE initiative is a provider of tools and means for increased CBRN governance. It facilitates CBRN governmental officials from partner countries, belonging to all relevant ministries and agencies involved in CBRN governance, to meet regularly at the national level but also twice a year at the regional level between CBRN (round tables). This cross agency cooperation is key to stimulate further networking and has been much appreciated by partner countries. It **funding for CBRN activities identified and agreed by partner countries** during these regional round tables meetings. By implementing these activities, Member States come together and work to create action and provide CBRN governance support. More than fifty CoE projects have been funded in the last 5 years. These activities include a wide variety of formats, such as workshops and trainings, train the trainers programmes, capacity building or even equipment. Interagency cooperation, team building and support for CBRN administrative reforms are also part of these activities. Furthermore, the CoE provides a funding platform and a **sound methodology to first assess CRBN gaps needs at the national levels** (NAQs with hundreds of supporting questions) which is activated only upon request from a partner country, and, secondly, **a methodology to develop CBRN National Action Plans based on the needs assessments**. Results are fully confidential and belong entirely to the country.In the last two years, more than 25 partner countries completed their CBRN needs assessments and more than 15 started to develop their own National Action Plans. Some of the first NAPs developed within the initiative will be presented shortly this afternoon by their CoE country representatives.

The European External Action Service (EEAS), the body responsible for the EU foreign policy, is responsible for the strategic orientation of the initiative. DG DEVCO — International Cooperation and Development — is the decision-making body and is responsible for implementing the initiative's budget. It prepares the annual action programmes of the IcSP and monitors the work of the main implementing bodies: the Commission's Joint Research Centre (JRC) and the UN Interregional Crime and Justice Research Institute (UNICRI).

Further detailed info: http://www.cbrn-coe.eu/

4.6 LIFE+

The LIFE (the Financial Instrument for the Environment) Regulation, which was published on 20 December 2013, sets a budget for the next funding period, 2014–2020, of €3.4 billion in current prices. The LIFE programme is the EU's funding instrument for the environment and climate action. The general objective of LIFE is to contribute to the implementation, updating and development of EU environmental and climate policy and legislation by co-financing projects with European added value. The European Commission (DG Environment and DG Climate Action) manages the LIFE programme. The Commission has delegated the implementation of many components of the LIFE programme to the Executive Agency for Small and Medium-sized Enterprises (EASME). External selection, monitoring and communication teams provide assistance to the Commission and EASME. The European Investment Bank will manage the two new financial instruments (NCFF and PF4EE). The LIFE programme will contribute to sustainable development and to the achievement of the objectives and targets of the Europe 2020 Strategy, the 7th Union Environmental Action Programme and other relevant EU environment and climate strategies and plans.

4.7 Structural funds

Solutions exist that can help our regions become the best that they can be. Today, the EU's emphasis is very much on paving the way for regions to realise their full potential – by helping them to capitalise on their innate strengths while tapping into opportunities that offer possibilities for economic, social and environmental progress. Interreg Europe helps regional and local governments across Europe to develop and deliver better policy. By creating an environment and opportunities for sharing solutions, the programme aims to ensure that government investment, innovation and implementation efforts all lead to integrated and sustainable impact for people and place. By building on its forerunner, INTERREG IVC (2007-2013), Interreg Europe aims to get maximum return from the EUR 359 million financed by the European Regional Development Fund (ERDF) for 2014-2020. To achieve this goal, Interreg Europe offers opportunities for regional and local public authorities across Europe to share ideas and experience on public policy in practice, therefore improving strategies for their citizens and communities.

4.8 Education and Training

Erasmus+ is the EU's programme to support education, training, youth and sport in Europe. Its budget of €14.7 billion will provide opportunities for over 4 million Europeans to study, train gain experience, and volunteers abroad. Set to last until 2020, Erasmus+ does not just have opportunities for students. Merging seven prior programmes, it has opportunities for a wide variety of individuals and organisations. Erasmus+ has opportunities for people of all ages, helping them develop and share knowledge and experience at institutions and organisations in different countries. Erasmus+ has opportunities for a wide range of organisations, including universities, education and training providers, think-tanks, research organisations, and private businesses. The aim of Erasmus+ is to contribute to the Europe 2020 Strategy for growth, jobs, social equity and inclusion, as well as the aims of ET2020, the EU's strategic framework for education and training.

Erasmus+ Jean Monnet activities[51] are part of Erasmus+ dedicated to promoting excellence in EU studies in higher education around the world. Jean Monnet Actions (divided in Modules and Chairs) aim to build bridges between academics, researchers and EU policymakers. There is an emphasis on the study of and research on EU integration and in understanding Europe's place in a globalised world. Jean Monnet Modules are short teaching programmes or courses on EU studies. They can be introductory modules on the EU, courses that concentrate on a specific aspect or discipline within EU studies, or be more multi-disciplinary in approach. Jean Monnet Chairs are teaching posts with a specialisation in European Union studies for university professors or senior lecturers. These are posts lasting 3 years.

51 https://ec.europa.eu/programmes/erasmus-plus/opportunities/jean-monnet_en.

Individual scholarships within the Marie Skłodowska-Curie Actions[52] are a set of major research fellowships created by the European Union/European Commission to support research in the European Research Area. MSCA fellowships are among Europe's most competitive and prestigious awards, aimed at supporting the best and most promising scientists.

Cooperation for innovation[53] and the exchange of good practices are managed by the Education, Audiovisual and Culture Executive Agency (EACEA) and make it possible for organisations from different participating countries to work together, to develop, share and transfer best practices and innovative approaches in the fields of education, training and youth. EACEA manages the following actions in this field:

- Sector Skills Alliances ensuring cooperation between education and employment in tackling skills gaps with regard to one or more occupational profiles in a specific sector;
- Knowledge Alliances cooperation between higher education institutions and enterprises;
- Capacity Building in the field of youth supporting cooperation with Partner Countries;
- Capacity Building in the field of higher education supporting cooperation with Partner Countries.

4.9 JRC

4.9.1 JRC's CBRNE activities

The extensive ongoing work in CBRNE in the European Commission's Joint Research Centre is bringing together JRC's competences in chemical, biological, radiological, nuclear and explosive risks to respond to the needs of policy DGs in successfully addressing CBRNE as an emerging issue in the EU and in global security. In this context, the JRC collaborates with DG HOME for actions inside the EU in the implementation of the EU CBRN and Explosives action plans, and in aviation security; with DG DEVCO to support the mirroring of activities with partner countries of the EU, acknowledging that security issues are not limited by borders; and with several other partner DGs to fulfil their technical and scientific needs in the CBRNE areas. Security and non-proliferation issues remain an important pillar of the JRC's Euratom activities, extending our support to international safeguards, combating illicit trafficking of nuclear and radioactive materials, enhancing nuclear forensics, export control, and supporting several activities of training (in nuclear safeguards and nuclear and radiological security), as well as research agreements with several institutions in the EU MS. International cooperation with key partners (US, IAEA) in activities such as the Border Monitoring Working Group is also very important in this regard. Finally, standardisation in security is a key issue for the EU market, and the JRC actively supports the development of standards by providing scientific inputs to the European and International technical committees.

The activities in CBRNE security are strongly synergic and are aggregated in JRC's CBRNE cluster, currently including 34 projects focused on several key areas: support to the implementation and monitoring of EU CBRN security policy and international cooperation, support to CBRNE standardisation, improving CBRNE detection, optimising the prevention and detection approach to the emergence of new psychoactive drugs, implementing capacity building and training in nuclear security, supporting export control of dual use items, enhancing critical infrastructure protection and developing nuclear forensics.

52 https://ec.europa.eu/research/mariecurieactions/actions/individual-fellowships_en

53 https://eacea.ec.europa.eu/erasmus-plus/actions/key-action-2-cooperation-for-innovation-and-exchange-good-practices_en

Some examples of JRC's activities in CBRNE security include:

- The establishment and running of EUSECTRA - European nuclear security training centre, located in the JRC premises in Karlsruhe and Ispra, inaugurated in April 2013. EUSECTRA offers hands-on training using a wide variety of radioactive and nuclear materials and a broad selection of equipment and measurement instruments. So far, EUSECTRA has conducted trainings for several partners, among them DG TAXUD (Front Line Officers Training Course on Radiation Detection Techniques; customs experts from all the EU Member States will be trained over in total five sessions between June 2015 and February 2016), DG HOME (training for law enforcement officers being planned) and DG ENER but also external customers such as the US' Second Line of Defence programme. It remains at the disposal of MS needs.
- The JRC leads the ITRAP+10 Phase II project, which aims at testing various families of the RN detection equipment produced in the European Union. Manufacturers of instruments used against illicit trafficking of radioactive sources and nuclear material have been invited to participate in an extensive test programme, based on available IEC and ANSI standards, and IAEA recommendations. The important results of the project have been the basis for the input given to International Standardisation Organisations to review and improve the standards. Also, a certification scheme is being set up to capacitate MS laboratories to perform the same verifications.
- The CBRN Centres of Excellence initiative (see section 6.5), launched in 2010 by the European Union, provides a platform for voluntary regional cooperation on all CBRN-related hazard issues, be it of criminal (trafficking, terrorism), natural (pandemics, volcanic eruptions) or accidental (e.g. Fukushima) origin. It also includes the JRC support to the EU outreach activities in export control for dual-use items. The initiative is managed by DG DEVCO and the EEAS, with the technical and scientific support of a task force from the JRC and the collaboration of the United Nations' UNICRI institute. The JRC supports countries participating in the initiative to work together to identify risks, assess gaps and needs, draft National Action Plans and design capacity building projects to be implemented in the partner regions by EU MS consortiums. Fifty-two countries are now partners of the initiative, and a further 25 are looking to join.
- The JRC - Institute for reference materials and measurements (IRMM) supports the development of advanced measurement standards and training in several fields including safety and security linked to CBRN-E threats. For example the institute provides nuclear reference measurements and conformity assessment tools to safeguards authorities, industry and the international community helping to stop illicit trafficking of nuclear and radiological materials. JRC-IRMM reviews and tests the performance of new and existing chemical, biological and explosives threat detection equipment for current and emerging substances of interest, and develops testing protocols for first responder (hand-held) equipment. Scientific studies are performed on request for DG HOME and the Standing Committee for Precursors. JRC-IRMM will also produce explosives simulants as quality control tools to i) check that regulatory requirements for explosives detection equipment are met and ii) to support the end users in the Member States. JRC-IRMM provides impartial analysis and technical support to the continuous development and implementation of EU aviation security policies. JRC-IRMM supports the implementation EU requirements for explosives trace detection (ETD), by i) assisting the Commission's own team of aviation security inspectors, ii) providing reference materials to EU test centres who carry out testing of ETD equipment, and iii) developing training tools for personnel involved in operating ETD equipment at security checkpoints. JRC-IRMM supports a new Commission Regulation aiming at harmonising the certification of aviation security equipment, by providing impartial technical analysis of the conformity assessment practices.

4.9.2 ERNCIP

The Joint Research Centre set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) project in 2009 (https://erncip-project.jrc.ec.europa.eu/). This took place under the mandate of the DG HOME, in the context of the European Programme for Critical Infrastructure Protection (EPCIP), and with the agreement of Member States. ERNCIP is a European effort with the mission to "foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities", with three strategic goals to:

- Improve the protection of critical infrastructure in the EU
- Support the development of the EU's single market for security
- Identify gaps in EU security product testing capabilities.

To achieve these goals, ERNCIP maintains an online inventory of experimental capabilities in Europe ("The ERNCIP Inventory") and has developed a network of experts to identify and promote good test practices to form the basis of common European testing standards, aiming at harmonisation of test methodologies and test protocols, where practical. Currently, ERNCIP brings together over 200 active volunteers in this network.

The ERNCIP Inventory (https://erncip-project.jrc.ec.europa.eu/inventory) is a free-to-use search tool for information on European security experimental and testing facilities. It helps all types of critical infrastructure stakeholders to identify and make contact with CIP-related experimental expertise located in the EU. For the laboratories that are registered in the ERNCIP Inventory it provides greater visibility and increased business potential.

Member States and the Commission jointly define the Thematic Areas (TA) of concern, for ERNCIP to address at the EU level. When the need for a TA is identified, ERNCIP forms a Thematic Group (TG) to address this concern. A TG consists of nominated experts from research facilities, and also other stakeholders such as manufacturers and vendors of security solutions, government authorities, academia, and operators of critical infrastructures. Each group is led by an appointed Coordinator, who is responsible for the work programme for the TG to deliver against, in order to achieve the objectives agreed with ERNCIP.

4.9.3 Disaster Risk Management Knowledge Centre (DRMKC)

The Knowledge Centre for Disaster Risk Management is an initiative of the European Commission to further enhance and exploit the knowledge and evidence base of the Commission and the EU member states in disaster risk management. The Knowledge Centre adopts a networked approach to the science/knowledge-policy interface in Disaster Risk Management to support translating complex scientific data and analyses into usable information and provide science-based advice for DRM policies, as well as timely and reliable scientific-based analyses for emergency preparedness and response coordinated activities.

The Knowledge Centre could become a focal point of reference to support the work of Member States, relevant Commission services and the wider DRM community within and beyond the EU. For example, through taking up the results of other projects such as FP7 DRIVER, the Knowledge Centre can advise and inform Member States and others on DRM tools and cooperate with other initiatives (Community of Users). In addition, via the international dimension of the Knowledge Centre, the EU could support the Sendai framework for Disaster Risk Reduction to promote a more systematic and reinforced science-policy interface to strengthen the contribution of DRM to smart, sustainable and inclusive growth globally.

4.9.4 Joint Investment Programme (EDA)

The European Commission (EC) and the European Defence Agency (EDA) aim at maximising the complementarity and synergy of civilian security and defence-related research activities. This synchronisation of Research & Technology (R&T) investment takes place in the context of the European Framework Cooperation (EFC). In September 2011 the EFC cooperation agreement was signed on the CBRN protection by high representatives of EDA and the EC. The EDA contribution takes the form of a Joint Investment Programme (JIP-CBRN), with a centrally managed budget funded by all contributing Members (cM). The cooperation encompasses research activities identified under the security research theme of the Union's seventh research framework programme (FP7 SEC) and the EDA JIP CBRN. The JIP CBRN is a so called EDA R&T CAT A programme managed by a Management Committee comprising one representative from each cM. This committee is chaired by EDA and also comprises a non-voting representative from the Commission. The Management Committee is in charge of the management of the programme, the technological content and the selection of the proposals. Furthermore, they will follow the projects and do the dissemination of the results. As the JIP CBRN is an R&T Cat A programme, all the outcomes are research results (technology demonstration may be included) to be used by all the contributing Members.

Contributing Members of JIP CBRN are Austria, Belgium, Czech Republic, Germany, Spain, France, Ireland, Italy, Netherlands, Poland, Portugal, Sweden and Norway. The budget allocated to the JIP CBRN programme is 12 Million Euro. CBRN Protection is an important dual use domain in which Member States are prepared to jointly invest at a European level. In view of existing and emerging CBRN threats mid- to long-term, Member States see a need for enhanced technological development to protect against these threats. Examples of research funded by the JIP CBRN are described in this report.

1. Disaster risk and crisis management

Most of the research projects listed in this section directly or indirectly support the UCPM (see section 3.2) which address all aspects of the DRM cycle by strengthening cooperation and facilitating coordination within Europe in the areas of disaster prevention, preparedness and response. The mechanism indeed includes an action to 'improve the knowledge base on disaster risks and facilitate the sharing of knowledge, best practices and information'.[54] The use of various Union funds that may support sustainable disaster prevention is promoted and EU Member States and regions are encouraged to exploit those funding opportunities.

1.1 Multi-hazards

Series of projects are of generic nature and address tools and technologies related to DRM (from prevention to recovery) that can be applied to all types of (natural) disasters. The inter-operability of tools/technologies is actually mentioned in the CBRN Action Plan and UCPM as a mean to improve planning of disaster response operations, scenario building and response capacities (of direct support to the ERCC mission). The UCPM also promotes consistency in the response of disasters (networking), and the support to coordination of operational organisations (UN Office for the Coordination of Humanitarian Affairs (OCHA) and Member States).

The following section provides a snapshot of projects categorised according to specific sectors / themes related to natural hazards.

1.1.1 Multi-risk assessment, including cascading effects

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multi-risk assessment, including cascading effects	BEYOND MATRIX RASOR SMALLDIS

54 Art.5.1(a), Council Decision No. 1313/2013/EU, Official Journal of the European Union, L347, 20.12.2013

In the DG ECHO framework, the following project has been funded and falls into the multi-risk assessment category.

ARIMA	
Title	Assessment and Simulation of Present and Future Multi-hazard Risk in the Marrakesh-Safi Region
Objective	Development of a multi-hazard risk information platform for Marrakech-Safi region
Contract details	2018/PREV/826542 1-1-2019 - 31-12-2020; EUR: 697.057,12
Abstract	ARiMA will develop a spatial multi-hazard risk information platform (MRIP) for the benefit of the Marrakech-Safi Regional stakeholders based on innovative risk assessment and simulation methods, currently lacking. The platform will provide spatial information on current and future multi-hazard risks for the vulnerable social-ecological system within the whole region.
Consortium	Coordinator: 1. Industrieanlagen Betriebsgesellsc Haft Mbh (DK) Consortium: 2. United Nations University (JP) 3. Centro Internazionale in Monitoraggio Ambientale - Fondazione CIMA (IT) 4. Ressources Ingenierie (MA) 5. Universite Cadi Ayyad (MA)

1.1.2 Multi-hazard risk reduction, preparedness, resilience enhancement

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multi-hazard risk reduction, preparedness, resilience enhancement	CAPACITIES CAPHAZ-NET CARISMAND CATALYST CRISMA EMBRACE EMPREP ENHANCE EVAPREM GRADe GREEN IncREO IPCAM 2 I-REACT RockTheAlps TACTIC

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

RESILOC	
Title	RESILOC *This project is also relevant for 8.1.3 Societal resilience to disasters*
Objective	Development of new software instruments for the assessment of resilience indicators of a community
Contract details	H2020 Secure Societies Call: H2020-SU-SEC-2039; Topic code: SU-DRS01-2018-2019-2020 1/6/2019 - 31/5/2022; EUR 5 281 562,50
Abstract	RESILOC aims at studying and implementing a holistic framework of studies, methods and software instruments that combines the physical with the less tangible aspects associated with human behaviour. The study-oriented section of the framework will move from a thorough collection and analysis of literature and stories from the many approaches to resilience adopted all over the World. The results of the studies will lead to the definition of a set of new methods and strategies where the assessment of the resilience indicators of a community will be performed together with simulations on the "what-if" certain measures are taken. These studies and methods will serve for designing and implementing two software instruments: the RESILOC inventory, a comprehensive, live, structure for collecting, classifying and using information on cities and local communities, implemented as a Software as a Service (SaaS) and the RESILOC Cloud-based platform for assessing and calculating the resilience indicators of a city or a community, for developing localised strategies and verifying their impacts on the resilience of the community. The Cloud platform, a combination of SaaS and PaaS, includes the inventory as its repository. The project will make use of built solutions in four field trials and includes a high-profile communication plan, heavily based on Social Media platforms.
Consortium	Coordinator: 1. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) Consortium: 2. Intelligence For Environment And Security Srl Ies Solutions Srl (IT) 3. Ethniko Kai Kapodistriako Panepistimio Athinon (EL) 4. Tavistock Institute Of Human Relations Lbg (UK) 5. Istituto Di Sociologia Internazionale Di Gorizia Isig (IT) 6. Institut Jozef Stefan (SL) 7. Stiftinga Vestlandsforskingstiftelse (NO) 8. Resilience Advisors Ltd (UK) 9. Balkanski Institut Po Truda I Socialnata Politika Association (BU) 10. Comune Di Catania (IT) 11. Dimos Ditikis Achaias (EL) 12. Bergen Kommune (NO) 13. Regione Sicilia (IT) 14. Bulgarian Red Cross (BU) 15. Ministry Of National Defence, Greece (EL) 16. Uprava Rs Za Zaščito In Reševanje, Ministrstvo Za Obrambo (SL)

These projects were complemented by new projects funded in 2018:

ARCH	
Title	Advancing Resilience of Historic Areas against Climate-related and other Hazards *This project is also relevant for 1.2.1 Multi-climate hazard risk prevention, awareness, preparedness, resillence and 4.4.1 Screening of persons, bags, vehicles*
Objective	Development of disaster risk management framework for the resilience of historic areas to climate change-related and other hazards.
Contract details	H2020-LC-CLA-2018-2; 1/6/2019 - 31/5/2022; EUR: 5.999.962,50
Abstract	ARCH will develop a unified disaster risk management framework for assessing and improving the resilience of historic areas to climate change-related and other hazards. This will be achieved by developing tools and methodologies that will be combined into a collaborative disaster risk management platform for local authorities and practitioners, the urban population, and (inter)national expert communities. To support decision-making at appropriate stages of the management cycle, different models, methods, tools, and datasets will be designed and developed. These include: technological means of determining the condition of tangible and intangible cultural objects, as well as large historic areas; information management systems for georeferenced properties of historic areas and hazards; simulation models for what-if analysis, ageing and hazard simulation; an inventory of potential resilience enhancing and reconstruction measures, assessed for their performance; a risk-oriented vulnerability assessment methodology suitable for both policy makers and practitioners; a pathway design to plan the resilience enhancement and reconstruction of historic areas; and an inventory of financing means, categorised according to their applicability in different contexts. The project ensures that results and deliverables are applicable and relevant by applying a co-creation process with local policy makers, practitioners, and community members. This includes the pilot cities Bratislava, Camerino, Hamburg, and Valencia. The results of the co-creation processes with the pilot cities will be disseminated to a broader circle of other European municipalities and practitioners. ARCH includes a European Standardisation organization (DIN) as a partner in order to prepare materials that ensure that resilience and reconstruction of historic areas can be progressed in a systematic way, through European standardisation, which will ensure practical applicability and reproducibility.
Consortium	Coordinator: 1. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) Consortium: 2. "Iclei European Secretariat Gmbh (Iclei Europasekretariat Gmbh)" (DE) 3. Din Deutsches Institut Fuer Normung E.V. (DE) 4. Fundacion Tecnalia Research & Innovation (ES) 5. Agenzia Nazionale Per Le Nuove Tecnologie, L'energia E Lo Sviluppo Economico Sostenibile (IT) 6. Universita Degli Studi Di Camerino (IT) 7. Istituto Nazionale Di Geofisica E Vulcanologia (IT) 8. Sogesca S.R.L. (IT) 9. Research For Science, Art And Technology (Rfsat) Limited (IE) 10. Mestsky Ustav Ochrany Pamiatok (SK) 11. Univerzita Komenskeho V Bratislave (SK) 12. Hlavne Mesto Slovenskej Republiky Bratislava (SK) 13. Fundacion De La Comunitat Valenciana Para La Promocion Estrategica El Desarrollo Y La Innovacion Urbana (ES) 14. Comune Di Camerino (IT) 15. Freie Und Hansestadt Hamburg (DE)

REMESH	
Title	Research Network on Emergency Resources Supply Chain *This project is also relevant for 9.4.2 Communication systems with focus on disaster management (general).*
Objective	Setting up and exploitation of the Research Network on Emergency Resources Supply Chain
Contract details	H2020-MSCA-RISE-2018; 1/5/2019 - 30/4/2023; EUR: 1.104.000
Abstract	The ability of national and international agencies to cope effectively with large-scale natural disasters is becoming more and more important. The United Nations Office for the Co-ordination of Humanitarian Affairs (OCHA, 2016) reports an increase in the frequency and impact of large-scale natural disasters in both the developed and developing world. Recent extreme events such as Storm Jonas (2016, USA), the earthquake and tsunami in Tōhoku (2011) and New Zealand (2016) have demonstrated the need for a rapid and effective external response to complex events, and the impact on the human population when this is delayed or inadequate. The Emergency Resources Supply Chain (ERSC) has a crucial role in promoting the effective application of disaster management, and differs from conventional supply chains in several ways. The unique characteristics of ERSC include: a) having to analyse all the demands in a very short period of time, using limited resources. b) having to be designed, constructed and maintained in order to support continuous and smooth materials and information flows, and c) having to include a set of diverse plans, resources, authorities, agencies, and their associated human resources.
Consortium	Coordinator: 1. Liverpool John Moores University (UK) Consortium: 2. "The University Of Manchester (UK) 3. Lunds Universitet (SE) 4. Dublin City University (IE) 5. Rheinische Friedrich-Wilhelms-Universitat Bonn (DE) 6. Universidad De Granada (ES) 7. Mahidol University (TH) 8. University Of Engineering And Technology - Vietnam National University - Ha Noi (VN) 9. Wuhan University of Technology (CN)

The projects were complemented by the following projects funded by the LIFE+ CLIMA programme.

LIFE METRO ADAPT	
Title	METRO ADAPT: enhancing climate change adaptation strategies and measures in the Metropolitan City of Milan
Objective	Mainstreaming adaptation strategies and measures in territorial plan for Metropolitan City of Milan
Contract details	LIFE17 CCA/IT/000080; 03/09/2018 - 30/09/2; Total budget: EUR 1,306,010.00; EU funding: EUR 670,417.00
Abstract	LIFE METRO ADAPT aims to mainstream adaptation strategies and measures in the development of a territorial plan for CMM and in the planning and building rules of the 134 CMM municipalities. It will achieve this aim through the adoption of an innovative approach that identifies the role of intermediate governing bodies. The project also plans to promote nature-based solutions to meet a range of objectives, such as the reduction of the flooding risk and the heat-island effect, while also regenerating neglected urban spaces. The project plans moreover to enhance bottom-up initiatives and thus increase citizen awareness and engagement in issues related to climate change adaptation. The implementation of demonstration facilities will directly involve stakeholders from the building sector and engineering professionals working in water management. Furthermore, the project will develop innovative meteorological satellite data and high precision soil sealing maps, in order to produce detailed vulnerability analysis (focusing in particular on heat islands and floods). The aim is to ensure the availability of information specific to each municipality. Finally, the project aims to develop a network of metropolitan areas in Italy and elsewhere in Europe to enhance the mainstreaming of adaptation policies and measures and support the implementation of nature-based solutions.
Consortium	Coordinator: 1. Citta Metropolitana Di Milano (IT) Consortium: 2. Ambiente Italia srl (IT) 3. Italy CAP Holding S.p.A (IT) 4. Italy Legambiente Lombardia Onlus (IT) 5. Italy Association des Agences de la Democratie Locale (IT) 6. France e-GEOS s.p.a (FR) 7. Italy (IT)

1.1.3 Multi-hazards situation awareness / early warning

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	
Multi-hazards situation awareness / early warning	A4A AIRBEAM COPE INACHUS MOSAIC OPTI-ALERT PHAROS

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

RESPONDRONE	
Title	RESPONDRONE *This project is also relevant for 1.1.4 Multi-hazard emergency response and crisis management, including cascading effects*
Objective	Develop and validate an integrated solution for first responders to operate drones for increased situation assessment capacity
Contract details	H2020-SU-SEC-2044; Topic code: SU-DRS02-2018-2019-2020 1/5/2019 - 30/4/2022; EUR 7 996 187,50
Abstract	RESPONDRONE will develop and validate an integrated solution for first responders to easily operate a fleet of drones with multiple synchronized missions to enhance their situation assessment capacity and own protection. This System of Systems will simplify and accelerate situation assessment and sharing, decision making and operations management, while requiring a small crew to operate it. Moreover, it will deliver high-level information to any involved control centre through an intelligent web-based system that can be operated and accessed from a remote site as well as serving as on-demand airborne communications network to allow people on the ground to communicate with the command centre in case of cellular coverage collapse. With these situational-awareness enhancing tools, emergency response teams will be able to more rapidly, effectively and efficiently respond to an emergency or disaster and therefore save more lives. The fleet of drones will provide enhanced capabilities to support assessment missions, search and rescue operations, as well as forest fire fighting. The deployment will still be very simple. Each fleet or unit of drones will be able to be operated by a single pilot and few observers. To ensure seamless uptake and adaption by first responder organizations, RESPONDRONE will be fully integrated and embedded within the current processes and procedures of real emergency response agencies and teams, among others through advanced training programs. Therefore, RESPONDRONE will increase the effectiveness and efficiency of civil protection operations as it will consider the first responder total mission time, cost, and effectiveness (and not just considering the deployment time). RESPONDRONE will be demonstrated through participation in actual civil protection exercises on Corsica, involving several agencies simultaneously.
Consortium	Coordinator: 1. Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (DE) Consortium: 2. Israel Aerospace Industries Ltd. (IL) 3. Alpha Unmanned Systems Sl (ES) 4. Thales Six Gts France Sas (FR) 5. Korea Aviation Technologies Co Ltd (KR) 6. Haut Comite Francais Defense Civile (FR) 7. Ministry Of Defense (IL) 8. Service Departemental D'incendie Et De Secours De La Haute-Corse (FR) 9. Veiligheidsregio Haaglanden (NL) 10. State Fire And Rescue Service (LV) 11. Ministry Of Emergency Situations (AM) 12. Perifieria Dytikhs Makedonias (EL) 13. Region Of Central Macedonia (EL) 14. Regional Administration Varna (BU) 15. Inesc Tec - Instituto De Engenharia De Sistemas E Computadores, Tecnologia E Ciencia (PT) 16. Commissariat A L Energie Atomique Et Aux Energies Alternatives (FR) 17. American University Of Armenia Foundation (AM) 18. Time.Lex (BE) 19. Agora P.S.V.D. (IL) 20. Inha University Research And Busines Foundation (KR)

The projects were complemented by the following projects funded by DG ECHO.

LODE	
Title	Loss Data Enhancement for DRR and CCA Management
Objective	Develop optimal damage and loss data information systems for DRR and CCA to enhance understanding of disaster impact
Contract details	2018/PREV/826567 15-1-2019 - 14-1-2021; EUR: 799.108,96
Abstract	Evidence-based, effective and efficient disaster risk reduction (DRR) and climate change adaptation (CCA) assessments, policies and strategies require knowledge and data. This action focus is on developing optimal damage and loss data information systems for DRR and CCA to enhance our understanding of disaster impacts and by doing so support the requirements set by a number of policies and strategies at national, European and international levels.
Consortium	Coordinator: 1. Politecnico Di Milano (IT) Consortium: 2. Departament D'interior – Generalitat De Catalunya (ES) 3. Ilmatieteen Laitos (FI) 4. Fondazione Centro Euromediterraneosui Cambiamenti Climatici (IT) 5. Regione Umbria (IT) 6. Centre National De La Recherche Scientifique Cnrs (FR) 7. Organismos Antiseismikou Sxediasmoukai Prostasias (EL) 8. Earthquake Planning And Protection Organization) (EL) 9. Universidade Do Porto (PT) 10. Institute Of Forestry (RS) 11. Agencia Estatal Consejo Superior De Investigaciones Cientificas (ES)

The projects were complemented by the following projects funded by the INTERREG programme.

JORIMA	
Title	Joint risk management and partnership in the border region Calarasi – Dobrich *This project is also relevant for category 1.1.4 Multi-hazard emergency response and crisis management, including cascading effects and 7.2 Maritime security*
Objective	Improve and ensure an efficient management for joint interventions in emergency situations on the border Calarasi-Dobrich
Contract details	2014 - 2020 INTERREG V-A Romania – Bulgaria 2019/03/13 - 2021/03/12; EUR: 680.183,74
Abstract	Calarasi ESI and Dobrichka Municipality Administration willing to solve the common challenge, jointly decided to participate in this project. JORIMA aims to improve and to ensure an efficient management for joint interventions in emergency situations in the border Calarasi-Dobrich, to increase co-ordination and efficiency in response of authorities in joint early warning, in line with the EU policies and guidelines. During its 2-years duration, the project endeavors to increase the cross-border cooperation in emergency management by means of several actions: To purchase modern equipment for early warning and quick reaction to the emergency situation – a electronic wallscreen will be delivered in the Calarasi ESI headquarters and delivery of equipment for quick reaction to prevent the negative effect of disasters (like floods, fire, storms etc) in Dobrichka Muicipality . The new solutions for minimizing the time for reaction in emergency will ensure the localization of the risk event, the easy contact of local decision maker which ensures administrative functions. Additional to this a common Strategy and Action Plan will be elaborated for responding to various possible types of risk situations of natural and anthropic characteristic of Calarasi County and Dobrich District. A network of partnerships among territorial entities involved in civil protection activities will be created.
Website	http://www.interregrobg.eu
Consortium	Coordinator: Dobrichka Municipality Administration (BU)

These projects were complemented by new projects funded in 2018:

CAOS	
Title	Containment, Avalanches and Optimisation in Spreading-processes *This project is also relevant for 1.1.1 Multi-risk assessment, including cascading effects.*
Objective	Gain insights into the conditions for the onset of abrupt transitions and avalanche outbreaks
Contract details	H2020-MSCA-IF-2018; 1/8/2019 - 31/7/2021; EUR 224 933,76
Abstract	In this project, we will investigate the signs for abrupt transitions and avalanche outbreaks both macroscopically and in specific instances, to gain insight into the conditions for their onset. We will develop methods to contain (or facilitate) the outbreaks by optimal deployment of resources, such as applying vaccines or distributing promotion material by employing the recently developed dynamic message passing techniques from statistical physics. We will collaborate with British Telecom to promote product marketing and service provision by using thenew optimisation algorithms. This project will have significant impact on the scientific understanding of non-equilibrium spreading processes, provide algorithmic solutions for practical problems in specific instances, will support policy making decisions and offer optimal resource allocation for commercial marketing tasks.
Consortium	Coordinator: Aston University (UK)

1.1.4 Multi-hazard emergency response and crisis management, including cascading effects

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	
Multi-hazard emergency response and crisis management, including cascading effects	ACRIMAS BRIDGE CASCEFF CENTAURO COBACORE DISASTER DRIVER EMILI EVACUATE FLOEQ FORTRESS HEIMDALL HIT-GATE IDIRA IN-PREP MAGIC Partners in Safety PREDICT Reaching Out SAFER SICMA SMOKEBOT SNOWBALL S(P)EEDKITS SYSEP TransCrisis Transfer of knowledge and skills in chemical and ecological rescue Uramet USCORE 2

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

ASSISTANCE	
Title	ASSISTANCE *This project is also relevant for 8.3.5 Training and Networking and 8.3.1 Civil Protection Operations, including volunteers involvement*
Objective	To enhance first responders' capabilities for facing complex situations providing them advanced training based on Virtual Reality (VR), Mixed Reality (MR) and Augmented Reality (AR)
Contract details	H2020-SU-SEC-2028; Topic code: SU-DRS02-2018-2019-2020 1/5/2019 - 30/4/2022; EUR 6 393 691,25
Abstract	The main purpose of ASSISTANCE project is twofold: On the one hand to help and protect different kind of first responders' (FR) organizations that work together taking into account the type of disaster/crisis they are mitigating in each moment and on the other hand, to enhance their capabilities for facing complex situations providing them advanced training based on Virtual Reality (VR), Mixed Reality (MR) and Augmented Reality (AR), tailored to their real needs depending on the type of incident. ASSISTANCE project will use novel technologies such as; UAV, Robots, drones' swarms and advanced training based on VR, MR and AR for increasing the FR's situation awareness (SA) taking into account their need in terms of data (e.g. real time video, persons and objects location, evacuation routes status, ad-hoc network coverage and so on). Different types of adapted SA modules will be developed inside a common SA framework capable of offering the sensor outcome needed by each FR organization (e.g. real time video and resources location for firemen, evacuation routes status for emergency health services and so on). Regarding training, an advanced training network based on VR, MR, AR and other novel technologies and methodologies (e.g. tailored curricula, immersive interfaces, adapted training methodology definition, etc.) will be established in order to share different VR platforms and scenarios for enhancing the current training capabilities and skills of different FRs organization. All the ASSISTANCE results will be tested under controlled conditions in three different demostration pilots. Solutions will be developed in compliance with EU societal values, fundamental rights and applicable legislation, including in the area of privacy and personal data protection. Societal aspects (e.g. perception of security, possible effects of technological solutions on societal resilience, gender diversity) have to be taken into account in a comprehensive and thorough manner.
Consortium	Coordinator: 1. Universitat Politecnica De Valencia (ES) Consortium: 2. Etra Investigacion Y Desarrollo Sa (ES) 3. Thales Sa (FR) 4. Agencia Valenciana De Seguridad Yrespuesta A Las Emergencias (ES) 5. Siec Badawcza Lukasiewicz - Przemyslowy Instytut Automatyki I Pomiarow Piap (PL) 6. Fundacion Andaluza Para El Desarrollo Aeroespacial (ES) 7. Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (NL) 8. Rise Research Institutes Of Sweden Ab (SE) 9. Instituut Fysieke Veiligheid (NL) 10. Universidad De Cantabria (ES) 11. Openbaar Lichaam Gezamenlijke Brandweer (NL) 12. Ambulance And Emergency Physicians Association (TR) 13. Ministerio Del Interior (ES) 14. Viasat Antenna Systems Sa (CH) 15. E-Lex - Studio Legale (IT) 16. Sodertorns Branforsvarsforbund (SE) 17. Centrum Naukowo-Badawcze Ochrony Przeciwpozarowej Im. Jozefa Tuliszkowskiego - Panstwowy Instytut Badawczy (PL) 18. Cyberethics Lab Srls (IT)

FASTER	
Title	FASTER *This project is also relevant for 1.1.2 Multi-hazard risk reduction, preparedness, resilience enhancement*
Objective	To support a comprehensive and rapid crisis management response involving all emergency responders
Contract details	H2020-SU-SEC-2038; Topic code: SU-DRS02-2018-2019-2020 1/5/2019 - 30/4/2022; EUR 6 999 750
Abstract	The term first responders usually refers to law enforcement, fire, and emergency medical personnel. These responders, however, are not the only assets that may be required in the aftermath of a strike on the homeland. In contrast, the more appropriate term, emergency responders, comprises all personnel within a community that might be needed in the event of a natural or technological (man-made) disaster or terrorist incident. These responders might include hazardous materials response teams, urban search and rescue assets, community emergency response teams, anti-terrorism units, special weapons and tactics teams, bomb squads, emergency management officials, municipal agencies, and private organizations responsible for transportation, communications, medical services, public health, disaster assistance, public works, and construction. In addition, professional responders and volunteers, private nonprofit, nongovernmental groups (NGOs), such as the Red Cross, can also play an important role in emergency response. As a result, the tasks that a national emergency response system would be required to perform are more complex than simply aiding victims at the scene of a disaster, carried out by several kinds of professional users with different roles and expertise. Moreover, emergency preparedness and response lifecycle is a complex process that consists of the preparation, response, and recovery from a disaster, including planning, logistical support, maintenance and diagnostics, training, and management as well as supporting the actual activities at a disaster site and post-recovery after the incident.
Consortium	Coordinator: 1. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) Consortium: 2. Engineering - Ingegneria Informatica Spa (IT) 3. Hellenic Telecommunications Organization S.A. - Ote Ae (Organismos Tilepikoinonion Tis Ellados Ote Ae) (EL) 4. Diginext (FR) 5. Crisisplan B.V. (NL) 6. Drone Hopper Sl (ES) 7. Robotnik Automation Sll (ES) 8. Synelixis Lyseis Pliroforikis Automatismou & Tilepikoinonion Anonimi Etairia (EL) 9. Inov Inesc Inovacao - Instituto De Novas Tecnologias (PT) 10. Fondazione Links - Leading Innovation & Knowledge For Society (IT) 11. Kpeople Research Foundation (MT) 12. Kajaanin Ammattikorkeakoulu Oy (FI) 13. Vrije Universiteit Brussel (BE) 14. Panepistimio Dytikis Attikis (EL) 15. Ayuntamiento De Madrid (ES) 16. Servicio Madrileno De Salud (ES) 17. Ecole Nationale Superieure Des Officiers De Sapeurs-Pompiers (Ensosp) (FR) 18. Wyzsza Szkola Policji W Szczytnie (PL) 19. Kajaanin Kaupunki (FI) 20. Elliniki Omada Diasosis Attikis (EL) 21. Municipio De Grandola (PT) 22. Consorzio Per Il Sistema Informativo (Csi Piemonte) (IT) 23. Kwansei Gakuin Educational Foundation (JP)

INGENIOUS	
Title	INGENIOUS *This project is also relevant for 8.3.6 Protective equipment and 9.3 Communication systems (Interoperability and communication with focus on security)*
Objective	Develop, integrate, test, deploy and validate a Next Generation Integrated Toolkit (NGIT) for Collaborative Response between first responders
Contract details	H2020-SU-SEC-2040; Topic code: SU-DRS02-2018-2019-2020 1/9/2019 - 31/8/2022; EUR 8 616 111,25
Abstract	Today's First Responders (FR) are using technology of the past. During their primary mission of saving lives and preserving society's safety and security, FRs face a multitude of challenges. In both small scale emergencies and large scale disasters, they often deal with life-threatening situations, hazardous environments, uncharted surroundings and limited awareness. Threats and hazards evolve rapidly, crossing municipalities, regions and nations with speed and ease. Armouring public safety services with all the tools that modern technology has to offer is critical. Such tools holistically enhance their protection and augment their operational capacities, assisting them in saving lives as well as ensuring their safe return from the disaster scene. INGENIOUS will develop, integrate, test, deploy and validate a Next Generation Integrated Toolkit (NGIT) for Collaborative Response, which ensures high level of Protection & Augmented Operational Capacity to respond to the disaster scene. This will comprise a multitude of the tools and services required: 1) for enabling protection of the FRs with respect to their health, safety and security; 2) for enhancing their operational capacities by offering them with means to conduct various response tasks and missions boosted with autonomy, automation, precise positioning, optimal utilisation of available resources and upgraded awareness and sense-making; 3) for allowing shared response across FR teams and disciplines by augmenting their field of view, information sharing and communications between teams and with victims. The NGIT armours the FRs at all fronts. The NGIT will be provided at the service of the FRs for extensive testing and validation in the framework of a rich Training, Testing and Validation Programme – of Lab Tests (LSTs), Small-Scale Field Tests (SSTs) and Full-Scale Field Validations (FSXs) – towards powering the FR of the future being fully aware, fully connected and fully integrated.
Consortium	Coordinator: 1. Institute Of Communication And Computer Systems (EL) Consortium: 2. Universiteit Twente (NL) 3. Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (DE) 4. Diginext (FR) 5. Fundacion Tekniker (ES) 6. Exus Software Monoprosopi Etairia Periorismenis Evthinis (EL) 7. Sintef As (NO) 8. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 9. Totalforsvarets Forskningsinstitut (SE) 10. Satways - Proionta Kai Ypiresies Tilematikis Diktyakon Kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis Epe (EL) 11. Alpes Lasers Sa (CH) 12. Technische Universitaet Wien (AT) 13. Cy.R.I.C Cyprus Research And Innovation Center Ltd (CY) 14. Universidad Pompeu Fabra (ES) 15. Singularlogic Anonymi Etaireia Pliroforiakon Systimaton Kai Efarmogon Pliroforikis (EL) 16. Korea Institute Of Robot And Convergence (KR) 17. Gobierno Vasco - Departamento Seguridad (ES) 18. Assistance Publique - Hopitaux De Paris (FR) 19. Sodertorns Branforsvarsforbund (SE) 20. I.S.A.R. Germany Stiftung Ggmbh (DE) 21. Police Service Of Northern Ireland (UK) 22. Elliniki Omada Diasosis Attikis (EL) 23. Trilateral Research Limited (IE)

The projects were complemented by the following projects funded by DG ECHO.

BALTPREP	
Title	Enhancing regional preparedness and response capacity for major accidents in the Baltic Sea region
Objective	Improve and optimise quality and interoperability of the Red Cross and Civil Protection Authorities regional response capacity for major accidents and severe disruptions.
Contract details	2018/PREP/826529; 1/1/2019 – 31/12/2020; EUR: 456.181,93
Abstract	This project improves and optimises quality and interoperability of the Red Cross and Civil Protection Authorities regional response capacity for major accidents and severe disruptions. The project strengthens collaboration in and between 7 EU member states: Finland, Denmark, Germany, Poland, Lithuania, Latvia and Estonia.
Consortium	Coordinator: 1. Dansk Rode Kors (Danish Red Cross) (DK) Consortium: 2. Deutsches Rotes Kreuz Ev (DE) 3. Eesti Punane Rist Mtu (EE) 4. Latvijas Sarkanais Krusts (LV) 5. Lietuvos Raudonojo Kryziaus Draugija (LT) 6. Polski Czerwony Krzy (PL)

ReadytoRespond	
Title	Modernised Preparedness and Response Capacity in South Caucasus
Objective	Improve the level of preparedness of civil protection systems in Armenia and Georgia by enhancing cooperation between and capacity of civil protection and humanitarian aid actors.
Contract details	2018/PREP/826442; 1-1-2019 - 31-12-2020; EUR: 425.652,43
Abstract	This Action will contribute to improving the level of preparedness of civil protection systems in Armenia and Georgia by enhancing cooperation between civil protection and humanitarian aid actors and increase and diversify preparedness and response capacities of key actors. The Action will significantly improve the technical capacity of both Armenia Red Cross (ARCS) and Georgia Red Cross (GRCS) to provide aid at scale, through diversified assistance options.
Consortium	Coordinator: 1. Dansk Rode Kors (Danish Red Cross) (DK) Consortium: 2. Armenian Red Cross Society (AM) 3. Georgia Red Cross Society (GE) 4. Osterreichisches Rotes Kreuz (AT) 5. Raudi Krossinn A Islandi (IS) 6. Federation Internationale Des Societes De La Croix-Rouge Et Du Croissant Rouge (CH)

These projects were complemented by new projects funded in 2018:

Plant/FATE	
Title	Predicting global vulnerability of forests to drought using plant functional trait evolution *This project is also relevant for 1.2.5 Forest fire risk prevention*
Objective	To advance our abilities to predict evolutionarily emergent plant strategies, plant productivity, and ecosystem services under current climatic conditions, and identify species and regions that are likely to be vulnerable to future changes in climate
Contract details	MSCA/IF/2018 / Individual Fellowships; 1/8/2019 - 31/7/2021; EUR 186 167,04
Abstract	To understand what plant traits are responsible for drought-resistance, we aim to push the envelope of contemporary eco-evolutionary dynamic vegetation modelling. Accounting for trade-offs in growth via acquisition of resources and resistance to drought-induced mortality, we will allow plant traits to evolve under realistic drought regimes. We will calibrate and test our model using data on plant traits and long-term demography available from two tropical forest sites – a wet site from Costa Rica, and a seasonally dry site from southern India. We will then parametrize our model at a wider scale, using available data on traits and environmental fluxes from sites across the globe in different biomes. Bringing together expertise from plant physiology, evolutionary dynamics, and high-performance computing, our approach will advance our abilities to predict evolutionarily emergent plant strategies, plant productivity, and ecosystem services under current climatic conditions, and identify species and regions that are likely to be vulnerable to future changes in climate. Our models and methods could potentially be adopted for similar analyses in the agriculture sector. We will communicate our results to policymakers and the public via an interactive web-based dashboard. IIASA will provide the researcher with the perfect platform for research training, and for a dialogue with policymakers and other stakeholders to prepare for mitigating and adapting to climate change.
Consortium	Coordinator: Internationales Institut Fuer Angewandte Systemanalyse (AT)

STOPFIRE	
Title	Emergency Decision Support System of Offshore Platform Fires
Objective	Develop an emergency decision support system of offshore platform fires, including evacuation simulation model and risk warning model
Contract details	H2020/MSCA/IF/2018; 20/12/19- 19/12/2021; EUR 224 933,76
Abstract	In this project, fire accidents on offshore oil and gas platform will be analysed to identify the typical fire scenarios, followed by numerical simulation on the temporal and spatial evolution of the fires. Secondly, the coupling mechanism between human behavior and fire development will be investigated to quantitatively characterize the impact of fire on people and other assets. Thereafter, based on fire numerical simulation and multi-agent theory, an evacuation simulation model of offshore platform fires will be proposed. Thirdly, the dynamic risk of offshore platform fire evacuation will be evaluated by considering both failure consequences and their probabilities. A risk warning model of offshore platform fire evacuation will be built based on the Wavelet Genetic Neural Network. Finally, a dynamic decision-making support system for fire emergency evacuation will be designed by integrating Computation Fluid Dynamic (CFD), multi-agent theory and the Virtual Reality (VR) technology. This project covers a wide range of disciplines including CFD, multi-agent-based evacuation simulations, probabilistic inference (Bayesian inference and system dynamic model) and the VR technology. This Individual Fellowship will significantly accelerate the development of interdisciplinary knowledge, innovative research skills and new career of the nominated Fellow.
Consortium	Coordinator: Liverpool John Moores University (UK)

DRONECOP	
Title	The first integral control and command system for managing missions which delivers 3D cartography and georeferenced data in real-time *This project is also relevant for 9.4.2 Communication systems with focus on disaster management (general).*
Objective	Development of DRONECOP, the first integral general operation system for combating natural disasters able to process data captured by a drone and automatically generate 3D cartography and georeferenced targets
Contract details	H2020-SMEInst-2018-2020-1; 1/6/2019 - 30/9/2019; EUR: 50.000
Abstract	Over the last 3 years, we have developed DRONECOP, the first integral general operation system for managing missions for combating natural disasters able to process data captured by a drone (video, photogrammetry) in real-time and automatically generate 3D cartography and georeferenced targets. Several regional and global emergency mechanisms exist to support disaster management, but they lack efficiency due to the unstructured existing management systems: unable to process information in real-time and to provide accurate tools for critical decision making based on objective information. With DRONECOP, natural disasters management bodies will have access to critical catastrophic areas and get accurate and updated 3D mapping information and georefereced targets in real time. This will allow them to plan their missions and make fast decision in critical moments in a much more effective way due to the objective information they will count with. Consequently, there will be a reduction in fatalities and injured among their crews and in social, environmental and economic impact of the disasters. DRONECOP will disrupt in the Mapping for Incident and emergency Market (valued at €10,440Mill in 2018) creating a new niche of integral management system for missions with real-time 3D mapping and georeferenced data that no other competitor has already achieved. DRONECOP will make any disaster management operation safer, faster and more efficient than ever. It will positively impact on the human, environmental and economic scope of any natural disaster in which it will be used.
Consortium	Coordinator: Geointelligence Systems Sl (ES)

FOTOKITE-SME-P1	
Title	Aerial Situational Awareness for Every Firefighter *This project is also relevant for 8.3.1 Civil Protection Operations, including volunteers involvement.*
Objective	Development of Fotokite, a situational awareness solution
Contract details	H2020-SMEInst-2018-2020-1; 1/2/2019 - 31/5/2019; EUR: 50.000
Abstract	Fotokite is a breakthrough situational awareness solution whose unique characteristics constitute it as a valuable public safety tool for firefighters. Fotokite aims to ensure operational safety, increase response efficiency, decrease associated workload and operational risks, and help in life-saving efforts.
Consortium	Coordinator: Perspective Robotics AG (CH)

1.1.5 Earth observation support

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	FP7 projects
Earth Observation support	AIOSAT AVERT BONAS CEASELESS COMMONSENSE E2mC EGSIEM EMPHASIS ENCOUNTER EOPEN EUGENIUS GEO VISION HOMER LOTUS OPTIX PREVAIL ROSFEN SALIANT SUBCOP

These projects were complemented in the H2020 framework by the following project.

ExtremeEarth	
Title	From Copernicus Big Data to Extreme Earth Analytics *This project is also relevant for 3.1 Food safety.*
Objective	Develop Remote Sensing and Artificial Intelligence techniques that are needed for extracting information and knowledge out of the petabytes of Copernicus data, making Europe a pioneer in Extreme Earth Analytics
Contract details	H2020-ICT-2018-2; 1/1/2019 - 31/12/2021; EUR: 5.988.301,25
Abstract	Copernicus is the European program for monitoring the Earth. The geospatial data produced by the Sentinel satellites puts Copernicus at the forefront of the Big Data paradigm, giving rise to all the relevant challenges: volume, velocity, variety, veracity and value. ExtremeEarth concentrates on developing the technologies that will make Europe a pioneer in the area of Extreme Earth Analytics i.e., the Remote Sensing and Artificial Intelligence techniques that are needed for extracting information and knowledge out of the petabytes of Copernicus data. The ExtremeEarth consortium consists of Remote Sensing and Artificial Intelligence researchers and technologists with outstanding scientific track records and relevant commercial expertise. The research and innovation activities undertaken in ExtremeEarth will significantly advance the frontiers in Big Data, Earth Analytics and Deep Learning for Copernicus data and Linked Geospatial Data, and make Europe the top player internationally in these areas. The ExtremeEarth technologies will be demonstrated in two use cases with societal, environmental and financial value: the Food Security use case and the Polar use case. ExtremeEarth will bring together the Food Security and Polar communities, and will work with them to develop technologies that can be used by these communities in the respective application areas. The results of ExtremeEarth will be exploited commercially by the industrial partners of the consortium.
Consortium	Coordinator: 1. Ethniko Kai Kapodistriako Panepistimio Athinon (GR) Consortium: 2. "Vista Geowissenschaftliche Fernerkundung Gmbh (DE) 3. Universitetet I Tromsoe - Norges Arktiske Universitet (NO) 4. Universita Degli Studi Di Trento (IT) 5. Kungliga Tekniska Hoegskolan (SE) 6. ""National Center For Scientific Research """Demokritos""""" (GR) 7. Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (DE) 8. Polar View Earth Observation Limited (UK) 9. Meteorologisk Institutt (NO) 10. Logical Clocks AB (SE) 11. United Kingdom Research And Innovation (UK)"

1.1.6 Cost assessments of hazards

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	FP7 projects
Cost assessments of hazards	CONHAZ COACCH H2020_Insurance NAIAD

In this iteration of the CoU Mapping Document, no new projects related to cost assessments of hazards were identified.

1.2 Climate hazards

Preparedness and adaptation planning to threats related to climate change are defined in the EU Adaptation Strategy to Climate Change, which calls for bridging the knowledge gap, in particular on damage and adaptation costs and benefits, regional and local-level analyses and risk assessments, tools to support decision-making, monitoring and evaluating past adaptation efforts. Links with Horizon2020 DRS topics have been designed in this respect. This section highlights projects dealing with risk management-related tools and technologies that are applicable mainly to climate-related hazards – Forest fires are included in this category, keeping in mind that they also may be due to intentional man-made actions.

1.2.1 Multi-climate hazard risk prevention, awareness, preparedness, resilience

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multi-climate hazard risk prevention, awareness, preparedness, resilience	ANYWHERE beAWARE BRIGAID CaseXtreme CENTAUR CLARA Climate Europe Climateurope CLIMB CLISEL CLUVA DERMR DJ-VR: R.A.E.S ERA4CS EU-CIRCLE EUPORIAS EXTREMA FLOOD-serv HERACLES HydroSocialExtremes IMPREX INTACT KNOW4DRR KULTURISK PLACARD PROTECT RAIN RESCCUE RESIN SINCERE STORM WASSERMED

The projects were complemented by the following projects funded by DG ECHO.

CASCADE	
Title	Community Safety Action for Supporting Climate Adaptation and Development
Objective	Improve capacity to understand, assess, and treat current and future climate change related risks on the local level, focusing on BSR conditions.
Contract details	2018/PREV/826518; 1-1-2019 - 31-12-2020; EUR: 635.839,22
Abstract	The project will create improved capacity to understand, assess, and treat current and future climate change related risks on the local level, focusing on BSR conditions. It will increase practical risk management capabilities of local authorities, creating positive cascading effects through training trainers who will use the training materials to enhance the capacity of urban communities.
Consortium	Coordinator: 1. CITY OF TURKU (FI) Consortium: 2. The Council Of The Baltic Sea States Secretariat (SE) 3. Myndigheten For Samhallsskydd Och Beredskap (SE) 4. The Main School Of Fire Service (FI) 5. Hamburg Fire And Rescue Service (DE) 6. Liepajas Pilsetas Pasvaldibas Policija (LV) 7. Sihtasutus Stockholmi Keskkonnainstituudi Tallinna Keskus (EE) 8. Frederiksborg Brand Og Redning (DE) 9. Abo Akademi (FI)

SCORCH	
Title	Supportive Risk Awareness and Communication to Reduce impact of Cross-Border Heatwaves
Objective	Reduce the impact of heat waves on vulnerable, urban populations through improved risk communication strategies informed by existing EU plans and guidelines
Contract details	2018/PREV/826565; 1-2-2019 - 31-1-2021; EUR: 715.212,09
Abstract	The overall objective of this project is to reduce the impact of heat waves on vulnerable, urban populations through improved risk communication strategies informed by existing EU plans and guidelines. It will measure risk perception and behaviour in communities through surveys and foster a culture of prevention and cooperation across countries.
Consortium	Coordinator: 1. Evaplan Gmbh Am Universitatsklini Kum Heidelberg (DE) Consortium: 2. Universite Catholique De Louvain (BE) 3. Educational Research Center For Environment And Health (GE) 4. Stichting International Network Onchildren's Health Environment And Safety (NL) 5. Tel Aviv University (IL)

These projects were complemented by new projects funded in 2018:

ANDANTE	
Title	AttributioN of DynAmic and thermodyNamic components in exTreme weather and climate Events *This project is also relevant for 1.1.3 Multi-hazards situation awareness / early warning*
Objective	To developm the next-generation prediction and event attribution system, through separating human-induced dynamic (i.e. circulation/flow) and thermodynamic contributions to the risk of selected extreme events in Europe and Africa
Contract details	H2020/MSCA/IF/2018; 1/3/2020 - 28/2/2022; EUR 224 933,76
Abstract	The main goal of ANDANTE is to separate human-induced dynamic (i.e. circulation/flow) and thermodynamic contributions to the risk of selected extreme events in Europe and Africa. Since we are dealing with rare events we need large or even better very large ensembles of model simulations (~1,000 members) to do the flow-conditional probabilistic event attribution in statistically sound way (i.e. to get well-resolved probability distributions) with the methods of flow clusters (weather regimes/climate modes) and flow analogues. The project will make a key contribution to the development of the next-generation prediction and event attribution system. The produced new very large ensembles will be combined with the current-generation ensembles as well as multi-model climate simulations and multi-member reanalysis products to perform robust multi-method estimates of the univariate and multivariate (i.e. multi-variable) risk indicators. The risk assessment of selected extreme events manifested in surface temperature, precipitation, potential evapotranspiration and fire weather index can be useful to a wide spectrum of stakeholders interested in climate change impacts.
Consortium	Coordinator: The Chancellor, Masters And Scholars Of The University Of Oxford (UK)

CASCADES	
Title	CAScading Climate risks: towards ADaptive and resilient European Societies
Objective	Increase understanding of the conditions under which climate risks propagate beyond their geographical and temporal location in ways that may affect European stability and cohesion
Contract details	H2020-LC-CLA-2018-2; 1/9/2019 - 31/8/2023; EUR: 6.944.384,75
Abstract	Climate change amplifies existing risks and vulnerabilities in a globalised world. New risks are also emerging from complex cross-sectoral and multi-dimensional interactions that aggregate gradually, and sometimes emerge abruptly. Recent examples of links between crop damage in Russia, international food prices and political instability in North Africa, as well as impact chains from drought, migration, civil unrest and war in the Middle East, demonstrate how climate-induced risks outside Europe can cascade and threaten Europe. CASCADES strives to understand the conditions under which climate risks propagate beyond their geographical and temporal location in ways that may affect European stability and cohesion. It does so via a broad 360° risk assessment and deeper thematic analyses of trade, value chain, financial and political connections between Europe and the rest of the world. CASCADES' ambition is to identify the policy leverage points that can help the EU to adapt and respond to such cascading climate risks. CASCADES integrates a wide range of established and innovative methodologies – many of which have not been seriously applied to adaptation questions before – ranging from biophysical climate impact modelling, economic modelling of trade and financial networks, and data integration methods, to qualitative approaches including hotspot case study analysis original social science research and serious games. CASCADES combines leading expertise in climate change impacts, vulnerability and adaptation, international trade and commodity flows, foreign policy and security, and finance and business, with deep knowledge and proven experience of co-creating with – and influencing – stakeholders from private sectors, public policy and civil society. CASCADES will provide knowledge and tools to support policy and decision-making processes, thus helping Europe to strategically navigate a sustainable and resilient path through a rapidly changing, interconnected world.
Consortium	Coordinator: 1. Potsdam Institut Fuer Klimafolgenforschung (DE) Consortium: 2. "Stiftelsen The Stockholm Environment Institute (SE) 3. Adelphi Research Gemeinnutzige Gmbh (DE) 4. Fondazione Centro Euro-Mediterraneosui Cambiamenti Climatici (IT) 5. Eidgenoessische Technische Hochschule Zuerich (CH) 6. University Of York (UK) 7. Suomen Ymparistokeskus (FI) 8. Centre For International Information And Documentation In Barcelona (ES) 9. The Royal Institute Of International Affairs (UK) 10. European Centre For Development Policy Management (NL) 11. Stowarzyszenie Centrum Rozwiazan Systemowych (PL) 12. Wirtschaftsuniversitat Wien (AT)"

CAFE	
Title	Climate Advanced Forecasting of sub-seasonal Extremes
Objective	Train interdisciplinary researchers to advance sub-seasonal predictability of extreme events
Contract details	H2020-MSCA-ITN-2018; 1/3/2019 - 28/2/2023; EUR: 3.155.771,88
Abstract	Climate extremes such as heat waves or tropical storms have huge social and economic impact. The forecasting of such extreme events at the sub-seasonal time scale (from 10 days to 3 months) is challenging. Since the atmosphere and the ocean are coupled systems of enormous complexity, in order to advance sub-seasonal predictability of extreme events, it is crucial to train a new kind of interdisciplinary top-level researchers. CAFE research is structured in three WP: Atmospheric and oceanic processes, Extreme events and Tools for predictability, and brings together an interdisciplinary team of scientists. Objectives: Study of the relation between RWPs and the large scale environment, and the resulting limit of predictability; Statistical characterization of MJO events, dependence on climatic factors, and simple modelling to evaluate predictability; Development of diagnosis tools for identification and tracking of the MJO, blocking, waves and oceanic structures; Analysis of climatic changes in weather patterns and their relation with new climatic phenomena and extreme events in Europe; Estimation of probabilities for severe damages due to extreme events associated to ENSO; Validation of the hypothesis of cascades of extreme events and effects of a non-stationary climate; Estimation of exceedance probabilities for intensity of severe atmospheric events, including windstorms and hurricanes; Assessment of the response of extreme weather events for different levels of stabilized global warming and comparison with their response to internal modes of climate variability; Development of a procedure to improve the predictability of the onset of monsoon; Advanced statistical analysis of dynamic associations between SSS and extreme precipitation events; Study of predictability of large-scale atmospheric flow patterns over the Mediterranean connected to extreme weather; Systematic quantification of the predictability potential of a SWG of analogues of atmospheric circulation.
Consortium	Coordinator: 1. Consorci Centre de Recerca Matematica (ES) Consortium: 2. "Potsdam Institut Fuer Klimafolgenforschung (DE) 3. Max-Planck-Gesellschaft Zur Forderung Der Wissenschaften Ev (DE) 4. Technische Universitaet Bergakademie Freiberg (DE) 5. Agencia Estatal Consejo Superior Deinvestigaciones Cientificas (ES) 6. Universitat Politecnica De Catalunya (ES) 7. Universidad De La Republica (UY) 8. Meteo-France (FR) 9. Aria Technologies Sa (FR) 10. European Centre For Medium-Range Weather Forecasts (UK)"

Bufferblock	
Title	Water buffering and drainage in urban areas by using drainage blocks under the road
Objective	Assess the rules and regulations of a road/ground construction and the drainage into the soil in Germany, Belgium, England and Italy, in order to judge feasibility of Bufferblock implementation
Contract details	H2020-SMEInst-2018-2020-1; 1/6/2019 - 30/11/2019; EUR: 50.000
Abstract	Bufferblock is a concrete block with drainage and water buffering properties underneath roads, squares or parking areas. It forms a solution for stormwater drainage and buffering in the urban area. The function is similar to that of plastic infiltration crates, but because of the high strength of Bufferblock they can be placed almost directly underneath the road surface where crates need an extra top layer of 75cm. This results in a smaller installation depth, higher buffer capacities and a more cost-effective solution. The relative light construction of Bufferblocks has an average density of around 800 kg/m3. This density is comparable to pumice (lava stone), but has a much higher storage capacity with the same volume. Bufferblock therefore has a lot of potential to become the most important solution against road overflows. The Bufferblock is a patented invention (WO2018143808). With this SME application, Bufferblock wants to investigate the market opportunities in Europe, particularly Germany, Belgium, England and Italy. These countries have problems with stormwater and need a solid solution for flooding in the dense urban areas. They also have a good industry for local block production and they invest in a good civil infrastructure. The company thinks these countries are the best step to other countries in Europe. The most important research-question lies in an assessment of the rules and regulations of a road/ground construction and the drainage into the soil in these countries.
Consortium	Coordinator: Bufferblock B.V. (NL)

1.2.2 Flood risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Flood risks	ADAPT CORFU DAREnet DCGGEOPHYS FLADAR FLOODarc FLOODCHANGE FLOODIS FLOODPROBE FLOODRESC FLOODSAT FLOODSTAND FRISCO1 IMPRINTS INFLATER INFLATER-DEMO INUNDO k-NOW-casting LIFE AERFIT LIFE CERSUDS LIFE FRANCA LIVING Vecht-Dinkel MAN-U PLATFORM PROTERINA-3 Raab Flood 4cast RainBO Life RAINMAN Risk management and flood protection in cross-border regions Calarasi and Polski Trambesh SMARTEST STARFLOOD URBANFLOOD

The projects were complemented by the following projects funded by DG ECHO.

FLORIS	
Title	Innovative tools for improving Flood risk reduction strategies
Objective	Develop a supporting decision tool for the comparative analysis of disaster reduction strategies in flood risk management
Contract details	2018/PREV/82656; 1 1-1-2019 - 31-12-2020; EUR: 442.668,62
Abstract	FLORIS (Innovative tools for improving FLood risk reductiOn stRategleS) project aims at studying innovative approaches for the development of integrated flood risk scenarios considering the specific critical issues of areas at risk and the consequences of high frequency/low damage events that affect them. In particular, the main idea is to develop a supporting decision tool for the comparative analysis of disaster reduction strategies in flood risk management, able to support various actors (Civil Protection, municipalities, administrations, professionals, etc.) in planning and design measures to improve all aspects of risk management under different and variable risk scenarios including climate and global change
Consortium	Coordinator: 1. Universita Degli Studi Di Messina (IT) Consortium: 2. Middlesex University Higher Education Corporation (UK) 3. Univerzitet U Sarajevu (BA) 4. Centro Internazionale In Monitoraggio Ambientale - Fondazione Cima (IT) 5. Prefekt I Qarkut Berat (AL)

The projects were complemented by the following projects funded by the INTERREG programme.

C5A	
Title	Cluster for Cloud to Coast Climate Change Adaptation *This project is also relevant for 1.2.1 Multi-climate hazard risk prevention, awareness, preparedness, resilience*
Objective	Deliver a from 'Cloud-to-Coast' (C2C) approach to the management of flood risk in the North Sea Region (NSR)
Contract details	2014 - 2020 INTERREG VB North Sea; 2019/01/01 - 2021/12/31; EUR: 962.575
Abstract	The North Sea Region (NSR) is facing a significant increase in the frequency and severity of floods in response to climate change. Flood management approaches have to urgently adapt to this new reality to keep people safe, the environment healthy and our economies prosperous.To respond to this challenge the project Cluster for Cloud to Coast Climate Change Adaptation (C5A) will deliver a from 'Cloud-to-Coast' (C2C) approach to the management of flood risk . Our whole-of-system approach will integrate four constituent systems (catchment, coasts, cities, infrastructure networks) and enable the development of multifunctional and adaptable solutions that deliver more sustainable, integrated and multifunctional solutions across the NSR. To do so, we will build upon the outcomes of seven ongoing Interreg NSR projects to ensure our approach is both evidence-based and practical.Building on the seven ongoing Interreg NSR projects, C5A partners will co-create the C2C approach. We will develop a multi-beneficial, advantageous and resilient way of working on flood management from Cloud to Coast that can be applied in practice.We will organise 7 case studies, 2 sessions with EU DGs and a high level policy learning group. We will reach out to local, national, transnational and global networks to raise awareness and acceptance in- and outside the NSR. C5A builds capacity and support for the take-up of Cloud to Coast by relevant authorities and practitioners across the NSR, and beyond.
Website	https://northsearegion.eu/c5a/
Consortium	Coordinator: Ministry of Infrastructure and Watermanagement - The Netherlands, DG Rijkswaterstaat (NL)

The projects were complemented by the following projects funded by the ERASMUS+ programme.

Soil Erosion and Torrential Flood Prevention	
Title	Soil Erosion and Torrential Flood Prevention: Curriculum Development at the Universities of Western Balkan Countries *This project is also relevant for 1.1.2 Multi-hazard risk reduction, preparedness, resilience and 1.1.4 Multi-hazard emergency response and crisis management, including cascading effects.*
Objective	Develop a Master programme for land degradation, spread improved knowledge of practical solutions against torrential floods and the education of local governments to create prevention programs
Contract details	598403-EPP-1-2018-1-RS-EPPKA2-CBHE-JP; 15/11/2018 - 14/11/2021; EUR: 865.070,00
Abstract	Land degradation, especially physical degradation, with soil erosion as the most common degradation process, is a significant problem for the conservation of resources and has a large negative effect. One of the consequences of soil erosion is the occurrence of torrential floods. The floods that occurred in the last time, again point to the need to improve the education of professionals who will enable better prevention of torrential floods. The field of soil erosion control and protection against torrential floods are not included in the study process at all the faculties of forestry and other related faculties of the universities in Serbia and B&H. The Faculty of Forestry of the University of Belgrade has the academic studies devoted to these issues, while other universities have individual subjects whose syllabuses are partially related to this field. For these reasons, there is a need for the development of a new master and improvement of the existing bachelor curriculum by introducing new subjects or by changing the syllabuses of existing subjects. In addition to the development of new master and improvement of the bachelor curriculum, in compliance with the Bologna Process and the EU good practices, the specific objectives of the project are also the following: the implementation of improved knowledge of practical solutions against torrential floods and the education of local governments to create prevention programs. The project includes five universities of the partner countries (Serbia, Bosnia and Herzegovina), where the curricula will be developed, and universities from the four program countries. The project will be implemented through the 7 work packages with 34 activities. The Project implementation will contribute to the establishment of better cooperation between the participants, who, by improving the university curriculum with the support of the EU, will achieve harmonized approach to the methodology for flood prevention at the regional level.
Consortium	Coordinator: UNIVERZITET U BEOGRADU (RS)

The projects were complemented by the following projects funded by the LIFE+ CLIMA programme.

LIFE UrbanStorm	
Title	Development of sustainable and climate resilient urban storm water management systems for Nordic municipalities *This project is also relevant for 1.2.1 Multi-climate hazard risk prevention, awareness, preparedness, resilience*
Objective	Increase the climate resilience of Estonian municipalities, especially their ability to manage flush flooding caused by heavy rainfall
Contract details	LIFE17 CCA/EE/000122; 01/09/2018 - 28/02/23; Total budget: EUR 1,957,843.00; EU contribution: EUR1,011,654.00
Abstract	The main objective of the LIFE UrbanStorm project is to increase the climate resilience of Estonian municipalities, especially their ability to manage flush flooding caused by heavy rainfall. It will facilitate the development and implementation of integrated approaches for climate change adaptation strategies and action plans, at local, regional or national level, prioritising, where appropriate, ecosystem-based approaches. The project will also focus on setting up an innovative complex storm water management system, which entails storm water collection and re-use. The demonstration site will be the focal point for engaging local inhabitants to promote the sustainable use of storm water and a change in water habits.
Consortium	Coordinator: 1. Viimsi Vallavalitsus (EE) Consortium: 2. Eesti Maaülikool (EE) 3. Tallinna Kommunaalamet (EE) 4. MTÜ Balti Keskkonnafoorum (EE)

LIFE ASTI	
Title	Implementation of a forecAsting System for urban heaT Island effect for the development of urban adaptation strategies
Objective	Design, implement, pilot and validate a set of UHI forecasting systems in Thessaloniki and Rome based on state-of-the-art numerical models
Contract details	LIFE17 CCA/GR/000108; 01/09/2018 - 31/08/21; Total budget: EUR 1,265,395.00; EU budget: EUR 736,823.00
Abstract	The LIFE ASTI project aims to design, implement, pilot and validate a set of UHI forecasting systems in Thessaloniki and Rome based on state-of-the-art numerical models. It will also establish dissemination tools and allow end-users open access to UHI-related information using ICT applications. Furthermore, the project will assess the impact of future climate change scenarios on UHI for the two cities and evaluate the impact of promoting green activities (e.g. green roofs and ventilation areas) in urban areas on combating this effect. It will develop modelling systems for the two cities, along with good practice guides and efficient strategic plans for mitigating future urban heat island (UHI) effects. These can be adjusted for other EU urban areas that face the same adverse UHI effects. Finally, the project aims to raise awareness and encourage authorities to apply such urban adaptation strategies and mitigation initiatives. It will organise events to promote, replicate and transfer the designed modelling systems and the best urban adaptation strategies to other European cities that face the same climate issues arising from the UHI effect. p>The project will contribute towards the Greek Climate Change Adaptation Strategy of 2016 along with the ministerial decision of 2017 on the regional plans for climate change adaptation.
Consortium	Coordinator: 1. Aristotle University of Thessaloniki – Special Account for Research Funds (EL) Consortium: 2. Geospatial Enabling Technologies Ltd. (EL) 3. Institute of Atmospheric Sciences and Climate (EL) 4. National Research Council of Italy (IT) 5. Municipality of Thessaloniki (EL) 6. AZIENDA SANITARIA LOCALE ROMA 1 (It) 7. SYMPRAXIS TEAM P.C. (IT)

LIFE AGUA DE PRATA - AGUA DE PRATA	
Title	Adaptation and Watering in Green Urban Areas facing Climatic Heat Waves, Drought and Extreme Storms
Objective	Improve the resilience of the agricultural sector through changes in agricultural practices and policies
Contract details	LIFE17 CCA/PT/000076; 01/09/18 - 31/08/23; Total budget: EUR 2,439,287.00; EU budget: EUR 1,463,570.00
Abstract	Over the past few decades, the Netherlands have become warmer and wetter, with more extreme rainfall events. Climate scenarios indicate that these trends will continue, although the extent of such effects remains uncertain. In June 2016, large areas of agricultural land in the south of the Netherlands and in Flanders, Belgium, were flooded due to intense rainfall causing great damage to crops and resulting in failed harvests. Furthermore, the Netherlands, and the province of Noord-Brabant in particular, has also seen a gradual but steady impoverishment of the landscape and decreasing biodiversity that is expected to continue as a result of climate change. The need to improve the resilience of the agricultural sector is evident and crucial, and this requires drastic changes in agricultural practices and policies. Effective climate-adaptation policies should be based on creating synergies between agriculture, biodiversity and water management.
Consortium	Coordinator: 1. Stichting Van Hall Larenstein (NL) Consortium: 2. Flanders Research Institute for Agriculture, Fisheries and Food (ILVO) (BE) 3. Belgium Horst Beheer BV (BE) 4. The Netherlands Wendeland B.V. (NL) 5. The Netherlands Bosboom B.V (NL) 6. The Netherlands Boefkik BV (NL) 7. The Netherlands Stichting Landgoed De Koekoek (NL) 8. The Netherlands(NL)

LIFECOASTadapt	
Title	Coastal adaptation to climate change by multiple ecosystem-based measures
Objective	Demonstrate ecosystem-based measures against coastal erosion and floods that also strengthen coastal biodiversity and ecosystem services
Contract details	LIFE17 CCA/SE/000048; 15/06/18 - 31/12/22; Total budget: EUR 4,538,674.00; EU budget: EUR 2,232,578.00
Abstract	The objective of the LIFECOASTadapt project is to demonstrate ecosystem-based measures against coastal erosion and floods that also strengthen coastal biodiversity and ecosystem services. The project will also contribute to the 2002 EU Recommendation on Integrated Coastal Zone Management (ICZM) and the Commission's 2013 proposal for a new initiative on Maritime Spatial Planning and Integrated Coastal Management.
Consortium	Coordinator: 1. Region Skane (SE) Consortium: 2. Länstyrelsen Skåne (SE) 3. Sweden City of Helsingborg (SE) 4. Sweden Skåne Association of Local Authorities (SE) 5. Sweden Lund University(SE) 6. Sweden Lomma municipality (SE) 7. Sweden Ystad municipality (SE) 8. Sweden (SE)

LIFE SPARC	
Title	Space for Adaptating the River Scheldt to Climate Change
Objective	Propose measures to make the Scheldt estuary and its highly urbanised area resilient to climate change
Contract details	LIFE16 CCA/BE/000107; 01/09/17 - 31/08/22; Total budget: EUR 8,525,800.00; EU funding: EUR 2,351,175.00
Abstract	The LIFE SPARC project proposes measures to make the Scheldt estuary and its highly urbanised area resilient to climate change. In practice, this means providing much greater protection against floods by creating open space for water and developing a robust estuary ecosystem. More specifically, the project has the following goals: Reducing flood risk using nature-based solutions appropriate to tidal rivers, in line with the EU Floods Directive, such as the construction of flood areas that can safely fill with water during flood events, decreasing water levels on the river and reducing the risk of flooding in urban areas; Restoring habitats to make the ecosystem more resilient to the effects of climate change, and enabling tidal mud flats and freshwater tidal marshes to develop in line with the Habitats Directive. The aim is for the restored sites to form a network, to improve the implementation of the Habitats and Birds directives and to act as green infrastructure ('corridors') to give species greater opportunity for movement; Reinforcing public support, by actively engaging stakeholders and the general public, and sharing knowledge. Opportunities in the field of recreation and tourism will also be taken to boost the local economy; and Demonstrating the transferability and replicability of new techniques for nature-based solutions appropriate to tidal rivers.
Consortium	Coordinator: 1. Agentschap voor Natuur en Bos (NL) Consortium: 2. Waterwegen en Zeekanaal NV (NL) 3. Belgium Eigen Vermogen Flanders Hydraulics (BE) 4. Belgium Regionaal Landschap Schelde-Durme (BE) 5. Belgium (BE)

LIFE BEWARE	
Title	BEtter Water-management for Advancing Resilient-communities in Europe
Objective	Actively involve local communities in implementing Natural Water Retention Measures (NWRM) in Santorso and Marano Vicentino, as well as other EU municipalitie, based on the EU strategy on adaptation to climate change
Contract details	LIFE17 GIC/IT/000091; 03/09/18 - 30/06/20; Total budget: EUR 2,103,964.00; EU budget: EUR1,188,160.00
Abstract	The overall objective of the LIFE BEWARE project is to implement the EU strategy on adaptation to climate change in regards to flood risks by increasing water infiltration and storage in urban and rural areas. The project aims to actively involve local communities in implementing Natural Water Retention Measures (NWRM) in Santorso and Marano Vicentino, as well as other EU municipalities. The project will seek to create the favourable local administrative, financial and technical environment for NWRM. Best practices will demonstrate how to ensure that communities are safe from flood risks and the role that they can play in achieving EU climate change goals. These actions will be then supported in other areas of Italy and elsewhere in Europe.
Consortium	Coordinator: 1. Santorso Municipality (IT) Consortium: 2. Association des Agences de la Démocratie Locale / Association of Local Democracy Agencies (FR) 3. Consorzio di bonifica Alta Pianura Veneta (IT) 4. Comune di Marano Vicentino (IT) 5. Dipartimento Territorio e Sistemi Agro-forestali - Università degli Studi di Padova (IT) 6. Agenzia veneta per l'Innovazione nel Settore primario – Veneto Agricoltura (IT)

HEGS	
Title	Hydrologic Extremes at the Global Scale: teleconnections, extreme-rich/poor periods, climate drivers and predictability *This project is also relevant for 1.1.3 Multi-hazards situation awareness / early warning*
Objective	Enhance understanding of the global space-time variability of hydrologic extremes, using a three-pillar research strategy based on methodological innovation, extensive data analysis and proof-of-concept case studies
Contract details	H2020-MSCA-IF-2018;17/5/2019 - 16/5/2022; EUR 281 827,20
Abstract	The project's ambition is to better understand the global space-time variability of hydrologic extremes, using a three-pillar research strategy based on methodological innovation, extensive data analysis and proof-of-concept case studies. The specific objectives are to: Develop a statistical framework to describe the global-scale variability of extremes in relation to climate; Analyse global precipitation/streamflow datasets with the aim of quantifying teleconnections, spatial clustering, trends and extreme-rich/poor periods, along with their climate drivers; Explore practical applications such as global early warning systems allowing international disaster response organisations to trigger early actions. Successful completion of the project will deliver new tools to analyse extremes at the global scale and will hence contribute to more efficient risk management.
Consortium	Coordinator: Institut National De Recherche En Sciences Et Technologies Pour L'environnement Et L'agriculture (FR)

FLARE	
Title	Flooding Accident REsponse
Objective	Develop a Risk-Based methodology for 'live' flooding risk assessment and control on passenger ships
Contract details	H2020-MG-2018-TwoStages 1/6/2019 – 31/5/2022; EUR: 9.375.730
Abstract	The FLARE consortium comprises key stakeholders from industry, academia and policy makers, involved in ship flooding risk research as a Group for over twenty years (HARDER, SAFEDOR, GOALDS, EMSA III, eSafe), the latter three focussing on passenger ships. This offers a unique knowledge base and capability to support targeted new developments and expedite implementation. The overriding objective is to develop a Risk-Based methodology for 'live' flooding risk assessment and control, to be achieved by: - Creating an updated accident database for passenger ships and damages. Using this with support from suitably verified flooding simulation tools to develop a generic risk model for flooding incidents, accounting for collision and grounding with focus on cost-effective risk containment in emergencies. - Ensuring the risk model is generic (all incidents in one model), holistic (active and passive measures) with potential application to new buildings and existing ships. - A risk-aware approach post-flooding incidents from susceptibility to flooding to emergency response, including mustering and abandonment in extreme flooding scenarios. - Innovative technical solutions at TRL5 in ship concepts and equipment targeting risk containment, including: crashworthiness; minimising the risk from WT doors; use of highly expandable foam post-incident; decision support for crisis management. - Developing a proposal for the revision of relevant IMO regulations towards a risk-based approach to contain and control risk in passenger ships from flooding incidents.
Consortium	Coordinator: 1. Balance Technology Consulting Gmbh (DE) Consortium: 2. "University Of Strathclyde (UK) 3. Aalto Korkeakoulusaatio Sr (FI) 4. Brookes Bell Llp (UK) 5. Bureau Veritas Marine & Offshore Registre International De Classification De Navires Et De Plateformes Offshore (FR) 6. Carnival Plc (UK) 7. Color Line Marine As (NO) 8. Dnv Gl As (NO) 9. Fincantieri Spa (IT) 10. Hamburgische Schiffbau-Versuchsanstalt Gmbh (DE) 11. Association De Gestion De L Institut Catholique D Arts Et Metiers De Nantes (FR) 12. Lloyd's Register Emea Ips (UK) 13. Stichting Maritiem Research Instituut Nederland (NL) 14. Meyer Werft Papenburg Gmbh & Co Kg (DE) 15. Meyer Turku Oy (FI) 16. Napa Oy (FI) 17. Shipyards And Maritime Equipment Association Of Europe (BE) 18. Chantiers De L'atlantique (FR) 19. Rina Services Spa (IT) 20. RStena Rederi Ab (SE)

FOReSEE	
Title	Market replication of a cutting-edge FlOod Risk ScrEEning Tool *This project is also relevant for 1.1.2 Multi-hazard risk reduction, preparedness, resilience and 1.1.4 Multi-hazard emergency response and crisis management, including cascading effects.*
Objective	Enable a more systemic approach to flood risk management, leading to strategic decisions at various levels for a range of end-users, through spreading use of an online platform harnessing big geometric data sets
Contract details	H2020-SMEInst-2018-2020-1; 1/1/2019 - 31/5/2019; EUR: 50.000
Abstract	Based on cutting-edge algorithm technology, we have developed a disruptive online platform that harnesses the descriptive power of big geometric data sets to provide cost-effective and updated decision support for end-users working with flood risk and climate change adaptation. We aim to pursue a major market opportunity by expanding our business into new geographical markets, addressing standing technical and market-related challenges by adapting and demonstrating the capabilities of our platform with reference end-users. Overall, leveraging on the opportunity provided by the SME instrument, this project opens not only an important economic opportunity for SCALGO ApS, but will importantly enable a more systemic approach to flood risk management, leading to strategic decisions at various levels for a range of end-users (the public sector, businesses, and individuals), and supporting EU mitigation and adaptation policies.
Consortium	Coordinator: Scalgo Development Aps (DK)

FloodFrame	
Title	A Life Jacket For Your House In Flood Times *This project is also relevant for 4.4.1 Resilience of urban built environments, including cultural heritage.*
Objective	Enhance TRL of FloodFrame (patent pending): an automatic and pre-installed Flood Protection Technology for houses and buildings based on a waterproof membrane, which wraps the building during flood events protecting also its foundation.
Contract details	H2020-SMEInst-2018-2020-1; 1/5/2019 - 31/8/2019; EUR: 50.000
Abstract	Climate change has increased the occurrence and frequency of flood events worldwide, and 215 million people are currently under flood risk. Flooding can be devastating for both homes and businesses, causing economic loss. An estimated cost of a flood is €98,000 per household, and, to date, there is a lack of effective individual solutions for houses and buildings in the flood protection market. At FloodFrame A/S (DK, 2017), we have developed FloodFrame (patent pending): an automatic and pre-installed Flood Protection Technology for houses and buildings based on a waterproof membrane, which wraps the building during flood events protecting also its foundation. It does not require a flat surface to be effective and is activated by the rising water functioning without any electricity or human interaction while giving the possibility to increase the protection height during the flood automatically as high the water rises. FloodFrame is currently offered at a competitive price of €300/m. Today there is no solution in the flood protection market that could fulfill the specific needs of home owners and at an affordable price. Our primary target customers are homeowners who have already experienced a flood, like our 12 Early Adopters in Roskilde Fjord and Houston (US). Today, our prototype is at TRL7, and this project will help us to reach the TRL9 by optimizing and testing the final design and the installation process as well as to complete the commercial activities still needed to reach the market (e.g. supply chain consolidation and fulfilment of legal and quality requirements). By 2024 and based on a two-fold business model – direct sales and license holders – we expect to reach at least 0.7% of the market across Europe and US (least 7,387 properties protected by FloodFrame).Thus, we have forecasted €29.72 million of cumulated revenues (€18.63 cumulative profit - ROI 4.45) and at least 40 new employees (20 technical support, 10 trainers, 4 engineers and 6 sales experts)
Consortium	Coordinator: Floodframe AS (DK)

1.2.3 Drought risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Drought risks	DEWFORA DROUGHT-R&SPI DRY-2-DRY WATER DROP

In this iteration of the CoU Mapping Document, no new projects related to drought risks were identified.

1.2.4 Coastal risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Coastal risks	MAREGOT MICORE PEARL RISC-KIT SIM.COAST THESEUS

This overview is complemented by the following projects funded in 2018.

CHES	
Title	Resilience of Coastal Human-Environment Systems *This project is also relevant for 1.1.2 Multi-hazard risk reduction, preparedness, resilience enhancement*
Objective	Provide a holistic view of coastal environment resilience against storms under climate change by accounting for both the human and ecosystem elements
Contract details	H2020-MSCA-IF-2018; 3/2/2020 - 2/2/2022; EUR 171 473,28
Abstract	Coastal cities face an increasing threat from storms due to the growing coastal populations and the intensifying storms under global warming. Coastal ecosystems can significantly reduce catastrophic damage from storms; however, existing risk assessments for coastal cities either do not include this crucial factor or do not consider future ecosystem changes. The proposed project, Resilience of Coastal Human-Environment Systems, CHES, will provide a holistic view of coastal environment resilience against storms under climate change by accounting for both the human and ecosystem elements. This work will quantify the protective effect of coastal ecosystems, forecast the future ecosystem conditions, and estimate the resilience of the coupled human-environment systems under different coastal urban development and climate scenarios. This project will greatly advance our understanding of the vulnerability of coastal human-environment systems to storms and the value of coastal ecosystems in storm protection, contributing to the development of sustainable coastal management plans coping with climate change.
Consortium	Coordinator: The Chancellor, Masters And Scholars Of The University Of Oxford (UK)

DURCWAVE	
Title	Amending the Design criteria of URban defences in LECZs through Composite-modelling of WAVE overtopping under climate change scenarios
Objective	Identify new design criteria for wave action by modelling wave overtopping and post-overtopping processes of urban defences
Contract details	H2020-MSCA-IF-2017 1/3/2019 - 4/4/2021; EUR: 170.121,60
Abstract	The present project, named "DURCWAVE" (amending the Design criteria of URban defences in LECZs through Composite-modelling of WAVE overtopping under climate change scenarios), aims to identify new design criteria for wave action by modelling wave overtopping and post-overtopping processes of urban defences (storm walls, stilling wave basins, buildings along coastal boulevards). To reach these objectives the project will implement a composite-modelling approach, consisting of both physical and numerical modelling. Physical model tests will be carried out in two different wave flume facilities at the host organization (UPC), meanwhile the numerical modelling will be performed through the secondment at the partner organization (UVigo). The mesh-free DualSPHysics model will be used for the scope. The EPR data-driven technique will be used to find new correlations between wave impacts and overtopping flows. The Action will provide a methodology to help decision-makers to estimate the vulnerability of coastal zones to climate change, by assess the threats for sea frontages and buildings on the coastline. The project outcomes will trace the path at National and European levels for further extensions from urban defences in LECZs to all kind of coastal defences. Furthermore, a unique numerical model technique to simulate post-overtopping processes and estimate wave loadings on coastal defences will be release open-source for public use.
Consortium	Coordinator:Universitat Politecnica De Catalunya (ES)

1.2.5 Forest fire risk prevention

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Forest fire risk prevention	AF3 ASPIRES DANTE DroneHopper DUF FIRE FireAndRiskPrevention FIRE-IN FIRESENSE FIRESMART FireSpec FUME GEO-SAFE LIFETEC NET RISK WORK PREFER

The projects were complemented by the following projects funded by DG ECHO.

PREVAIL	
Title	Prevention Action Increases Large fire response preparedness
Objective	Demonstrate how wildfire prevention can make large fire suppression more effective and less costly
Contract details	2018/PREV/826400; 1-2-2019 - 31-1-2021; EUR: 496.891,58
Abstract	This is a cooperative project among 5 research organisations of fire prone European countries (Italy, Spain, Portugal, Greece), that aims at demonstrating how wildfire prevention can make large fire suppression more effective and less costly. PREVAIL will provide empirical knowledge, practical tools and analytical techniques to improve UCPM effectiveness in the fire disaster management cycle (prevention-preparedness response) in terms of cost optimisation and large fire risk reduction.
Consortium	Coordinator: 1. Universita Degli Studi Della Tuscia (IT) Consortium: 2. Universita Degli Studi Di Napoli Federico Ii (IT) 3. Consorci Centre De Ciencia I Tecnologia Forestal De Catalunya (ES) 4. Ellinikos Georgikos Organismos – Dimitra (EL) 5. Instituto Superior De Agronomia (PT)

WUIVIEW	
Title	Wildland-Urban Interface VIrtual Essays Workbench
Objective	Design, test and operate a virtual workbench service for the analysis of fire hazards and buildings vulnerabilities at different European WUI realities
Contract details	2018/PREV/826522; 1-2-2019 - 31-1-2021; EUR: 572.015,58
Abstract	This project aims at reinforcing WUI (Wildland-Urban Interface) fires risk reduction strategies by designing, testing and operating a virtual workbench service for the analysis of fire hazards and buildings vulnerabilities at different European WUI realities. WUIVIEW will become a powerful and innovative platform to perform essays and simulation studies dealing with structures survivability and sheltering capability.
Consortium	Coordinator: 1. Universitat Politecnica De Catalunya (ES) Consortium: 2. Associacao Para O Desenvolvimento Da Aerodinamica Industrial (PT) 3. Fundacio D'ecologia Del Foc I Gestio D'incendis Pau Costa Alcubierre (ES) 4. Association Pour La Recherche Et Le Developpement Des Methodes Et Processus (FR) 5. Alma Mater Studiorum - Universita Di Bologna (IT) 6. Rise Research Institutes Of Sweden Ab (SE)

The projects were complemented by the following projects funded by the LIFE+ CLIMA programme.

LIFE RESILIENT FORESTS	
Title	Coupling water, fire and climate resilience with biomass production in Forestry to adapt watersheds to climate change *This project is also relevant for 1.2.1 Multi-climate hazard risk prevention, awareness, preparedness, resilience*
Objective	Develop a Decision Support System (DSS) for forest managers, which introduces them to the climate change adaptation processes
Contract details	LIFE17 CCA/ES/000063; 01/10/2018 - 30/09/22; Total budget: EUR 2,013,973.00; EU funding: EUR 1,192,420.00
Abstract	The first objective of the LIFE RESILIENT FORESTS is to develop a Decision Support System (DSS) for forest managers, which introduces them to the climate change adaptation processes. This system will comprise updated management practices on the watershed scale and climate change-related issues. The support system will be then demonstrated on two levels, sub-catchment and catchment, in Germany, Portugal and Spain. At each location the DSS will be modified by involving the relevant stakeholders.The project also plans to develop a complete monitoring system, including a Life Cycle Assessment of the forest management approach (following ISO 14040/44), that will demonstrate the positive environmental impact of the project, as well as its socioeconomic impact. A further objective is to develop a strategy for transferring management approaches around Europe and to organise networking activities to facilitate the transfer of information on forest management and climate change initiatives. The project will contribute to the Roadmap for moving to a competitive low carbon economy by 2050, as well as 2020 Energy Strategy targets and the EU's strategy on adaption to climate change, among other EU policy areas.
Consortium	Coordinator: 1. Universitat Politcnica de Valncia (ES) Consortium: 2. Ayuntamiento de Serra (ES) 3. Forschungszentrum Jülich GmbH (DE) 4. European Biomass Industry Association (BE) 5. Associação para o Desenvolvimento da Aerodinâmica Industrial (PT)

1.3 Geological hazards

Research and studies about geological hazards have been mainly undertaken by the Space and Environment programmes, covering tools and technological developments supporting various steps of crisis and disaster risk management.

1.3.1 Multi-geo hazard risk prevention, awareness, preparedness, resilience

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multi-geo hazard risk prevention, awareness, preparedness, resilience	GEO-RAMP SLATE SUBITOP PanGEO QSave

The projects were complemented by the following projects funded by the LIFE+ CLIMA programme.

LIFE Veneto ADAPT	
Title	Central VENETO Cities netWorking for ADAPTation to Climate Change in a multi-level regional perspective
Objective	Enhance capacity of Central VENETO cities to respond to the impacts of climate change, with a focus on hydro-geological risk and by means of a multi-level governance approach
Contract details	LIFE16 CCA/IT/000090; 01/09/17 - 01/03/21; Total budget: EUR 2,933,134.00; EU budget: EUR 1,478,586.00
Abstract	LIFE Veneto ADAPT aims to enhance regional capacity to respond to the impacts of climate change, with a focus on hydro-geological risk and by means of a multi-level governance approach. The project will develop a methodology for an effective integration of climate change-related adaptation policies at regional and local levels.
Consortium	Coordinator: 1. Comune di Padova (IT) Consortium: 2. Città Metropolitana di Venezia (IT) 3. Municipality of Vicenza (IT) 4. Comune di Treviso (IT) 5. Università Iuav di Venezia (IT) 6. SOGESCA srl (IT) 7. Unione dei Comuni del Medio Brenta (IT) 8. Associazione Coordinamento Agende 21 Locali Italiane (IT)

This overview is complemented by the following H2020 project.

SEISMAZE	
Title	Data-intensive analysis of seismic tremors and long period events: a new paradigm for understanding transient deformation processes in active geological systems
Objective	Develop a new paradigm for understanding transient deformation processes in active geological systems
Contract details	ERC-2017-ADG; 1/1/2019 - 31/12/2023; EUR: 2.490.000
Abstract	I will develop an innovative and holistic approach based on massive analysis of observations that requires high performance computing and will be combined with advanced physical modeling of the generating dynamical processes. This will produce the new framework that can be used on the one hand for an understanding of the physical tremor-generating mechanisms, and on other hand for the development of new adaptive methods for monitoring volcanoes and seismic faults. The implementation of these will involve machine learning approaches to gain information from continuous fluxes of data from dense seismological networks. This project is also relevant for 1.3.3 Seismic and earthquake risks and 1.3.2 Volcanic risks
Consortium	Coordinator: Centre National De La Recherche Scientifique CNRS (FR)

1.3.2 Volcanic risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Volcanic risks	APhoRISM CHRONOS ESPSI EUROVOLC EVOSS FEVER FUTUREVOLC MED-SUV MIAVITA PERIL TREMOR VOLCANOWAVES VOLCAPSE VUELCO

The projects were complemented by the following projects funded by DG ECHO.

EVE	
Title	EUROPEAN VOLCANO EARLY WARNING SYSTEM
Objective	Facilitate prevention and preparedness of European Civil Protections in front of volcanic destructive phenomena by anticipating to new volcanic eruptions
Contract details	2018/PREP/826292; 1-1-2019 - 31-12-2020; EUR: 718.300,06
Abstract	The EVE project will promote actions focusing on supranational and cross border risk awareness and risk communication by facilitating the interaction and cooperation between scientists and Civil Protection Agencies (CPs) to timely anticipate to volcanic disasters. The main objective of EVE is to facilitate prevention and preparedness of European Civil Protections in front of volcanic destructive phenomena by anticipating to new volcanic eruptions.
Consortium	Coordinator: 1. Agencia Estatal Consejo Superior De Investigaciones Cientificas (ES) Consortium: 2. Haskoli Islands (IS) 3. Universite Clermont Auvergne (FR) 4. Centre National De La Recherche Scientifique Cnrs (FR) 5. Istituto Nazionale Di Geofisica E Vulcanologia (IT) 6. Faculdade De Ciencias Da Universidade De Lisboa (PT)

This overview is complemented by the following projects, funded in 2018.

IMAGINE	
Title	Geographical imaginations and the (geo)politics of volcanic risk: cultures, knowledges, actions
Objective	Provide a holistic approach to volcanic risk through a consideration of the geographical imaginations of scientists and populations, combining social and physical scienses methods in Latin America and East Africa
Contract details	ERC-2018-STG 1/7/2019 - 30/6/2024; EUR 1.437.933
Abstract	Volcanoes can be cultural symbols, a source of fear, of fascination and of scientific study and a practical problem for civil protection: they involve complex social, cultural and political dynamics, and often have multi-scalar, trans-border impacts. Yet the management of volcanic risk tends to be strongly dependent on uncertain information from physical scientists about volcanic activity, with social scientific studies concentrating on social vulnerability and communication, and there is a relative dearth of studies that address the cultural and (geo)political contexts of scientific knowledge production in particular places. Geographers have explored the role of "geographical imaginations" in scientific discourses in other fields such as climate change: people, including scientists, imagine the social and physical landscapes around them. This project seeks to combine science studies, human geography and disaster risk reduction to provide a holistic approach to volcanic risk, and inform ongoing discussions about scientific advice in disasters more broadly, through a consideration of the geographical imaginations of scientists and populations. It focuses on understanding volcanic and disaster risk as a consequence of complex interactions and relationships between landscape, community, science and politics that blur the boundaries between society and nature. It combines methods from the social and physical sciences in Latin America and East Africa to investigate: (i) the ways in which scientists and people who live on volcanoes interpret and live with their environment; (ii) the interaction of national authorities with these modes of living, and how national borders affect them; (iii) the power dynamics of warnings within these contexts and across them; (iv) the implications of this approach for disaster risk reduction more broadly. Outcomes will include two books, several sets of scientific papers and three international meetings.
Consortium	Coordinator: The Chancellor Masters And Scholars Of The University Of Cambridge (UK)

PICVOLC	
Title	DePICting the interior of active VOLCanoes to reduce volcanic hazards: application to the present unrest at Nevado del Ruiz (Colombia) – PICVOLC *This project is also relevant for 1.3.1 Multi-geo hazard risk prevention, awareness, preparedness and resilience.*
Objective	Develop a new methodology that integrates seismic, gravity, and deformation data with 3D numerical inversion to create a detailed representation of the source of volcanic unrest
Contract details	H2020-MSCA-IF-2017; 1/2/2019 - 31/1/2021; EUR: 168.277,20
Abstract	PICVOLC aims to overcome the limitations in the current approach in the modeling of volcanic unrest by developing a new, original methodology that integrates seismic, gravity, and deformation data with 3D numerical inversion to create a detailed representation of the source of volcanic unrest. The current volcanic unrest at Nevado del Ruiz volcano will be the case study used to implement, calibrate, and verify this original approach. In 1985, a lahar generated by a modest eruption of Ruiz completely destroyed the town of Armero, killing 25,000 people. PICVOLC involves the integration of fieldwork with Finite Element Methods modeling and joint numerical inversions of geodetic and geophysical data. PICVOLC´s multi-/ interdisciplinary nature aims to better constrain the conceptual and numerical models of volcanic unrest and reduce the ambiguity in the identification of the location, depth, volume change, and nature of the source of unrest. The project involves national and international collaboration; it is academic but has also important implications for the monitoring and reduction of volcanic hazards at Ruiz. In particular, it will provide the following innovative products: (a) definition of the subsurface structures with a new map of Bouguer anomalies; (b) 3D FEM model of the volcano; (c) 3D Image of the source(s) of volcanic unrest from inversion of geodetic data; (d) training of graduate students and the staff of the local volcano observatory in numerical modeling. Finally, PICVOLC will be a key step in achieving my professional maturity by extending and reinforcing my knowledge and skills in the design of, involvement in, and management of an international research project.
Consortium	Coordinator: Universita Degli Studi Di Roma La Sapienza (IT)

1.3.3 Seismic and earthquake risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described. As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Seismic and earthquake risks	BLACKSEAHAZNET CoQuake CSEM DatA ESPerT EASER EQRESFRAME ICARUS ITERARE KaIROS MARSITE NERA NIKER PARTNER PERPETUATE PRE-EARTHQUAKES REAKT SEISMIC SERA SGL FOR USAR SHARE SYNER-G TCAINMAND

This overview is complemented by projects funded via H2020 in 2018.

MULTIRES	
Title	MULTI-level framework to enhance seismic RESilience of RC buildings *This project is also relevant for 1.1.2 Multi-hazard risk reduction, preparedness, resilience.*
Objective	MULTIRES aims to develop an advanced, harmonised, multi-level framework to assess earthquake risk of existing Reinforced Concrete (RC) buildings in earthquake-prone regions and to design/select practice-oriented, cost-effective, seismic resilience-enhancing solutions (e.g. structural retrofit, risk-transfer products).
Contract details	H2020-MSCA-IF-2018; 1/11/2019 - 31/10/2021; EUR: 212.933,76
Abstract	MULTIRES aims to develop an advanced, harmonised, multi-level framework to assess earthquake risk of existing Reinforced Concrete (RC) buildings in earthquake-prone regions and to design/select practice-oriented, cost-effective, seismic resilience-enhancing solutions (e.g. structural retrofit, risk-transfer products). The framework will benefit several seismic-prone countries (e.g. Greece, Italy, Romania), for which most of the existing buildings are designed according to pre-seismic codes and where RC buildings represent the highest share from 1960s onwards (e.g. 48% in Italy). Two levels of analysis refinement will be considered, single buildings vs. building portfolios, specifically tailored to the expected needs/goals of different stakeholders: building owners and government agencies/(re)insurance companies. A coherent treatment of risk and uncertainty in each project's task will promote dynamic and informed decision-making aiming at seismic resilience. MULTIRES builds on the probabilistic catastrophe risk modelling expertise of the Earthquake and People Interaction Centre (EPICentre) at the University College London (UCL), UK – the Host Institution - and seismic performance assessment of existing RC building expertise of the Fellow. State of the art/practice will be advanced providing flexible analysis methods for fragility and vulnerability assessment and their implementation tools (e.g. guidelines, computer codes). The framework will be applied to a large-scale building portfolio in Italy, where the Fellow and the Supervisor have strong links with local stakeholders, thus ensuring availability of data, knowledge transfer and true impact of the research on local communities. Through world-leading research training and co-development, the project will contribute to create a holistic culture of risk awareness and resilience in Europe, reflecting a strong commitment to the Sendai Framework for Disaster Risk Reduction.
Consortium	Coordinator: University College London (UK)

TURNkey	
Title	Towards more Earthquake-resilient Urban Societies through a Multi-sensor-based Information System enabling Earthquake Forecasting, Early Warning and Rapid Response actions *This project is also relevant for 1.1.3 Multi-hazards situation awareness / early warning*
Objective	Develop a flexible, extendable, robust and easy-to-use OEF/EEW/RRE system based on low-cost multi-sensor units and a cloud-based computer platform
Contract details	H2020-SC5-2018-2; 1/6/2019 - 31/5/2022; EUR: 7.999.948,75
Abstract	TURNkey aims to make significant advances in the fields of Operational Earthquake Forecasting (OEF), Earthquake Early Warning (EEW) and the Rapid Response to Earthquakes (RRE), particularly when applying these systems in practice in Europe. The project will develop a flexible, extendable, robust and easy-to-use OEF/EEW/RRE system based on low-cost multi-sensor units and a cloud-based computer platform, which can be distributed as a fully-operational TURNkey product to public authorities (including search-and-rescue teams) and private companies (including operators of critical infrastructure). These developments will contribute to improved seismic resilience before, during and after a damaging earthquake and hence a reduction in losses. The project's outcomes will be demonstrated in six European Testbeds (TBs) with different hazard, vulnerability and exposure characteristics, spatial extents and monitoring networks as well as in two roaming TBs, one based on crowdsourcing and one for temporary installations. The six geographically-focused TBs are: the city of Bucharest(Romania), the Pyrenees mountain range (France), the towns of Hveragerdi and Husavik (Iceland), the cities of Patras and Aigio (Greece), the maritime port of Gioia Tauro (Southern Italy), and the Groningen province (Netherlands), which is affected by induced seismicity.
Consortium	Coordinator: 1. Stiftelsen Norsar (NOR) Consortium: 2. "Stichting Deltares (NL) 3. Koninklijk Nederlands Meteorologisch Instituut-Knmi (NL) 4. Bureau De Recherches Geologiques Et Minieres (FR) 5. Euro-Mediterranean Seismological Centre (FR) 6. Haskoli Islands (IS) 7. Centro Europeo Di Formazione E Ricerca In Ingegneria Sismica (IT) 8. University Of Strathclyde (UK) 9. Bauhaus-Universitaet Weimar (DE) 10. Universidad De Alicante (ES) 11. Anglia Ruskin University Higher Education Corporation (UK) 12. Universita' Degli Studi Di Bergamo (IT) 13. University College London (UK) 14. Institutul National De Cercetare-Dezvoltare Pentru Fizica Pamantului (RO) 15. Yetitmoves Srl (IT) 16. Gempa Gmbh (DE) 17. National Observatory Of Athens (EL) 18. Nutcracker Research Limited (UK) 19. Beta 80 Spa Software E Sistemi (IT) 20. Siminn Hf (IS) 21. Panepistimio Patron (EL)"

FaultScan	
Title	Passive seismic scanning of the preparation phase of damaging earthquakes *This project is also relevant for 1.1.5 Earth observations support and 1.3.1 Multi-geo hazard risk prevention, awareness, preparedness, resilience.*
Objective	Develop a new, noise-based, high resolution, seismic monitoring approach
Contract details	ERC-2018-COG; 1/6/2019 - 31/5/2024; EUR: 2.524.630
Abstract	My FaultScan project will revolutionize our ability to directly observe transient deformation within the core of active faults and provide unprecedented accuracy in the detection of earthquake precursors. My ambition is to develop a new, noise-based, high resolution, seismic monitoring approach. I intend to grasp the opportunity of a recent step change in seismic instrumentation and data processing capabilities to achieve a dream for seismologists: reproduce repeatable, daily, virtual seismic sources that can probe the core of active faults at seismogenic depths using only passive seismic records. I plan to target the San Jacinto Fault (a branch of the San Andreas Fault system) that is currently believed to pose one of the largest seismic risks in California. It is an ideal fault for this project because it is very active, already extensively studied and easily accessible for the pilot field data acquisition work.
Consortium	Coordinator: 1. Universite Grenoble Alpes (FR) Consortium: 2. The Regents Of The University Of California (US)"

DAMAGE	
Title	Seismic off-fault Deformation: A multi-scale iMAGing to constrain Earthquake energy budget
Objective	Systematically study off-fault coseismic damage in carbonates, which are the rocks where most of the destructive seismicity striking Europe is hosted
Contract details	H2020-MSCA-IF-2018; 1/12/2019 - 30/11/2021; EUR: 184.707,84
Abstract	Earthquakes are one of the deadliest geo-hazards in the world causing huge societal and economic impact. Destructive earthquakes are generally represented by ruptures which nucleate, grow and terminate along pre-existing faults with catastrophic strain energy release. Seismological observations and theoretical arguments demonstrated that most of earthquake energy is dissipated into heat by friction within the core of faults at depth. The remaining energy amount is the one driven to the Earth surface by seismic waves and associated to the generation of extensive DAMAGE in the vicinity of seismic faults. Vast research was recently performed to investigate on-fault mechanisms during earthquakes whereas much less has been done to constrain the physical processes and energy sinks associated to coseismic off-fault deformation. I propose here to systematically study off-fault coseismic damage in carbonates, which are the rocks where most of the destructive seismicity striking Europe is hosted. The proposed research is innovative since it tackles a scientific topic which was so far overlooked with a multiscale interdisciplinary approach combining: detailed field structural and geophysical characterization of exhumed active fault zones, compressive and tensile dynamic loading tests on carbonate rocks, and microstructural-petrophysical characterization of natural and experimental fault rocks. This integrated strategy will lead to build a wealth of novel datasets to quantify the damage structure and scaling relations of seismogenic fault zones in carbonates. Newly conceived rock deformation experiments will then help to determine the mechanical origin of coseismic damage in carbonates. The research will be conducted at Université Grenoble-Alpes with a secondment at University of Manchester. The experience of the supervisors and the equipment at both organizations will guarantee the successful progress of the research and my professional growth as independent researcher..
Consortium	Coordinator: Universite Grenoble Alpes (FR

RISE	
Title	Real-time Earthquake Risk Reduction for a Resilient Europe *This project is also relevant for 1.3.1 Multi-geo hazard risk prevention, awareness, preparedness, resilience.*
Objective	Promote a paradigm shift in how earthquake risk is perceived and managed
Contract details	H2020-SC5-2018-2; 1/9/2019 - 31/8/2022; EUR: 8.000.000
Abstract	The key concept and vision of RISE is to promote a paradigm shift in how earthquake risk is perceived and managed. We believe that by taking advantage of advances in scientific understanding, and dramatically changing technological capabilities, earthquake hazard and risk will soon be appreciated not as a constant in time, but as an evolving, integrated and dynamic risk. In our concept, dynamic risk depends on location, changing with soil conditions, topography, structural type, occupancy and use and even location within a structure. However, dynamic risk also includes changes with time, for example increasing when a seismic sequence is active nearby and due to an improved dynamic geophysical understanding of faulting and earthquake processes. RISE proposes a series of coordinated activities in the domains of Operational Earthquake Forecasting, Earthquake Early Warning, Rapid Loss Assessment and Recovery and Rebuilding Efforts. Our approach is multi-disciplinary, involving earth-scientists, engineering-scientists, computer scientists, and social scientists. It is multi-scale in space and time, and addresses these scales in a highly systemic and consistent way. RISE joins with EPOS Integrated Core Service and several of the Thematic Core Services (TCS), with ARISTOTLE and the Copernicus Emergency Management Service. Integration will also include responsible national agencies in Italy, Turkey, Iceland, Israel and Switzerland and with selected industry partners. To maximise the impact of RISE, we have assembled an interdisciplinary team of truly outstanding researchers and practitioners, 37 PIs from 24 institutions (including 5 contributing partners from outside of Europe), in 13 countries, with documented experience on the topics of the project developed in previous FP6, FP7, and H2020 projects.
Consortium	Coordinator: 1. Eidgenoessische Technische Hochschule Zuerich (CH) Consortium: 2. "Helmholtz Zentrum Potsdam Deutschesgeoforschungszentrum Gfz (DE) 3. Istituto Nazionale Di Geofisica E Vulcanologia (IT) 4. Vedurstofa Islands (IS) 5. Alma Mater Studiorum - Universita Di Bologna (IT) 6. University Of Bristol (UK) 7. The University Of Edinburgh (UK) 8. Universita Degli Studi Di Napoli Federico Ii (IT) 9. Bar Ilan University (IL) 10. Centro Europeo Di Formazione E Ricerca In Ingegneria Sismica (IT) 11. Euro-Mediterranean Seismological Centre (FR) 12. Universite Grenoble Alpes (FR) 13. The Chancellor Masters And Scholars Of The University Of Cambridge (UK) 14. Bogazici Universitesi (TR) 15. Koninklijk Nederlands Meteorologisch Instituut-Knmi (NL) 16. Stmicroelectronics Srl (IT) 17. Universita' Degli Studi Di Bergamo (IT) 18. United Kingdom Research And Innovation (UK) 19. Quakesaver Gmbh (DE)"

1.3.4 Tsunami risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described. As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Tsunami risks	ASTARTE SEISMIC URBANWAVES

In this iteration of the CoU Mapping Document, no new projects related to tusnami risks were identified.

1.3.5 Landslide risks

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Landslide risks	LAMPRE

This overview is complemented by a Marie Skłodowska-Curie Actions project.

kelbus2	
Title	kelbus2
Objective	Perform laboratory experiments and fully 3D simulations of granular flows using simultaneous pressure and velocity measurements to test the acoustic fluidization hypothesis to explain landslide runouts
Contract details	H2020/MSCA/IF/2018; 15/01/20 - 14/01/22; € 196 707,84
Abstract	Landslides, the violent motion of large masses of debris, rock or snow, are an ever-present danger in mountainous regions the world over. After the landslide material falls down the mountainside, it will run out some distance away from the mountain even on relatively flat surfaces until the energy it gained from falling is dissipated by friction with the terrain. Although a simple energy balance argument suggests that a single rock cannot travel farther than the height from which it fell, many landslide runouts extend their ruin to seemingly safe distances far removed from their origin. These long runout landslides have baffled scientists for over a century, ever since Albert Heim recorded his study of the Elm rock landslide that devastated the village of Elm, Switzerland in 1881. There are many explanations for this phenomenon, such as lubrication by an interstitial fluid, but none of these satisfactorily addresses how a completely dry landslide can run out so far. Not understanding how and when long runouts will occur makes hazard mitigation and prediction extremely difficult, highlighting the urgency of this issue. Recently, Melosh and coworkers have provided support for a mechanism borrowed from the fluidization of impact craters, “acoustic fluidization”, by using idealized 2D simulations of circular disks, but more work is needed to show that this mechanism is a feature of real 3D flows and robust for a range of conditions. We will perform laboratory experiments and fully 3D simulations of granular flows using simultaneous pressure and velocity measurements to test the acoustic fluidization hypothesis. We will also look for a crossover between this dry mechanism and the lubrication mechanisms for wet landslides. Besides application to landslide engineering, we will also explore for the first time how fundamental features of granular flows such as shear flow instabilities (clustering and longitudinal stripes) affect the rheology of landslides and long runouts.
Consortium	Coordinator: Universite De Bordeaux (FR)

1.3.6 Earth-surface ground deformations

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Earth-surface ground deformations	DORIS MELINA SEMEP SENSUM STEADY SUBCOAST U-GEOHAZ

In this iteration of the CoU Mapping Document, no new projects related to were earth-surface ground deformations identified.

2. Health threats

The Decision 1082/2013 requires sharing best practice and experience in response planning among the Member States, and the establishment of early warning and response system (EWRS) for alerting, assessing public health risks and determining the measures that may be required to protect public health in consideration of relevant information. Besides, the CBRN Action Plan promotes strengthening sharing medical counter-measures across borders in the case of an incident. Recommendations also concern ways in which medical staff and other first responders can receive guidance on dealing with large scale CBRN emergencies and a rapid increase of the number of victims. Various projects support these goals:

2.1 Victims triage

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Earth-surface ground deformations	BIO-PROTECT BOOSTER FASTID MIRACLE MULTIBIODOSE

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

CURSOR	
Title	CURSOR
Objective	Develop new and innovative ways of detecting victims under debris
Contract details	H2020-SU-SEC-2021; Topic code: SU-DRS02-2018-2019-2020; 1/9/2019 - 31/8/2022; EUR 6 999 822,50
Abstract	The CURSOR proposal aims at developing new and innovative ways of detecting victims under debris. This includes the coordinated use of miniaturized robotic equipment and advanced sensors for achieving significant improvements in search and rescue operations with respect to (a) the time used to detect trapped victims after a building structure has collapsed, and (b) an informed and accelerated decision making by first responders during rescue operations allowing for the deployment of expert personnel and, in particular for operations in hazardous environments, suitable equipment at prioritized locations. CURSOR is proposing a system consisting of several integrated technological components. It includes Unmanned Aerial Vehicles (UAVs) for command & control, 3D modelling and transportation of disposable miniaturized robots, that are equipped with advanced sensors for the sensitive detection of volatile chemical signatures of human beings. Information and data collected are transferred in real time to a handheld device operated by first responders at the disaster site.
Consortium	Coordinator: 1. Bundesministerium Des Innern (DE) Consortium: 2. Entente Pour La Forêt Méditerranéenne (FR) 3. Merseyside Fire & Rescue Authority (UK) 4. Service Departemental Incendie Et Secours De La Savoie (FR) 5. Elliniki Omada Diasosis Attikis (EL) 6. Institute Of Communication And Computer Systems (EL) 7. Exus Software Monoprosopi Etairia Periorismenis Evthinis (EL) 8. C4controls Ltd (UK) 9. Iscc Gmbh (AT) 10. National University Corporation Tohoku University (JP) 11. Sintef As (NO) 12. Commissariat A L Energie Atomique Et Aux Energies Alternatives (FR) 13. The University Of Manchester (UK) 14. Din Deutsches Institut Fuer Normung E.V. (DE) 15. Trilateral Research Limited (IE) 16. Arttic (FR)

This overview is complemented by the following Erasmus+ project.

PREVENT IT	
Title	Risk Management and PREVENTion of AntIbioTics Resistance
Objective	Address the deficiency of academic modules on antibiotics prevention and risk management, and a total absence of awareness in the Indian society, and establish the European-Indian Network for Antibiotics Resistance Prevention and Risk Management
Contract details	598515-EPP-1-2018-1-IN-EPPKA2-CBHE-JP; 15/1/2019 - 14/1/2022; EUR: 988.201,00
Abstract	Antibiotic resistance is rising to dangerously levels in all parts of the world. New resistance mechanisms are emerging and spreading globally, threatening our ability to treat common infectious diseases. A project commissioned by the British government has released estimates of the near-future global toll of antibiotic resistance: 10 million deaths per year, more than cancer, and at least 124 trillion euros in sacrificed gross national product. Without urgent prevention and risk management actions, we are heading for a post-antibiotic era, in which common infections and minor injuries would kill. Following WHO Global Action Plan on Antimicrobial Resistance and the UN Heads of State political declaration on antimicrobial resistance, Indian and European policy makers has designed framework national plans fighting antibiotics resistance. PREVENT IT consortium has conducted a preliminary study that has highlight an alarming deficiency of academic modules on antibiotics prevention and risk management, and a total absence of awareness in the Indian society. As response, PREVENT IT plans to I) permanently introduce interdisciplinary curricula on antibiotics resistance - prevention and risk management – in per-existent studies programs – differentiating students' target audience; II) Disseminate as open educational resource, a MOOC for students, health sciences experts, and civil society organizations working with health in rural communities; II) Conduct nine regional dissemination events; III) Involve new stakeholders with the organization - in different area of India - of sixteen workshops and one symposium; IV) Create social media campaign to increase awareness in Indian society; V) To ensure sustainability, Lab for regular training in projects' proposals design. VI) During the last month of the funded period, to provide new impetus: establish the European-Indian Network for Antibiotics Resistance Prevention and Risk Management.
Consortium	Coordinator: Chitkara University (IN)

This overview is complemented by projects funded via H2020 in 2018.

A-Patch	
Title	Autonomous Patch for Real-Time Detection of Infectious Disease *This project is also relevant for 2.2 Contagions, pandemics.*
Objective	Research and demonstrate innovative use of Flexible and Wearable Electronics
Contract details	H2020-ICT-2018-2; 1/1/2019 - 31/12/2021; EUR: 4.009.087,50
Abstract	The A-Patch Research & Innovation project will research, innovate, push technology barriers, and demonstrate innovative use of Flexible and Wearable Electronics in the medical and well-being sectors, validate its prototype devices in lab and hospital environments (TRL 4-5). Industrial exploitation of the A-Patch applications will be clearly identified. The project will develop non-invasive autonomous wearable diagnostic patches for real-time remote monitoring of infection status. The A-Patch will use a novel intelligent hybrid sensor array with multiplexed detection capabilities to detect disease-specific volatile organic compounds (VOCs) from the surface of the skin, enabling rapid and highly-accurate diagnosis using a small device. Product innovations for professionals and consumers will be incorporated, and benefits demonstrated. Integration of electronic devices in connected wearable, flexible and stretchable settings, low-power interconnection, compatibility with low-cost manufacturing, efficient energy scavenging and storage, functional performance, and durability will be successfully demonstrated. To ensure reliability and enable extended usage periods, the sensor array will be self-repairing and the device will be self-powered, by advancing cutting-edge research on chemical hybrid sensors and materials. A-Patch will incorporate secure transmission to enable privacy-ensured diagnosis monitoring by physicians, national health systems and worldwide health organisations. The project partners include a health-maintenance organisation, a diagnostic test implementer with in-depth understanding of end-user needs, technology developers, academic / research institutes and a system integrator. The project is planned for a 36-month duration and is estimated to require total funding of 4 M€.
Consortium	Coordinator: 1. Technion - Israel Institute Of Technology (IL) Consortium: 2. "Bio-Rad (FR) 3. Interuniversitair Micro-Electronica Centrum (BE) 4. Latvijas Universitate (LT) 5. Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (NL) 6. Rivierawaves Sas (FR) 7. Foundation For Innovative New Diagnostics (CH) 8. Teknologian tutkimuskeskus VTT Oy (FI)"

2.2 Contagions, pandemics

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Contagions, pandemics	ANTIBOTABE BIO-PROTECT CCHFVaccine COMPARE CONCORDE EQUATOX EurHealth-1Health IMPRESS INSECTRISK PANDEM PANDHUB PIGSs PULSE S-HELP THEMIS ZIKAVAX

This overview is complemented by a Marie Skłodowska-Curie Actions project.

SENTIMOUV	
Title	Spatial and demographic dynamics of disease transfer at the wildlife/human interface
Objective	Develop a mechanistic understanding of the factors affecting prevalence and transmission of infectious diseases by seabirds at the wildlife-human interface
Contract details	H2020/MSCA/IF/2018; 1/1/2020 - 31/12/2021; EUR 196 707,84
Abstract	Our study will combine targeted field data collection, laboratory analysis, and quantitative modeling to develop a mechanistic understanding of the factors affecting prevalence and transmission of infectious diseases by seabirds at the wildlife-human interface. We will explore spatial and demographic factors affecting exposure and transmission rates for two key zoonotic diseases, toxoplasmosis and avian influenza, by a generalist coastal seabird, the yellow-legged gull (Larus michahellis) in the western Mediterranean basin. Within this study system, we will combine movement analysis using biologging, serological sampling, habitat and demographic analysis, and agent-based models to develop a comprehensive understanding of epidemiological dynamics. We will also use experimental studies to directly test the development of disease immunity in nestling birds and the effects of management actions on disease transfer. We will then apply scenario planning to study the effects of both management and habitat change on disease dynamics. Our results will not only improve understanding of gulls as vectors for infectious agents, but also provide a comprehensive quantitative framework for modeling disease dynamics that can be adapted to predicting and managing the spread of infectious disease at the wildlife-human interface.
Consortium	Coordinator: Centre National De La Recherche Scientifique Cnrs (FR)

DRmov	
Title	Deciphering the RBPome in mosquitoes during virus infection
Objective	Profile comprehensively the compendium of mosquito RBPs (RBPome) using RNA-interactome capture (RNA-IC), and identify the role of mosquito RBPs during virus infection.
Contract details	H2020/MSCA/IF/2018; 1/1/2020 - 31/12/2021;€ 224 933,76
Abstract	The impact of mosquito-borne diseases has expanded dramatically in the last few decades to become an emerging global health problem, with around 1 billion new infections and 1 million deaths each year. In Europe there are more than 20 countries with established populations of invasive Aedes mosquitoes. Aedes mosquitoes are the principle vectors responsible for transmitting high-risk pathogens such as ZIKA virus (ZIKV), dengue (DENV), yellow fever virus (YFV), chikungunya virus (CHKV) and Venezuelan equine encephalitic virus (VEEV). Despite our vulnerabilities to mosquito-borne diseases, virus replication dynamics is still poorly understood especially in the invertebrate vectors. No treatment against these viruses targeting essential viral proteins are currently available. Thus, the World Health Organisation (WHO) and its Vector Control Advisory Group has urged for insect vector control. Vector control is usually performed through insecticides; however, resistance can emerge in mosquitoes leading to persistence of the disease. Therefore, virologists are turning their interests toward host factors that play essential roles in infection as novel antiviral targets, since they can potentially exhibit broad-spectrum efficacy. In particular, scientists envision that genetically modified mosquitoes with disrupted genes required for infection can be re-inserted into natural habitats or through targeting these genes by RNAi in order to control viral spread. As all mosquito-borne viruses have RNA genome, cellular RNA-binding proteins (RBPs) emerge as ideal targets for antiviral therapies, as they are key players in cellular and viral RNA metabolism . Thus, we propose here to profile comprehensively the compendium of mosquito RBPs (RBPome) using RNA-interactome capture (RNA-IC). Furthermore, we will apply different cutting-edge methods to identify the role of mosquito RBPs during virus infection
Consortium	Coordinator: The Chancellor, Masters And Scholars Of The University Of Oxford (UK)

DIGDEEP	
Title	Digging deeper into genes to track infectious disease outbreaks
Objective	Develop alternative control strategies tailored to the characteristics of AIV evolution and transmission in order to minimize the global economic and health impact of the epidemics
Contract details	H2020-MSCA-IF-2018; 1/9/2020 - 31/8/2022; € 203 149,44
Abstract	DIGDEEP aims at developing alternative control strategies tailored to the characteristics of AIV evolution and transmission in order to minimize the global economic and health impact of the epidemics. The project will use cutting-edge phylodynamic inference methods to explore devastating and unprecedented epidemics of AIV in Europe and Asia. The outcomes of the project will allow us to infer key epidemiological parameters of the virus spread, such as the basic reproduction number or the likelihood of spillover between host species, and characterize the determinants of the epidemics, such as the importance of population structure or super-spreaders. DIGDEEP will also help to assess the effectiveness of public and animal health interventions in bringing the epidemic under control which are crucial for a well-informed response. Throughout the project, the fellow will gain a strong experience in phylodynamic inference methods, complementing her experience in epidemiology of infectious disease transmission. DIGDEEP will consolidate her scientific expertise in the field of public and animal health and develop transferable skills in team-working, communication and project management, which will be paramount to boost her career as a successful and internationally-recognized researcher.
Consortium	Coordinator: Eidgenoessische Technische Hochschule Zuerich (CH)

This overview is complemented by projects funded via H2020 in 2018.

SoNAR-Global	
Title	A Global Social Sciences Network for Infectious Threats and Antimicrobial Resistance *This project is also relevant for 9.3 Communication systems (interoperability and communication with focus on security).*
Objective	Build a sustainable international social science network to promote complementarity and synergy in the governance of prevention and response to infectious threats and AMR
Contract details	H2020-SC1-2018-Single-Stage-RTD; 1/1/2019 - 31/12/2021; EUR: 2.894.250
Abstract	SoNAR-Global is a global consortium led by social scientists specializing in emerging infectious diseases (EID) and antimicrobial resistance (AMR). It will build a sustainable international social science network to engage the active participation of social sciences and promote complementarity and synergy in the governance of prevention and response to infectious threats and AMR. As such, it will become an integral part of emergency response. Partnering with major international and regional institutions, it will lead activities through a program that builds governance from the ground up. It will: develop an open-access platform to support the SoNAR-Global activities and to share them broadly, adapt, test, and evaluate vulnerability assessment tools on the ground and engagement models to facilitate collaboration across multiple stakeholders, create, pilot, and evaluate curricula for training social scientists in preparedness and response to infectious threats and through curricular development and piloting social science knowledge of infectious threats among non-social sciences actors.
Consortium	Coordinator: 1. Institut Pasteur (FR) Consortium: 2. "Stichting Amsterdam Institute For Global Health And Development (NL) 3. Stichting Nederlands Instituut Voor Onderzoek Van De Gezondheidszorg (NL) 4. Medizinische Universitaet Wien (AT) 5. Mahidol University (TH) 6. State Institution Public Health Center Of The Ministry Of Health Of Ukraine (UA) 7. Brac University (BD) 8. University College London (UK) 9. Makerere University (UG) 10. Centre Regional De Recherche Et De Formation A La Prise En Charge Clinique Du Vih Sida Et Maladies Associees De Dakar Crcf (SN) 11. Institute Of Development Studies (UK)"

VIRUSES AND RNA	
Title	RNA regulation during viral infection
Objective	Discover and dissect RNA-based virus-host interactions and related regulatory mechanisms of gene expression
Contract details	ERC-2018-STG; 1/7/2019 - 30/6/2024; EUR: 1.500.000
Abstract	Viral infections are responsible for significant morbidity and mortality and frequency and impact of epidemics are expected to increase. Thorough understanding of basic virology is critical for informed development of prevention and control. Most systematic studies of virus-host interactions have focused on proteins, however, with recent methodological advances the intersecting fields of viral infection and RNA biology hold great promise for basic and therapeutic exploration. The goal of this application therefore is to discover and dissect RNA-based virus-host interactions and related regulatory mechanisms of gene expression. Micro-RNAs (miRNAs) fine-tune gene expression by repressing mRNA targets. However, cellular miRNAs increase translation and replication of certain viruses. Thus, hepatitis C virus (HCV) critically depends on the liver specific miR-122, which emerged as a therapeutic target. Further, HCV sequesters enough miR-122 to indirectly regulate cellular gene expression. I hypothesize that this RNA-based mechanism contributes to virus induced liver cancer, and aim to address this using our recently developed rodent model for HCV infection (Aim 1). Better understanding of viral RNA (vRNA) interactions could significantly contribute to basic infection biology and novel therapeutics. I therefore aim to systematically identify vRNA interactions with other cellular RNAs and proteins (Aim 2). I expect to identify interactions of value for functional regulation and therapeutic targeting. I finally hypothesize that translation of certain cellular mRNAs – similarly to viruses – increase upon miRNA binding, and aim to systematically screen for such virus-like alternative regulation, with potential to change understanding of post-transcriptional regulation (Aim 3). In conclusion, this high-risk high-gain project has potential to shape novel dogmas for virus and RNA biology and to identify novel RNA-based therapeutic targets; a promising upcoming field of discovery
Consortium	Coordinator: Kobenhavns Universitet (DK)

INITIATE	
Title	INnate-ImmunomeTabolIsm as Antiviral TargEt *This project is also relevant for 8.3.5 Training and Networking.*
Objective	Develop metabolic re-programming strategies to improve the innate immune systems' antiviral defences (host antiviral and inflammatory response to virus infections)
Contract details	H2020-MSCA-ITN-2018; 1/5/2019 - 30/4/2023; EUR: 4.054.106,16
Abstract	Viral outbreaks and epidemics continue to impose high morbidity and mortality burdens in mankind and animals, emphasizing the urgent need for the continuous improvement and innovation of our antiviral strategies. The innate immune system is pivotal for effective anti-viral defences. This field is now being revolutionised by the recognition that metabolic re-programming has a major impact on the host antiviral and inflammatory response to virus infections. The development of strategies targeted to these pathways represents an exciting new frontier for antiviral remedies. To drive this emerging field of antiviral immunometabolism and its application to viral diseases, INITIATE (INnate-ImmunomeTabolIsm as Antiviral TargEt) brings together a highly complementary team of world leaders, both academic and corporate, from the historically distinct research fields of virology, innate immunity and cellular metabolism in order to train a new generation of interdisciplinary scientists. Specifically, INITIATE will deliver training on the interrelationships between viral infection, host metabolism and immune defences through related and interdependent research projects, complemented with interdisciplinary and intersectoral secondments. Local and network-wide scientific workshops will be supplemented with transferrable skill workshops devoted to academia/industry collaboration, research dissemination and translation of knowledge into novel therapeutic interventions, public engagement and a successful research environment. INITIATE will result in a new generation of creative, entrepreneurial and innovative top-level interdisciplinary researchers, who will be at the forefront of the emerging research field of 'antiviral immunometabolism'. These scientists will be able to face the inevitable future challenges in combating viral and other diseases, and they will be highly attractive to European Life Sciences industry and academia.
Consortium	Coordinator: 1. Erasmus Universitair Medisch Centrum Rotterdam (NL) Consortium: 2. "Instituto Pasteur Italia Fondazionecenci Bolognetti (IT) 3. The Provost, Fellows, Foundation Scholars & The Other Members Of Board Of The College Of The Holy & Undivided Trinity Of Queen Elizabeth Near Dublin (IE) 4. Academisch Ziekenhuis Leiden (NL) 5. Cemm - Forschungszentrum Fuer Molekulare Medizin Gmbh (AT) 6. Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO) 7. Universiteit Utrecht (NL) 8. Stimunity Sas (FR) 9. Janssen Vaccines & Prevention Bv (NL) 10. Astrazeneca Ab (SE) 11. Elsevier Bv (NL) 12. Biocrates Life Sciences Ag (AT) 13. Agilent Technologies Sales & Services Gmbh & Co Kg (DE) 14. Sovalacc B.V. (NL)"

MeningoSpeed	
Title	A unique cost-effective and point of care (PoC) kit for the non-invasive rapid in vitro diagnosis of meningococcal disease *This project is also relevant for 2.3 Medical Responses.*
Objective	MeningoSpeed feasibility study covering the technological, commercial and financial issues of the business plan
Contract details	H2020-SMEInst-2018-2020-1; 1/3/2019 - 30/6/2019; EUR: 50.000
Abstract	Meningococcal disease (MD), caused by Neisseria meningitidis serogroups (mainly ABCXWY), annually affects 1.2 million people worldwide (mainly children and young). Due to its high lethality (8-15% treated patients), permanent sequelae and epidemic potential, MD represents a major public health problem. Despite the societal burden, there is a lack of rapid and accurate diagnostic tools for timely and early treatment that results very costly for healthcare systems (e.g. direct costs valued in € 68 m/hospital/year). In response to the unmet need, BioSpeedia (spin-off from the Institute Pasteur, France) has vast experience in infectious diseases management and is developing the first-ever gold nanoparticle-based immunochromatographic test with demonstrated diagnostic capability for the six Nm serogroups. MeningoSpeed is a non-invasive, accurate (sensitivity and specificity >93%), rapid (<15 min vs PCR: 3h) and cost-competitive in vitro diagnostic test (€45 sample, at least 25 % cheaper than latex agglutination tests and PCR alternatives) for MD diagnosis. Our one-step solution will result on added value for patients, physicians and healthcare purchasers by improving disease monitoring in an accurate and timely fashion way, reducing deaths and sequelae. MeningoSpeed will provide healthcare systems with limited resources with a reliable and cost-effective diagnostic tool, leading to significant cost-savings. MeningoSpeed´s high accuracy and performance under a faster and cheaper cost make it a disruptive solution with great potential for commercial success in the growing point-of-care market (€33 B by 2022, CAGR 10%). Thus, MeningoSpeed is projected to be a profitable business opportunity and a core source of growth for the company (ca. €33 M of accumulated net profit during 2022-2026). A next feasibility study covering the technological, commercial and financial issues will enable us to finalize our business plan and secure our steps towards the successful market launch.
Consortium	Coordinator:Biospeedia (FR)

2.3 Medical Responses

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Medical responses	CONCORDE f EU MFH i-4-1-Health IMPRESS INNOPROCITI NMFRDISASTER NO FEAR OSAS PULSE Q4HEALTH S-HELP

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

iProcureSecurity	
Title	iProcureSecurity *This project is also relevant for 9.2 Standardisation, Testing & Certification*
Objective	Improve response capacities and increasing the cooperation of the European Emergency Medical Services Systems (EMSS)
Contract details	H2020-SU-SEC-2020; Topic code: SU-GM02-2018-2019-2020; 1/5/2019 - 31/12/2020; EUR 999 975
Abstract	Emergency Medical Services in Europe are characterised by a pluralistic landscape with diverse organisational setups, professional standards, coordination mechanisms and actors which result from different historical and institutional contexts in EU member states. However, diversity is united by the common aim, of providing timely care to victims of sudden and life-threatening injuries, emergencies or disasters within EU-member states (EUMS), in cross-border settings and international humanitarian missions. Fostering the response capacities and increasing the cooperation of the European Emergency Medical Services Systems (EMSS) is of decisive importance for strengthening the resilience of European societies in the light of multiple hazards: Climate change is increasing the frequency and severity of disasters, terrorism is becoming a very real scenario for mass causality events challenging both out-of-hospital as well as in-hospital emergency care, and health related hazards are calling for close cooperation of public safety and health authorities on an international level. Not only hazards but also the system's diversity poses a challenge for preparedness planning and cooperation, which needs to involve the whole EMS system at regional and/or national level and integrate it into the whole health system and fully coordinate with the public safety system to be effective. The iProcureSecurity project seeks to identify the major challenges the system's diversity poses to the ability to work together, stimulate R&I uptake with a view to increasing standardisation of operations across Europe, and deliver technical requirements for R&I activities to create a European system of Medical Emergency Teams that is more homogeneous and capable to work as singly unit. To achieve this aim, the project will engage in several exchange cycles with practitioners and other stakeholders in the innovation landscape as a preparation for major R&I activities as part of a PCP action.
Consortium	Coordinator: 1. SYNYO GmbH (AT) Consortium: 2. Johanniter International (BE) 3. Servicio Madrileno De Salud (ES) 4. Johanniter Osterreich Ausbildung Und Forschung Gemeinnutzige Gmbh (AT) 5. Ambulance And Emergency Physicians Association (TR) 6. Elliniki Etaireia Epeigousas Pronosokomeiakis Frontidas (EL) 7. Fundacion Para La Investigacion Biomedica Hospital Infantil Universitario Nino Jesus (ES) 8. Italian Resuscitation Council (Irc)Gruppo Italiano Cardiopolmonare (IT) 9. Association Medicale Europeenne (BE) 10. The Provost, Fellows, Foundation Scholars & The Other Members Of Board of The College Of The Holy & Undivided Trinity Of Queen Elizabeth Near Dublin (IE)

In addition, another relevant H2020 project was funded.

SECONDS	
Title	On Time Emergency Response System *This project is also relevant for 1.1.4 Multi-hazard emergency response and crisis management, including cascading effects.*
Objective	Commercialisation of On Time Emergency Response System (SECONDS)
Contract details	H2020-SMEInst-2018-2020-1; 1/3/2019 - 30/6/2019; EUR: 50.000
Abstract	SECONDS is an innovative, real-time vehicle management system for emergency dispatchers, maximizing coverage and reducing response time. It provides +35% ambulance arrivals below 12-min threshold time; it is able to manage simultaneous incidents in the same area; it forecasts locations with a higher emergency probability and provides predictive incident location, which means 25% less vehicle driving mileage, higher vehicle availability; faster patient delivery to hospital; less pollution. For EMS dispatch center operators, it will provide 2.5 faster response time, asset (vehicle + medical staff) usability management, reduced cost and crew overtime, as well as better decisions – less pressure on operators – and better monitoring. For citizens/persons in need, it will bring a higher survival rate (up to 14% mortality reduction) and richer experience – better care. SECONDS will bring our company international expansion, valuable IP assets, €24.6M profits over 5 years via subscriptions/consulting, a ROI of 844% and the creation of 59 additional qualified jobs.
Consortium	Coordinator: Stokhos B.V. (NL)

2.4 Digital security in Health Services

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Digital security in Health Services	CHINO KONFIDO SHIELD MH-MD health-i-care

These projects were complemented in the H2020 framework by the following projects.

PANACEA	
Title	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people *This project is also relevant for 6.3.1 Cyber Security Management (for SMEs/business, local public authorities)*
Objective	Deliver two toolkits for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices
Contract details	H2020-SC1-FA-DTS-2018-1; 1/1/2019 - 31/12/2021; EUR: 4.961.143,75
Abstract	PANACEA will deliver people-centric cybersecurity solutions in healthcare. The Partners will execute on a leanly-orchestrated research workplan, which envisages continuous involvement of the end-user Partners at three European health care centres, including also devices utilised in remote care & homecare settings. Ultimately, PANACEA delivers two toolkits for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices: the Solution Toolkit and the Delivery Toolkit. The first one comprisesfour technological tools (for dynamic risk assessment & mitigation, secure information sharing, security-by-design & certification, identification & authentication) and three organisational tools (for training & education, resilience governance, secure behaviours nudging). The second one, specifically supporting adoption of the solution toolkit, comprises two tools (methodology to evaluate the ROI of cybersecurity interventions, guidelines to adopt the solution toolkit and implement other ex-ante mitigation actions). The toolkit will benefit from ninePANACEA ambitious research goals, achieved by moving beyond the current state of the art in the strategic areas of dynamic risk assessment & mitigation (threat modelling, attack modelling, response management, visual analytics), blockchain for secure information sharing, identification/ authentication (cryptographic authentication protocols, biometric recognition/digital identity, IoMT identification), secure behaviours decision models and influencers. Impact creation will be supported by designing and executing on an effective communication, dissemination and exploitation strategy involving all partners, from project onset. The PANACEA Consortium is committed, competent and complementary. The Consortium is led by a private hospital, supported by 3 research organisations, 3 large enterprises, 5 SMEs. Severalend-user scenarios, developed in Italy, Crete and Ireland, will provide a solid test-bed..
Consortium	Coordinator: 1. Universita Cattolica Del Sacro Cuore (IT) Consortium: 2. "Fondazione Policlinico Universitario Agostino Gemelli Irccs (IT) 3. Rina Consulting Spa (IT) 4. Idryma Technologias Kai Erevnas (GR) 5. Idemia Identity & Security France (FR) 6. Rhea System (BE) 7. University Of Northumbria At Newcastle (UK) 8. Aon Spa Insurance & Reinsurance Brokers (IT) 9. Stelar Security Technology Law Research Ug (DE) 10. Universita Degli Studi Di Roma La Sapienza (IT) 11. Trust-It Services Limited (UK) 12. Dioikhsh Ygeionomikhs Perifereias Krhths (GR) 13. Health Service Executive Hse (IE) 14. Irish Centre For Emergency Management (IE) 15. Innovation Sprint (BE)"

ProTego	
Title	Data-protection toolkit reducing risks in hospitals and care centers *This project is also relevant for 6.3.1 Cyber Security Management (for SMEs/business, local public authorities).*
Objective	Develop a toolkit and guidelines to help health care systems users address cybersecurity risks
Contract details	H2020-SC1-FA-DTS-2018-1; 1/1/2019 - 31/12/2021; EUR: 4.457.722,50
Abstract	Health care is an essential service that uses a great deal of sensitive personal data which has a high black market value being a lucrative target for data theft and ransomware attacks.The EU NIS Directive (EU 2016/1148) and GDPR (EU 2016/679) will harmonize and improve information security in Europe. Both require relevant ICT infrastructure operators to perform risk assessments, introduce appropriate security measures to manage identified risks, and report security breaches. Unfortunately, risk-based approaches are notoriously difficult to implement in a consistent and comprehensive fashion. They depend on a high level of understanding of both cybersecurity and of the system or network to be protected, are labour intensive and costly and typically done by small teams. This is increasingly inappropriate as health care providers introduce IoT systems, cloud services and (in the near future) 5G networks to provide services in which patients are more engaged, may own some of the devices used, and want access in hospitals, on the move or at home. The ProTego project will develop a toolkit and guidelines to help health care systems users address cybersecurity risks in this new environment by introducing 3 main advances over current approaches: Extensive use of machine intelligence: a combination of machine inference exploiting a priory knowledge for security-by-design, and machine learning from data for run-time threat detection and diagnosis; Advanced data protection measures: advanced encryption techniques and hardware based full memory encryption, and multi-stakeholder IAM to control access to and by user devices, to protect data at rest and provide ultra-secure data exchange portals; Innovative protocols for stakeholder education: using security-by-design analysis to target training and support stakeholders to contribute to networok overall security.The toolkit will be integrated and validated in IoT and BYOD-based case studies at two hospitals.
Consortium	Coordinator: 1. Grupo Corporativo Gfi Informatica Sa (ES) Consortium: 2. "University Of Southampton (UK) 3. Ibm Israel - Science And Technology Ltd (IL) 4. Ospedale San Raffaele Srl (IT) 5. Marina Salud Sa (ES) 6. Universidad De Alcala (ES) 7. Interuniversitair Micro-Electronica Centrum (BE) 8. Katholieke Universiteit Leuven (BE) 9. Information Catalyst For Enterprise LTD (UK)"

SPHINX	
Title	A Universal Cyber Security Toolkit for Health-Care Industry *This project is also relevant for 6.3.3 Cyber Crime*
Objective	Introduce a Universal Cyber Security Toolkit able to proactively assess and mitigate (known and unknown) cyber-security threats, imposed by devices and services within a corporate ecosystem
Contract details	H2020-SC1-FA-DTS-2018-1; 1/1/2019 - 31/12/2021; EUR: 4.999.435
Abstract	Hospitals and care centres are prime targets for cyber criminals, especially concerning data theft, denial-of-service and ransomware. This reflects the need of Healthcare Institutions for a Holistic Cyber Security vulnerability assessment toolkit, that will be able to proactively assess and mitigate cyber-security threats known or unknown, imposed by devices and services within a corporate ecosystem. SPHINX aims to introduce a Universal Cyber Security Toolkit, thus enhancing the cyber protection of Health IT Ecosystem and ensuring the patient data privacy and integrity. SPHINX toolkit will provide an automated zero-touch device and service verification toolkit that will be easily adapted or embedded on existing, medical, clinical or health available infrastructures, whereas a user/admin will be able to choose from a number of available security services through SPHINX cyber security toolkit. The SPHINX toolkit will enable service providers to specify complete services and sell or advertise these through a secure and easy to use interface. SPHINX Toolkit will be validated through pan-European demonstrations in three different scenarios. The operational properties of the proposed cyber-security ecosystem and overall solution will be validated and evaluated against performance, effectiveness and usability indicators at three different countries (Romania, Portugal and Greece). Hospitals, care centers and device manufacturers participating in the project's pilots will deploy and evaluate the solution at business as usual and emergency situations across various use case scenarios.
Consortium	Coordinator: 1. National Technical University Of Athens - Ntua (GR) Consortium: 2. "Fint Future Intellingence Limited (CY) 3. Konnekt Able Technologies Limited (IE) 4. Vilabs (CY) Ltd (CY) 5. Siveco Romania Sa (RO) 6. Aideas Ou (EE) 7. Technological Educational Institute Of Crete (GR) 8. Pdm E Fc Projecto Desenvolvimento Manutencao Formacao E Consultadorialda (PT) 9. Edgeneering Lda (PT) 10. Tech Inspire Ltd (UK) 11. Vrije Universiteit Brussel (BE) 12. Fundacion Tecnalia Research & Innovation (ES) 13. Intracom Sa Telecom Solutions (GR) 14. Imprensa Nacional - Casa Da Moeda, S. A. (PT) 15. Polaris Medical Clinica De Tratament Si Recuperare Sa (RO) 16. Hospital Do Espirito Santo De Evora Epe (PT) 17. 5 Ygionomiki Periferia Thessalias & Stereas Elladas (GR)"

FeatureCloud	
Title	Privacy preserving federated machine learning and blockchaining for reduced cyber risks in a world of distributed healthcare
Objective	Delivery of software toolkit for substantially reducing cyber risks to healthcare infrastructure by employing the world-wide first privacy-by-architecture approach
Contract details	H2020-SC1-FA-DTS-2018-1; 1/1/2019 - 31/12/2023; EUR: 4.646.000
Abstract	The digital revolution, in particular big data and artificial intelligence (AI), offer new opportunities to transform healthcare. However, it also harbors risks to the safety of sensitive clinical data stored in critical healthcare ICT infrastructure. In particular data exchange over the internet is perceived insurmountable posing a roadblock hampering big data based medical innovations. FeatureCloud's transformative security-by-design concept will minimize the cyber-crime potential and enable first secure cross-border collaborative data mining endeavors. FeatureCloud will be implemented into a software toolkit for substantially reducing cyber risks to healthcare infrastructure by employing the world-wide first privacy-by-architecture approach, which has two key characteristics: (1) no sensitive data is communicated through any communication channels, and (2) data is not stored in one central point of attack. Federated machine learning (for privacy-preserving data mining) integrated with blockchain technology (for immutability and management of patient rights) will safely apply next-generation AI technology for medical purposes. Importantly, patients will be given effective means of revoking previously given consent at any time. Our ground-breaking new cloud-AI infrastructure only exchanges learned model representations which are anonymous by default. Collectively, our highly interdisciplinary consortium from IT to medicine covers all aspects of the value chain: assessment of cyber risks, legal considerations and international policies, development of federated AI technology coupled to blockchaining, app store and user interface design, implementation as certifiable prognostic medical devices, evaluation and translation into clinical practice, commercial exploitation, as well as dissemination and patient trust maximization. FeatureCloud's goals are bold, necessary, achievable, and paving the way for a socially agreeable big data era of the Medicine 4.0 age.
Consortium	Coordinator: 1. Technische Universitaet Muenchen (DE) Consortium: 2. "Philipps Universitaet Marburg (DE) 3. Medizinische Universitat Graz (AT) 4. Syddansk Universitet (DK) 5. Sba Research Gemeinnutzige Gmbh (AT) 6. Universiteit Maastricht (NL) 7. Concentris Research Management Gmbh (DE) 8. Research Institute Ag & Co Kg (AT) 9. Gnome Design Srl (RO)

3. Food safety and security

3.1 Food safety and security

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Digital security in Health Services	AUTHENT-NET EMPHASIS-PREP EuroMix PLANTFOODSEC POnTE

This overview is complemented by Erasmus+ projects.

Food Governance in the European Union	
Title	Food Governance in the European Union
Objective	Establish the Jean Monnet Chair for Food Governance in the European Union, which accelerates and deepens teaching, research and dissemination on the sustainability aspects relating to the production and consumption of food
Contract details	600036-EPP-1-2018-1-NL-EPPJMO-CHAIR; 1/9/2018 - 31/8/2021; EUR: 50.000,00
Abstract	The Jean Monnet Chair Food Governance in the European Union seeks to accelerate and deepen teaching, research and dissemination on the sustainability aspects relating to the production and consumption of food (environmental impacts, overfishing, food safety, food security, health and nutrition, animal welfare) through a dedicated governance perspective that allows for a comprehensive examination of the roles of different public stakeholders (at the local, national and eu level) and private stakeholders (ngos, farmers, retailers, food producers). The chair is based at University College Roosevelt (ucr), the liberal arts and sciences honours college which is academically affiliated to Utrecht University and is located in Middelburg, in the province of Zeeland, the Netherlands.
Consortium	Coordinator: Stichting University College Roosevelt (NL)

Central European Initiative on Agricultural Land Protection	
Title	Central European Initiative on Agricultural Land Protection
Objective	Foster a dialogue between the crucial stakeholders of agricultural land protection in Central Europe affecting the achieving the objectives of EU agri-environmental and EU food policy
Contract details	600441-EPP-1-2018-1-SK-EPPJMO-PROJECT; 1/9/2018 - 31/8/2019; EUR: 36.798,75
Abstract	Central Europe is specific geographical region with significant influence share of agricultural land in Europe with a good quality and climate conditions. The proposal of the project arises from the need to contribute to sustain quality of agricultural land and food security in the EU. Therefore, the main objective of the proposed project is to foster a dialogue between the crucial stakeholders of agricultural land protection in Central Europe affecting the achieving the objectives of EU agri-environmental and EU food policy. The main objective will be achieved through following activities:- strengthening the discussion Central European stakeholders at different levels of competences in the field of agricultural land protection- encouraging cooperation between researchers, academics and experts within the field of land protection in Central Europe and in the EU;- gathering and exchanging the knowledge and expertise among stakeholders from Central Europe;- providing information about the agricultural land protection to involved stakeholder in Central Europe as well as in the EU.Activities of the project are oriented on following target groups: researchers, academics, professionals, students involved in the EU and environmental studies, and general public.Outcomes of the proposed project will be:- reinforced mutual cooperation among all stakeholders (academics, managing and control authorities, practice) and within specific fields individually;- improved knowledge of teaching and research activities of educational and research institutions in the EU and in Central European countries;- enhanced governance of agricultural land protection in Central European countries and subsequently in the EU.Visibility and sustainability of the project will be maintained by designed deliverables: interactive website, online conference proceedings, scientific mongraph, and baseline study on land protection in Central Europe.
Consortium	Coordinator: Slovenska Polnohospodarska Univerzita V Nitre (SL)

This overview is complemented by projects funded via H2020 in 2018.

BIOIMPROVE	
Title	Improvement of food safety applied biosensors by protein engineering
Objective	Develop an improved and highly sensitive portable biosensing device for the quantification of histamine in the lower concentration range (<5 mg/l)
Contract details	H2020/MSCA/IF/2018; 1/5/2019 - 18/8/2021;€ 172 932,48
Abstract	Determination of the histamine content is of paramount importance for the food industry as a parameter of the hygienic quality and freshness of food, as well as to prevent scombroid fish poisoning, an allergy-like food poisoning. At present, more sensitive and user-friendly methods for histamine monitoring are needed to early detect products and raw materials susceptible of becoming hazardous for consumers. BIOIMPROVE aims to develop an improved and highly sensitive portable biosensing device for the quantification of histamine in the lower concentration range (<5 mg/l). To reach this objective, an innovative and powerful semi-rational protein engineering strategy will be used to maximize the sensitivity of the currently available histamine enzyme-based biosensor. Rather than addressing this goal by the generation and screening of large libraries, a careful selection of the most promising mutational hotspots will be performed using the structural available information in tandem with advanced computational modelling tools. Dr. Gangoiti will carry out BIOIMPROVE project at BIOLAN Microbiosensores, a Spanish SME focused on the development of biosensors capable of detecting health and food-related molecules. To support her research, she will conduct a secondment at CIC bioGUNE, a research centre that has a strong reputation in protein computational design. Thanks to this multidisciplinary research environment, Dr. Gangoiti will have the opportunity of gaining not only a high level of complementary expertise in areas of key importance in the enzyme technology field, but also the competences required for pursuing a successful research career either in industry or academy. Most importantly, the implementation of BIOIMPROVE project is expected to ensure histamine contamination to be identified at all stages of the food chain, ultimately guaranteeing food safety for European consumers
Consortium	Coordinator: Biolan Microbiosensores Sl (ES)

CIFTRESS	
Title	Climatic Impact on Food Trade RESilience and Security
Objective	Examine the joint climate, agro-environmental, and economic induced changes to the trade network topologies of five staple foods, i.e., maize, rice, wheat, barley, and soybeans, up to the year 2050 in the European and Mediterranean region
Contract details	H2020-MSCA-IF-2018; 15/5/2019 - 14/5/2021; €171 473,28
Abstract	Global climate change adversely affects crop yields and undermines humanity's food security and resilience; while previous research has focused on regional agricultural adaptation, the opportunities and vulnerabilities of trade networks have remained less explored. In this vein, this research examines the joint climate, agro-environmental, and economic induced changes to the trade network topologies of five staple foods, i.e., maize, rice, wheat, barley, and soybeans, up to the year 2050 in the European and Mediterranean region. This proposed research adopts an interdisciplinary methodology drawing on crop yield modeling, economic trade modeling, network science, and quantitative scenario building approaches. More specifically, this research will enhance the International Model for Policy Analysis of Agricultural Commodities and Trade (IMPACT) Model with fitness network formation and gravity trade models to reveal the regional origin and destination of staple commodities. Through the enhanced model, the network topologies of current and future scenario staple food trade will be investigated and linked to the notions of resilience and security. Scenarios describing alternative dynamics of staple food trade network topologies for each crop will be developed through a comprehensive literature review focusing on agricultural trends, investments, and regional strategies and semi-structured interviews with agro-economists, agriculture policy specialists, and agricultural trade practitioners.
Consortium	Coordinator: Universita Ca' Foscari Venezia (IT)

FANTASTICAL	
Title	Novel Tools For Food Safety Management Based On Qmra With A Robust Modelling Of Unnovel Tools For Food Safety Management Applying Qmra With Robust Modelling Of Uncertainty And Variability
Objective	Develop novel approaches and tools for QMRA that can be implemented by all the stakeholders, i.e. agencies related to consumer protection (EFSA, ECDC) and industry
Contract details	H2020-MSCA-IF-2018; 2/9/2019 - 1/9/2021; € 175 572,48
Abstract	FANTASTICAL aims to develop novel approaches and tools for QMRA that can be implemented by all the stakeholders, i.e. agencies related to consumer protection (EFSA, ECDC) and industry. It will link a database of microbial responses with robust statistical functions for variance analysis and stochastic simulation in a user friendly software. This project will reach out to the potential users and provide them with hands-on, open access tools to better understand microbial variability and uncertainty, resulting in more realistic QMRA. Thus, it will lead to an improvement in consumer protection and safer products. It will also complement Dr Garre's curriculum and provide him with soft skills required to take the next step of his scientific career towards becoming an R3 – Experienced Researcher.
Consortium	Coordinator: Wageningen University (NL)

HMCS	
Title	Handheld Molecular Contaminant Screener
Objective	Feasibility study on real-time detection of risk related substance using handheld molecular contaminant screener (HMCS) based on a novel portable mass spectrometry technology
Contract details	H2020-SMEInst-2018-2020-1; 1/2/2019 - 31/7/2019; EUR: 50.000
Abstract	There is an ever-increasing need for real time detection for risk related substances (e.g. pesticides, bacteria and antibiotics) in agro and food products. Food quality, food frauds and food scandals are becoming a major issue these days. Prime examples of recent food disasters are the Fipronil Dutch egg scandal and Salmonella French baby milk scandal. These scandals have not only resulted in health effects but also resulted in massive economic losses (> € 600m), losses in jobs and damage of the reputation of the European agro and food industry which takes pride in being the best in the world. Current high-end screening methods are laboratory based which are time consuming (5-12 days) and expensive (€200 per hour of testing cost at central labs). By the time results are out, food is already in the processing stage or in the supermarkets. We propose real-time detection of risk related substance using handheld molecular contaminant screener (HMCS) based on a novel portable mass spectrometry technology. With HMCS rather than bringing the sample to the lab you bring the lab to the sample. HMCS enables food companies to test food or food products for contaminants before collecting food from the farms and at various stages of the food value chain. We have validated by speaking with customers such as Freisland Campina (the world's largest dairy co-operative) and Vion food group to name a few who indicated to pilot HMCS based on the success of feasibility study. The feasibility study in phase 1 will technically validate the value of HMCS in terms of sensitivity (parts-per-billion), portability (< 9kg) and speed of detection (< 30 seconds). The economic feasibility study should provide lacking information about the decision making unit (farmer-food companies relationship) in order to validate the business plan.
Consortium	Coordinator: Next Generation Sensors BV (NL)

ImpactVision	
Title	A new standard for food safety and quality *This project is also relevant for 9.2 Standardisation, Testing & Certification.*
Objective	Provide objective, real-time food quality data to the 30,000+ food processing facilities across the USA and improve efficiency of the global food supply chain
Contract details	H2020-SMEInst-2018-2020-1; 1/1/2019 - 30/6/2019; EUR: 50.000
Abstract	ImpactVision is a machine learning company, applying advanced imaging technology to food supply chains in order to improve food quality, generate consistent products and reduce waste. Our software provides insights about the quality of foods and is aimed at food processors, manufacturers, distributors and retailers. For example, our system is able to determine the freshness of fish, the ripeness of avocados or the presence of foreign objects rapidly, non-invasively and at production grade speeds. Hyperspectral imaging technology captures information our eyes cannot, in other parts of the electromagnetic spectrum. Our goal is to provide objective, real-time food quality data to the 30,000+ food processing facilities across the USA and improve efficiency of the global food supply chain. Currently, a third of all food produced is wasted. To illustrate the environmental impact at scale, managing food waste sustainably could reduce greenhouse gas emissions by over 500 million tonnes - the equivalent of taking all the cars off the road in the European Union. By digitizing food quality control, we improve yields and prevent waste, whilst increasing food companies' revenues, which is particularly prescient considering the industry has razor thin profit margins. ImpactVision combines a hyperspectral sensor installed above a conveyor belt with software that analyzes images and provides real time insights about quality. By pursuing the present feasibility study, the management team aims to improve its understanding of international market conditions and the associated risks that need to be considered as the company develops a deeper business plan for rolling out, and scaling up ImpactVision as a marketable innovative solution. SME Instrument Phase-1 and Phase-2 will be extremely beneficial in helping the company to accelerate development and market penetration of the solution in target segments, boosting the company's growth to 94 employees and $109M revenues by 2024.
Consortium	Coordinator: Impactvision UK LTD (UK)

3.2 Supply chain

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Digital security in Health Services	DELTA-FLU MycoKey MyToolBox SNIFFER 2 SPICED

In this iteration of the CoU Mapping Document, no new projects related to supply chain issues were identified.

4. Critical infrastructure protection and urban built environment

The European Programme for Critical Infrastructure Protection (see section XX) is an all-hazards programme with a broad range of activities and areas related to prevention, preparedness and response. In this respect, risk management is taking stock of existing research and innovation activities conducted notably in the FP7 Environment (including climate change) programme, in particular the Group on Earth Observation (GEO) such as the Supersites Initiative and research on "stress tests" for critical infrastructures. The programme is furthermore enhancing links with management activities undertaken within the Union Civil Protection Mechanism.

4.1 Urban soft targets and Urban critical infrastructures

4.1.1 Screening of persons, bags, vehicles

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Screening of persons, bags, vehicles	AIRIMGO ART Bio-AX ColdNano-X HOLOSCAN PMT4NIIS SPIDERS

This overview is complemented by the following H2020 project.

CLAYONRISK	
Title	Bricks manufacturing technologies to increase built heritage resilience and to raise common identities of peoples *This project is also relevant for 1.3.3 Seismic and earthquake risks.*
Objective	Foster bricks manufacture processes in order to mitigate the negative impact of extreme weather events and earthquakes on historical structures
Contract details	H2020-MSCA-IF-2018;15/4/2019 - 14/4/2021; EUR 171.473,28
Abstract	The CLAYONRISK project mainly aims to foster bricks manufacture processes in order to mitigate the negative impact of extreme weather events and earthquakes on historical structures. As a traditional building material widely used from ancient times and worldwide, both eco-innovative solutions and socio-cultural values of peoples will be tackled. For first time, the manufacturing of building bricks is addressed as a preventive measure for Disaster Risk Reduction management. Starting from: i) bricks decay due to climate change make ancient structures much more vulnerable to seismic risk, and ii) the negative impact of disasters on historical structures could be mitigated by improving the physical properties of bricks, directly influenced by the manufacturing parameters, a multidisciplinary and comparative study of bricks -both ancient and currently produced- is accomplished. Archaeometric methodologies by means of multianalytical approach is followed and building bricks resistance over time is assessed considering their mechanical behavior after ageing tests performance. Northern Italy entails an outstanding site to accomplish the project, as it is a high humidity area with regular seismic activity where the geology has enhanced an exceptional architecture shaped by bricks and a ceramic industry leadership. With a cutting-edge scope, CLAYONRISK will state bricks resistance over time and the achievement of technological improvements and sustainable solutions towards the strengthening of heritage (and new) constructions, ensuring peoples traditions and the socio-cultural values of ancient structures. The intersectorial transfer of knowledge fostered by CLAYONRISK will promote a protocol development, launched by the academy-industry cooperation and where bricks entail a transnational understanding resource to aware the European cultural identity. The project entails a broad range of opportunities for the candidate and will enlarge her research prospects in the future.
Consortium	Coordinator: Universita Degli Studi Di Padova (IT)

4.1.2 Detection of potential CBRN-E threats at urban soft targets / urban critical infrastructures

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Detection of potential CBRN-E threats at urban soft targets / urban critical infrastructures	EXTREMDRON

In this iteration of the CoU Mapping Document, some projects categorised under other themes also related to detection of potential CBRN-E threats at urban soft targets / urban critical infrastructures, these include UCTIL, PRINCE and SATIE

4.1.3 Cyber and physical threats to urban critical infrastructures and urban soft targets

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Cyber and physical threats to urban critical infrastructures and urban soft targets	CAPTOR SmartPatch StandBy-U

This overview is complemented by projects funded by ISF.

EU HRS Network	
Title	European Union High Risk Security Network *This project is also relevant for 6.1 Terrorist threats and 4.3.5 Risk assessment and monitoring*
Objective	Connect representatives from European operational units or civil organizations, police organizations with military status and/or military units in order to enhance best practices sharing, training and tactics and to improve preparedness against future terror attacks and acts of severe violence
Contract details	ISFP-2017-AG-IBA-EUSTP; 1/11/2018 - 31/10/2020; EUR 326.189,50
Abstract	Considering there is a real and imminent threat of acts of severe violence and/or terrorism against (civil) critical infrastructure, soft targets and transport hubs in all European countries; Acknowledging that (governmental) security preparations to prevent such acts are increasing throughout Europe; Emphasizing that better preparedness and stronger security in the countries concerned are recommended to protect all European citizens against such acts ; Recognizing that policy makers, practitioners and private partners should try to work towards a common approach in order to achieve a better level of preparedness and security;Cooperating with as many European countries as possible; The European Union High-Risk Security (HRS) Network, aims to connect representatives from European operational units or civil organizations, police organizations with military status and/ or military units tasked with the prevention, detection, armed protection and securing of civil critical infrastructure, soft targets and transport hubs against acts of terror and severe violence, in order to enhance best practices sharing, training and tactics, and to improve preparedness against future attacks. The focus of these units includes the prevention, detection and response to the 1st phase of a terrorist attack, but does not include the organized response and intervention normally carried out by the government.

This overview is complemented by the following H2020 project.

UDE	
Title	Artificial Intelligence and Computer Vision for real-time diagnosis of public spaces
Objective	Develop UDE, an innovation for real time diagnosis of public spaces taking data captured from existing live urban cameras
Contract details	H2020-SMEInst-2018-2020-1; 1/6/2019 - 30/11/2019; EUR: 50.000
Abstract	Urban Data Eye brings to the market UDE, a paramount innovation for real time diagnosis of public spaces taking data captured from existing live urban cameras. UDE solves the main needs for three important market segments: 1) Smart Cities, where there exist a loss of profitability in many shops and real estate assets caused by saturation of public spaces, lack of use or insecurity; 2) Commerce, lacking precise urban data to help in the location of stores or measure the impact of window displays, urban ads or digital screens; 3) Security (detect urban terrorism, suspicious behaviour and insecure spots). To cope with these needs we have developed three product lines: Urban Public Eye (up to 30% effectiveness in urban decision-making and 1.5% reduction in GHG), Urban Business Eye (+50% gain in marketing campaigns) and Urban Security Eye (predict over-crowding and dangerous situations). Success cases developed at the Callao Square in Madrid and Market Square in Pittsburgh prove the current TRL6 stage. During the Feasibility Study we will perform a technical, commercial and financial feasibility assessment, so as to define the requirements to enhance the predictive models and the cloud analytics functionality, and make a platform scalability study for each market segment. Regulation, distribution channels and IPR issues will also be addressed, along with detailed economic projections and analysis of funding requirements. Regarding benefits to society, accurate urban diagnosis will be fundamental in achieving the 17 Sustainable Development Goals of the 2030 Agenda for Sustainable Development. To cope with this challenge, UDE addresses Goal 11, by making cities and human settlements inclusive, safe and sustainable.
Consortium	Coordinator: Urban Data Eye SL (ES)

4.1.4 Protection of Public Spaces

Some ISF projects are relevant to this newly added theme.

STEPWISE	
Title	A Simulation, Training, and Evaluation Platform for the Protection of Crowded Public Spaces *This project is also relevant for 6.1 Terrorist Threats*
Objective	Deliver an innovative product to support the cooperation, coordination, and cross-sectoral preparedness of Law Enforcement Agencies and their partners (public and private) involved in the design and protection of public spaces
Contract details	ISFP-2017-AG-PROTECT; 1/11/2018 – 31/10/2020; EUR 2.108.704,64
Abstract	STEPWISE will deliver an innovative product to support the cooperation, coordination, and cross-sectoral preparedness of Law Enforcement Agencies and their partners (public and private) involved in the design and protection of public spaces. The STEPWISE platform aims to enable the rapid creation of Virtual Reality mock-ups of real-world spaces and buildings where security and crisis plans can be devised and assessed against a wide variety of threat scenarios. STEPWISE brings innovative security design without claiming the public space and bothering or frightening populations: The STEPWISE immersive approach helps police experts to work on simulated situations with private security officers, fire crews, urban planners, public space operators, city managers, etc. to assess the vulnerability of public spaces and jointly develop and evaluate strategies to improve both their security and resilience without having to descend upon each of them.The STEPWISE action aims to industrialise the research prototype resulting from the VASCO FP7 project to deliver an operational product that will be extremely useful to implement the EU's action plan for the protection of public spaces. In addition, an innovative training programme will be prepared to foster its rapid adoption across Europe's practitioner community.

SafeCi	
Title	Safer Space for Safer Cities *This project is also relevant for 6.1 Terrorist Threats.*
Objective	Enhance the protection of public spaces, urban areas and other soft targets via the exchange of best practice
Contract details	ISFP-2017-AG-PROTECT; 1/1/2019 -31/12/2020; EUR: 594.028,10
Abstract	The two-year project "Safer Space for Safer Cities" ("SafeCi") aims at enhancing the protection of public spaces, urban areas and other soft targets via the exchange of best practice. Of particular interest is the increase in the protection against existing and new threats. The project has a clear European dimension, as ten European police forces declared their interest in participating by signing a letter of intent. The exchange of best practice, lessons learnt and innovative ideas will take place during three workshops with attendees of all project partners as well as external experts. Furthermore, peer reviews (study visits at the sites of all project partners) will be organised. The results of the workshops and, following an interview questionnaire, the results of the peer reviews will be fed into a handbook, which will include best practice, innovative concepts as well as recommendations. The dissemination of the handbook to all Member States of the European Union during the final conference will assure the sustainability of the project results. Dissemination activities through the social media channels of the Berlin Police will reach the general public and enhance the citizens' sense of security. In addition, the project will strengthen mutual trust among the police forces' specialists and lead to the development of a network between the project partners. The project partners will optimise their business processes according to the project results, e. g. as regards a fast and comprehensive cross-sectoral cooperation, efficient internal and external communication processes and other processes enhancing the security of public spaces. The established bonds between them will ensure further exchange and business process optimisation. Consequently, the results and outcomes of the planned activities will lead to a better protection of public places and will impact beyond the end of the project.

SECUR-CITIES	
Title	Prévention et sécurité dans les espaces publics des villes européennes *This project is also relevant for 6.1 Terrorist Threats*
Objective	Secur'Cities va se focaliser sur les lieux de grands rassemblements et leurs abords, et développer une approche dynamique et globale de la protection, pour prendre en compte le caractère mobile des attaquants et la gestion de nombreuses manifestations programmées au même moment
Contract details	ISFP-2017-AG-PROTECT; 1/1/2019 – 31/12/2021; EUR: 3.086.688,92
Abstract	Le projet Secur'Cities, conduit par les villes de Lyon et Barcelone, vise à renforcer les mesures de protection mises en œuvre sur l'espace public par l'ensemble des acteurs luttant contre les attaques terroristes. Il va s'attacher à prévenir l'attaque terroriste en la rendant moins facile, moins mobile et en limitant le nombre de victimes potentielles, grâce à la parfaite maîtrise de l'environnement (depuis la planification jusqu'à l'équipement). L'achat de matériels amovibles permettra une adaptation en fonction de la configuration de la manifestation. Ils perturberont aussi la préparation d'actes terroristes lors de repérages. Nous optimiserons l'observation et la détection des attitudes ou situations suspectes lors de la mise en place de filtrages et en recourant aux systèmes vidéo d'identification et de recherche. Il s'agit enfin, d'organiser l'alerte de manière efficace pour assurer une évacuation rapide des personnes en première ligne, et de sécuriser les autres en cas de progression des assaillants. La coordination des différents types d'opérateurs et la fluidité dans la chaîne de décision participent du même souci : limiter au maximum l'espace et le temps captés par l'action de terroristes et, au final, sauver des vies. Secur'Cities va se focaliser sur les lieux de grands rassemblements et leurs abords, et développer une approche dynamique et globale de la protection, pour prendre en compte le caractère mobile des attaquants et la gestion de nombreuses manifestations programmées au même moment. Toutes ces réflexions seront initiées par la recherche d'un partage d'expériences avec les villes européennes mobilisées sur ces sujets. Nos résultats seront ensuite diffusés auprès des villes européennes partageant les mêmes ambitions, et désireuses que leur population conserve leur qualité de vi(ll)es. Nous organiserons un colloque européen, invitant des experts internationaux, pour partager les acquis et poursuivre la réflexion de manière commune à long terme.

PACTESUR	
Title	Protect Allied Cities against TErrorism in Securing Urban aReas *This project is also relevant for 6.1 Terrorist threats.*
Objective	Empower cities and local actors in the field of security of urban public spaces facing terrorist threats
Contract details	ISFP-2017-AG-PROTECT; 1/1/2019 – 31/12/2021; 3.222.188,37
Abstract	PACTESUR aims to empower cities and local actors in the field of security of urban public spaces facing terrorist threats. Through a bottom-up approach, PACTESUR federates local decision makers, security forces, urban security experts, urban planners, IT developers, trainers, front-line practitioners, designers and others in order to shape new European local policies to secure public spaces against terrorist attacks. It is based on four pillars: the reflection on standards, legal frames and local governance; the development of specialised training for local security operators; the awareness-raising of citizens and politicians on their role on prevention and as security actors; the identification of the most adapted local investments for securing open and touristic public spaces by sharing field experience. PACTESUR involves three flagship cities (Nice, Torino, Liege) committed to strengthening their cooperation and having convergent strategies on urban security and an important number of municipalities directly engaged as follower cities (at least 10) or reached by the project dissemination activities within the European Forum for Urban Security. Main project activities are: the setting up of local demonstrator sites equipped to prevent and promptly react to terrorist threats while preserving the urban environment; the deployment of transnational training programmes for local security operators; the elaboration of common standards, response protocols and soft laws. The main project outcome is a well-structured framework defining how cities and local police forces can better protect their vulnerable public spaces and citizens. In order to feed the work that DG Home has launched, PACTESUR will draw conclusions from lessons learnt and create training materials for security forces, information tools for citizens and guidelines for local authorities to build up better knowledge on how to design better policies to secure public spaces..

PRoTECT	
Title	Public Resilience using TEchnology to Counter Terrorism *This proejct is also relevant for 6.1 Terrorist threats and 6.4.5 Support to law enforcement*
Objective	Strengthen local authorities' capabilities in Public Protection by putting in place an overarching concept where tools, technology, training and field demonstrations will lead to situational awareness and improve direct responses to secure public places pre, in, and after a terrorist threat
Contract details	ISFP-2017-AG-PROTECT; 1/11/2018 – 31/10/2020; 1.457.821,50
Abstract	The PRoTECT project aims to strengthen local authorities' capabilities in Public Protection by putting in place an overarching concept where tools, technology, training and field demonstrations will lead to situational awareness and improve direct responses to secure public places pre, in, and after a terrorist threat. This cross sectoral project is an initiative of the Core group of the European Network of Law Enforcement Technology Services (ENLETS). The main outcomes of the project are, as follows: Risk and Cost reduction, Developing training materials related to the protection of public spaces for municipalities and LEAs and Putting in place and implementing a pan European technology capability assessment tool for cities. Initiated by ENLETS, the PRoTECT project will support the policy of the European Commission by providing local actors -the cities in Europe- with guidance, training and awareness on the usage of technology as an indispensable tool for a secure municipality. It will -in close cooperation with DG Home and the European Forum for Urban Security (EFUS) - use the developed Commission's Soft Target Site Assessment tool, and it will provide the Policy group, the Commission, the Practitioners network and the to be established Operators Forum with tangible results, such as valuable feedback and practical recommendations based on the technology and soft target site assessment tool.

Pericles	
Title	Pericles: preventing vehicle ramming attacks *This project is also relevant for 6.1 Terrorist threats.*
Objective	Improving physical security measures in vulnerable public spaces as well as the knowledge and skills of law enforcement on how to respond to vehicle-ramming attacks
Contract details	ISFP-2017-AG-PROTECT; 1/1/2019 – 31/12/2021; EUR 2.349.677,20
Abstract	Vehicle-ramming attacks against human targets in public spaces constitute still a threat. Therefore measures need to be taken in order to prevent such attacks and to safeguard European citizens. Currently some initiatives are ongoing but are mainly focused on installing temporary vehicle barriers. The general objective of the PERICLES project is to better prevent and respond to vehicle-ramming attacks by improving physical security measures in vulnerable public spaces as well as the knowledge and skills of law enforcement on how to respond to vehicle-ramming attacks. The project will also raise the awareness of the public on how to react in case of such an attack. In order to achieve the general objective of the Pericles project, the project will develop a comprehensive European vulnerability tool that will allow local authorities to assess their local public spaces. Secondly, in order to improve the physical security of public spaces a white book will be edited. This white book will be edited listing different possible physical security measures and create new ones. This will be done by bringing together European specialist in the field of security as well as urban landscaping in order to exchange good practices and ideas. There will be a focus on security by design in which aesthetics and the public, open and economic nature of public spaces are taken into account in order to minimize the impact on society the public as well as economic nature of public spaces. The project aims also at improving the knowledge and skills of EU LEA's on how to respond to vehicle-ramming attacks. A focus will be laid on SIU's and first line police officers. Hereby we will not only focus on neutralizing the terrorists but also on bringing EU citizens into safety. Lastly, a public awareness campaign for the members of the general public will be created. This information campaign will inform EU-citizens about what to do when a vehicle-ramming attacks occur.

4.2 Critical Infrastructure Sectors

4.2.1 Critical Energy Infrastructure: Electrical Power (Electricity) and Smart Grids, Oil, Gas

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Critical Energy Infrastructure: Electrical Power (Electricity) and Smart Grids, Oil, Gas	AFTER ARGOS CYPRES DEFENDER E-LOCKS EURACOM INSPIRE INSPIRE-INTERNATIONAL LineVu MEREPUV MIMODETECT MONOFFSHORE NANO OMIS ReCETT Safe2LPG SCISSOR SESAME SEGRID SHEER SPARKS SPEAR SUCCESS PRECISE TM Field Analyzer VIKING

These projects were complemented in the H2020 framework by the following projects funded by the Secure Societies programme:

SecureGas	
Title	SecureGas *This project is also relevant for 1.1.2 Multi-hazard risk reduction, preparedness, resilience enhancement and 4.1.3 Cyber and physical threats to urban critical infrastructures and urban soft targets.*
Objective	Provide methodologies, tools and guidelines to secure existing and incoming gas network installations and make them resilient to cyber-physical threats
Contract details	H2020-SU-SEC-2045; Topic code: SU-INFRA01-2018-2019-2020 ; 1/6/2019 - 31/5/2021; EUR 6 993 400,76
Abstract	SecureGas focuses on the 140.000Km of the European Gas network covering the entire value chain from Production to Distribution to the users, providing methodologies, tools and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats. Three business cases, addressing relevant issues for the Gas sector and beyond (e.g. oil), have been identified so that to ensure the delivery of solutions and services in line with clear needs and requirements, focused on: risk-based security asset management of gas transmission and distribution networks; impacts (economic, environmental and social) and cascading effects of cyber-physical attacks on interdependent and interconnected European Gas grids; integrity and security, through the operationalization of resilience guidelines, of strategic installations across the EU Gas network. SecureGas tackles these issues by implementing, updating, and incrementally improving extended components, integrated and federated according to an High-Level Reference Architecture built upon the SecureGas Conceptual Model, a blue print on how to design, build, operate and maintain the EU gas network to make it secure and resilient against cyber-physical threats. The components are contextualized, customized, deployed, demonstrated and validated in each business case, according to the scenarios defined by the end-users. Related services provided by SecureGas will be offered to the end-users via a Platform as a Service (PaaS), that allows modularity, flexibility, cooperation and third-party interoperability, thus securing a long-lasting impact, supporting the project exploitation strategy. A multidisciplinary consortium (Gas operators, technology providers, research institutions, sector-related associations), supports the project implementation across Construction, Demonstration and Validation phases, as well as a Stakeholder Platform ensures inputs, advise, and a wider Diffusion of the project outcomes.
Consortium	Coordinator: 1. Rina Consulting Spa (IT) Consortium: 2. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 3. Leonardo - Societa Per Azioni (IT) 4. Kentro Meleton Asfaleias (EL) 5. Dimosia Epikhirisi Aerii Anonimi Etairia (EL) 6. Eni Spa (IT) 7. Guardtime As (EE) 8. Wings Ict Solutions Information & Communication Technologies Ike (EL) 9. Idemia Identity & Security Germanyag (DE) 10. Ab Amber Grid (LT) 11. Adpm Drones Srl (LT) 12. Rigas Tehniska Universitate (LV) 13. Elbit Systems Land And C4i Ltd (IL) 14. Jrc -Joint Research Centre- European Commission 15. Exus Software Monoprosopi Etairia Periorismenis Evthinis (EL) 16. Gap Analysis Societe Anonyme Risk And Environmental Quality Ae (EL) 17. Innov-Acts Limited (CY) 18. Agenzia Per La Promozione Della Ricerca Europea (IT) 19. Technologicka Platforma Energetickabezpecnost Cr Zs (CZ) 20. Etaireia Dianomis Aeriou Attikis Anonymi Etaireia (EL) 21. D.M.A.T. Consulting Kg (AT)

InfraStress	
Title	InfraStress *This project is also relevant for 4.1.3 Cyber and physical threats to urban critical infrastructures and urban soft targets.*
Objective	Develop an integrated framework including cyber and physical threat detection, integrated C/P Situational Awareness, Threat Intelligence, and an innovative methodology for resilience assessment
Contract details	H2020-SU-SEC-2046; topic code: SU-INFRA01-2018-2019-2020 ; 1/6/2019 - 31/5/2021; EUR 7 999 622,88
Abstract	InfraStress addresses cyber-physical (C/P) security of Sensitive Industrial Plants and Sites (SIPS) Critical Infrastructures (CI) and improves resilience and protection capabilities of SIPS exposed to large scale, combined, C/P threats and hazards, and guarantee continuity of operations, while minimizing cascading effects in the infrastructure itself, the environment, other CIs, and citizens in vicinity, at reasonable cost. In fact, InfraStress will develop TRL4+ solutions from preceding research and innovation towards TRL7 level producing maximum adoption of the proposed methods and solutions. Addressing the current fragmentation of available security solutions and technology, InfraStress will provide an integrated framework including cyber and physical threat detection, integrated C/P Situational Awareness, Threat Intelligence, and an innovative methodology for resilience assessment – all tailored to each site. InfraStress adopts a user-driven approach carried out through: a) delivery of usable and user-friendly Services and Applications for C/P protection and resilience; b) technical activities driven by and receiving active input from end users, i.e. SIPS and relevant stakeholders; c) a comprehensive set of 5 real-world Pilots and Evaluation activities to be carried out by User partners. InfraStress matches key impacts not only in response to the Work Programme Call but also at Strategic, Socio-economic and Market levels. In fact InfraStress was conceived since the beginning with a strong business vision in mind and will carry out effective exploitation actions ensureing successful go-to-market. Tailored activities are also planned to rise a a culture of participatory security to involve all stakeholders including companies, workers, public authorities, citizens and civil society.
Consortium	Coordinator: 1. Engineering - Ingegneria Informatica Spa (IT) Consortium: 2. Motor Oil (Hellas) Diilistiria Korinthou Ae (EL) 3. Attilio Carmagnani Ac - Societa Per Azioni (IT) 4. Sgl Composites, S.A. (PT) 5. Petrol Slovenska Energetska Druzba Dd Ljubljana (SL) 6. Depuy (Ireland) Unlimited (IE) 7. Luka Koper, Port And Logistic System, D.D. (SL) 8. Municipio Do Barreiro (PT) 9. European Virtual Institute For Integrated Risk Management Eu Vri Ewiv (DE) 10. Consorzio Interuniversitario Nazionale Per L'informatica (IT) 11. Rina Consulting Spa (IT) 12. Steinbeis Advanced Risk Technologies Gmbh (DE) 13. Inov Inesc Inovacao - Instituto De Novas Tecnologias (PT) 14. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 15. Dr Frucht Systems Ltd (IL) 16. United Technologies Research Centre Ireland, Limited (IE) 17. Satways - Proionta Kai Ypiresies Tilematikis Diktyakon Kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis Epe (EL) 18. National Observatory Of Athens (EL) 19. Holo-Industrie 4.0 Software Gmbh (DE) 20. G & N Silensec Ltd (CY) 21. Institut Jozef Stefan (SL) 22. Stam Srl (IT) 23. Uniwersytet Technologiczno Przyrodniczy Im Jana I Jedrzeja Sniadeckich W Bydgoszczy (PL) 24. Institut Za Korporativne Varnostne Studije Ljubljana (SL) 25. Atrisc (FR) 26. Din Deutsches Institut Fuer Normung E.V. (DE) 27. Katholieke Universiteit Leuven (BE)

4.2.2 Critical Transport / Transportation Infrastructure

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Critical Energy Infrastructure: Electrical Power (Electricity) and Smart Grids, Oil, Gas	CONSORTIS DEMASST INFRA-NAT ISTIMES PROTECTRAIL SAFE-10-T SAFERtec SECRET SECUR-ED SENSKIN SERON SF-TLS STAR-TRANS TRANSRISK Tunnelsafe2020

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

PREVENT	
Title	PREVENT
Objective	Enable earlier detection of terrorists and potentially dangerous objects, tracking of detected individuals or situations and coordinating the response of security forces
Contract details	H2020-SU-SEC-2029; Topic code: SU-GM02-2018-2019-2020; 1/5/2019 - 31/7/2020; € 1 894 305
Abstract	PREVENT focuses on pre-empting attacks in public transport by enabling earlier detection of terrorists and potentially dangerous objects, tracking of detected individuals or situations and coordinating the response of security forces. This focus is shared, from the start, by 22 organisations from 10 countries, public transport operators, security forces, public buyers, city authorities of which 12 are consortium partners and 10 are members of the PREVENT User Observatory Group (UOG). PREVENT implements a progressive and iterative process to deliver 6 jointly defined Common Security Scenarios that capture threats and vulnerabilities. It also delivers a vulnerabilities and threats taxonomy directly applicable to the public transport world. For these scenarios, PREVENT undertakes a gap analysis between available solutions, existing standards, on-going research and identified needs, from which it elaborates a multi-dimensional roadmap of innovations and solutions. The roadmap is an online interactive tool that feeds the sustainability of PREVENT's community. The highest priority innovations in the roadmap are selected by practitioners and public buyers to define a Common Challenge. This Common Challenge serves as the basis for a PCP, for which the buyers' group is created, the lead buyer is selected, tender documents are generated. PREVENT includes a governance mechanism that ensures that the different phases are open to additional practitioners and public buyers. PREVENT includes a Security Advisory Board to manage the confidentiality of the sensitive knowledge generated by its activities, and a GDPR advisor to guide the elaboration of a Common Challenge fully compliant with Europe's privacy and data protection regulations. PREVENT structures its governance and results (public and confidential) to foster sustainability of the collaboration beyond the end of the project.
Consortium	Coordinator: 1. Engineering - Ingegneria Informatica Spa (IT) Consortium: 2. Conseil Regional Provence Alpes Cote D'azur (FR) 3. Kentro Meleton Asfaleias (EL) 4. Stowarzyszenie Polska Platforma Bezpieczenstwa Wewnetrznego (PL) 5. Societe Des Transports Intercommunaux De Bruxelles Ssf (BE) 6. Pkp Szybka Kolej Miejska W Trojmiescie (PL) 7. Sncf (FR) 8. Hellenic Railways Organization Ae (EL) 9. Union Internationale Des Transports Publics (BE) 10. Ayuntamiento De Sevilla (ES) 11. Hellenic Police (EL) 12. Ministry Of Public Security (IL) 13. Departament D'interior - Generalitat De Catalunya (ES) 14. Corvers Procurement Services Bv (NL) 15. Istituto Italiano Per La Privacy (IT) 16. Instytut Technologii Bezpieczenstwa Moratex (PL)

This overview is complemented by projects funded by ISF.

SHERPA	
Title	Shared and coHerent European Railway Protection Approach *This project is also relevant for 6.1 Terrorist threats.*
Objective	Improve the overall protection level for stations and trains in Europe against terrorist attacks by implementing multiple synergistic actions towards the relevant stakeholders
Contract details	ISFP-2017-AG-PROTECT; 1/11/2018 – 31/10/2020; EUR: 940.669,10
Abstract	The SHERPA project aims at improving the overall protection level for stations and trains in Europe against terrorist attacks by implementing multiple synergistic actions towards the relevant stakeholders, such as: providing and sharing an up-to-date, high-value knowledge base on threats and countermeasures (both technical and procedural); defining a coherent approach for risk assessment, risk management, crisis and disaster recovery management; strengthening co-operation among stakeholders through high-level international trainings and other practical tools; outlining needs and requirements for industry and research to focus on to better help railways in coping with both present and future threats. Five among the most relevant key-players in the European railway sector (DB, FS, PKP, SNCB, SNCF) take part as co-applicants in the SHERPA project proposal: their joint participation brings it to the highest levels of credibility, representativeness and authoritativeness. Furthermore, the consortium itself is led by UIC, whose aggregative nature, together with its solid expertise and experience in participating and leading European projects, may favour synergies among the co-applicants and between them and police, first responders and other relevant stakeholders represented in the Advisory Board such as CER, COLPOFER, and RAILPOL.

4.2.3 Critical Water Infrastructure

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Critical Water Infrastructure	BactiLine LIFE CLEAN UP LIFE-EMPORE ProbSenS SEGU STOP-It Tunnelsafe2020 VIGI-LEAK

This overview is complemented by a H2020 project.

SCOREwater	
Title	Smart City Observatories implement REsilient Water Management *This project is also relevant for 4.4.1 Resilience of urban built environments, including cultural heritage.*
Objective	Enhance the resilience of cities against climate change and urbanization by enabling a water smart society that fulfils SDGs 3, 6, 11, 12 and 13 and secures future ecosystem services
Contract details	H2020-SC5-2018-2; 1/5/2019 - 30/4/2023; EUR: 4.998.727,50
Abstract	SCOREwater focuses on enhancing the resilience of cities against climate change and urbanization by enabling a water smart society that fulfils SDGs 3, 6, 11, 12 and 13 and secures future ecosystem services. We introduce digital services to improve management of wastewater, stormwater and flooding events. These services are provided by an adaptive digital platform, developed and verified by relevant stakeholders (communities, municipalities, businesses, and civil society) in iterative collaboration with developers, thus tailoring to stakeholders' needs. Existing technical platforms and services (e.g. FIWARE, CKAN) are extended to the water domain by integrating relevant standards, ontologies and vocabularies, and provide an interoperable open-source platform for smart water management. Emerging digital technologies such as IoT, Artificial Intelligence, and Big Data are used to provide accurate real-time predictions and refined information. We implement three large-scale, cross-cutting innovation demonstrators and enable transfer and upscale by providing harmonized data and services. We initiate a new domain "sewage sociology" mining biomarkers of community-wide lifestyle habits from sewage. We develop new water monitoring techniques and data-adaptive storm water treatment and apply to water resource protection and legal compliance for construction projects. We enhance resilience against flooding by sensing and hydrological modelling coupled to urban water engineering. We will identify best practices for developing and using the digital services, thus addressing water stakeholders beyond the project partners. The project will also develop technologies to increase public engagement in water management. Moreover, SCOREwater will deliver an innovation ecosystem driven by the financial savings in both maintenance and operation of water systems that are offered using the SCOREwater digital services, providing new business opportunities for water and ICT SMEs.
Consortium	Coordinator: 1. Ivl Svenska Miljoeinstitutet Ab (SE) Consortium: 2. "Fundacio Institut Catala De Recerca De L'aigua (ES) 3. Fundacio Eurecat (ES) 4. Institut D Estudis Metropolitans De Barcelona (ES) 5. Scan Iberia Sistemas De Medicion Sl (ES) 6. Talkpool Ab (SE) 7. Swedish Hydro Solutions Ab (SE) 8. Goteborgs Kommun (SE) 9. Civity Bv (NL) 10. Gemeente Amersfoort (NL) 11. Stichting Future City (NL) 12. Barcelona Cicle De L'aigua Sa (ES) 13. Hydrologic Research Bv (NL) 14. Universeum Ab (SE)"

4.2.4 Critical Finance Infrastructure

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Critical Finance Infrastructure	Loca Credibilia FINSEC REDSENTRY

In this iteration of the CoU Mapping Document, no new projects related to critical finance structure were identified.

4.3 Risk assessment and monitoring

4.3.1 Multi-sector cyber and physical threats to critical infrastructures, including ICT

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multi-sector cyber and physical threats to critical infrastructures, including ICT	ATENA CITADEL CIPSEC CorreAssess CyberWiz DAPS HIPOW INSPIRE MICIE SAFURE POLARIS PRECYSE PROGRESS RESISTO SAFECARE SAURON SealedGRID SecTrap SECRIT RESPONSE 5G SERENITI SERSCIS SPARKS STRUCTURES VIKING V-SPHERE WSAN4CIP

In this iteration of the CoU Mapping Document, no new projects related to Multi-sector cyber and physical threats to critical infrastructures, including ICT were identified.

4.3.2 Cascading effects from natural disasters related to critical infrastructures

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Effects from natural disasters related to critical infrastructures	SECRIT SERSCIS RESPONSE 5G ResFrameFireSeismic

In this iteration of the CoU Mapping Document, no new projects related to effects from natural disasters related to critical infrastructures were identified.

4.3.3 Multihazard assessment, stress tests

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multihazard assessment, stress tests	CIPRNET HIPOW INFRARISK STREST STRUCTURES VIKING

4.3.4 Remote monitoring and surveillance tools / technologies

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Remote monitoring and surveillance tools/technologies	ALLADIN ARENA BASYLIs ePatriot GaSeS Invest KNOX LIFE SENSSEI PATH PROTECT-2 ROBIN SafeSky SMS Starlight SOLOMON SURVEIRON Theseus UAN UPAC S-100

This overview is complemented by one relevant H2020 project.

POSPORI	
Title	Polymer Optical Sensors for Prolonged Overseeing the Robustness of civil Infrastructures
Objective	Accelerate the deployment and use of polymer optical fibre Bragg grating (POFBG) sensing technology for prolonged overseeing the robustness of civil infrastructures
Contract details	H2020/MSCA/IF/2018; 19/6/2019 - 18/6/2021; EUR 157 941,12
Abstract	The POSPORI project is dedicated to accelerating the deployment and use of polymer optical fibre Bragg grating (POFBG) sensing technology for prolonged overseeing the robustness of civil infrastructures. The two key research objectives are to develop optical fibre sensing systems to assess the stability of (i) reinforced concrete and (ii) reinforced soil structures, which are the key elements for safe construction in civil engineering. The project seeks to take a significant step beyond the current technology readiness level and enhance the creative and innovative potential of experienced researcher (Andreas Pospori) in the field of optical fibre sensors.
Consortium	Coordinator: Technologiko Panepistimio Kyprou (CY)

4.3.5 Detection, prevention of intruders; Access Control

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Detection, prevention of intruders; Access Control	ARIA CRISALIS IDETECT 4ALL IMPRINT iNTACT OneCard RIBS WARDIAM PERIMETER

In this iteration of the CoU Mapping Document, one project categorised under another theme is also relevant for Detection, prevention of intruders; Access Control, namely: EU HRS Network

4.4 Resilience

4.4.1 Resilience of urban built environments, including cultural heritage

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Resilience of urban built environments, including cultural heritage	Adapt Northern Heritage BESECURE CLARITY DESURBS DUST ECOSSIAN ELASSTIC EPICURO EU-SEC II HARMONISE LightningPro LIQUEFACT NOTE SPIRIT ProteCHt2save PUCS RESCULT SEE URBAN THE HOUSE VASCO VITRUV Warmest UD-RASP

This overview is complemented by a project funded by DG ECHO.

CULTURE CANNOT WAIT	
Title	Protecting Cultural Heritage from the Consequences of Disasters
Objective	Develop a common European methodology along with standard operating procedures for protecting cultural heritage during emergencies
Contract details	2018/PREP/826517; 1-1-2019 – 31-12-2020; EUR: 599.307,00
Abstract	The project aims at developing a common European methodology along with standard operating procedures for protecting cultural heritage during emergencies; promoting the development of preparedness arrangements in this sector in a number of UCPM participating States; creating a multi-national, multi-stakeholder and multi-sectoral asset able to provide guidance to interested States for developing preparedness measures for the protection of cultural heritage during emergencies and to intervene globally, in case of international emergency, to support national response efforts of affected countries in this sector.
Consortium	Coordinator: 1. Presidenza Del Consiglio Dei Ministri – Dipartimento Della Protezione Civile (IT) Consortium: 2. Fondazione Hallgartenfranchetti Centro Studi Villa Montesca (IT) 3. International Centre For The Study Of The Preservation And Restoration Of Cultural Property (IT) 4. Ministere De L'interieur (FR) 5. Consejeria De Cultura Y Turismo De La Junta De Castilla Y Leon (ES) 6. Basbakanlik Afet Ve Acil Durum Yonetimi Baskanligi (TR)

This overview is complemented by the following Erasmus+ project.

Building Resilient Urban Communities	
Title	Building Resilient Urban Communities
Contract details	599312-EPP-1-2018-1-UA-EPPJMO-PROJECT; 1/9/2018 – 31/8/2020; EUR: 60.000
Abstract	The project 'Building Resilient States and Societies: EU's Response to New Security Challenges in the European Neighbourhood Area' aims to bridge a major gap in knowledge and understanding of current and new threats in Eu-rope's strategic orbit and contribute to development of research-led teaching and evidence-based policy making in European Security Studies by considering theoretical and practical issues relating to security cooperation between the EU and its neighbourhood.
Consortium	Coordinator: Public Organisation Ukrainian Institute Of Crisis Management And Conflict Solution (UA)

This overview is complemented by the following H2020 project.

RAMBEA	
Title	Realistic Assessment of Historical Masonry Bridges under Extreme Environmental Actions *This project is also relevant for 1.2.1 Multi-Climate hazard risk prevention, awareness, preparedness, resilience.*
Objective	Develop a novel computational strategy for accurate and efficient simulations of historical masonry bridges subject to extreme environmental actions, including loadings induced by earthquakes and flooding
Contract details	H2020-MSCA-IF-2018 1/9/2019 - 31/8/2021; EUR: 224.933,76
Abstract	The RAMBEA project will develop a novel computational strategy for accurate and efficient simulations of historical masonry bridges subject to extreme environmental actions, including loadings induced by earthquakes and flooding. The aim is to provide a comprehensive tool for realistic assessment with the potential of transforming current practice related to strengthening of critical assets, contributing to an increased resilience of the built environment and the preservation of important elements of the architectural heritage, thus responding to the safety and socio-economic needs highlighted in Horizon 2020. Old masonry bridges still play a critical role within the European transportation system. Moreover, they belong to the architectural heritage representing a valuable expression of past construction technology. Many of these structures are located in seismic regions and in areas subject to floods and hydrogeological instability which have been aggravated by climate change. Thus they can be exposed to extreme environmental actions which may potentially lead to bridge failure causing significant economic damage and the loss of structures with cultural and historical value. Currently, the response of masonry bridges under extreme loading is evaluated using simplified models due to the lack of efficient detailed models. However, these approaches do not allow for the complex 3D behaviour potentially leading to unrealistic and unsafe predictions. The main challenge of this project is the development of a more advanced strategy, based on a novel numerical description allowing for the 3D interaction between the different bridge components under extreme loading. More specifically, I will develop an efficient 3D finite element representation with macro-elements for the masonry parts of the bridge, an accurate description for the physical interface between masonry and backfill and an effective model calibration strategy utilising the results of non-destructive tests.
Consortium	Coordinator: Imperial College Of Science Technology And MEDICINE (UK)

4.4.2 Critical Infrastructure Resilience

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Critical Infrastructure Resilience	COCKPITCI DARWIN IMPROVER INSPIRE PROGRESS RESILENS RESOLUTE SERENITI SERSCIS SmartResilience TRUEPIVOT

In this iteration of the CoU Mapping Document, no new projects related to Critical Infrastructure Resilience were identified.

5. CBRNE threats

The CBRN Action Plan as well as the Explosives Action Plan include various requirements regarding detection, surveillance and control, for example requirements for appropriate measures to ensure that security plans/ security management systems are in place in high-risk chemical facilities. Controls also concern the delivery of high-risk chemicals and equipment by chemical industry to legitimate users and licensing schemes in particular for Chemical Warfare Agents (CWA) precursors. In the radiological and nuclear areas, controlling measures are focused on e.g. the causes and consequences of the loss of control over radioactive sources, on current status of used and disused sources in the EU and transport patterns for legal uses of radioactive sources.

5.1 Major accident hazards

Related to the major accident hazards and its risk management, the Directive 2012/18/EU on major-accidents hazards involving dangerous substances sets a number of obligations both to the Member States (e.g., legislation, organisation of the Inspections, reporting to the EC, etc.) as well as to the industrial establishments. As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Major accident hazards	EU-SENSE HBM4EU INTeg-Risk LIFE CHEREE LIFE-FLAREX LIFE MATHER LIFE VERMEER MIRACLE NANOELECTROCHEM OILBLOCK SECURENV SNIFFER 2 TOSCA XP-RESILIENCE

In this iteration of the CoU Mapping Document, no new projects related to major accident hazards were identified.

5.2 Chemical threats

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following project was described.

Research sub-category	Project Acronyms
Major accident hazards	ChemSniff

This overview is complemented by the following H2020 project.

UCTIL	
Title	Urban Chemical Threat Location and Identification *This project is also relevant for 4.1.2 Detection of potential CBRN-E threats at urban soft targets/ urban critical infrastructures.*
Objective	Launch a product in the nascent Urban Chemical Threat Identification and Location (UCTIL) market by deploying a sensor network that can continuously monitor ambient air for multiple target compounds with high sensitivity and specificity
Contract details	H2020-SMEInst-2018-2020-1; 1/2/2019 - 31/7/2019; EUR: 50.000
Abstract	"Catch the bomb maker, not the bomb" reflects a paradigm change in security where threat detection methods allowing for preventive measures rather than localized checkpoint systems are deployed. The Brussels 2016 explosions, and recent use of military grade CWA in Salisbury UK have exposed vulnerabilities of our urban centers. Global terrorism, illicit drug distribution networks and foreign insurgent activities force governments to strengthen security measures to protect the population especially in metropolitan areas. We call this Urban Chemical Threat Identification and Location (UCTIL). Karsa intends to launch a product into the nascent UCTIL market by deploying a sensor network that can continuously monitor ambient air for multiple target compounds with high sensitivity and specificity. The base technology already exists and has been proven robust for ambient and mobile measurements. Continuously monitoring ambient air in a complex urban environment for low concentrations of many chemicals stretches the limits of state-of-the-art technology. However, Karsa is extremely well positioned to address this challenge because it originates from the world-leading institute in atmospheric sciences (INAR) that has revolutionized the way chemical composition of the atmosphere is studied. We are seeking support to conduct a feasibility study to further explore this opportunity and prepare a plan to address R&D and business related activities to be undertaken in a potential phase 2 project.
Consortium	Coordinator: Karsa OY (FI)

5.3 Biological threats

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Biological threats	ANTIBOTABE BIO-PROTECT EQUATOX EuroBioTox Glyco-DeCon MULTISENSE CHIP PLANTFOOSEC SPICED TWOBIAS

In this iteration of the CoU Mapping Document, no new projects related to biological threats were identified.

5.4 RN risk management

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are describe.

Research sub-category	Project Acronyms
RN risk management	COCAE DETECT LIFE ALCHEMIA MODES-SNM MULTIBIODOSE NARSIS NESPRINT NERIS-TP Illicit Trafficking Radiation Assessment Program + 10 phase II Round Robin Tests INSIDER PREPARE Radiation Detector REWARD SCINTILLA

This overview is complemented by the following Marie Skłodowska-Curie Actions project.

PLASTICERA	
Title	Plastic ceramic films to improve safety of modern nuclear energy *This project is also relevant for 5.1 Major accident hazards*
Objective	Develop a new accident tolerant fuel (ATF) concept for modern nuclear light water reactors (LWR)
Contract details	H2020/MSCA/IF/2018; 16/4/2019 - 15/4/2020; EUR 91 736,64
Abstract	Aim of the project PLASTICERA is to prevent nuclear accidents similar to Fukushima Daiichi from happening in Europe. Primary objective of PLASTICERA is to develop a new accident tolerant fuel (ATF) concept for modern nuclear light water reactors (LWR). Today, nuclear energy is an essential environmental issue as it is one of the key scalable technologies to battle climate change. Promoting the use of nuclear energy is largely based on public opinion and therefore creating safer and more sustainable ways to produce nuclear energy is more important than ever. The concept of PLACTICERA relies on amorphous oxide thin films to protect the primary fuel cladding from catastrophic damage during nuclear accident conditions. The oxide thin film can provide unique combination of a strong oxygen diffusion barrier with the capability to accommodate the plastic strain originating from the fuel bar thermal expansion. This functional coating could significantly delay the onset of uncontrollable degradation of the primary fuel cladding, allowing timely emergency cooling, and preventing the release of radioactive substances. The primary objective will be achieved by training Dr. Erkka J. Frankberg (fellow) with new skills in disruptive material manufacturing technologies capable of producing ceramic materials, especially amorphous oxides, with prerequisites for low temperature plasticity. These materials will then be tested for mechanical and corrosion properties in relevant environment resembling LWR normal operating conditions and conditions occurring during “loss of cooling water” (LOCA) -type accident.
Consortium	Coordinator: Fondazione Istituto Italiano Di Tecnologia (IT)

5.5 Explosives and their precursors

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Explosives and their precursors	ACES AIRS AVERT BONAS COMMONSENSE D-BOX EMPHASIS ENCOUNTER ENTRAP EXERTER HOMER I-MUST JEROME LOTUS Minimising insider threats within the supply chain of the precursors for explosives NASUM OPTIX PREVAIL ROSFEN SALIANT SENEX SUBCOP PyroProf TIRAMISU

This overview is complemented by ISF-funded projects.

EEODN Activities (training and expertise)	
Title	EEODN Activities (training and expertise) *This project is also relevant for 5.7 CBRNE (Cross-cutting)*
Objective	Reinforce the activities promoted by the EEODN both in explosives and CBRN areas of expertise
Contract details	ISFP-2016-AG-IBA-EEODN; 1/8/2017 – 31/7/2019; 298.074,60
Abstract	The overall objective of this programme is to reinforce the activities promoted by the EEODN both in explosives and CBRN areas of expertise, in order to further develop technical skills of the bomb technicians and the CBRN experts from Competent Authorities of the EU-MS dealing with different threats and new modus operandi.

iTplus	
Title	iTrace Plus: Support for the European Agenda on Security to provide field-based data on access to and the deployment of dangerous substances such as explosives by terrorist networks. *This project is also relevant for 6.1 terrorist threats*
Objective	Provide critical information to EU internal security organs and intelligence on supplies of material support to terrorist and criminal organisations
Contract details	ISFP-2017-AG-IBA-ITRACE; 1/12/2018 – 30/11/2020; 1.578.041,65
Abstract	The iTrace Plus Action will provide critical information to EU internal security organs and intelligence on supplies of material support to terrorist and criminal organisations, which have the potential to threaten EU internal security. The Action will provide information from areas well beyond the EU's borders—extending deep into conflict- and terrorism-affected regions of the world, which have previously proved opaque to European security scrutiny. Conflict Armament Research's (CAR) capacity to generate such information rests on its unparalleled access to frontline areas afflicted by war, organised crime, and terrorism, and a network of access agreements that CAR has built with national governments within the framework of the existing iTrace project (2013-present). CAR has consistently demonstrated its capacity to recover critical information on commercial products, including improvised explosive device (IED) parts and chemical precursors, used by groups such as AQIM and Islamic State. Many of these commodities originate in the EU. Their proliferation also poses critical threats to EU domestic security, which CAR's findings on bomb-makers, and bomb-making technologies underscore. The Action will enhance CAR's capacity to track supplies of explosives, precursors, improvised explosive device component parts, and the migration of bomb-makers, and bomb-making technologies. CAR will subsequently stream this information to EU internal security organs and processes, including inter alia: Europol, DG Home (including the Standing Committee on Precursors), DG Grow, and DG Trade. CAR will also facilitate security dialogues between institutions in key partner countries and relevant EU bodies on the aforementioned threats and responses.

XClanLab	
Title	Application for mobile devices to identify a clandestine laboratory for homemade explosives
Objective	Develop a mobile application for Android & IOS (A&O) to provide information on precursors for homemade explosives listed in Annex I&II of Regulation 98/2013
Contract details	IISFP-2017-AG-PROTECT; 1/12/2018 – 30/11/2021; EUR: 585.925,58
Abstract	XClanLab will develop a mobile application for Android & IOS (A&O) to provide information on precursors for homemade explosives listed in Annex I&II of Regulation 98/2013. This will include chemicals and equipment for improvised explosive devices and procedures to handle situations where homemade explosives are involved. Also a report function is included. The app will help MS authorities to increase awareness on Regulation 98/2013 within rescue services and provide them with a powerful tool to handle potentially dangerous situations professionally. The app will be available in sev. languages depending on demand. An important part is to establish a network of National Contact Points (NCPs) in as many MS as possible to ensure the distribution of the app. The network will also gather feedback and make recommendations on new/updated contents based on incidents in the MS.

5.6 Water Safety & Security

Water security threats are directly related to the risks of quality degradation, either from an user's viewpoint (quality of drinking water) or ecological standpoint (ecological or chemical water status). While intentional degradation of water quality is not specifically covered by EU water policies, the quality deterioration is nevertheless regulated by the Water Framework Directive and its parent directives dealing with drinking water, priority substances and groundwater. As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Water Safety & Security	AquaSHIELD BIWAS CyanoALERT EnviroALARM ISIS REGROUND SAFEWATER SECUREAU TAWARA_RTM WATERGUARD WATERPROTECT TIRAMISU

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

aqua3S	
Title	aqua3S
Objective	Standardise existing sensor technologies for drinking water safety, complemented by state-of-the-art detection mechanisms
Contract details	H2020-SU-SEC-2042; topic code: SU-DRS03-2018-2019-2020; 1/9/2019 - 31/8/2022; € 5 997 067,88
Abstract	Exposure of citizens to potential disasters has led to vulnerable societies that require risk reduction measures. Drinking water is one main source of risk when its safety and security is not ensured. aqua3S combines novel technologies in water safety and security, aiming to standardise existing sensor technologies complemented by state-of-the-art detection mechanisms. On the one hand sensor networks are deployed in water supply networks and sources, supported by complex sensors for enhanced detection; on the other hand sensor measurements are supported by videos from Unmanned Aerial Vehicles (UAVs), satellite images and social media observations from the citizens that report low-quality water in their area (e.g. by colorisation), creating also social awareness and an interactive knowledge transfer. Semantic representation and data fusion provides intelligent DSS alerts and messages to the public through first responders' mediums. The proposed technical solution is designed to offer a very effective detection system, taking into account the cost of the aqua3S platform and targets at very high return over investment ratio. A strategy for the insertion of aqua3S solution into the market is designed towards the standardisation of the proposed technologies and the aqua3S secure platform.
Consortium	Coordinator: 1. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) Consortium: 2. Vivaqua Scrl (BE) 3. Water Board Of Lemesos (CY) 4. Draxis Environmental S.A. (EL) 5. Sheffield Hallam University (UK) 6. Fyzikalni Ustav Av Cr V.V.I (CZ) 7. Mirsense (FR) 8. Autorita' Di Bacino Distrettuale Delle Alpi Orientali (IT) 9. Etairia Hydrefsis Kai Apochetefsis Thessalonikis Ae (EL) 10. The University Of Exeter (UK) 11. Acegasapsamga S.P.A. (IT) 12. Institut Po Otbrana (BU) 13. Suez Smart Solutions (FR) 14. Institute Of Communication And Computer Systems (EL) 15. Sofiyska Voda Ad (BU) 16. Everis Spain Sl (ES) 17. European Water Supply And Sanitation Technology Platform (BE) 18. Trilateral Research Limited (IE) 19. Vodosnabdyavane I Kanalizacya (BU 20. Region Of Central Macedonia (EL) 21. Azienda Unita Locale Socio Sanitaria N 2 Marca Trevigiana (IT) 22. Universitaet Stuttgart (DE) 23. Easy Global Market Sas (FR)

This overview is complemented by another H2020 project.

AIRWAVES	
Title	Automated high resolution water sampler for environmental monitoring
Objective	Further develop and explore commercialization pathways for new automated water sampling technology
Contract details	ERC-2018-PoC; 1/1/2019 - 30/6/2020; EUR: 149.711
Abstract	A new automated water sampling technology was developed under the ERC Consolidator Grant STEEPclim with the potential to revolutionize environmental monitoring worldwide. A changing climate and growing scarcity of water strongly increase the need of reliable standardized and highly automated environmental monitoring, thus creating a growing market for our innovative solution. Our first prototype successfully operated under field conditions. Now we seek funding to further develop this device and explore commercialization pathways. Today, rain water, river discharge and climate are monitored routinely with high temporal resolution using quality sensors, but no adequate automated technology for obtaining representative samples for laboratory grade analysis is available for weather services, hydromet offices, chemical industry or research institutions. So far taking, preserving and analyzing samples from natural waters is meticulous, labor intensive and expensive. Isotope signatures in water are ideal tracers of processes in the water cycle. Stable isotope analysis of precipitation can identify changing atmospheric circulation patterns and the origin of groundwater. They can also be used for the reconstruction of paleoclimate from ancient waters locked in geological archives. The analysis of fruits, food and drink products, of drugs, explosives and human remains is used to identify their regional provenance. For this purpose a robust understanding of the modern distribution of isotopes in space and time is indispensable. The autonomous and robust sampler introduced here is designed to fulfill the high demands on sampling and storage for isotope analysis. It is portable, has low power consumption and can be accessed remotely for maintenance and to adapt the sampling protocol strategy. The obtained water samples are not restricted to isotope analysis but can be used for any type of environmental water analysis.
Consortium	Coordinator: Helmholtz Zentrum Potsdam Deutschesgeoforschungszentrum Gfz (DE)

5.7 CBRNE (Cross-cutting)

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
CBRNE (cross-cutting)	ATOM EU AITRAP CATO CELECTIVE Coordinated trans-national training programme for prevention and mitigation of CBR release induced by non-state actors COUNTERFOG DAIMON DECOTESSC1 D-EMERSYS EDEN ENCIRCLE eNOTICE ERNCIP CBRN EU Police Intervention and Response Training Centre of Excellence STDS 16 HANDHOLD IMSK PRACTICE Preventing and fighting CBRN-E terrorism – building capacity of actors involved in the detection and mitigation of CBRN-E risks at air and road border crossings on European level ROCSAFE Shielding South-east Europe from CBRN-E threats SNIFFER 2 TOXI-TRIAGE

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

PROACTIVE	
Title	PROACTIVE *This project is also relevant for 8.3.2 Population alerting and 8.3.3 Public Protection*
Objective	Enhance societal CBRN preparedness by increasing Practitioner effectiveness in managing large, diverse groups of people in a CBRN environment
Contract details	H2020-SU-SEC-2031; Topic code: SU-FCT01-2018-2019-2020; 1/5/2019 - 30/4/2022; € 4 970 028,75
Abstract	In line with the EU Action Plan to enhance preparedness against chemical, biological, radiological and nuclear (CBRN) security risks and the overall Security Union approach to fight crime and terrorism, PROACTIVE aims to enhance societal CBRN preparedness by increasing Practitioner effectiveness in managing large, diverse groups of people in a CBRN environment. This will be achieved by testing common approaches between European Practitioners such as Law Enforcement Agencies (LEAs) and First Responders. These will be evaluated and validated against the requirements of civil society, including vulnerable groups of citizens reflected in the European Security Model. A Practitioner Stakeholder Advisory Board and a Civil Society Advisory Board will extend the representation of both sides in several surveys, focus-groups, workshops and field exercises. A benchmark study between LEAs will identify common approaches in assessing CBRN threats and the protocols and tools used to help citizens. Liaising with the eNOTICE H2020 project, three joint exercises will include role play volunteers recruited by PROACTIVE. They will evaluate the acceptability and usability of existing procedures and test new tools developed within PROACTIVE to provide innovative recommendations for Policy-makers and safety and security Practitioners. PROACTIVE will result in toolkits for CBRN Practitioners and for civil society organisations. The toolkit for Practitioners will include a web collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a mobile app. The toolkit for the civil society will include a mobile app adapted to various vulnerable citizen categories and pre-incident public information material. These will provide valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRN activities and help consolidate the EU Action Plan to enhance preparedness for CBRN threats.
Consortium	Coordinator: 1. UNION INternationale Des Chemins De Fer (FR) Consortium: 2. Cbrne Ltd (UK) 3. Ministry Of The Interior Of The Czech Republic (CZ) 4. Deutsche Bahn Ag (DE) 5. Inspectoratului General Pentru Situatii De Urgenta (RO) 6. Umea Universitet (SE) 7. Deutsche Hochschule Der Polizei (DE) 8. Rinisoft Ltd (BU) 9. West Midlands Police Authority (UK) 10. Eticas Research And Consulting Sl (ES) 11. State Emergency Service Of Ukraine (UA) 12. Department Of Health (UK) 13. Iekslietu Ministrijas Valsts Policija State Police Of The Ministry Of Interior (LV) 14. An Garda Siochana (IE) 15. Forsvarets Forskninginstitutt (NO)

This overview is complemented by ISF projects.

BULLSEYE	
Title	Harmonised procedures and awareness of all agencies involved in the response of a chemical or a biological terrorist attack: education- training and train the trainer. *This project is also relevant for 6.1 Terrorist threats and 5.3 Biological threats*
Objective	Improve the knowledge and skills of professionals in all EU member states on how to PREVENT terrorist attacks using CBRN agents and explosives by improving detection capabilities as well as on how to properly MITIGATE & RESPOND in case of an emerging CBRN attack
Contract details	ISFP-2017-AG-PROTECT; 1/4/2019 – 31/3/2022; 2.458.620,32
Abstract	The general objective of this project is to further improve the knowledge and skills of police and forensic officers as well as fire, medical and civil protection services in all EU member states on how to PREVENT terrorist attacks using CBRN agents and explosives by improving detection capabilities as well as on how to properly MITIGATE & RESPOND in case of an emerging CBRN attack. The knowledge and experience of the military services will be used to enforce the 'civil' procedures. In this proposal, the choice is made to focus on the Chemical (C) and Biological (B) threat. Nowadays the first responders of the EU countries use different procedures. Aim is to harmonize the different procedures on C and B through a gap analysis concerning the existing procedures and equipment. Next step will be the organization of expert meetings where the first responders exchange knowledge and procedures with well-chosen CBRNe experts (from civil services and armed forces). These harmonized procedures and other useful tools will be trained per group based on different procedures to be implemented during the terrorist attack or immediately after the attack (first responders – SWAT units, EOD teams, CBRN police teams, fire fighters, civil protection, DVI and forensics) and will be finally tested and evaluated in 1 cross -sectoral exercise. Taken the lessons-learnt into account of these trainings and exercise, the procedures and tools will be fine-tuned, adapted and validated. Finally, a train the trainer course is developed that can be used for all first responders, DVI and forensic officers of the EU countries.

CERBERUS	
Title	The establishment of the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit *This project is also relevant for 6.1 Terrorist threats.*
Objective	Establish the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit
Contract details	ISFP-2017-AG-PROTECT; 1/12/2018 – 30/11/2021; 3.132.762,05
Abstract	The CERBERUS project aims to establish the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit. This initiative will create and maintain a regional, mobile, first responder capability to address the threats posed by the illicit use of chemical, biological, radioactive and nuclear (CBRN) materials especially when they are combined with explosives devices (hereinafter: dirty bomb). Project CERBERUS will create a response capability and develop a unique cross-border and cross-sectoral cooperation and coordination mechanism for CBRN-E/dirty bomb first responders that currently does not exist within the European Union. This proposal is initiated by the dedicated agencies of Member States cooperating within the framework of the Central European CBRN-E Training Centre (hereinafter: Centre) namely: EKO Cobra of Austria, the Police Presidium of the Czech Republic, the Hungarian National Police Bomb Disposal Unit, the Presidium of the Police Corps of the Slovak Republic. In the Centre, consortium members have already maintained trusted professional relationship and having a mutual understanding in the current targets. The project also focuses on the professional CBRN-E knowledge maintenance as well, that includes the improvement of the training facilities of the Centre.The short-term beneficiaries of the project are CBRN-E experts who are involved in the establishment of the Unit. Mid-term beneficiaries are the police forces of the Central European countries cooperating within the Centre and will be trained and prepared for operating as Unit members. The long-term beneficiaries are the citizens of the EU Member States because the Unit will establish a CBRN-E/dirty bomb response capability that is currently missing within the EU and the availability of such asset highly contributes to the increased security of EU citizens.

DirtyBomb	
Title	Increased preparedness to CBRN incidents via first responders' joint exercises
Objective	Develop training materials for EU LEAs for dealing with "dirty bomb" terrorist attacks
Contract details	ISFP-2017-AG-PROTECT; 1/2/2019 – 30/4/2020; 420.419,05
Abstract	The project is focused on verifying preparedness of services, including realization police unit officers (RPUOs) from EU countries participating in exercises, on terrorist attacks with the use of the so-called "dirty bomb", identifying critical points to be improved and development of, on this basis, training materials for LEAs from EU, focusing primarily on the key issues identified during the exercises. The concept of exercises assumes gathering information from partners regarding schemes of conduct in their countries to a "dirty bomb" threat and then conducting activities according to the scenario and arrangements with partners in order to check the current state of preparation and practical knowledge of participants. Then, a training session will be held to discuss the mistakes and correct procedures. The next day we will carry out II exercises according to a similar scenario, using the discussed procedures. Both days of the exercises will be summed up, with a detailed discussion and consolidation of the right patterns of conduct. The expected and real impact of the activities is even better preparedness of first responders to CBRN incidents.Hard results consist of a scenario of exercises, exercises themselves with training and a summing-up conference, as well as specialized equipment to secure exercises. Soft results assume better preparedness of EU first responders, esp. LEAs to take proper actions in case of "dirty bomb" threat, including ensuring security for civilians in the endangered / contaminated area; as well as promotion of the programme and the project.

ECCOFEX	
Title	On the feasibility of the creation of a European CBRN Centre of Excellence *This project is also relevant for 6.8 Civil-military*
Objective	Feasibility study of developing a CBRN centre of excellence (ECCofEX) for the EU, through the development of a Concept of Operations (CONOPS) for such a centre
Contract details	ISFP-2017-AG-PROTECT; 1/11/2018 – 31/10/2021; 818.544,65
Abstract	This project proposal is a direct reaction to the European Parliament Resolution 2012/C 169 E/02 which calls for the establishment of a European crisis-response mechanism, based in the Commission's services, which should coordinate civilian and military means so as to ensure that the EU has a rapid response capability. It also addresses the need stated in the recently adopted CBRN action plan on reinforcing resilience against CBRN threats in terms of prevention, preparedness and response, which requires significant investments on the part of Member States and 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 general objective of this project is to conduct a study, in consultation with EU Member States and the Commission Services, into the feasibility of developing a CBRN centre of excellence (ECCofEX) for the EU through the development of a Concept of Operations (CONOPS) for such a centre. This project will also seek to create a business plan to identify how such a centre can be established and operated, taking into account/advantage of existing capabilities such as the EC ERCC and how the centre can network with existing EU mechanisms and external bodies. The project will run for 36 months and will take the form of surveys, interviews, workshops and meetings with relevant agencies in order to gather the information outlined in the work packages. This information will then be analysed by the project partners and will form the basis of the project deliverables. The project comprises several work packages: WP1: Project Management; WP2: Identification of opportunities to improve MS preparedness and response to CBRN (accidental/Intentional); WP3: inventory of reach-back capabilities, assets and experts available in the EU and could be available to other EU MS; WP4: inventory of FP6, FP7 and H2020 research outcomes; WP5 Proof of concept and WP6: Dissemination

MELODY	
Title	A harmonised CBRN training curriculum for first responders and medical staff
Objective	Define, develop and deploy a harmonized CBRN training curriculum for first responders and medical staff
Contract details	ISFP-2017-AG-PROTECT; 1/11/2018 – 31/10/2021; 3.103.481,50
Abstract	The main objective of this project proposal is to define, develop and deploy a harmonized CBRN training curriculum for first responders and medical staff, by medical staff it is meant ambulance drivers, paramedics and emergency room (ER) personnel. The objectives set out for the project will be achieved through 7 logically designed work packages (WPs), which cover the consultation with existing training facilities in the consortium, leading to a draft document, which will then through consultation with end-users/ practitioners will determine how far we are from the actual training needs. Additional effort will be spent in correcting the departures from the existing training material with respect to the actual practitioner's needs. The improved CBRN training curriculum will be assessed and evaluated through a number of dedicated exercises and training activities which will lead to a new set of improvements. A WP has been devoted to demonstration and dissemination activities. The former will deal with showcasing the final product through a set of full scale exercises, whereas the latter will be a continuous effort in raising awareness on the project and its activities at all levels: from practitioner to policy makers. It is expected that, a fully fit-for-purpose CBRN training curriculum for EU first responders and medical staff, properly quality assured and controlled will be delivered three years after the initiation of the project.

PRINCE	
Title	PRINCE- Preparedness Response for CBRNE INCidEnts *This proejct is also relevent for 4.1.2 Urban soft targets and Urban critical infrastructures*
Objective	Support first aid responders and law enforcement/security authorities by providing them with an evidence base for strategic level decisions related to prevention, detection, Respiratory Protection, Decontamination and response to CBRN event
Contract details	ISFP-2017-AG-PROTECT; 1/1/2019 – 31/12/2021; 2.875.646,40
Abstract	Chemical, Biological, Radiological, Nuclear, and high-yield Explosive (CBRNE) events have the potential to destabilize governments, create conditions that exacerbate violence, or promote terrorism. These events can quickly overwhelm the infrastructure and capability of the responders. PRINCE aims to support first aid responders and law enforcement/security authorities by providing them with an evidence base for strategic level decisions related to prevention, detection, Respiratory Protection, Decontamination and response to CBRN event. PRINCE aims to produce a roadmap based on EU & International Actions plans and recommendations by creating a PRINCE catalogue of training curricula in line with the INTERNATIONAL CBRN TRAINING CURRICULUM and EU, based on best practises and international proven CBRNE exercises. PRINCE aims to produce CBRNE SOPs and plans for two incidents (Chemical and Radiological) in two major exercises (Greece, Portugal). The exercises will be performed with representatives from all responders to (1) share information on CBRN threat and risks; (2) exchange best practices; (3) perform joint trainings and exercises. PRINCE will provide recommendations to CBRNE equipment, systems, and training content and to develop ICT tools (E-training platform, CBRN Emergency system). PRINCE aims to enhance protection of public spaces, community and infrastructure by sharing project outcomes with wider audience through online information material, presentations to public events and media. Short term beneficiaries are CBRN responders and authorities from GR, PT, CY, FL and DE, Medium term beneficiaries: EU CBRN authorities, stakeholders, Long term beneficiaries: Citizens, public authorities, CBRNE technology partners, business, Government advisors, R&D and industry. PRINCE increases sustainability through cross-border / cross-sectoral collaboration and by exchanging best practices and knowledge on joint exercises and training courses between five member states.

This overview is complemented by H2020 projects.

EURAD	
Title	European Joint Programme on Radioactive Waste Management
Objective	Coordinate activities on agreed priorities of common interest between European Waste Management Organisations (WMOs), Technical Support Organisations (TSOs) and Research Entities (REs)
Contract details	NFRP-2018; 1/6/2019 - 31/5/2024; EUR: 32.500.000
Abstract	Following decades of RD&D in support of the safe management and disposal of radioactive waste, and building on the preparatory work of the recent EC JOPRAD project, a European Joint Programme on Radioactive Waste Management (EURAD) is now proposed to coordinate activities on agreed priorities of common interest between European Waste Management Organisations (WMOs), Technical Support Organisations (TSOs) and Research Entities (REs). Such Joint Programming will complement National RD&D Programmes, by jointly establishing and carrying out activities jointly where there is added value at the European level. It is the logical next step in deepening collaboration between European actors in the field of radioactive waste management (RWM). It builds on existing and emerging networks of European actors (IGD-TP, SITEX and REs network), preceding coordination and support actions (in particular, SecIGD2, SITEX-II project and JOPRAD). The Joint Programme will generate and manage knowledge to support EU Member States with their implementation of the Directive 2011/70/Euratom (Waste Directive), taking into account the different magnitudes and stages of advancement of Member State National Programmes. This will encompass: supporting Member-States in developing and implementing their national RD&D programmes for the safe long-term management of their full range of different types of radioactive waste through participation in the RWM Joint Programme; in particular: consolidating existing knowledge for the safe start of operation of the first geological disposal facilities for spent fuel, high-level waste, and other long-lived radioactive waste, and supporting optimization linked with the stepwise implementation of geological disposal; and enhancing knowledge management and transfer between organisations, Member-States and generations.

EURAD	
Consortium	Coordinator: 1. Agence Nationale Pour La Gestion Des Dechets Radioactifs (FR) Consortium: 2. "Arao-Agencija Za Radioaktivne Odpadke Ljubljana Zavod (SI) 3. Bel V (BE) 4. Bundes-Gesellschaft Fur Endlagerungmbh (Bge) (DE) 5. Commissariat A L Energie Atomique Et Aux Energies Alternatives (FR) 6. Centro De Investigaciones Energeticas, Medioambientales Y Tecnologicas-Ciemat (ES) 7. Public Union Chornobyl Research And Development Institute (UA) 8. Centre National De La Recherche Scientifique Cnrs (FR) 9. Centrale Organisatie Voor Radioactief Afval Nv (NL) 10. Valstybinis Moksliniu Tyrimu Institutas Fiziniu Ir Technologijos Mokslu Centras (LT) 11. Centrum Vyzkumu Rez Sro (CZ) 12. Dansk Dekommissionering (DK) 13. Greek Atomic Energy Commission (GR) 14. Empresa Nacional De Residuos Radiactivos S.A. (ES) 15. Forschungszentrum Julich Gmbh (DE) 16. Gesellschaft Fur Anlagen Und Reaktorsicherheit (Grs) Ggmbh (DE) 17. Valstybes Imone Ignalinos Atomine Elektrine (LT) 18. Instytut Chemii I Techniki Jadrowej (PL) 19. Institut De Radioprotection Et De Surete Nucleaire (FR) 20. Instituto Superior Tecnico (PT) 21. Associacao Do Instituto Superior Tecnico Para A Investigacao E Desenvolvimento (PT) 22. Institut Jozef Stefan (SI) 23. Jrc -Joint Research Centre- European Commission (BE) 24. Karlsruher Institut Fuer Technologie (DE) 25. Lietuvos Energetikos Institutas (LT) 26. Magyar Tudomanyos Akademia Energiatudomanyi Kutatokozpont (HU) 27. Nationale Genossenschaft Fuer Die Lagerung Radioaktiver Abfaelle (CH) 28. ""National Center For Scientific Research """"Demokritos""""" (GR) 29. Nuclear Engineering Seibersdorf Gmbh (AT) 30. Narodny Jadrovy Fond (SK) 31. Nuclear Research And Consultancy Group (NL) 32. Nationale Instelling Voor Radioactief Afval En Verrijkte Splijstoffen (BE) 33. Posiva Oy (FI) 34. Paul Scherrer Institut (CH) 35. Radioaktiv Hulladekokat Kezelo Kozhasznu Nonprofit Korlatolt Felelossegu Tarsasag (HU) 36. Regia Autonoma Tehnologii Pentru Energia Nucleara - Raten (RO) 37. Radioactive Waste Management Limited (UK) 38. Studiecentrum Voor Kernenergie / Centre D'etude De L'energie Nucleaire (BE) 39. Svensk Karnbranslehantering Aktiebolag (SE) 40. State Enterprise State Scientific And Technical Center For Nuclear And Radiation Safety (UA) 41. Slovenska Technicka Univerzita V Bratislave (SK) 42. Radioactive Waste Repository Authority (CZ) 43. Statni Ustav Radiacni Ochrany V.V.I. (CZ) 44. Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (NL) 45. Ts Enercon Mernokiroda Kft (HU) 46. Technical University Of Sofia (BG) 47. University Of Cyprus (CY) 48. Helsingin Yliopisto (FI) 49. United Kingdom Research And Innovation (UK) 50. Teknologian Tutkimuskeskus Vtt Oy (FI) 51. Vuje AS (SK)

5.8 Marine pollution

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Marine pollution	APP4SEA CHEMSAR eURready4OS NAMIRG OPENRISK SAFESEA

This overview is complemented with the following DG ECHO project.

West MOPoCo	
Title	Western Mediterranean Region Marine Oil & HNS Pollution Cooperation
Objective	Support Algeria, France, Italy, Malta, Monaco (*), Morocco, Spain and Tunisia in strengthening their collaboration and cooperation in the field of preparedness for and response to oil and HNS marine pollution
Contract details	2018/PREP/826397 1-1-2019 - 31-12-2020; EUR: 651.312,30
Abstract	The Project Western Mediterranean Region Marine Oil and HNS Pollution Cooperation (West MOPoCo) will support Algeria, France, Italy, Malta, Monaco (*), Morocco, Spain and Tunisia in strengthening their collaboration and cooperation in the field of preparedness for and response to oil and HNS marine pollution by enhancing the quality and interoperability of their response capacities. (*)Although Monaco is not an eligible country it will be invited to contribute.
Consortium	Coordinator: 1. Secrétariat Général De La Mer (FR) Consortium: 2. International Maritime Organization (UK) 3. Centre De Documentation De Recherches Et D'experimentation Sur Les Pollutions Accidentelles Des Eaux Association (FR) 4. Itopf Limited (UK) 5. Istituto Superiore Per La Protezione E La Ricerca Ambientale (IT) 6. The Baltic Marine Environment Protection Commission (FI) 7. Ospar Commission For The Protectionof The Marine Environment Of The North-East Atlantic (UK) 8. Commissariat National Du Littoral (DZ) 9. Authority For Transport In Malta (MT) 10. Secretariat D'etat Apres Du Ministere Charge De L'energie, Des Mines Et Du Developpement Durable, Chargee Du Developpement Durable (MA) 11. Ministerio De Fomento (ES) 12. Agence Nationale De Protection De L'environnement (TN)

This overview is complemented by the following INTERREG project.

OIL SPILL	
Title	Enhancing Oil Spill Response Capability in the Baltic Sea Region
Objective	Improve cooperation between competent authorities, NGOs and volunteers in combatting oil spills in shallow and coastal waters of the Baltic Sea faster, more effectively and more efficiently
Contract details	2014 - 2020 INTERREG VB Baltic Sea 2019/01/01 - 2021/06/30; EUR: 1.606.681
Abstract	The OIL SPILL project helps to improve cooperation between competent authorities, NGOs and volunteers in combatting oil spills in shallow and coastal waters of the Baltic Sea faster, more effectively and more efficiently. Together with universities, the partners identify procedures across borders that need to be aligned, develop and carry out trainings and exercises, and clarify key legal issues of cooperation in oil spills response.
Website	Website https://projects.interreg-baltic.eu/projects/oil-spill-189.html
Consortium	Coordinator: Turun yliopisto (FI)

This overview is complemented by the following Marie Skłodowska-Curie Actions project.

LitRivus	
Title	Assessment of riverine litter (plastics) inputs to the marine environment
Objective	Implement innovative monitoring methods to study riverine litter input, providing details on dynamics and variability of litter flux in rivers
Contract details	H2020/MSCA/IF/2018; 1/4/2020 - 31/3/2022; € 160 932,48
Abstract	The project will be focused on innovative monitoring methods to study riverine litter input, providing details on dynamics and variability of litter flux in rivers, which is the missing information necessary to validate models for assessment of riverine litter loads to the sea. Empirical data will facilitate formulation of models to reduce uncertainties and improve estimations. Moreover, the use of international data from RIMMEL project (DG Joint Research Centre, European Commission) and collaboration with experts through RiLiNet will provide the project a large scale. Publication of these results will be very welcome internationally, providing a new approach to the topic based on field data, and serving larger goals pursued by the scientific community, e.g. calculation of marine litter mass balances at different geographical and temporal scales. Furthermore, this will be the first time comprehensive data on riverine litter inputs will be evaluated in relation to policy and decision-making frameworks, such as the Marine Strategy Framework Directive, Water Framework Directive and the EU Strategy for plastics, thus guaranteeing that science-policy knowledge transfer is achieved in order to improve plastic mitigation measures.
Consortium	Coordinator: Universidad De Cadiz (ES)

6. Crime and terrorism

6.1 Terrorist threats

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Terrorist threats	ADABTS ADVISE ATLAS ATLAS 2015 COREPOL DECOTESSC1 DETECTER EWISA EXPEDIA GIFT-CBRN GTCMR HYPERION INDECT PRIME PROACTIVE RAPTOR RECONASS SAFE-COMMS SAMURAI SMARTPREVENT TACTICS TENSOR TransSec VICTORIA VOX-POL

This overview is complemented by the following ISF projects.

ATLAS 2016	
Title	ATLAS 2016
Objective	Support the activities of the transnational law enforcement network "ATLAS"
Contract details	ISFP-2016-AG-IBA-ATLAS; 1/3/2017 – 30/4/2018; 1.263.149,47
Abstract	Project proposal to support the activities of the transnational law enforcement network "ATLAS": Implementation of projects to improve solutions for aircraft-hijacking situations (AIRSHARP), improve medical support for victims and own forces in hostile areas (MEDIC), improve skills in the context of naval based operations (NAVAL), improve the cooperation between ATLAS and other parties, like EUROPOL and covert surveillance networks (C2/C4), improve tactical skills and approaches to encounter terror related incidents in urban areas (BUILDING), enhancing the capacities of Special Intervention Units for managing drone-related risks (DRONES), improve concepts of marksmen deployment in counter-terrorism operations (SNIPER), enhance the efficiency of Close Protection operations in high risk environments (BLACK GRIFFIN), develop breaching methods to open special armored doors from a safe distance (SAD), improve the education of tactical diffusers to disarm improvised explosive devices (EOD), enhance the capabilities to respond to spontaneous armed terrorist attacks for small tactical teams (RAPID RESPONSE). All topics will be carried out in form of meetings, workshops, training sessions and table-top exercises. The outcome will be summarized and distributed amongst all ATLAS members via different communication media (Europol EPE, Standard Operating Procedures and guidelines).

ATLAS 2017	
Title	ATLAS 2017
Objective	Support the activities of the transnational law enforcement network "ATLAS"
Contract details	ISFP-2017-AG-IBA-ATLAS; 1/3/2018 – 30/9/2019; 2.631.577,26
Abstract	Project proposal to support the activities of the transnational law enforcement network "ATLAS": Implementation of projects to improve tactical skills and approaches to encounter terror related incidents in urban areas (BUILDING), enhance the capacities of Special Intervention Units for managing drone-related risks (DRONES), improve concepts of marksmen deployment in counter-terrorism operations (SNIPER), enhance the capabilities to respond to spontaneous armed terrorist attacks for small tactical teams (RAPID RESPONSE), enhance the capacities of SIU's for explosive entry methods for aircraft-hijacking situation (EEOA), develop methods to breach objects from a distance by using 40mm ammunition (ENTRY), improve medical support for victims and own forces in hostile areas (MEDIC), improve skills in the context of naval based operations (NAVAL), develop best practice methods to integrate negotiation capabilities during Counter Terrorism operations (NEGO), enhance the cooperation between SIU's in case of operations related to public means of transport (TRANSPORT), carry out a Europe-wide CT exercise to prove the readiness of ATLAS SIU's in cross-border and multinational operations (ACC 2018), enhance the capacities of SIU's to lead and coordinate multinational joint operations (C2/C4), prepare the advanced operational cooperation between the ATLAS network and EUROPOL. all topics will be carried out in form of meetings, workshops, training sessions and table-top exercises. The outcome will be summarized and distributed amongst all ATLAS members via different communication media (Europol EPE, Standard Operating Procedures and guidelines).

BeCaNet	
Title	Best practice, capacity building and networking initiative among public and private actors against Terrorism Financing *This project is also relevant for 6.7 Financial crime*
Objective	Develop and facilitate public-private-sector cooperation between CT financial investigation units, financial Intelligence Units (FIUs), money and value transfer services (MVTS), payment service providers, online marketplace platforms and virtual currency providers; and promote and develop a network among counter-terrorism (CT) financial investigators of EU LEAs
Contract details	ISFP-2017-AG-TERFIN; 1/12/2018 – 30/11/2020; 1.561.243,42
Abstract	The proposed 24-months project "BeCaNet" pursues two main strands of action: 1. The project will promote and develop a network among counter-terrorism (CT) financial investigators of Law Enforcement Agencies (LEAs) from EU MS with the following purposes: institutionalising an annual practioners' forum for CT financial investigators where important information on legal, practical, operational and strategic aspects of counter-terrosim financing (CTF) measures will be presented and discussed on expert level, preparing, updating and sharing a list of national contact points of CT financial investigation units, strengthening financial data analysis capabilities and IT capacities of CT financial investigation units. This will be accomplished with the help of expert meetings and briefings, best practice workshops, training courses and the distribution of professional financial data analysis software to CT financial investigation units of LEAs from EU MS. The project partners U.S. FBI and the world's largest money remittance service provider Western Union will facilitate network building. Both U.S. FBI and Western Union participate in the project but do not incur costs. EUROPOL will also support the project. The project will develop and facilitate public-private-sector cooperation between key actors of LEAs from EU MS, in particular CT financial investigation units, financial Intelligence Units (FIUs), money and value transfer services (MVTS), payment service providers, online marketplace platforms and virtual currency providers. FBI und EUROPOL will complement cooperation efforts as international players against Terrorist Financing (TF). The project objective will be accomplished by best practice workshops, expert briefings and active involvement in training courses for CT financial investigators of LEAs from EU MS. An international conference on financial monitoring measures against islamists will bring public and private financial experts together.

BLACK WALLET	
Title	Counter terrorism financing risks and monitoring measures of new payment initiation service providers *This project is also relevant for 6.7 Financial crime*
Objective	Increase knowledge among authorities and to assess possible risks of usage of new payment services in terrorism financing
Contract details	ISFP-2017-AG-TERFIN; 1/3/2019 – 28/2/2021; 647.973,81
Abstract	hThis project will increase the risk of getting caught on financing terrorism by improving knowledge, understanding and co-operation between the private sector actors and the law enforcement. It will seek to hinder the terrorist operations and possibly even prevent a terrorist attack by stopping and confiscating its financing. The project concentrates on getting an overall picture of the new payment service providers and account information services in European Union area in order to increase knowledge among authorities and to assess possible risks of usage of these new payment services in terrorism financing. The project will develop a report which will contain basic information concerning new products and services, their capabilities and how they function, containing much of the information and insights concerning risk assessment and montoring. Second, the project is aimed at improving the anti-money laundering (AML) and terrorism financing (TF) monitoring and reporting mechanisms by enhancing cooperation between Financial Intelligence Units and private operators through effective training and information sharing. This is partly achieved by organizing interactive training sessions and seminars for the private services. The findings and results will be disseminated European-wide to all relevant counterparties. The partners of this project are the National Bureau of Investigation in Finland (applicant) and the National Operations Department in Sweden (co-applicant). The beneficiaries include all financial intelligence units, financial supervisory authorities and security intelligence agencies in Europe as well as national and local authorities.

ESCN	
Title	European Strategic Communications Network *This project is also relevant for 6.5 Radicalisation and 9.3 Communication systems (Interoperability and communication with focus on security).*
Objective	Intensify the exchange of expertise in the field of strategic communications to counter violent extremism and terrorism
Contract details	ISFP-2016-AG-IBA-SCAT; 1/10/2016 -31/12/2017; 1.266.987,00
Abstract	The European Strategic Communications Network will build on the work of the SSCAT project and intensify the exchange of expertise in the field of strategic communications to counter violent extremism and terrorism. The ESCN will continue to support Member States to develop their domestic capacity so that they are able to work on a sustainable long-term basis and create innovative communication responses to terrorism and violent extremism.

ESCN	
Title	Supporting the activities developed by the European Strategic Communication Network *This project is also relevant for 6.5 Radicalisation and 9.3 Communication systems (Interoperability and communication with focus on security).*
Objective	Intensify the exchange of expertise in the field of strategic communications to counter violent extremism and terrorism
Contract details	ISFP-2017-AG-IBA-ESCN; 1/1/2018 – 31/12/2019; 3.684.211,16
Abstract	The European Strategic Communications Network will build on the work of the first iteration of the ESCN project and intensify the exchange of expertise in the field of strategic communications to counter violent extremism and terrorism. The ESCN will continue to support Member States to develop their domestic capacity so that they are able to work on a sustainable long-term basis and create innovative communication responses to terrorism and violent extremism.

IDEAINTERPOL	
Title	Databases Enhanced Access in European Union *This project is also relevant for 6.4.1 Organised crime.*
Objective	Prevent and detect movement of terrorist and FTFs and fight against transnational crimes by assisting the least performing EU Member Countries (MC) with improving their use and population of INTERPOL's Stolen and Lost Travel Document (SLTD), Travel Document Associated With Notices(TDAWN) and NOMinal databases.
Contract details	ISFP-2017-AG-IBA-SLTD; 1/2/2019 – 31/1/2021; 2.038.769,44
Abstract	INTERPOL SLTD – a unique global repository, created in 2002 by INTERPOL, the world's largest international police organization, c as a tool for law enforcement to detect and prevent the use of fraudulent identity documents. Today, the database includes more than 75 million records from 176 countries. In 2016 alone, the database was checked more than 1,59 billion times, generating more than 100,000 alerts where individuals tried to use travel documents registered as stolen or lost. The widespread and systematic use of SLTD has the potential to stop criminals and terrorist in their track and so protect global public safety. Global interchange of information on lost or stolen travel documents provides improved border integrity and helps identify identity theft either at the border or in other situation where travel documents are presented as a form of identification. The Project aims to enhance with the support and using INTERPOL policing capacities the cooperation among EU MC for fighting terrorism and transnational crime through effective border management. This project aims to prevent and detect movement of terrorist and FTFs and fight against transnational crimes through the assistance to the least performing EU Member Countries (MC) by improving their use and population of INTERPOL's Stolen and Lost Travel Document (SLTD), Travel Document Associated With Notices(TDAWN) and NOMinal databases.

ParTFin	
Title	Public-Private Partnerships on Terrorism Financing *This project is also relevant for 6.7 Financial crime*
Objective	Improve the effectiveness of the struggle against terrorism by a more effective tracing and disruption of illicit financial flows
Contract details	IISFP-2017-AG-TERFIN; 1/4/2019 – 31/3/2021; 689.722,00
Abstract	The objective of the action is to improve the effectiveness of the struggle against terrorism by a more effective tracing and disruption of illicit financial flows. More specifically, this project aims at developing and strengthening public-private partnerships (PPPs) in order to enhance information sharing between competent authorities (including regulators) and financial and payment service providers at the national and EU levels. Another aim is to facilitate the cross-border information exchange between PPPs. To this end, the project will provide best-practice guidance to policy makers at the EU and national levels. Research activities will include (i) comparative legal analyses of PPP involving eight countries in- and outside the EU in the area of AML/ as well as PPP in other areas of security law; (ii) research spanning security law, data protection law, and public international law; and (iii) socio-legal research on PPPs, including interviews with competent authorities and relevant private stakeholders; (iv) an interdisciplinary investigation into the relationship between law and technology in the context of financial analytics. In the short term, the project will benefit competent authorities engaged in counter-terrorism investigations in four EU Member States (France, Germany, Italy, and Spain), which form the core of the present pilot project, as well as European agencies. In the mid-term, it will provide guidance for legislators in the four above-mentioned States and for the EU legislator. In the long term, it will contribute to creating or enhancing PPP in other EU Member States and stimulate political action in support of such mechanisms outside the area of terrorism financing.

Skyfall	
Title	Skyfall: LEA training for Counter-UAV *This project is also relevant for 6.4.5 Support to law inforcement.*
Objective	Develop an European matrix how to protect and respond on different types of UAV incidents
Contract details	ISFP-2017-AG-PROTECT; 1/1/2019 – 31/12/2020; EUR: 1.146.368,99
Abstract	In order to achieve the general objective, the project will develop an European matrix how to protect and respond on different types of UAV incidents, in relation to the location and the kind of event that is going. The Belgian integrated police (Local+federal) has already worked out such a matrix but wants to take the step forward by bringing together expertise across the European Union and develop an validated European Matrix. Secondly, the project will make a study of all systems currently available and which are suitable for physical drone interception. Criteria such easy-deployment, handheld transportable, effectiveness, efficiency, applicable for various types of UAV. This study will result in a report in which a ranking will be made. The highest ranked counter system will be integrated into the training curriculum. The incident based response interception training will focus on where and when to intercept an UAV. Much depends on the situation and an immediate interception will not always be the best suitable solutions as UAV can be weaponized or can carry IED's. The training will set up an interception plan adapted to the diverse threats not only limited to the physical interception but also managing the actions to be taken towards the public, VIP's or critical infrastructure. In order to achieve the largest impact possible, two train the trainer sessions will be organized order to ensure that all EU LEA's have the necessary skills and knowledge to counter an UAV attack.

W.E.	
Title	Wider Eyes *This project is also relevant for 6.4.1 Organised Crime*
Objective	Develop the technical works to provide direct connection from the current Integrated System of Operational Management of Guardia Civil (SIGO) and the current Investigations System of Guardia Civil (SINVES) for querying external databases – Interpol SLTD, SMV, iARMS, TDAWN, SV, and Notices and Nominal Data from their common Single Search Interfaces
Contract details	ISFP-2017-AG-SLTD 20/2/2019 – 19/8/2020; EUR: 833.312,40
Abstract	The main objective of this proposal is to develop the technical works to provide direct connection from the current Integrated System of Operational Management of Guardia Civil (SIGO) and the current Investigations System of Guardia Civil (SINVES) for querying external databases –Interpol SLTD, SMV, iARMS, TDAWN, SV, and Notices and Nominal Data from their common Single Search Interfaces. The interconnection will provide more information and increase the efficiency of the agents while consulting. Guardia Civil agents won´t need an access to Interpol databases through different interfaces other than SIGO and SINVES in case they need to check data on persons, documents, vehicles and vessels.

This overview is complemented by relevant projects funded in 2018.

LINSEC	
Title	LINSEC
Objective	Study the logic of informal security cooperation
Contract details	H2020/MSCA/IF/2018; 01/09/20 - 31/08/22; € 219 312
Abstract	This MSCA research project on the logic of informal security cooperation (LINSEC) combines the research fields of security studies, IR, international history, and intelligence studies to answer the project's overarching research question: What drives and sustains informal counterterrorism cooperation? To answer this question, LINSEC builds on the University of Southern Denmark's (SDU) expertise in security studies, my research experience in history and intelligence studies, interviews with intelligence officers, and my recently obtained unprecedented access to over 30,000 intelligence records from 1971 to 1979. These records are from a counterterrorism intelligence-sharing framework called the Club de Berne, which is still today's main cooperation platform for informal intelligence-sharing on terrorism.
Consortium	Coordinator: Syddansk Universitet (DK)

6.2 Forensics

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Forensics	3D-FORENSICS ASGARD BEAT CRIM-TRACK EPOOLICE EUROFORGEN-NOE FORENSOR FORLAB Genomcore Identity GIFT-CBRN GRAFFOLUTION IDENTITY LASIE MEPROCS MIDAS MISAFE ODYSSEY P-REACT RAMSES RECOBIA SALUS SAWSOC SCIIMS SHUTTLE SIIP TRACE VALCRI VISAGE

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

INCLUDING	
Title	Innovative Cluster for Radiological and Nuclear Emergencies *This project is also relevant for 6.3.2 Privacy and Data Protection and 6.4.1 Organised crime*
Objective	INCLUDING pursues to develop a Federation in which individual Members will cooperate together to provide a common framework to standardize access to their respective facilities, enhance interoperability and to allow a more intensive use of expensive equipment
Contract details	H2020-SU-SEC-2018; Topic code: SU-GM01-2018-2019-2020; 1/8/2019 - 31/7/2024; € 3 585 528,75
Abstract	INCLUDING connects 15 Partners from 10 EU Member States (MS), bringing together infrastructure, equipment and experts coming from Medical Organizations, Fire Corps, Government Department, Municipalities, Law Enforcement Agencies, Ministries, Governmental and Civilian Research Institutes and Industries operating in the field of radiological and nuclear emergencies. Far from being a simple aggregation of entities separated geographically and with complementary expertise, INCLUDING pursues to develop a Federation in which individual Members will cooperate together to provide a common framework to standardize access to their respective facilities, enhance interoperability and to allow a more intensive use of expensive equipment. The operative tool to manage the Federation will be a web-based platform with a sophisticated architecture and whose functionality has been proven in a previous EU project. At the same time the project aims to enhance practical know-how and to boost a European sustainable training and development framework for practitioners in the Radiological and Nuclear Security sector. The INCLUDING project will be flexible in order to include new facilities and innovation in technology, organizations and procedures. The plurality of facilities and expertise in the INCLUDING Federation reflects the complex and intertwined structure of the prevention and response phases of RN threats and will provide to the practitioners a set of real or emulated scenarios where to test concept of operations in a controlled environment. The Joint Actions will be the focal points of the project. They are multidisciplinary field exercises, tabletop exercises, training, serious gaming and simulation organized at their premises by the project partners and with the objective of demonstrating the added value of the Federated scheme and of the use of an innovative tool like the INCLUDING web based Platform to manage a pan European network of training facilities and resources.
Consortium	Coordinator: 1. Agenzia Nazionale Per Le Nuove Tecnologie, L'energia E Lo Sviluppo Economico Sostenibile (IT) Consortium: 2. Astri Polska Spolka Z Ograniczona Odpowiedzialnoscia (PL) 3. Inesc Tec - Instituto De Engenharia De Sistemas E Computadores, Tecnologia E Ciencia (PT) 4. Istituto Affari Internazionali (IT) 5. Universita Cattolica Del Sacro Cuore (IT) 6. Iscc Gmbh (AT) 7. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 8. Valstybes Sienos Apsaugos Tarnyba Prie Vidaus Reikalu Ministerijos (Lt) 9. Magyar Tudomanyos Akademia Energiatudomanyi Kutatokozpont (HU) 10. Ethniko Kai Kapodistriako Panepistimio Athinon (EL) 11. Tekever Asds (PT) 12. Ministry Of National Defence, Greece (EL) 13. Commissariat A L Energie Atomique Et Aux Energies Alternatives (FR) 14. Mikkelin Kaupunki (FI) 15. Ministerio Da Administracao Interna (PT)

FORMOBILE	
Title	FORMOBILE *This project is also relevant for 6.3.2 Privacy and Data Protection and 6.4.1 Organised crime*
Objective	Establish a complete end to end forensic investigation chain, targeting mobile devices
Contract details	H2020-SU-SEC-2023; Topic code: SU-FCT02-2018-2019-2020; 1/5/2019 - 30/4/2022; € 6 983 030
Abstract	Mobile devices, especially smartphones represent a unique challenge for law enforcement. Criminal offenders use phones to communicate, coordinate, organise and execute criminal actions. This is especially true for organised crime and terrorist organisations. This development provides new challenges for criminal prosecution and it is vital to empower law enforcement to access the data stored on mobile devices to use it as court evidence in a trustworthy and reliable manner. The overarching objective of FORMOBILE is to establish a complete end to end forensic investigation chain, targeting for mobile devices. To achieve this goal three objectives will be pursued. Novel tools shall be developed that include the acquisition of previously unavailable mobile data, unlocking mobile devices, as well as the decoding and analysis of mobile data. Based on the definition of requirements of law enforcement and legal and ethical issues a new mobile forensics standard shall be developed. With the developments of the new standard and the new tools, training for police and criminal prosecution will be established, providing the end users with the latest knowledge in a novel and an innovative curriculum to ensure a quality standard of investigations. The European Union has developed as a Security Union, building on the European Agenda on Security. This aims to ensure that people live in an area of freedom, security and justice, without internal frontiers. To strengthen digital forensics in the context of criminal investigations is crucial to achieve this vision. FORMOBILE contributes to the fight against virtually all forms of crime. This is because mobile devices are widely used in crimes, especially in the arrangement of conspiracies. Yet, there are crimes more closely related to mobile devices; this includes child abuse and emerging forms of cybercrime in particular. To fight crime effectively, law enforcement has to be empowered to access all evidence stored on mobile devices.=
Consortium	Coordinator: 1. HOCHSCHULE MITTWEIDA (FH) (DE) Consortium: 2. Netherlands Forensic Institute (NL) 3. Micro Systemation Ab (SE) 4. Austrian Standards International (AT) 5. Zentrale Stelle Für Informationstechnik Im Sicherheitsbereich (DE) 6. Home Office (UK) 7. Ministerio Del Interior (ES) 8. Komenda Wojewodzka Policji W Poznaniu (PL) 9. Malta Police Force (MT) 10. Ministério Da Justiça (PT) 11. Technische Universiteit Delft (NL) 12. Panepistimio Patron (EL) 13. Idryma Technologias Kai Erevnas (EL) 14. Norwegian Ministry Of Justice And Public Safety (NO) 15. Pravo I Internet Foundation (BU) 16. Stowarzyszenie Polska Platforma Bezpieczenstwa Wewnetrznego (PL) 17. Time.Lex (BE) 18. Strane Innovation Sas (Fr) 19. Kyrgyz State Technical University Named After I. Razzakov (KG)

LOCARD	
Title	LOCARD *This project is also relevant for 6.4.5 Support to law enforcement and 9.3 Communication systems (Interoperability and communication with focus on security)*
Objective	Provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain
Contract details	H2020-SU-SEC-2030; Topic code: SU-FCT02-2018-2019-2020; 1/5/2019 - 30/4/2022; € 6 833 385
Abstract	LOCARD aims to provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain. Each node of LOCARD will be able to independently set its own permission policies and to selectively share access to digital evidence with other nodes when deemed necessary and upon proper authorization through fine-grained policies. LOCARD's modularity will also allow diverse actors to tailor the platform to their specific needs and role in the digital forensic workflow, from preparation and readiness, to collection, to analysis and reporting. LOCARD will have a crowdsource module to collect citizen reports of selected violations, a crawler to detect and correlate online deviant behaviour, and a toolkit for investigators that will assist them in collecting online and offline evidence. This will be powered by an immutable storage and an identity management system that will protect privacy and handle access to evidence data using a Trusted Execution Environment. Blockchain technology will not only guarantee that information about the evidence cannot be tampered with, but allow interoperability without the need for a trusted third party.
Consortium	Coordinator: 1. Athina-Erevnitiko Kentro Kainotomias Stis Technologies Tis Pliroforias, Ton Epikoinonion Kai Tis Gnosis (EL) Consortium: 2. Guarino Alessandro (IT) 3. Fundacion Apwg, European Union Foundation (ES) 4. Motivian Eood (BU) 5. Imc Diachirisi Pliroforion Kai Epikinonion Anonymos Etairia (EL) 6. Universita Degli Studi Di Padova (IT) 7. Telefonica Investigacion Y Desarrollo Sa (ES) 8. European Electronic Messaging Association Aisbl (BE) 9. Neurosoft Cyprus Limited (CY) 10. Vrije Universiteit Brussel (BE) 11. Vlaamse Ict Organisatie Vzw (BE) 12. Infotrend Innovations Company Limited (CY) 13. Universita Ta Malta (MT) 14. Kentro Meleton Asfaleias (EL) 15. Technische Universitat Berlin (DE) 16. Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO) 17. Hellenic Police (EL) 18. Inspectoratul General Al Politiei Romane (RO) 19. Hochschule Fur Den Offentlichen Dienst In Bayern (DE)

This overview is complemented by ISF-funded projects.

BALTFORDEX	
Title	Increasing Capacity of Baltic State to Stimulate the Exchange of Forensic Data via Prüm
Objective	Stimulate the exchange of forensic data (DNA–profiles and fingerprints) via Prüm and improving its quality by increasing the capacity of Baltic States in the forensic science field
Contract details	ISFP-2017-AG-FORENSIC; 1/1/2019 – 30/6/2020; 639.923,13
Abstract	General objective: to stimulate the exchange of forensic data (DNA–profiles and fingerprints) via Prüm and improving its quality by increasing capacity of Baltic States on forensic science field. Project objective will be achieved by implementation of joint Project participants activities: Joint trainings, workshops, hands-on trainings and study visits to EU MS; Exchanging of best practices between EU MS; Joint development of mechanisms for prompt, mutual notification, describing automated exchange of dactyloscopic data (Prüm); Development of new system on DNA database digitalization and integration (LV SP) with a potential for transferability to other MS (LPFSC and EFSI); Improving the process and thus also the quality of DNA and dactyloscopic samples taken at the crime scene by joint development of the Manual; Acquisition of equipment (hardware and software) for work with captured fingerprint images increasing the quality of fingerprint evidence and fulfilling the Prüm Decisions. All Project activities are connected with fulfilling the Prüm Decisions putting specific focus on DNA – profiles and fingerprints data quality and exchange.

DNAxs2.0	
Title	Developing DNAxs2.0: the next generation DNA eXpert System accommodating DNA-profile matching, mixture interpretation and statistical analysis with validation and dissemination across Europe *This project is also relevant for 6.4.5 Support to law enforcement*
Objective	Develop DNAxs2.0: the next generation DNA eXpert System accommodating DNA-profile matching, mixture interpretation and statistical analysis with validation and dissemination across Europe
Contract details	ISFP-2017-AG-FORENSIC; 1/12/2018 – 31/5/2020; 499.086,52
Abstract	DNA-profiling is one of the most valuable forensic approaches: it can generate investigative leads by retrieving names from DNA database searches and high weights of evidence when suspects and evidential traces are compared. The growing number of markers in profiling systems makes DNA-profile comparison increasingly time-consuming and error-prone. Software tools may change this to the better, which prompted the development of the expert system DNAxs. In December 2017, a basic version was implemented in the applicant's laboratory after in house development and validation. This version includes a matchbox tool facilitating automatic comparison of sets of profiles within seconds and summary statistics on allele numbers and genotyping reproducibility. DNAxs excels in visual representation and generates export files for forensic reporting. DNAxs2.0 aims to integrate statistical analysis into DNAxs, based on selected functionalities of the advanced probabilistic model EuroForMix developed within an earlier EU consortium. This requires 1) research regarding the EuroForMix settings that provide optimal performance 2) software engineering and 3) thorough validation. Validation will take place at three levels: i) DNAxs results will be compared to EuroForMix results; ii) a test engineer will build integration tests to automatically check updated versions; iii) partner laboratories will test software performance under varying environments and provide input for broadened use. Various dissemination activities are scheduled. The need for a forensic DNA expert system is widely recognised as it will enhance the process of DNA-profile interpretation to be cost and labour efficient, robust and uniform. The user-friendliness of the software carrying a selection of EuroForMix functionalities will assist implementation of this advanced statistical model. Thus, the capacity and quality of forensic laboratories is increased with positive impact on society and crime solving.

MEMO	
Title	Mutual Exchange of Modi Operandi in Violent Crimes Cases *This proeject is also relevant for 6.4.5 Support to law enforcement*
Objective	Stimulate exchange of forensic information on modi operandi (MO) for homicides, violent sexual crimes and paedophilia and seeks to explore the interoperability of the existing/ potential databases for violent crimes linkage analysis at EU level
Contract details	ISFP-2017-AG-FORENSIC; 1/10/2018 – 31/3/2020; 527.296,00
Abstract	This transnational project aims at stimulating exchange of forensic information on modi operandi (MO) for homicides, violent sexual crimes and paedophilia and seeks to explore the interoperability of the violent crimes linkage analysis systems at EU level of the existing/ potential databases. SO1. Exchanging best practices in order to create an EU wide automatic analysing system of the MO for homicides, violent sexual crimes and paedophilia. SO2. Determine the interconnection capacity at EU level of the analysing systems based on ViCLAS (Violent Crime Linkage Analysis System) programme, used currently in some MS, or any similar system via consultation with EU MS and relevant agencies

VERBUM_SAT	
Title	Developing forensic statement analysis standards to fight CAE: A victim centered approach
Objective	Establish a coordinated contribution to law enforcement with a forensic statement based analytical tool (FSA)
Contract details	ISFP-2017-AG-CYBER; 1/4/2019 – 31/3/2021; EUR: 641.861,97
Abstract	The projects main objective, through its activities and results, is to specifically establish a coordinated contribution to law enforcement with a forensic statement based analytical tool (FSA) and broadly to remedy the problematic of secondary victimization of child victims of sexual abuse and exploitation (CAE), a field of police procedure which has not yet been addressed in more detail. Detecting, investigating and preserving evidence of child abuse is a discouraging undertaking, especially in the light of recent studies which refer to experts who are reporting a disquieting lack or absence of hard evidence. This means, that material evidence cannot be relied on as they are not sufficiently applicable. In order to fulfill these expectations, an approach has to be built upon victim's full engagement. By altering the approach in its initial phase, we can minimize the risks. Implementing FSA into process at its very beginning would represent the victims' need to disclose tragic content only once at his first encounter with the authorities. To establish the veracity of his allegations no further interview would be necessary. All with the same goal of protecting the victim but still gather the relevant information and evidence without exposing a child to unnecessary risks. With the development of FSA standards adjusted to subjected forms of crime, our aim is to empower a victim-centered approach wherein the benefit of the most vulnerable would be the main focus.

TELEFI	
Title	Towards the European Level Exchange of Facial Images *This project is also relevant for 6.4.5 Support to law enforcement.*
Objective	Promote and improve the future exchange of forensic information between national databases
Contract details	ISFP-2017-AG-FORENSIC; 1/1/2019 – 30/6/2020; EUR: 566.715,87
Abstract	The overall objective of the project "Towards the European Level Exchange of Facial Images" (TELEFI) is to promote and improve the future exchange of forensic information between national databases. The proposed action will focus on facial recognition as one of the most promising new biometric technologies for forensic investigation and for forensic data exchange. The action will review the organisational, technical and legal aspects of forensic facial recognition at the European level, identify the existing facial databases and their availability for cross-border use, and establish the best practices and quality standards in the field across the EU Member States.

STEFA	
Title	Steps Towards a European Forensic Science Area
Objective	Promote cooperation between police and judicial authorities across EU Member States in the field of forensic science
Contract details	ISFP-2016-AG-IBA-ENFSI; 1/1/2018 – 31/12/2019; EUR: 1.578.950,50
Abstract	The combatting of global crime (e.g. people trafficking, terrorism, organized crime) is increasingly reliant on forensic science for investigation & prosecution. Thus, the sharing of forensic information across international borders requires mutual confidence in the forensic work undertaken in different countries. The EU Vision for European Forensic Science 2020 with the creation of a European Forensic Science Area aims to promote cooperation between police and judicial authorities across EU Member States in the field of forensic science. The STEFA project is an important stepping stone in the realisation of the European Forensic Science Area contributing to key work streams that have been specified in the relevant EU Council Decisions. It brings together teams of experts from 31 organisations in 18 EU Member States (forensic institutes, research establishments, universities & other forensic service providers) along with 5 more organisations from other countries.

Prevent CAM online	
Title	Prevent CAM online
Objective	The main objective of this Action is to offer practice-oriented training on methodologies and tools to prevent child sexual abuse online
Contract details	ISFP-2017-AG-CYBER; 1/09/2019 – 30/06/2021; 321201,20
Abstract	The main objective of this Action is to offer practice-oriented training on methodologies and tools to prevent child sexual abuse online. The Action will be structured around six training events organised throughout Europe over twenty-two months. Each event will last 1.5 days. The main target group of the Action will be EU law enforcers, judges, prosecutors, academics, ministry officials and representatives of the civil society. Each of these six seminars will be targeted at different groups of selected Member States (ca. 4-5 Member States per seminar, ca. 50 participants per seminar) which are, to the extent possible, geographically close to each other ("regional approach"), so that the need for cross-border cooperation is particularly important. The decentralised series of events will guarantee a good geographical mixture among EU participants and networking opportunities which will encourage close contacts and cooperation among different professions. In order to guarantee valuable practical training on preventing child sex abuse material online, the topics will be dealt with by means of concrete case studies and demonstrations. National experts will analyse the topics and present case studies based on the individual national penal system and EU legislation in place. In this way, participants will benefit from training that is tailor-made to deal with the questions and problems arising in their daily practice when dealing with cases involving child sex abuse material. In order to benefit from different perspectives, the groups of experts conducting the seminars will consist of judges, prosecutors, academics, ministry officials and NGOs' representative with experience in fighting child abuse material online. All in all the Action will guarantee that the seminars will effectively train 300 different EU legal practitioners (direct beneficiaries: 50 participants per event x 6 events).

6.3 Cybercrime & cyber security

6.3.1 Cyber Security Management (for SMEs / business, local public authorities)

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Cyber Security Management (for SMEs / business, local public authorities)	AF-CYBER ANASTACIA ASTRIC BITCRUMBS BOXMATE C3ISP CANVAS certMILS CIPSEC COMPACT ConnectProtect CS-AWARE CYBECO CYBER-TRUST CYBERWISER.EU DiSIEM DOGANA EU-SEC FACCESS FORTIKA FutureTPM GHOST HERMENEUT HDIV IDAaas INSTET iSAVE LIGHTest LipVerify OCTAVE NK-25-2016 PerfectDashboard 2.0 PROTECTIVE PRECYSE SCR SHIELD SERENITI SIGNA2.0 SISSDEN SMESEC STORM TFENCE VESSEDIA WISER YAKSHA

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

ROXANNE	
Title	ROXANNE *This project is also relevant for 9.3 Communication systems (Interoperability and communication with focus on security)*
Objective	Technical development of the ROXANNE platform, which will enhance criminal network analysis capabilities by providing a framework for extracting evidence and actionable intelligence based on speech, language and video technologies
Contract details	H2020-SU-SEC-2022; Topic code: SU-FCT02-2018-2019-2020; 1/9/2019 - 31/8/2022; EUR 6 999 458,75
Abstract	ROXANNE will achieve a significant increase in the speed of investigation processes and an improvement in identification of individuals by means of speech, in the scope of criminal cases where large amounts of lawfully intercepted communications (with multilingual attributes) are analysed. The technical development will be centred around the ROXANNE platform, which will enhance criminal network analysis capabilities by providing a framework for extracting evidence and actionable intelligence based on speech, language and video technologies. The intention is not to replace humans but automate time-consuming tasks, and support LEA decision-making. Its early version will offer preliminary SLT, VA and NA capabilities to collect end-user feedback. The final version will provide multilingual, probabilistic tools interfacing SLT and NA technologies, boosted by natural language processing (NLP) and relation analysis in the synoptic criminal activity graph. ROXANNE will achieve full compliance with relevant INTERPOL and EU legal and ethical frameworks, including innovative approaches to data protection management such as privacy by design. Special efforts will be expended to ensure ROXANNE outcomes achieve widespread adoption by law enforcement. The effort will be enhanced through a series of education and awareness campaigns and the direct involvement of LEAs from nine European countries, that will test our solutions on real case data. In addition, ROXANNE partner INTERPOL and EUROPOL (member of the External Advisory Board) will provide advice and guidance.
Consortium	Coordinator: 1. Fondation De L'institut De Recherche Idiap (CH) Consortium: 2. Trilateral Research Ltd (UK) 3. Vysoke Uceni Technicke V Brne (CZ) 4. Phonexia Sro (CZ) 5. Sail Labs Technology Gmbh (AT) 6. Capgemini Consulting (FR) 7. The International Criminal Police Organization (FR) 8. Universitat Des Saarlandes (DE) 9. Kentro Meleton Asfaleias (EL) 10. Gottfried Wilhelm Leibniz Universitaet Hannover (DE) 11. Universita Cattolica Del Sacro Cuore (IT) 12. Aegis It Research Ug (Haftungsbeschrankt) (DE) 13. Airbus Defence And Space Sas (FR) 14. Policejni Prezidium Ceske Republiky (CZ) 15. Ministerul Afacerilor Interne (RO) 16. Lietuvos Teismo Ekspertizes Centras (LT) 17. Police Service Of Northern Ireland (UK) 18. Aditess Advanced Integrated Technology Solutions & Services Ltd (CY) 19. Ministry Of Interior (HR) 20. Netherlands Forensic Institute (NL) 21. Internet Of Things Applications Andmulti Layer Development Ltd (CY)) 22. Ministry Of Public Security (IL) 23. Hellenic Police (EL) 24. An Garda Siochana (IE)

SPIDER	
Title	SPIDER *This project is also relevant for 8.3.5 Training and Networking*
Objective	Deliver an innovative Cyber Range as a Service platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges into a unified facility
Contract details	H2020-SU-SEC-2058; Topic code: SU-DS01-2018; 1/7/2019 - 30/6/2022; € 5 746 595
Abstract	The increasing complexity of the telecommunication domain's cyber threat landscape intensifies the need for new security solutions and for improving the technical security skills of experts and non-experts in the multi-tenant and multi-service environments coming with the domain's 5th generation (5G). At the same time, attack mechanisms are increasingly sophisticated, pervading critical infrastructures despite billions of euros invested in cybersecurity measures. To address the above, SPIDER delivers an innovative Cyber Range as a Service platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges into a unified facility for (i) testing new security technologies, (ii) training modern cyber defenders in near real-world conditions, and (iii) supporting organisations and relevant stakeholders in making optimal cybersecurity investment decisions. At its core, it is a highly customisable dynamic network modelling instrument that enables real-life virtualisation and real-time emulation of networks and systems. It also offers real-time interaction and information sharing capabilities by acting as a serious gaming repository for multiple stakeholders to share material and maximise efficiency in delivering complex cyber exercises. SPIDER's gamified learning environment enables trainees to master how to use domain-specific cyber protection technologies and collaboratively improve their ability in handling incidents and risks. Complemented by cyber econometric capabilities, SPIDER also enables users to forecast the evolution of attacks and their associated economic impact through the application of innovative risk analysis methodologies, econometric models and real-time attack emulation. The proposed cyber range model will be validated in five highly realistic pilot use case scenarios aimed at demonstrating its applicability and validity for all requirements of the SU-DS01-2018 Call (simulation, training, and economics).
Consortium	Coordinator: 1. Ericsson Telecomunicazioni Spa (IT) Consortium: 2. Consorzio Nazionale Interuniversitario Per Le Telecomunicazioni (IT) 3. Telefonica Investigacion Y Desarrollo Sa (ES) 4. Thales Six Gts France Sas (FR) 5. Atos Spain Sa (ES) 6. Gioumpitek Meleti Schediasmos Ylopoiisi Kai Polisi Ergon Pliroforikis Etaireia Periorismenis Efthynis (EL) 7. Universidad Politecnica De Madrid (ES) 8. Fondazione Bruno Kessler (IT) 9. Singularlogic Romania Computer Applications Srl (RO) 10. Eight Bells Ltd (CY) 11. Idryma Technologias Kai Erevnas (EL) 12. Serious Games Interactive Aps (DK) 13. University Of Piraeus Research Center (EL) 14. City University Of London (UK) 15. Cyberlens Ltd (UK) 16. Infalia Private Company (EL) 17. Infocom Srl (IT) 18. Sphynx Technology Solutions Ag (CH) 19. K3y (BU)

EnergyShield	
Title	EnergyShield *This project is also relevant for 4.2.1 Critical Energy Infrastructure: Electrical Power (Electricity) and Smart Grids, Oil, Gas*
Objective	Develop an integrated toolkit covering the complete EPES value chain (generator, TSO, DSO, consumer)
Contract details	H2020-SU-SEC-2059; Topic code: SU-DS04-2018-2020; 1/7/2019 - 30/6/2022; € 7 421 437,50
Abstract	The EnergyShield project will develop an integrated toolkit covering the complete EPES value chain (generator, TSO, DSO, consumer). The toolkit combines novel security tools from leading European technology vendors and will be validated in large-scale demonstrations by end-users. The EnergyShield toolkit will combine the latest technologies for vulnerability assessment (automated threat modelling and security behaviour analysis), monitoring & protection (anomaly detection and DDoS mitigation) and learning & sharing (security information and event management). The integrative approach of the project is unique as insights produced by the various tools will be combined to provide a unique level of visibility to the users. For example, it will be possible to combine vulnerability scanning with automated threat modelling to provide insights into software vulnerabilities present in an architecture in combination with insights into what are the key assets, risks and weak links of the architecture. The toolbox will allow end-users to predict future attacks (as it provides insights to what attacks can be applied to the weakest links of the architecture) and learn from past attacks (for example using the insights from the vulnerability assessment and threat modelling to prevent attacks, and learning from attacks to update the probabilistic meta-model of the threat modelling). The toolkit will be implemented with the complete EPES value chain who will contribute to the specification, prototyping and demonstration phases of the project. Although the toolkit will be tailored to the needs of EPES operators, many of the technology building blocks and best practices will be transferable to other types of critical infrastructures.
Consortium	Coordinator: 1. Siveco Romania Sa (RO) Consortium: 2. Psi Software Ag (DE) 3. Si-Ga Data Security (2014) Ltd (IL) 4. Foreseeti Ab (SE) 5. L7 Defense Luxembourg Sarl (LU) 6. Tech Inspire Ltd (UK) 7. Konnekt Able Technologies Limited (IE) 8. City University Of London (UK)) 9. Kungliga Tekniska Hoegskolan (SE) 10. National Technical University Of Athens - Ntua (EL) 11. Software Company Eood (BU) 12. Kogen Zagore Eood (BU) 13. Mvets Lenishta Ood (BU) 14. Elektroenergien Sistemen Operator Ead (BU) 15. Cez Distribution Bulgaria Ad (BU) 16. Mig 23 Ltd (BU) 17. Dil Diel (BU) 18. Iren Spa (IT)

SDN-microSENSE	
Title	SDN-microSENSE *This project is also relevant for 6.3.2 Privacy and Data Protection and 4.2.1 Critical Energy Infrastructure: Electrical Power (Electricity) and Smart Grids, Oil, Gas*
Objective	Provide a set of secure, privacy-enabled EPES that is resilient to cyberattacks tools
Contract details	H2020-SU-SEC-2061; Topic code: SU-DS04-2018-2020; 1/5/2019 - 30/4/2022; € 7 992 462,50
Abstract	The smart energy ecosystem constitutes the next technological leap of the conventional electrical grid, providing multiple benefits such as increased reliability, better service quality and efficient utilization of the existing infrastructures. However, despite the fact that it brings beneficial environmental, economic and social changes, it also generates significant security and privacy challenges, as it includes a combination of heterogeneous, co-existing smart and legacy technologies. Based on this reality, the SDN-microSENSE project intends to provide a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of EPES as well as the integrity and the confidentiality of communications. In particular, adopting an SDN-based technology, SDN-microSENSE will develop a three-layer security architecture, by deploying and implementing risk assessment processes, self-healing capabilities, large-scale distributed detection and prevention mechanisms, as well as an overlay privacy protection framework. Firstly, the risk assessment framework will identify the risk level of each component of EPES, identifying the possible threats and vulnerabilities. Accordingly, in the context of self-healing, islanding schemes and energy management processes will be deployed, isolating the critical parts of the network in the case of emergency. Furthermore, collaborative intrusion detection tools will be capable of detecting and preventing possible threats and anomalies timely. Finally, the overlay privacy protection framework will focus on the privacy issues, including homomorphic encryption and anonymity processes.
Consortium	Coordinator: 1. Ayesa Advanced Technologies Sa (ES) Consortium: 2. Panepistimio Dytikis Makedonias (EL) 3. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 4. Preduzece Za Telekomunikacijske Usluge Realaiz Doo Beograd (Savski Venac) (RS) 5. Atos Spain Sa (ES) 6. Schneider Electric France Sas (FR) 7. Public Power Corporation S.A. (EL) 8. Fundacion Tecnalia Research & Innovation (ES) 9. Dimos Avdiron (EL) 10. Innovative Energy And Information Technologies Ltd (BU) 11. Elektroenergien Sistemen Operator Ead (BU) 12. Cez Distribution Bulgaria Ad (BU) 13. Ubitech Limited (CY) 14. Cyberlens Ltd (UK) 15. Sidroco Holdings Limited (CY) 16. 0 Infinity Limited (UK) 17. Eight Bells Ltd (CY) 18. Incites Consulting Sarl (LU) 19. Energynautics Gmbh (DE) 20. Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO) 21. Siaxampanis E.E. (EL) 22. Gottfried Wilhelm Leibniz Universitaet Hannover (DE) 23. Ravna Hydro Ltd (BU) 24. Fundacio Institut De Recerca De L'energia De Catalunya (ES) 25. Estabanell Y Pahisa Energia Sa (ES) 26. Checkwatt Ab (SE) 27. Independent Power Transmission Operator Sa (EL) 28. Sintef Energi As (NO) 29. Dil Diel (BU) 30. Optimizacion Orientada A La Sostenibilidad Sl (ES) 31. Geie Ercim (FR)

FORESIGHT	
Title	FORESIGHT *This project is also relevant for 4.2.2 Critical Transport / Transportation Infrastructure and 8.3.5 Training and Networking*
Objective	Develop a federated cyber-range solution to enhance the preparedness and skills of cyber-security professionals at all levels
Contract details	H2020-SU-SEC-2062; Topic code: SU-DS01-2018; 1/9/2019 - 31/8/2022; € 5 997 018,50
Abstract	The FORESIGHT project aims to develop a federated cyber-range solution to enhance the preparedness of cyber-security professionals at all levels and advance their skills towards preventing, detecting, reacting and mitigating sophisticated cyber-attacks. This is achieved by delivering an ecosystem of networked realistic training and simulation platforms that collaboratively bring unique cyber-security aspects from the aviation, smart grid and naval domains. The proposed platform will extend the capabilities of existing cyber-ranges and will allow the creation of complex cross-domain/hybrid scenarios to be built jointly with the IoT domain. Emphasis is given on the design and implementation of realistic and dynamic scenarios that are based on identified and forecasted trends of cyber-attacks and vulnerabilities extracted from cyber-threat intelligence gathered from the dark web; this will enable cyber-security professionals to rapidly adapt to an evolving threat landscape. The development of advanced risk analysis and econometric models will prove to be valuable in estimating the impact of cyber-risks, selecting the most appropriate and affordable security measures, and minimising the cost and time to recover from cyber-attacks. Innovative training curricula, guiding cyber-security professionals to implement and combine security measures using new technologies and established learning methodologies, will be created and employed for training needs; they will be linked to professional certification programs and be supported by learning platforms. Aside from the development of skills, the project aims at a holistic approach to cyber-threat management with the ultimate goal of cultivating a strong security culture. As such, the project puts considerable emphasis on research and development (i.e. research on cyber-threats, development of novel ideas, etc) as the key to increasing training dynamics and awareness methods for exceeding the rate of evolution of cyber-attackers
Consortium	Coordinator: 1. European Dynamics Luxembourg Sa (LU) Consortium: 2. Kentro Meleton Asfaleias (EL) 3. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 4. Cybercrime Research Institute Gmbh (DE) 5. Incites Consulting Sarl (LU) 6. Sheffield Hallam University (UK) 7. University Of Peloponnese (EL) 8. Minds & Sparks Gmbh (AT) 9. The University Court Of The University Of Abertay Dundee (UK) 10. Airbus Cybersecurity Sas (FR) 11. University Of Plymouth (UK) 12. Anoikto Panepistimio Kyprou (Open University Of Cyprus) (CY) 13. Ecole Navale (FR) 14. Cybexer Technologies (EE) 15. Athens International Airport S.A. (EL) 16. Thales Sa (FR) 17. Darzhavna Agentsiya Elektronno Upravlenie (BU) 18. Institut Po Otbrana (BU) 19. Innovative Energy And Information Technologies Ltd (BU) 20. Elektroenergien Sistemen Operator Ead (BU) 21. Cez Distribution Bulgaria Ad (BU)

SOTER	
Title	SOTER *This project is also relevant for 6.3.2 Privacy and Data Protection and 6.7 Financial crime*
Objective	Provide a comprehensive set of tools that will help the finance sector to increase their cybersecurity level, enabling the fight against present and future cyberattacks and vulnerabilities
Contract details	H2020-SU-SEC-2063; Topic code: SU-DS05-2018-2019; 1/7/2019 - 31/10/2021; € 3 026 246,13
Abstract	The Digitalization Era implies many advantages for businesses and citizens. However, new threats arise, especially in what concerns data privacy and the use of digital identities. These threats must be tackled under a holistic approach and pointing at their different origins, including the human factor. The European Union is reinforcing the legal framework to contribute to this need, including important requirements to be fulfilled, especially in the context of critical sectors identified under the NIS Directive. Finance is one of them, actually the most restrictive, because of the number of regulations to comply with. This makes finance the perfect scenario for testing tools, before transferring the results to other sectors. That is why SOTER is mainly focused on it, aiming at providing a comprehensive set of tools that will act as a transformative process of the finance sector, helping their players to increase their cybersecurity level, enabling the fight against present and future cyberattacks and vulnerabilities. The results will then increase their cyber-resilience. SOTER main results will be: SOTER Digital Onboarding Platform (the technology tool to provide a robust and sovereign digital identity, facilitating the interconnections between different services providers and the users), improved by the use of blockSOTER will offer tools that are able to determine the level of cyber security that exists in a certain entity, to improve if that is the case. We intend to get this through a comprehensive risk analysis to create contingency plans and direct action measures that can mitigate threats and security attacks. In the case of the finance sector, we propose to test and analyze a cloud platform of Digital Onboarding with two main features: use of technologies blockchain and innovative systems of biometric identification of users. Derived from this, training actions for end users will be generated so they are able to detect and deal with this type of threats.
Consortium	Coordinator: 1. Everis Spain Sl (ES) Consortium: 2. Banco Mediolanum Sa (ES) 3. Everis Aeroespacial Y Defensa Sl (ES) 4. Inauth Uk Ltd (UK) 5. Trunomi Limited (UK) 6. Trilateral Research Limited (IE) 7. Universitaet Graz (AT) 8. Research Industrial Systems Engineering (Rise) Forschungs-, Entwicklungs- Und Grossprojektberatung Gmbh (AT) 9. Fabrica Nacional De Moneda Y Timbre-Real Casa De La Moneda (ES)

Cyber-MAR	
Title	Cyber-MAR *This project is also relevant for 4.2.3 Critical Water Infrastructure*
Objective	Provide a cost-efficient cyber training solution covering the maritime logistics value chain
Contract details	H2020-SU-SEC-2064; topic code: SU-DS01-2018; 1/9/2019 - 31/8/2022; € 6 018 367,50
Abstract	Cyber-MAR is an effort to fully unlock the value of the use of cyber range in the maritime logistics value chain via the development of an innovative simulation environment adapting in the peculiarities of the maritime sector but being at the same time easily applicable in other transport subsectors. A combination of innovative technologies are the technology enablers of the proposed Cyber-MAR platform which is not only a knowledge-based platform but more importantly a decision support tool to cybersecurity measures, by deploying novel risk analysis and econometric models. CSIRTs/CERTs data collected will be analysed and feed the knowledge-based platform with new-targeted scenarios and exercises. Through Cyber-MAR, the maritime logistics value chain actors will increase their cyber-awareness level; they will validate their business continuity management minimizing business disruption potential. Cyber-MAR will act as a cost-efficient training solution covering the maritime logistics value chain.
Consortium	Coordinator: 1. Institute Of Communication And Computer Systems (EL) Consortium: 2. Naval Group (FR) 3. Teknologian Tutkimuskeskus Vtt Oy (FI) 4. Stathmos Emporevmatokivotion Peiraia Ae (EL) 5. Diateam (FR) 6. Fundacion De La Comunidad Valenciana Para La Investigacion, Promocion Y Estudios Comerciales De Valenciaport (ES) 7. World Maritime University (SE) 8. Fondazione Istituto Tecnico Superiore Mobilita Sostenibile Nei Settoritrasporti Marittimi E Della Pesca-Accademia Italiana Della Marina Merc (IT) 9. University Of Plymouth (UK) 10. Atos Spain Sa (ES) 11. Naytiliakes Metaforikes Kai Epikoinoniakes Epixeiriseis Seability Epe (EL) 12. Piraeus Europe Asia Rail Logisticsanonimi Etaireia Diaheirisis Efodiastikis Alysidas (EL) 13. Verisk Analytics Gmbh (DE)

PHOENIX	
Title	PHOENIX *This project is also relevant for 4.1.3 Cyber and physical threats to urban critical infrastructures and urban soft targets*
Objective	Develop a cyber-shield armour to European EPES infrastructure
Contract details	H2020-SU-SEC-2065; Topic code: SU-DS04-2018-2020; 1/9/2019 - 31/8/2022; € 7 995 004,25
Abstract	PHOENIX aims to offer a cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost. PHOENIX will realise 3 strategic goals: (1) Strengthen EPES cybersecurity preparedness by employing security a) "by design" via novel protective concepts for resilience, survivability, self-healing and accountability, and b) "by innovation" via adapting, upgrading and integrating a number of TRL5 developments to TRL7-8 and validating them in real-live large scale pilots; (2) Coordinate European EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national Member States and pan-European level, a novel fully decentralized inter-DLTs/blockchain based near real-time synchronized cybersecurity information awareness platform, among authorized EPES stakeholders, utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group; (3) Accelerate research and innovation in EPES cybersecurity by a novel deploy, monitor, detect and mitigate DevSecOps mechanism, a secure gateway, privacy preserving federated Machine Learning algorithms and establishment of certification methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre.
Consortium	Coordinator: 1. Capgemini Consulting (FR) Consortium: 2. Thales Six Gts France Sas (FR) 3. Thales Sa (FR) 4. Singularlogic Anonymi Etaireia Pliroforiakon Systimaton Kai Efarmogon Pliroforikis (EL) 5. Dnv Gl As (NO) 6. Intrasoft International Sa (LU) 7. Iskraemeco, Merjenje In Upravljanjeenergije, D.D. (SL) 8. Atos Spain Sa (ES) 9. Asm Terni Spa (IT) 10. Studio Tecnico Bfp Societa A Responsabilita Limitata (IT) 11. Emotion Srl (IT) 12. Elektro Ljubljana Podjetje Zadistribucijo Elektricne Energije D.D. (SL) 13. Blagovno Trgovinski Center Dd (SL) 14. Public Power Corporation S.A. (EL) 15. E.On Solutions Gmbh (DE) 16. Delgaz Grid Sa (RO) 17. Compania Nationala De Transport Alenergiei Electrice Transelectrica Sa (RO) 18. Societatea Pentru Servicii De Telecomunicatii Si Tehnologia Informatiei In Retele Electrice De Transportteletrans Sa (RO) 19. Centrul Roman Al Energiei - Cre (RO) 20. Cyberethics Lab Srls (IT) 21. Gridhound Gmbh (DE) 22. Synelixis Lyseis Pliroforikis Automatismou & Tilepikoinonion Anonimi Etairia (EL) 23. Comsensus, Komunikacije In Senzorika, Doo (SL) 24. Aalto Korkeakoulusaatio Sr (FI) 25. Rheinisch-Westfaelische Technische Hochschule Aachen (DE)

This overview is complemented by relevant H2020 projects.

PdbU	
Title	Securing Continuous Operations of Mission Critical IoT Endpoints
Objective	Feasibility study on developing and validating the market version of Power Drop BackUp (PdbU)
Contract details	H2020-SMEInst-2018-2020-1; 1/1/2019 - 30/4/2019; EUR: 50.000
Abstract	Energy Re-Connect has developed the Power Drop BackUp (PdbU), a patented native Power over Ethernet (PoE) platform that comes as a standalone device connected inline to any IoT Mission Critical Endpoint. The PdbU will be situated at the end of the network and provides combined solutions of power, communication backup and cyber IP gatekeeping. PoE enables converged cabling infrastructure, with the endpoints powered, connected and controlled over the Local Area Network (LAN) and no need for separate power cabling. This eliminates CAPEX and OPEX from dedicated AC cabling, which contributes to the PdbU's cost advantage (600% less compared to legacy systems). Further benefits of the PdbU include impenetrable cyber protection and predictive capabilities for possible IoT failures. The PdbU is at an advanced stage of development with commercial pre-series sales. During the feasibility study, we will develop a road map for the final version and Ph2 will see us developing and validating the market version of PdbU. Our turnover will come from the sale of our device to the surveillance and smart city markets. We target to achieve a collective turnover of €77M by the 5th year of commercialisation.
Consortium	Coordinator: Energy Re-Connect LTD (IL)

SECONDO	
Title	a Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era
Objective	Support professionals who seek cyber security investments, developed to support human decision making, and a complete well-founded security strategy
Contract details	H2020-MSCA-RISE-2018; 1/1/2019 - 31/12/2022; EUR: 1.600.800
Abstract	SECONDO addresses the question "How can decisions about cyber security investments and cyber insurance pricing be optimised?" SECONDO will support professionals who seek cyber security investments, developed to support human decision making, and a complete well-founded security strategy. This is a timely research problem, as the rapid growth of cyber-attacks is expected to continue its upwards trajectory. Such growth presents a prominent threat to normal business operations and the EU society itself. On the other hand, an interesting, well-known, finding is that an organisation's computer systems may be less secure than a competitor's, despite having spent more money in securing them. Budget setting, cyber security investment choices and cyber insurance, in the face of uncertainties, are highly challenging tasks with massive business implications. SECONDO aims to make impact on the operation of EU businesses who often: (i) have a limited cyber security budget; and (ii) ignore the importance of cyber insurance. Cyber insurance can play a critical role to the mitigation of cyber risk. This can be done by imposing a cost on firms' cyber risk through a premium that they have to pay and the potential for paying a smaller premium should they reduce their current cyber security risk. SECONDO has a cross-disciplinary nature, combining mathematical and engineering insights to empower innovative software. Apart from the novel research results, the project will offer a software platform to narrow the gap between theoretical understanding and practice. To achieve this, the four industrial project partners will i) lead the part of the project where industrial needs will be entered as input to the requirements collection phase, and, ii) provide their innovative software for risk assessment. The three academic partners will work together to i) design and thoroughly describe the proposed methodologies, but also ii) contribute to their software development.
Consortium	Coordinator: 1. University Of Piraeus Research Center (GR) Consortium: 2. "University Of Surrey (UK) 3. Technologiko Panepistimio Kyprou (CY) 4. Ubitech Limited (CY) 5. Lstech Espana Sl (ES) 6. Kromar Mesites Asfaleion Monoprosopi Epe (GR) 7. Fogus Innovations & Services P.C. (GR)"

ELEVATE	
Title	ELEVATE - Automated Detection & Response Control Access Network *This project is also relevant for 6.3.2 Privacy and Data Protection.*
Objective	Study technical, commercial and financial feasibility of ELEVATE - Automated Detection & Response Control Access Network, and develop business plan
Contract details	H2020-SMEInst-2018-2020-1; 1/2/2019 - 31/5/2019; EUR: 50.000
Abstract	Opencloud Factory brings to the market ELEVATE, a pioneering solution based on NAC (Network Access Control) technologies which intends to disrupt the digital cybersecurity market with a complete, integrated, autonomous and software-defined digital security solution for corporate networks. ELEVATE includes Security Automation and Orchestration (SA&O) and Managed Detection and Response (MDR) capabilities. Its main benefits stem from (1) obtaining 100% visibility and profiling in real-time of all kind of devices connected to the network, increasing visibility in 60% (2) reducing up to 35% on Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR), (3) allow a higher degree in the orchestration and integration of the cybersecurity tools, attaining a global synergy of all infrastructure, resulting in an efficiency increase of 25%, (4) maximising the efficiency of limited IT staff, reducing costs (20%), an increasing the overall productivity (25%), (5) increasing up to 50% the cybersecurity coverage of organizations.To complement these benefits we propose three unprecedented features: (1) Automated Provisioning, (2) Automated Threat Response and Integration and (3) Advanced Analytics. The novelty of ELEVATE mostly lies in the modular architecture and it is autonomous in the detection and response, minimizing the need for human resources both in the analysis (threat detection and diagnostic) and in the execution of tasks (threat response). To ensure the viability of ELEVATE we will assess its technical, commercial and financial feasibility and the IPR exploitation, and define our Business Plan so as to achieve the market uptake in the targeted European countries in 2021. ELEVATE meets the Cybersecurity policy stated in the Digital Single Market strategy to further improve EU cyber resilience and response and is also aligned with the objectives of the GDPR, whose aim is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world.
Consortium	Coordinator: Open Cloud Factory SL (ES)

SIMARGL	
Title	Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware *This project is also relevant for 6.3.3 Cyber crime*
Objective	Improve malware and stegomalware detection
Contract details	H2020-SU-ICT-2018; 1/5/2019 - 30/4/2022; EUR: 4.984.260
Abstract	With the prevailing risk of cybersecurity breaches, improving the cyber security posture and detection algorithms is of utmost importance. Malware is now recognized as the severe threat for commercial and critical IT systems (e.g. financial sector) , but also for citizens (e.g. mobile malware). Still, currently malware is well understood and can be tackled reasonably well. What is becoming more problematic, is the stegomalware and the use of the information hiding techniques by cyber criminals. And here comes SIMARGL: our goal is to focus on this emerging future threat and to significantly improve malware and stegomalware detection. Currently, cyber criminals use quite simple information hiding techniques, but they learn and improve quickly. Our consortium believes that we cannot stay many steps behind, but provide relevant techniques to be prepared for the future attacks and stegomalwre. SIMARGL consortium does not start from scratch (current solutions are described in the proposal) and it features relevant partners, expertise and links to fulfil the project goals.
Consortium	Coordinator: 1. Fernuniversitat In Hagen (DE) Consortium: 2. "Airbus Cybersecurity Sas (FR) 3. Consiglio Nazionale Delle Ricerche (IT) 4. Ustav Mezinarodnich Vztahu V.V.I. (CZ) 5. Itti Sp Zoo (PL) 6. Netzfactor Gmbh (DE) 7. Numera Sistemi E Informatica Spa (IT) 8. Pluribus One Srl (IT) 9. Siveco Romania Sa (RO) 10. Thales Six Gts France Sas (FR) 11. Politechnika Warszawska (PL) 12. Agentia De Administrare A Retelei Nationale De Informatica Pentru Educatie Si Cercetare (RO) 13. Stichting Cuing Foundation (NL) 14. Orange Polska Spolka Akcyjna (PL)"

CyberSec4Europe	
Title	Cyber Security Network of Competence Centres for Europe
Objective	Test and demonstrate potential governance structures for the network of competence centres in cybersecurity
Contract details	H2020-SU-ICT-2018-2 ; 1/2/2019 - 31/7/2022; EUR: 15.999.981,25
Abstract	CyberSec4Europe is a research-based consortium with 44 participants covering 21 EU Member States and Associated Countries. It has received more than 40 support letters and promises of cooperation from public administrations, international organisations, and key associations worldwide including Europe (such as ECSO), Asia, and North America. As pilot for a Cybersecurity Competence Network, it will test and demonstrate potential governance structures for the network of competence centres using the best practices examples from the expertise and experience of the participants, including concepts like CERN. CyberSec4Europe will support addressing key EU Directives and Regulations, such as GDPR, PSD2, eIDAS, and ePrivacy, and help to implement the EU Cybersecurity Act including, but not limited to supporting the development of the European skills-base, the certification framework and ENISA's role. The 26 ECSO participants in CyberSec4Europe are active in all 6 ECSO Working Groups, including chairing many subgroups in cybersecurity certification, vertical sectors, and international cooperation, as well as having representatives on the ECSO Board of Directors and the Cybersecurity Public-Private Partnership Board. CyberSec4Europe participants address 14 key cybersecurity domain areas, 11 technology/applications elements and nine crucial vertical sectors. With over 100 cybersecurity projects, CyberSec4Europe participants have been addressing a comprehensive set of issues across the cybersecurity domain. The project demonstration cases will address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and transportation. In addition to the demonstration of the governance structure and the operation of the network, CyberSec4Europe will develop a roadmap and recommendations for the implementation of the Network of Competence Centres using the practical experience gained in the project.
Consortium	Coordinator: 1. Johann Wolfgang Goethe-Universitatfrankfurt Am Main (DE) Consortium: 2. "Technische Universiteit Delft (NL) 3. Universidad De Murcia (ES) 4. Idryma Technologias Kai Erevnas (GR) 5. Nec Laboratories Europe Gmbh (DE) 6. Universita Degli Studi Di Trento (IT) 7. Masarykova Univerzita (CZ) 8. Cybernetica As (EE) 9. Trust In Digital Life (BE) 10. Conceptivity Sarl (CH) 11. Abi Lab-Centro Di Ricerca E Innovazione Per La Banca (IT) 12. Ait Austrian Institute Of Technology Gmbh (AT) 13. Archimede Solutions Sarl (CH) 14. Atos Spain Sa (ES) 15. Banco Bilbao Vizcaya Argentaria Sa* (ES) 16. Universidade Do Porto (PT) 17. Consiglio Nazionale Delle Ricerche (IT) 18. Institouto Technologias Ypologistonkai Ekdoseon Diofantos (GR) 19. Dawex Systems (FR) 20. Danmarks Tekniske Universitet (DK) 21. Engineering - Ingegneria Informatica Spa (IT) 22. Comune Di Genova (IT) 23. Informatique Banques Populaires (FR) 24. International Cyber Investigation Training Academy (BG) 25. Intesa Sanpaolo Spa (IT) 26. Jyvaskylan Ammattikorkeakoulu (FI) 27. Karlstads Universitet (SE) 28. Katholieke Universiteit Leuven (BE) 29. Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO) 30. Open & Agile Smart Cities (BE) 31. Politecnico Di Torino (IT) 32. Siemens Aktiengesellschaft (DE) 33. Sintef As (NO) 34. Time.Lex (BE) 35. University College Dublin, National University Of Ireland, Dublin (IE) 36. University Of Cyprus (CY) 37. Univerza V Mariboru (SI) 38. Universidad De Malaga (ES)"

CONCORDIA	
Title	Cyber security cOmpeteNce fOr Research anD Innovation
Objective	Address the current fragmentation of security competence by networking diverse competences into a leadership role via a synergistic agglomeration of a pan-European Cybersecurity Center
Contract details	H2020-SU-ICT-2018-2 1/1/2019 - 31/12/2022; EUR: 15.998.737,50
Abstract	Europe needs to step up its efforts and strengthen its very own security capacities to secure its digital society, economy, and democracy. It is time to reconquer Europe's digital sovereignty. The vision for Europe can only be to join forces across Europe's research, industry and public sector and to include all talents not just those that have representation in the EU mainstream or are within big organizations. Diversity and inclusion are keys for success. Europe has incredible coverage and talent in the area of IT and cybersecurity. The area of cybersecurity is geographically fragmented across Europe for competences, and often also technically fragmented with problem-specific development of security solutions. There is no doubt that excellent research exists in Europe. Nevertheless, it is a fact that this research does not result in IT products and solutions that contribute to the European Single Digital Market. On contrary, a lot of research, also financed by EU ERC grants, is tested on real data in large US companies that cooperate with them. Europe has to and is already rethinking this strategy. CONCORDIA addresses the current fragmentation of security competence by networking diverse competences into a leadership role via a synergistic agglomeration of a pan-European Cybersecurity Center. The vision of CONCORDIA is to build a community a strong cooperation between all stakeholders, understanding that all stakeholders have their KPIs, bridging among them, and fostering the development of IT products and solutions along the whole supply chain. Technologically, it projects a broad and evolvable data-driven and cognitive E2E Security approach for the ever-complex ever-interconnected compositions of emergent data-driven cloud, IoT and edge-assisted ICT ecosystems.

CONCORDIA	
Consortium	Coordinator: 1. Universitaet Der Bundeswehr Muenchen (DE) Consortium: 2. "Idryma Technologias Kai Erevnas (GR) 3. Universiteit Twente (NL) 4. Universite Du Luxembourg (LU) 5. Universite De Lorraine (FR) 6. Univerza V Mariboru (SI) 7. Universitat Zurich (CH) 8. Jacobs University Bremen Ggmbh (DE) 9. Universita Degli Studi Dell'insubria (IT) 10. Technologiko Panepistimio Kyprou (CY) 11. Panepistimio Patron (GR) 12. Technische Universitaet Braunschweig (DE) 13. Technische Universitat Darmstadt (DE) 14. Masarykova Univerzita (CZ) 15. Ben-Gurion University Of The Negev (IL) 16. Oslomet - Storbyuniversitetet (NO) 17. Imperial College Of Science Technology And Medicine (UK) 18. Universita Degli Studi Di Milano (IT) 19. Bayerische Akademie Der Wissenschaften (DE) 20. Eit Digital (BE) 21. Telenor Asa (NO) 22. Cassidian Cybersecurity Gmbh (DE) 23. Secunet Security Networks Ag (DE) 24. Infineon Technologies Ag (DE) 25. Stichting Internet Domeinregistratie Nederland (NL) 26. Surfnet Bv (NL) 27. Cyber-Detect (FR) 28. Telefonica Investigacion Y Desarrollo Sa (ES) 29. Ruag Schweiz Ag (CH) 30. Bitdefender Srl (RO) 31. Atos Spain Sa (ES) 32. Siemens Aktiengesellschaft (DE) 33. Flowmon Networks As (CZ) 34. Tuv Trust It Gmbh Unternehmensgruppe Tuv Austria (DE) 35. Telecom Italia Spa (IT) 36. Efacec Energia - Maquinas E Equipamentos Electricos Sa (PT) 37. Arthur's Legal Bv (NL) 38. Eesy-Innovation Gmbh (DE) 39. Dfn-Cert Services Gmbh (DE) 40. Caixabank Sa (ES) 41. Bayerische Motoren Werke Aktiengesellschaft (DE) 42. Ministry Of Digital Policy Telecommunication And Media (GR) 43. Rise Research Institutes Of Sweden Ab (SE) 44. Ericsson Ab (SE) 45. Sba Research Gemeinnutzige Gmbh (AT) 46. Institut Jozef Stefan (SI)"

ECHO	
Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Objective	Deliver an organized and coordinated approach to improve proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration
Contract details	H2020-SU-ICT-2018-2 1/3/2019 - 28/2/2023; EUR: 15.987.285
Abstract	ECHO delivers an organized and coordinated approach to improve proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration. The Partners will execute on a 48-month work plan to develop, model and demonstrate a network of cyber research and competence centres, with a central competence at the hub. The Central Competence Hub serves as the focal point for the ECHO Multi-sector Assessment Framework enabling multi-sector dependencies management, provision of an ECHO Early Warning System, an ECHO Federation of Cyber Ranges and management of an expanding collection of Partner Engagements. The ECHO Multi-sector Assessment Framework refers to the analysis of challenges and opportunities derived from sector specific use cases, transversal cybersecurity needs analysis and development of inter-sector Technology Roadmaps involving horizontal cybersecurity disciplines. The Early Warning System, Federation of Cyber Ranges and Inter-sector Technology Roadmaps will then be subject of Demonstration Cases incorporating relevant involvement of inter-dependent industrial sectors. The ECHO Cyber-skills Framework provides the foundation for development of cybersecurity education and training programmes including a common definition of transversal and inter-sector skills and qualifications needed by cybersecurity practitioners. The ECHO Cybersecurity Certification Scheme provides a sector specific and inter-sector process for cybersecurity certification testing of new technologies and products resulting from the proposed technology roadmaps. The project will develop and operate under an ECHO Governance Model, by which the efforts across the EU Network of Cybersecurity Competence Centres can be coordinated and optimized to provide lasting and sustainable excellence in cybersecurity skills development; research and experimentation; technology roadmaps delivery; and certified security products for improved cybersecurity resilience.
Consortium	Coordinator: 1. Ecole Royale Militaire - Koninklijke Militaire School (BE) Consortium: 2. "Rhea System (BE) 3. Institut Po Otbrana (BG) 4. Vitrociset Belgium Sprl (BE) 5. Acea Spa (IT) 6. Aon Spa Insurance & Reinsurance Brokers (IT) 7. Tallinna Tehnikaulikool (EE) 8. Fondatsiya Evropreyski Softueren Institut - Tsentar Iztochna Evropa (BG) 9. Institute Of Information And Communication Technologies (BG) 10. Telelink Business Services Ead (BG) 11. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (GR) 12. National University Of Ireland Maynooth (IE) 13. Telefonica Moviles Espana Sa (ES) 14. Exprivia Spa (IT) 15. Consorzio Italiano Per La Ricerca Medica (IT) 16. Akademia Gorniczo-Hutnicza Im. Stanislawa Staszica W Krakowie (PL) 17. Laurea-Ammattikorkeakoulu Oy (FI) 18. National Aerospace University Kharkiv Aviation Institute Named By N Zukovskiy (UA) 19. Semmelweis Egyetem (HU) 20. Visionspace Technologies Gmbh (DE) 21. Zanasi Alessandro Srl (IT) 22. Bournemouth University (UK) 23. Link Campus University (IT) 24. Guardtime As (EE) 25. Fincantieri Spa (IT) 26. Naval Group (FR) 27. Enquirya Bv (NL) 28. Siveco Romania Sa (RO) 29. Universitatea Nationala De Aparare Carol I (RO) 30. Certsign SA (RO)"

GUARD	
Title	A cybersecurity framework to GUArantee Reliability and trust for Digital service chains *This project is also relevant for 6.3.2 Privacy and Data Protection.*
Objective	Develop an open and extensible platform for advanced assurance and protection of trustworthy and reliable business chains spanning multiple administrative domains and heterogeneous infrastructures
Contract details	H2020-SU-ICT-2018 1/5/2019 - 30/4/2022; EUR: 4.684.700
Abstract	Tackling conflicting trends in the cybersecurity market, like fragmentation or vendor lock-ins, GUARD will develop an open and extensible platform for advanced assurance and protection of trustworthy and reliable business chains spanning multiple administrative domains and heterogeneous infrastructures. The purpose of GUARD is manifold: i) to increase the information base for analysis and detection, while preserving privacy, ii) to improve the detection capability by data correlation between domains and sources, iii) to verify reliability and dependability by formal methods that take into account configuration and trust properties of the whole chain, and iv) to increase awareness by better propagation of knowledge to the humans in the loop. The distinctive approach of GUARD will be the architectural separation between analysis and data sources, mediated by proper abstraction; this paradigm will result in an open, modular, pluggable, extendable, and scalable security framework. This holistic solution will blend security-by-design with enhanced inspection and detection techniques, raising situational awareness at different levels of the companies' structure by tailored informative contents, so to enable quick and effective reaction to cyber-threats. Demonstration and validation in two challenging scenarios is envisioned to bring the technology to an acceptable level of maturity, as well as direct involvement of relevant stakeholders for concrete business planning.
Consortium	Coordinator: 1. Maggioli Spa (IT) Consortium: 2. "Italtel Spa (IT) 3. Consorzio Nazionale Interuniversitario Per Le Telecomunicazioni (IT) 4. Fiware Foundation Ev (DE) 5. Wobcom Gmbh Wolfsburg Fur Telekommunikation Und Dienstleistungen (DE) 6. Minds & Sparks Gmbh (AT) 7. Ait Austrian Institute Of Technology Gmbh (AT) 8. Idryma Technologias Kai Erevnas (GR) 9. Eight Bells Ltd (CY) 10. Naukowa I Akademicka Siec Komputerowa - Panstwowy Instytut Badawczy (PL) 11. Mc2 Innovations Spolka Z Ograniczona Odpowiedzialnoscia (PL) 12. Pravo I Internet Foundation (BG) 13. J.I.G. Internet Consulting Sl (ES) 14. Universita Degli Studi Di Roma Tor Vergata (IT)"

TRINITY	
Title	Digital Technologies, Advanced Robotics and increased Cyber-security for Agile Production in Future European Manufacturing Ecosystems *This project is also relevant for 8.3.5 Training and Networking*
Objective	Create a network of multidisciplinary and synergistic local digital innovation hubs (DIHs) that can contribute to agile production
Contract details	H2020-DT-2018-1; 1/1/2019 - 31/12/2022; EUR: 15.997.267,25
Abstract	The main objective of TRINITY is to create a network of multidisciplinary and synergistic local digital innovation hubs (DIHs) composed of research centers, companies, and university groups that cover a wide range of topics that can contribute to agile production: advanced robotics as the driving force and digital tools, data privacy and cyber security technologies to support the introduction of advanced robotic systems in the production processes. The result will be a one-stop shop for methods and tools to achieve highly intelligent, agile and reconfigurable production, which will ensure Europe's welfare in the future. The network will start its operation by developing demonstrators in the areas of robotics we identified as the most promising to advance agile production, e.g. collaborative robotics including sensory systems to ensure safety, effective user interfaces based on augmented reality and speech, reconfigurable robot workcells and peripheral equipment (fixtures, jigs, grippers, ...), programming by demonstration, IoT, secure wireless networks, etc. These demonstrators will serve as reference implementation for two rounds of open calls for application experiments, where companies with agile production needs and sound business plans will be supported by TRINITY DIHs to advance their manufacturing processes. Besides technology-centered services, primarily laboratories with advanced robot technologies and know-how to develop innovative application experiments, TRINITY network of DIHS will also offer training and consulting services, including support for business planning and access to financing. Services of participating DIHs and dissemination of information to wider public will be provided through a digital access point that will be developed in the project. Another important activity of the project will be the preparation of a business plan to sustain the network after the end of the project funding.
Consortium	Coordinator: 1. Tampereen Korkeakoulusaatio Sr (FI) Consortium: 2. "Centria Ammattikorkeakoulu Oy (FI) 3. Universitetet I Tromsoe - Norges Arktiske Universitet (NO) 4. Institut Jozef Stefan (SI) 5. Panepistimio Patron (GR) 6. Budapesti Muszaki Es Gazdasagtudomanyi Egyetem (HU) 7. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 8. Flanders Make Vzw (BE) 9. Elektronikas Un Datorzinatnu Instituts (LV) 10. Leuven Security Excellence Consortium L-Sec Vzw (BE) 11. Fastems Oy Ab (FI) 12. Lp-Montagetechnik Gmbh (DE) 13. F6s Network Limited (UK) 14. Uab Civitta (LT) 15. Comite Europeen De Cooperation Des Industries De La Machine-Outil Cecimo Aisbl (BE) 16. Toppindustrisenteret As (NO)"

BAnDIT	
Title	Blockchain Attack and Defense Techniques *This project is also relevant for 6.3.2 Privacy and Data Protection and 8.3.5 Training and Networking.*
Objective	Provide an innovative research training network on Advanced Blockchain Attacks and Defense Techniques
Contract details	H2020-MSCA-ITN-2018; 1/3/2019 - 28/2/2023; EUR: 1.051.413,84
Abstract	BAnDiT or Advanced Blockchain Attacks and Defense Techniques is an innovative research training network with two beneficiary organizations, Universitat Pompeu Fabra (UPF) in the academic sector and Nokia Bell Labs in the private sector, which aims at bridging this gap. UPF will contribute through the network her knowledge and research experience in the departments of Information and Communication Technologies, Economics and Law and Nokia its hands-on experience in BCT. Partner organisations will contribute with transversal training events and providing access to existing blockchain ecosystems to test the results of the research conducted by the ESRs.
Consortium	Coordinator: 1. Universidad Pompeu Fabra (ES) Consortium: 2. Nokia Bell Labs France (FR)

This overview is complemented by two Marie Skłodowska-Curie Actions projects.

DIGIACT	
Title	Digital Authoritarian Practices: Internet Surveillance and Repression against Transnational Activist Networks
Objective	Investigate forms of digitally enabled information control, surveillance and repression against political activists, journalists and human rights defenders from the Middle East and North Africa (MENA) who reside in the European Union
Contract details	H2020-MSCA-IF-2018; 1/11/2019 - 31/10/2021; € 178 320
Abstract	Transnational advocacy networks play an important role in exposing rights violations and undermining media censorship under authoritarian regimes. Yet, repressive states increasingly resort to surveillance, malware attacks, online harassment and disinformation campaigns to compromise transnational civil society activists and mute their voices. DIGIACT investigates forms of digitally enabled information control, surveillance and repression against political activists, journalists and human rights defenders from the Middle East and North Africa (MENA) who reside in the European Union. The project provides an in-depth analysis of how threats to freedom of expression and privacy of transnational activists emerge and spread in an environment of rapidly evolving digital technologies. The research studies the motivations and capabilities of the regimes behind the threats, the effects on targeted communities and their strategies of resistance, and the implications both on a normative (international human rights law and other legal frameworks) and practical level (risk mitigation and capacity building). With this research agenda, DIGIACT aims to contribute to a) concept building on the relationship between digital technologies and authoritarian politics, and b) the debate on how to protect fundamental norms and rights in the digital age. To accomplish these goals, the project is embedded in the research group on Law, Science, Technology & Society (LSTS) at VUB where the applicant will receive training in theoretical and legal approaches to surveillance, privacy and data protection in the context of digital technologies.
Consortium	Coordinator: Vrije Universiteit Brussel (BE)

MAMONET	
Title	Massive MIMO for Securing Internet of Things Networks
Objective	Develop efficient and practical PhySec techniques that benefit from the surplus degrees of freedom and opportunities offered by massive MIMO (M-MIMO)
Contract details	H2020-MSCA-IF-2018; 1/4/2020 - 31/3/2022; € 214 158,72
Abstract	The aim of the MAMONET project is to develop efficient and practical PhySec techniques that benefit from the surplus degrees of freedom and opportunities offered by massive MIMO (M-MIMO), as a key technology for next generation networks, to guarantee secure and trusted communication links over IoT networks. The project will follow an interdisciplinary approach that bridges the gap between theoretical concepts and the industrial practices. Three novel research approaches will be considered: (i) a power-based approach, (ii) a location-based approach and (iii) a bandwidth-based approach. This research action will draw on my experience in PhySec and M-MIMO, supported by the supervisor and state-of-the-art equipment at the host institutio This project is also relevant for 6.3.2 Privacy and Data Protection and 8.3.5 Training and Networking. n. Additionally, the proposed activities will be complemented by training and collaboration with industry through a secondment. This creates a unique opportunity for me to consolidate my research and entrepreneurial skills. The impact of the proposed activities is in accordance with European initiatives, creating opportunities for the secure networked society and efficiency of European stakeholders. The outcomes will be aligned with the H2020 call for Digital Security for trustworthy ICT. The communication, dissemination and exploitation plans will build upon established contacts and actions by engaging the relevant stakeholders using different messages and media.
Consortium	Coordinator: Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO)

6.3.2 Privacy and Data Protection

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Privacy and Data Protection	AEGIS ARIES BlockChainKYC BPR4GDPR CREDENTIAL Cyberwatching.eu DEFeND EUNITY EYE-O-T FENTEC FutureTrust GO 4G IDENTITY OLYMPUS OPERANDO PANORAMIX PAPAYA PDP4E Pilot programme for data exchange of the Passenger Information Units PosEID-ON PRIVACY FLAG PRIVILEDGE PROMETHEUS PROTONSUIT REASSURE ReCRED SAFECLOUD SMOOTH SPECIAL SpeedXRays TRUESEC.EU TYPES VISION U2PIA ULTRAFiBi

This overview is complemented by the following H2020 projects.

SAPPAN	
Title	Sharing and Automation for Privacy Preserving Attack Neutralization *This project is also relevant vor 6.3.1 Cyber Security Management (for SMEs/business, local public authorities) and 9.2 Standardisation, testing & Certification.*
Objective	Develop a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning
Contract details	H2020-SU-ICT-2018 1/5/2019 - 30/4/2022; EUR: 4.175.070
Abstract	SAPPAN aims to develop a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning. SAPPAN will provide a cyber threat intelligence system that decreases the effort required by a security analyst to find optimal responses to and ways to recover from an attack. SAPPAN will enable this within a single organization as well as across organisations through novel models for privacy-preserving data processing and sharing. It will enable utilizing external experts for intrusion detection and sharing of knowledge on response and recovery actions while respecting the privacy and confidentiality requirements of individuals and organizations. SAPPAN will enable a European level perspective on advanced cyber security threats detection, response, and recovery making four key contributions that go beyond existing approaches: (1) privacy-preserving aggregation and data analytics including advanced client-side abstractions; (2) federated threat detection based on sharing of anonymised data and sharing of trained machine learning models; (3) standardisation of knowledge in the context of incident response and recovery to enable reuse and sharing; (4) visual, interactive support for Security Operation Center operators. SAPPAN aims to provide solutions for public international institutions and multinational companies who want to enrich their Situational Awareness by sharing cyber security intelligence as well as solutions for small and midsize companies enabling them to outsource intrusion detection. SAPPAN will be demonstrated in the relevant environments of 2 multinational companies, 1 National Research and Education Network (NREN) and 2 Computer Security Incident Response Teams (CSIRT). The consortium consists of 1 NREN, 3 multinational companies, 3 universities and 1 research institute so as to maximise the technical and societal impact, the dissemination and uptake of the results.
Consortium	Coordinator: 1. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) Consortium: 2. "Hewlett-Packard Galway Limited (IE) 3. Cesnet Zajmove Sdruzeni Pravnickych Osob (CZ) 4. Masarykova Univerzita (CZ) 5. F-Secure Oyj (FI) 6. Rheinisch-Westfaelische Technische Hochschule Aachen (DE) 7. Universitaet Stuttgart (DE) 8. Dreamlab Technologies AG (CH)"

C4IIoT	
Title	Cyber security 4.0: protecting the Industrial Internet Of Things *This project is also relevant for 6.3.1 Cyber Security Management (for SMEs/business, local public authorities) and 6.3.3 Cyber Crime.*
Contract details	Build and demonstrate a novel and unified Industrial Internet of Things (IIoT) cybersecurity framework for malicious and anomalous behavior anticipation, detection, mitigation, and end-user informing
Abstract	H2020-SU-ICT-2018 1/6/2019 - 31/5/2022; EUR: 4.993.533,75
Website	Recent trends in industrial technology and the adaptation of Industrial Internet of Things (IIoT), has emerged by the convergence of Operations Technology (i.e., traditional hardware and software systems) and Information Technology (i.e., advanced computing, data aggregation/analysis, and ubiquitous communication systems). IIoT has great potential to enable significant advances in optimizing operations among large number of increasingly autonomous control systems and devices, and can have a profound impact on many industry domains, where smart factories and logistics are among most notable cases. However, a major barrier towards IIoT adoption lies in cybersecurity issues that makes it extremely difficult to harness its full potential: IIoT systems dramatically increase the attack surface (introducing new security threats due to newly connected devices and protocols, making them more vulnerable to interference), the disruption of process controls, the theft of intellectual property, the loss of corporate data, and the industrial espionage. C4IIoT will build and demonstrate a novel and unified IIoT cybersecurity framework for malicious and anomalous behavior anticipation, detection, mitigation, and end-user informing. The framework provides a holistic and disruptive security-enabling solution for minimizing attack surfaces in IIoT systems, by exploiting i) emerging security software and hardware protection mechanisms; ii) state of the art machine and deep learning and privacy-aware analytics; iii) novel encrypted network flow analysis; iv) secure-by-design IIoT device fabrication; and v) blockchain technologies, to provide a viable scheme for enabling security and accountability, preserving privacy, enabling reliability and assuring trustworthiness within IIoT applications. The C4IIoT framework will be demonstrated and validated on two carefully selected use cases in real world environments, namely Enabling security IIoT in i) Inbound Logistics and ii) a Smart Factory
Consortium (prone to modification in case of GA amendment)	Coordinator: 1. Idryma Technologias Kai Erevnas (GR) Consortium: 2. "Centro Ricerche Fiat Scpa (IT) 3. Infineon Technologies Ag (DE) 4. Thales Six Gts France Sas (FR) 5. Hewlett Packard Italiana Srl (IT) 6. Commissariat A L Energie Atomique Et Aux Energies Alternatives (FR) 7. Ibm Israel - Science And Technology Ltd (IL) 8. Aegis It Research Ug (Haftungsbeschrankt) (DE) 9. Universite Paris I Pantheon-Sorbonne (FR) 10. Information Technology For Market Leadership (GR) 11. Sphynx Technology Solutions Ag (CH) 12. University Of Novi Sad Faculty Of Sciences (RS) 13. University Of Greenwich (UK) 14. Vip Mobile Doo Beograd (Novi Beograd) (RS)"

BiowatchID	
Title	A secure wearable for payments, ticketing, access control and ID management *This project is also relevant for 8.3.3 Public Protection.*
Objective	Develop BiowatchID, a secure vault that only the owner can use due to continuous biometric authentication
Contract details	H2020-SMEInst-2018-2020-1; 1/2/2019 - 31/5/2019; EUR: 50.000
Abstract	BiowatchID is a smart band worn on the wrist, which is a secure vault that only the owner can use due to continuous biometric authentication. BiowatchID uses a secure patented wrist vein identification technology with demonstrated 99,999% reliability. It is a tamper-proof, military grade security device which supports multiple protocols & communication channels. Once BiowatchID is closed on the wrist, it scans & recognizes the unique vein pattern, and then continuously monitors the presence of the wrist. BiowatchID is designed to replace ID cards & passports; credit cards, loyalty cards, mobility cards; car keys, passwords, access badges; (and in the long term) Touch ID, Face ID & other similar biometric authentication solutions. Most importantly, BiowatchID can combine all of the above in a single wearable. Our research shows that there will be at least 160m wearable devices with seamless biometric authentication solutions by 2020. Our commercial target is to sell 500,000 by 2023, reaching €100m+ in revenues.
Consortium	Coordinator: Biowatch SA (CH)

6.3.3 Cyber crime

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Cyber crime	3ants ANITA CAMINO CAPER COCKPITCI COUNTERCRAFT COURAGE CWIT CYBERROAD E-CRIME ECTEG 2.0 EKSISTENZ ESCORTS EU OF2CEN FREETOOl v2.0 HYRIM I-CARE KEEPERS PREEMPTIVE PRoBos SAINT SCOUT SENTER SERSCIS SPARKS ThreatMARK UNFRAUD

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

BorderSens	
Title	BorderSens
Objective	Enable highly accurate selective detection of trace levels of illicit drugs and precursors at the borders
Contract details	H2020-SU-SEC-2019; Topic code: SU-BES02-2018-2019-2020; 1/9/2019 - 31/8/2023; € 5 504 415
Abstract	Combining robust sensor technologies with the inherent advantages of electrochemical strategies, nano-molecularly imprinted polymers, and multivariate and pattern data analysis, BorderSens will enable highly accurate selective detection of trace levels of illicit drugs and precursors. With borders being important gateways for the entrance of illicit drugs and their precursors, custom and border control authorities are facing pertaining challenges to detect such dangerous substances and safeguard the public. The main challenges posed by currently used on-site methods to detect illicit drugs and precursors are low accuracy, in the case of colour tests, and high cost and low portability, in the case of spectroscopic tests. In the light of a pressing need for better drug test systems at EU borders, the ultimate research aim of the BorderSens is to develop a portable, wireless single prototype device with the capability to quickly test for different types of drugs, precursors and adulterants/cutting agents, with outstanding accuracy and reduced false positives and false negatives. BorderSens will demonstrate the innovative technological solutions at seven demonstrations sites at EU borders with end-users and ensure exploitation plans guaranteeing strong impact. BorderSens brings together universities, a big manufacturer of electrochemical sensors, a specialised SME, ten end-users i.e. forensic institutes, police forces and border authorities, and a high quality external advisory board, to provide an excellent scientific-technical perspective and a straightforward exploitation route, with great impact on the safety of EU citizens..
Consortium	Coordinator: 1. Universiteit Antwerpen (BE) Consortium: 2. University Of Leicester (UK) 3. Universitatea De Medicina Si Farmacie Iuliu Hatieganu Cluj-Napoca (RO) 4. De Federale Overheidsdienst Justitie - Le Service Public Federal Justice (BE) 5. Universitat Autonoma De Barcelona (ES) 6. Inspectoratul General Al Politiei Romane (RO) 7. Metrohm Dropsens Sl (ES) 8. Ministerie Van Financien (NL) 9. Scottish Police Authority (UK) 10. Izertis Sociedad Limitada (ES) 11. Service Public Federal Finances (BE) 12. Swedish Customs (SE) 13. Inspectoratul General Al Politiei De Frontiera (RO) 14. Police Grand-Ducale (LU) 15. Muitines Kriminaline Tarnyba (LT) 16. Home Officeuniversity Of Leicester (UK) 17. Universitatea De Medicina Si Farmacie Iuliu Hatieganu Cluj-Napoca (RO) 18. De Federale Overheidsdienst Justitie - Le Service Public Federal Justice (BE) 19. Universitat Autonoma De Barcelona (ES) 20. Inspectoratul General Al Politiei Romane (RO) 21. Metrohm Dropsens Sl (ES) 22. Ministerie Van Financien (NL) 23. Scottish Police Authority (UK) 24. Izertis Sociedad Limitada (ES) 25. Service Public Federal Finances (BE) 26. Swedish Customs (SE) 27. Inspectoratul General Al Politiei De Frontiera (RO) 28. Police Grand-Ducale (LU) 29. Muitines Kriminaline Tarnyba (LT) 30. Home Office (UK)

CRITICAL-CHAINS	
Title	CRITICAL-CHAINS *This project is also relevant for 6.7 Financial crime*
Objective	Deliver a novel triangular accountability model and integrated framework supporting secure and privacy-preserving financial contracts and transactions to protect against illicit transactions, illegal money trafficking and fraud on FinTech e-operations
Contract details	H2020-SU-SEC-2060; Topic code: SU-DS05-2018-2019; 1/7/2019 - 30/6/2022; € 4 182 154,25
Abstract	Irregular and unaccountable transactions, cyber threats, non-user-friendly inefficient or impractical banking processes, complex contracting procedures and cumbersome financial market and insurance infrastructures constitute obstacles to European open market development. CRITICAL-CHAINS delivers a novel triangular accountability model and integrated framework supporting accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions to protect against illicit tranasctions, illegal money trafficking and fraud on FinTech e-operations. This is an innovative cloud-based "X-as-a Service" solution stack including several layers: 1) Data integrity checking by involving financial institutions in the distributed Blockchain network; 2) Transaction and financial data flows analytrics, modelling and mining; 3) Threat Intelligence & Predictive Modelling for Inter-Banks and Internet Banking, insurnace and financial market infrastructures; 4) Multilateral Biometric-based and Role-based Authorisation & Authentication; 5) Hardware Security Module (HSM) enabled Cyber-Physical Security, embedded systems & IoT security for secure access using Security-Privacy-Contexts Semantic Modelling; 6) Secure and smart use of Blockchain based on keyless signature infrastructure and hybrid (a)symmetric cryptography utilising truly random key generation. CRITICAL-CHAINS is to be validated within 4 case studies aligned with 3 critical sectors: banking, financial market infrastructures and the insurance sector. This will evaluate system reliability, usability, user-acceptance, social, privacy, ethical, environmental and legal compliance by scrutiny of the geo-political and legal framework bridging the European economy with the rest of the world. The Consortium respresents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector.
Consortium	Coordinator: 1. The University Of Reading (UK) Consortium: 2. Commissariat A L Energie Atomique Et Aux Energies Alternatives (FR) 3. Ergunler Insaat Petrol Urunleri Otomotiv Tekstil Madencilik Su Urunler Sanayi Ve Ticaret Limited Sti. (TR) 4. Ey Advisory Spa (IT) 5. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 6. Guardtime As (EE) 7. Stichting Imec Nederland (NL) 8. Indra Sistemas Sa (ES) 9. Joanneum Research Forschungsgesellschaft Mbh (AT) 10. Netas Telekomunikasyon Anonim Sirketi (TR) 11. Poste Italiane - Societa Per Azioni (IT) 12. Rina Consulting Spa (IT)

This overview is complemented by ISF-funded projects.

4NSEEK	
Title	Forensic Against Sexual Exploitation of Children
Objective	Improve the overall process of preventing, detecting and arresting suspects of child sexual abuse (CSA)
Contract details	ISFP-2017-AG-CYBER; 1/1/2019 - 31/12/2020; 1.245.528,15
Abstract	This proposal action "Forensic Against Sexual Exploitation of Children" (4NSeek) aims at developing and reinforcing services for the benefit of affected children, families and educators. Addressing the problem from different points will help to improve the overall process of preventing, detecting and arresting suspects of child sexual abuse (CSA). Main objectives International Police Cooperation. Testing a CSA tool and providing feedback, Training. Specific CSA agenda included on the Cybersecurity Summer BootCamp event, Policy harmonization. Elaborate a forensic procedure to formalise devices analysis, Awareness and Dissemination. Elaboration and sharing of guides, Technology research development. Improve a CSA specific software to work over on entire devices with AI and ML techniques

AviaTor	
Title	Augmented Visual Intelligence and Targeted Online Research
Objective	Design and develop measures to assist LEAs and NGOs in combatting CSAM more effectively in the short term and to investigate future measures to end all forms of violence against children by 2030
Contract details	ISFP-2017-AG-CYBER; 1/12/2018 – 30/11/2020; 969.627,58
Abstract	Goal of the AviaTor project is to design and to develop measures to assist LEAs and NGOs in combatting CSAM more effectively in the short term and to investigate future measures to end all forms of violence against children by 2030. The amount of CSAM reports is growing rapidly and LEAs simply do not have the resources to handle these reports, leaving many reports untouched and victims unidentified. This Action aims at developing automation and intelligence tools (Forensic Delivery Channel - FDC) to greatly reduce the required amount of manual labour for LEAs in assessing reports, so that their effort can be spent on the actual investigating of reports and building cases. The impact of the AviaTor project is a smarter prioritization, assessment and handling of CSAM-reports which enables LEAs to focus on the most urgent and relevant cases. More effective police-time and capacity means more cases handled, more victims rescued, and more offenders caught, creating a safer (European) society better able to protect its citizens.

CERBERUS	
Title	Child Exploitation Response by Beating Encryption and Research to Unprotect Systems
Objective	Create a password cracking platform which can be used by any law enforcement agency of EU member states
Contract details	ISFP-2017-AG-CYBER; 1/2/2019 – 31/1/2021; 2.605.711,08
Abstract	This project will create a password cracking platform which can be used by any law enforcement agency of EU member states. Serving as a first layer of cracking, it is a complementary solution to the EC3 password cracking infrastructure. It will allow investigators to crack passwords used by criminals to protect their data (child pornographic images or movies, banking transactions, etc.) or their communications. Hence, it will help judges to prosecute authors of crimes since they will have at their disposal all evidences needed which are, until now, hidden thanks to strong passwords. Its two main added values relies on 1/ extracting "secrets" of devices, mandatory step before cracking the passwords used on the device, 2/ providing judges the evidence needed to prosecute and condemn authors. This solution meets the needs to all EU member states because each of them is facing cybercrime. Providing such a platform and such know-how to all EU member states, this project will help them coping with cybercrime, even if their own resource is not sufficient. Using this platform, each law enforcement agency will be able to raise its level of fighting cybercrime, and its level of expertise or rely on the ones of the participants. In doing so, CERBERUS aims at being one of the cyber watchdogs EU needs.

ECTEG 2.0	
Title	IT crime and IT forensics course package creation for LEA *This project is also relevant for 6.2 Forensics*
Objective	Create, update and distribute IT crime- and IT forensics training and education materials by ECTEG members, to remedy existing gaps identified by the governance model and the competency framework maintained by Europol-EC3, CEPOL, Eurojust and ECTEG
Contract details	ISFP-2016-AG-IBA-ECTEG; 1/11/2017 – 31/10/2019; 1.595.837,59
Abstract	The action will cover the creation, update and distribution of IT crime and IT forensics training and education materials by ECTEG members to remedy existing gaps identified by the governance model and the competency framework maintained by Europol-EC3, CEPOL, Eurojust and ECTEG. To improve synergies, coherency and quality, supporting activities will provide needed technical and pedagogical standards for the development and the deployment of the delivered training package on international and national level.Indirect outcome will be streamlining of cybercrime across the EU, sharing knowledge and expertise, promoting standardisation of methods and procedures for training programmes and cooperation with other international organisations, collaboration with academic partners to establish academic qualification in the field of cybercrime.

ENFORCE	
Title	ENhancing the skills of Cybercrime Fighters in a context of Rapid technology ChangEs
Objective	Design, set up, and disseminate a cybercrime training program at the European level
Contract details	ISFP-2017-AG-CYBER; 1/12/2018 – 31/5/2020; 504.184,00
Abstract	The ENFORCE project aims at designing, setting-up, and disseminating a cybercrime training program at the European level. This curriculum will be validated during a training exercise allowing different European public (law enforcement agencies and CERTs) and private actors fighting cybercrime to train together thanks to state-of-the-art training technology. The key outcomes of the project are: (1) A European cybercrime training curriculum to fill in the expertise gap in particular in the context of cross-border and public-private cooperation; (2) A European cybercrime exercise to validate the training curriculum and enable operational cooperation; (3) Recommendations to support the on-going effort to define EU-wide standards for cybercrime training. Community-building in ENFORCE will also seek to engage with law enforcement and academic experts beyond the consortium and facilitate the exchange of best practices.

FTv3.0	
Title	FREETOOL v3.0 - Integration and Consolidation
Objective	Enhance the usability and accessibility of the outputs from previous FREETOOL (FT) projects through a comprehensive programme of large scale user testing, tool refinement, tool packaging and resource development
Contract details	ISFP-2017-AG-CYBER; 1/2/2019 – 31/1/2021; 1.341.820,66
Abstract	The objective of FREETOOL v3.0 is to vastly enhance the usability and accessibility of the outputs from previous FREETOOL (FT) projects through a comprehensive programme of large scale user testing, tool refinement, tool packaging and resource development. The project activities will include: Two 'Testathon' events, where LE participants will run the tools through a range of investigation scenarios. The testathons will give LEAs and FT developers a chance to work together to address any bugs or issues with the software, and also identify further tool requirements. Further development of existing tools to address the most recent LE challenges: Virtual Currency detection/investigation will be introduced to a number of tools, as will extended functionality for use on mobile devices, OSx and Linux. Development of a FREETOOL toolbox where tools will be combined into 'sets' for use against a specific challenge and/or crime. There are already several FT tools that can support detection of encryption at various levels, and can also extract data to facilitate password recovery. These tools will be integrated into a single resource. There will also be other tool combinations for Triage (prioritisation of investigations), Image Analysis (identification of child exploitation material) and Dark Net Monitoring. As learning from hefty user manuals is time-consuming, the project will develop a series of 'how-to' videos that will provide practical examples of how the tools can be deployed. A web platform to facilitate communications and feedback between developers and users will also be developed.

P3 CyberFraud	
Title	Private-Public-Partnerhip against Cybercrime and Financial Fraud
Objective	Foster Law Enforcement and private sector (PS) partnership in Europe by organizing joint trainings for Law Enforcement and PS fraud prevention professionals, webinars, establishing working groups (WGs) and a P3 secondment program against specific problems and enabling Law Enforcement officers to liaise with relevant stakeholders of the private sector
Contract details	ISFP-2017-AG-CYBER; 1/1/2019 – 31/12/2020; 689.180,58
Abstract	P3 CyberFraud project is to take a giant leap forward in Private-Public-Partnership (P3) in EU against financial fraud and cybercrime. Cybercrime and online fraud is rising in all EU countries and the cross-border nature of cybercrime requires new approaches of private companies and the Law Enforcement (LEA) to find new ways to both prevent and investigate cybercrime and fraud. As Organized Crime Groups (OCGs) respect no jurisdictional borders, and as information and evidence needed in investigations is in many cases located in multiple jurisdictions in EU and beyond, new networks and transnational partnerships must be established. The project is an initiative to foster Law Enforcement and private sector (PS) partnership in Europe by organizing joint trainings for Law Enforcement and PS fraud prevention professionals, webinars, establishing working groups (WGs) and a P3 secondment program against specific problems and enabling Law Enforcement officers to liaise with relevant stakeholders of the private sector. The applicants will organize several activities during the project. The project will begin in 01.01.2019 and continue until 31.12.2020, lasting 24 months. With these activities we plan to join more than 200 LEA from all EU Member States to more than 200 PS cybercrime and fraud specialists, resulting in enhancing cooperation in operational cases and investigations. We expect to facilitate more than 100 operational cases within the project. As evidence in cybercrime and fraud investigations is nowadays located in PS companies' servers in multiple jurisdictions, the project will facilitate the exchange of evidence by legal means by increasing understanding and contacts between LEA and the PS in Europe. As private companies have high quality analyzing software to find new criminal hotspots much quicker than most LEA in EU, the project will greatly enhance the probability of the LEA in EU to have a better intelligence picture in EU.

ROAR	
Title	Empowering victims of cybercrime
Objective	Promote reporting and improve support to and protection of victims of cybercrime
Contract details	ISFP-2017-AG-CYBER; 1/1/2019 – 31/12/2020; EUR: 369.183,17
Abstract	At least a million people are victims of cybercrime daily, although many attacks go unnoticed. ROAR's objective is thus to promote reporting and improve support to and protection of victims of cybercrime. The project involves: establishment of specialised support services for cybercrime victims; increased multi-stakeholder cooperation; promotion of victim-sensitive investigations; engagement of technology industry; awareness raising. Increased understanding of cybercrime and multi-stakeholder cooperation will be attained through technical visits and thematic workshop targeted to law enforcement/judicial authorities, with involvement of key-stakeholders from technology industry and victim support experts. The knowledge gathered will be vital to promote victim-focused investigations and positive judicial outcomes, as well as the necessary commitment to further prevent and respond to cybercrime. A Policy Paper will be jointly issued by the whole partnership in order to seek action from policy makers and governments. Two Pilot Specialised Support Units for Victims of Cybercrime will be established relying on cooperation and referral with/to law enforcement/judicial authorities. A best practices manual will then be developed outlining a broad understanding of cybercrime and model intervention procedures, which will serve as basis to: creation of a training manual and courses for victim support workers; design of a Pilot Specialised Unit Case Management Platform. Awareness raising/prevention will follow, with input from industry partners and a communication agency, in order to draw an effective communication strategy for an online/offline awareness campaign and the delivery of 10 awareness raising sessions in schools, in Portugal and Romania. A final conference, gathering multi-stakeholder experts will be held in Portugal to present the project's results, strengthening long-lasting cooperation and promoting public debate on prevention of and fight against cybercrime

This overview is complemented by a projected funded by Marie Skłodowska-Curie Actions.

CYBERCULT	
Title	Strategic Cultures of Cyber Warfare
Objective	Examine why and how western states are developing Offensive Cyber Capabilities (OCC)
Contract details	H2020-MSCA-IF-2018; 1/7/2019 - 30/6/2021; EUR 166 320
Abstract	CYBERCULT is a project that examines why and how western states are developing Offensive Cyber Capabilities (OCC): human, technical and virtual tools to disrupt, destroy and exploit computer systems. CYBERCULT has three core objectives. First, it will establish a Strategic Culture-based theoretical concept that explains the development and use of OCC by western powers. This concept will move beyond rationalist and materialist explanations of OCC processes and consider the influence of Strategic Culture on OCC adoption, including the socio-political, historical, and perceptual/ideational factors involved. This will be achieved through a theory-building phase involving an Interdisciplinary Workshop on OCC, a literature review on Strategic Culture and new technologies, and sustained interaction with leading Strategic Culture academics. Second, CYBERCULT will produce a data set on perceptions of OCC in eight countries that are connected to the western alliance system: the US, Israel, France, Germany, the UK, Estonia, Japan and New Zealand. The data set will be based on an analysis of surveys sent out to cyber policymakers and practitioners in the eight countries. Third, CYBERCULT will produce an in-depth comparative analysis of OCC adoption in three of the world's leading cyber powers: the US, Israel, and France.
Consortium	Coordinator: Vrije Universiteit Brussel (BE)

6.4 Crime

6.4.1 Organised crime

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Organised crime	ANDRUPOS BIO-CRIME CRIMTANG HumanTrafficking PROTON TAKEDOWN UCOC

This overview is complemented by ISF-funded projects.

Chinese THB	
Title	Chinese Trafficking in Human Beings
Objective	Improve multidisciplinary international cooperation to identify and tackle Chinese trafficking in human beings (THB)
Contract details	ISFP-2017-AG-THBX; 1/8/2018 – 31/7/2020; 388.778,08
Abstract	Cooperation between EU MS is necessary to identify and to tackle Chinese THB in the EU. A project-based approach, where the exchange of information, knowledge and effective intervention strategies takes place and where possibilities on operational cooperation on investigations and prosecutions are discussed, is the only possibility to tackle Chinese THB in an effective way. Operational expert meetings for a project group of the EU MS are needed to carry out the project. Besides this, EU MS need aligned cooperation with China to be effective in the fight against THB in the EU, because recruitment, travel and money flows are very often linked to entities in China. OCGs involved in Chinese THB are operating fluently; in some cases victims are entering the EU in another country then where the exploitation takes place. The result of the project will be: multidisciplinary international cooperation to identify and tackle Chinese THB, with concrete operational results, such as investigations, an intelligence picture on the trafficking chain, links to other forms of organised crime and shared knowledge on the phenomenon and effective intervention strategies.

EURASIAN OC	
Title	Advanced Fight Against High Risk Eurasian Criminal Networks (EURASIAN OC) *This project is also relevant for 6.4.5 Support to law enforcement*
Objective	Introduce new pro-active methods for advanced fight against high value targets (HVTs) within Eurasian criminal networks
Contract details	ISFP-2016-AG-MC; 1/11/2017 – 31/10/2019; 787.819,60
Abstract	General objective: Introduction of new pro-active methods for advanced fight against high value targets (HVTs) within Eurasian criminal networks. This project aims at identifying and dismantling top transnational criminal networks (mafia-type structures) which are highly mobile in terms of fields of activity and geographical scope and which can be regarded as HVTs by these criteria: Criminal networks active in at least 2 EU MS; Applying sophisticated conspiracy and police awareness tactics; Criminal networks active in poly-crime areas. Due to wide geographical scope of activities of those HVTs, LEAs of other EU MS which are source, transit or destination will be involved based on identified threats and operational needs. Considering that traditional investigation techniques are inefficient against most dangerous transnational criminal networks, new advanced pro-active methods (cyber solutions for e-intelligence gathering and special technical equipment) will be applied. Manual for investigators on the use of pro-active advanced cyber technics will be developed and disseminated to EU MS LEAs.

FLOW	
Title	Flows of illicit funds and victims of labour trafficking; unrevealing the complexities
Objective	Promote a holistic approach to the prevention and investigation of THB in conjunction with economic crime, while engaging businesses in the prevention of THB
Contract details	ISFP-2017-AG-THBX; 1/10/2018 – 30/9/2020; 395.279,40
Abstract	The FLOW-project promotes a holistic approach to the prevention and investigation of THB in conjunction with economic crime and engages businesses in the prevention of THB. In WP1 Management team coordinates communication, monitoring, reporting & evaluation. In WP2 A strategic analysis tool and theoretical business model of THB is developed. The visual model outlines risks and vulnerabilities of victims in supply chains based on data collection & analysis. WP3 Increases the capacity of LEAs to investigate THB in conjunction with economic crime by developing investigation aids in close cooperation with national LEAs and labour inspectors who take part in the WP workshops. In WP4 Businesses are engaged in roundtables. Based on the dialogue a normative framework guide and risk management tool is developed. WP5 produces appealing materials on project results disseminated through partners' networks.

Forest Crime	
Title	Strengthening Networks and Investigation for a more effective Implementation of the EU Timber Regulation (EUTR) *This project is also relevant for 6.4.2 Corruption*
Objective	Enable effective law enforcement by stimulating networks that are able to detect forest crime and respond to it
Contract details	ISFP-2017-AG-ENV; 1/3/2019 – 28/2/2021; EUR 1.484.143,50
Abstract	Forest crime (FC) is a growing problem with links to organised crime (OC) and corruption - ranking 3rd in transnational crime in 2017. In 2013, the EU adopted the European Timber Regulation (EUTR) to halt illegal logging. However, loopholes in the EUTR and implementation gaps in Member States (MS) have hindered a real change in practice. The project aims to enable effective law enforcement by stimulating networks that are able to detect FC and respond to it. It will put FC high on their agenda. The innovation lies in bringing together INTERPOL's law enforcement expertise with WWF's practical experience in supporting companies to avoid illegal wood. The following approach will boost law enforcement and investigations: 1) information sharing 2) awareness raising 3) capacity development and 4) investigative mentorship. While pillars 1 to 3 will be carried out jointly by WWF and INTERPOL, INTERPOL will moderate pillar 4 with investigative authorities. A comprehensive gap analysis will serve as the basis for tailored trainings of police, customs, environmental authorities, prosecutors and judges. Trainings will cover knowledge-sharing on e.g. new forensic methods – a technique in which WWF has leading know-how – and guidance for effective controls by authorities. The project will empower civil society (CS) to raise suspicions and to be a knowledgeable partner for authorities. Two focal areas encompass the situations that MS face towards FC. In Belgium and France trainings will focus on products with complex Chains of Custody (CoC) and will discuss suspicious cases to motivate existing Envi-Crime networks to independent investigations. In Romania, Bulgaria, Slovakia and Ukraine the project will focus on illegal logging within the EU and on transboundary FC. The project will allow INTERPOL to set up National Environmental Security Taskforces (NEST) and mentor them on real case investigations. Best practices will be shared across Europe at the end of the project.

NET-COMBAT-THB CHAIN	
Title	Anti-trafficking stakeholders and economic sectors networking, cooperation to combat the business of human trafficking chain
Objective	Combat the wider chain of trafficking in human beings through an improved cooperation of the anti-trafficking stakeholders and the economic sectors
Contract details	ISFP-2017-AG-THBX; 1/9/2018 – 30/4/2020; 339.614,79
Abstract	The project's main objective consists in combating the wider chain of trafficking in human beings through an improved cooperation of the anti-trafficking stakeholders and the economic sectors. Specific objectives linked to the expected outcomes are: to analyse the link between trafficking in human beings and the economic sectors; to engage the economic sectors alongside civil society and other anti-trafficking stakeholders; awareness and education of the population from several EU states by exposing the THB chain implications, through online transnational campaign using social media networks; to enhance knowledge of various economic sectors with a potential to be involved in the trafficking chain; to develop training materials and organize events bringing together the economic sectors representatives and the anti-trafficking stakeholders; to explore and share good practices, expertize on legislation and practices to combat THB.

ONNET	
Title	Project Of The Aton Operational Network To Counter Mafia-Style Serious And Organised Crime Groups
Objective	Develop deeper operational cooperation against the mafia-type structures between the EU MS and expand European police coordination with other extra-EU countries
Contract details	ISFP-2017-AG-IBA-ONNET; 1/11/2018 – 31/10/2020; EUR 604.258,96
Abstract	Antimafia Investigation Department (D.I.A.), within the initiatives for EU 2014 Italian Presidency, presented the "Operational Network - @ON" that was approved on 4th, December 2014, in Brussels, by the EU Council - JHA. ONNET aims to fund the activity of @ON Network: Italy (D.I.A.) will be the beneficiary. D.I.A will avail itself of a sub-contracting company (SC) for financial, administrative and reporting activities . The affiliated entity will be France (SIRASCO and STRJD), Germany (BKA). Spain (Cuerpo National de Policia and Guardia Civil), Belgium (Federal Police), the Netherlands (Dutch National Police) and Europol.The Project Objectives are:1)To maintain and enlarge the @ON Network; 2)To promote the operational exchange of information and good practice in countering criminal and mafia-type organisations; 3)Medium-term deployment of experienced investigators in other Member States (MS), to assist in ongoing investigations. The related activities will be:1a) to guarantee the Network functioning by 3 Operational Committees, 2 Core Groups meetings and 2 LEWP meetings;1b) to promote within Europol and MS Investigation Units the use of the Network to initiate further @ON participation and requests of operational support by 2 HENU meetings, 2 EMB meetings and 4 informative Europol desk meetings;2) to promote the operational exchange of information and good practice in combating criminal and mafia-type organisations by 2 operational conferences;3) to carry out 8 Operational Task Forces to identify and monitor criminal High Value Targets and to give operational support to the requesting countries by up to 70 operational missions operated by @ON investigators to support on the spot their investigative activities. Furthermore, the management will be assured by 3 management meetings, 2 logistic support meetings and necessary coordination meetings. ONNET will develop deeper operational cooperation against the mafia-type structures between the EU MS and will expand the European police coordination even with other extra EU countries.

Wildlife Cybercrime	
Title	Disrupting and dismanteling wildlife cybercriminals and their networks in the European Union
Objective	Disrupt and dismantle organised criminal networks trafficking wildlife in, or via, the European Union (EU) using the internet and postal or fast parcel services
Contract details	ISFP-2017-AG-ENV 1/2/2019 – 31/1/2021; EUR: 959.064,65
Abstract	The proposed action is to disrupt and dismantle organised criminal networks trafficking wildlife in, or via, the European Union (EU) using the internet and postal or fast parcel services. The action will combine research and analysis, capacity building and training in online monitoring and investigations; strengthened cooperation between EU law enforcement, facilitate intelligence-led enforcement actions and strengthened cooperation among EU law enforcement agencies, and between these agencies and businesses through partnerships with online technology companies and the post and fast parcel companies in the EU. The action will involve at least 60 officials from law enforcement authorities across EU Member States; relevant EU agencies (e.g. EUROPOL, European Commission), international organisations (e.g. World Customs Organisation, Secretariat of the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), International Consortium on Combatting Wildlife Crime and a minimum of 20 key players from the private sector representing online technology companies and post and parcel services in the EU. NGOs and academics will also be engaged to inform and support the action.

WESTEROS	
Title	Enhancing the fight against trafficking of human beings and its proceeds through advanced financial investigation *This project is also relevant for 6.7 Financial Crime.*\
Objective	Improve and strengthen the exchange of information at strategic, operational and tactical levels between partners following the most recent trends in the THB area
Contract details	ISFP-2017-AG-THBX 14/9/2018 – 13/9/2020; EUR: 313.396,58
Abstract	The WESTEROS project seeks to improve and strengthen the exchange of information at strategic, operational and tactical levels between partners following the most recent trends in the THB area. The partners will benefit from advanced knowledge on how to effectively: identify the illegal financial networks generated by the trafficking in human beings, seize proceeds of crime, dismantle criminal networks. It will ensure a proper environment for exploring good practices; identify the proceeds of crimes, self-money laundering, the accompanying THB crimes and to set up a „financial tracking". The project intends to assist the practitioners (p) - prosecutors, police workers and financial investigators - in exchanging best practices in covering the communication between traffickers using encryption devices and apps, Bitcoin payments.

WasteForce	
Title	Deterring and disrupting illegal trade and management of Waste by developing Tools for Enforcement, Forensics and Capacity Building
Objective	Boost the operational activities and capacities of authorities involved in the fight against illegal trade and management of waste
Contract details	ISFP-2017-AG-ENV 1/12/2018 – 30/11/2020; EUR: 773.004,38
Abstract	The project aims at boosting the operational activities and capacities of authorities involved in the fight against illegal trade and management of waste through: (i) development of new practical tools and methodologies; (ii) implementation of multi-stakeholder capacity building activities; and (iii) support of operational networking among practitioners in Europe and with their counterparts in the Asia- Pacific region, one of the main regions of destination of illicit waste shipments.

SPECTRE Project	
Title	Struggling against and Pursuing Experienced Criminal Teams Roaming in Europe *This project is also relevant for 6.4.5 Support to law enforcement.*
Objective	Identify, disrupt and dismantle the most active, flexible and professional Mobile Organised Crime Groups (MOCGs) and criminal networks involved in burglaries, organised property crime and other related crimes
Contract details	ISFP-2016-AG-MC 1/10/2017 – 30/09/2019; EUR: 813.057,02
Abstract	The objective of the project is to identify, disrupt and dismantle the most active, flexible and professional Mobile Organised Crime Groups (MOCGs) and criminal networks involved in burglaries, organised property crime and other related crimes. The final goal is to dismantle at least 50 MOCGs (including top ones) and to recover a minimum of 2 million EUR of ill-gotten assets. MOCGs operate in Europe with a high degree of flexibility and generate a considerable increase in burglaries and property crimes, have a significant negative impact on businesses and affect numerous victims creating an accute sense of insecurity for European citizens. Transnational crime groups are increasingly professional and take countermeasures with sophisticated modus operandi. Thus police and prosecutors have to adapt their working methods and take concerted actions at the European level to fight these networks efficiently. The proposal must be considered as a pilot project, in line with the European Union Council priorities on organised domestic burglaries and property crime. It aims at building in-depth knowledge of mobile organised crime groups, developing operational cooperation between European Member States and third countries, using innovative tools and improving the training of police experts.

Silk Road	
Title	Immigrant smuggling control along the Silk Migration Route *This project is also relevant for 7.4 Multi-modal security, risk management, including migration.*
Objective	Control organized migrant-smuggling networks in view of the high migration figures along the Silk Route, more specifically in Afghanistan, Pakistan, Iran and Turkey, and further in the Eastern Mediterranean
Contract details	ISFP-2016-AG-SRMR 1/1/2018 – 31/12/2019; EUR: 1.420.858,35
Abstract	The objective of the ISF project is to control organized migrant-smuggling networks in view of the high migration figures along the Silk Route, more specifically in Afghanistan, Pakistan, Iran and Turkey, and further in the Eastern Mediterranean. Geographically speaking, Iran plays a key role in the fight against illegal immigration, followed by Afghanistan and Pakistan. From Turkey the migrants are smuggled along the Balkan route to Europe. While Austria and Germany are primary target countries, Bulgaria is one of the main transit countries. The criminal groups operating there cannot be effectively and sustainably controlled unless through intense co-operation and data exchange between the countries concerned. To this end, professional co-operation in pertinent investigations must be strengthened both at strategic and at operational level. In the first instance, it will be necessary to build up confidence in operations with Pakistan, Afghanistan and Iran as well as Turkey and to gauge the extent to which constructive co-operation is possible and the hierarchy levels that are best suited to this purpose. Its neutrality status places Austria in an advantageous position for gaining acceptance in the above-mentioned third countries. The identification of offender networks in the countries of origin and the analysis of the intelligence obtained in their respect make it possible to quickly exchange information, especially through the JOINT OPERATIONAL OFFICE in Vienna, and to take appropriate action for combating criminal smuggling networks. The involvement of Europol through its European Migrant Smuggling Center (EMSC), of Interpol and of Eurojust will speed up repressive action against international facilitating networks.

6.4.2 Corruption

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Corruption	ANTICORPOL

This overview is complemented by relevant ISF projects.

ACT	
Title	Anticorruption City Toolkit
Objective	Prevent corruption at local level, by providing municipalities with digital tools for improving detection and reporting of corruption, as well as civil society oversight on vulnerable sectors (legislative process, budgeting and public procurement)
Contract details	ISFP-2017-AG-CORRUPT; 1/2/2019 – 31/1/2021; 495.647,54
Abstract	The proposal aims at preventing corruption at local level, by providing municipalities with digital tools for improving detection and reporting of corruption, as well as civil society oversight on vulnerable sectors (legislative process, budgeting and public procurement). Tools will be made available on an online platform (the Anticorruption City Toolkit) and will be fine-tuned, developed and tested from November 2018 to October 2020 in 3 major European cities: Milan, Madrid, and Athens.

DATACROS	
Title	Strengthening of the cross-border police cooperation in the Baltic sea region *This project is also relevant for 6.4.5 Support to law enforcement and 6.7 External security threat.*
Objective	Develop a tool prototype to detect anomalies in firms' ownership structure that can flag high risks of collusion, corruption and laundering of corruption proceeds
Contract details	ISFP-2017-AG-SCHEN; 31/12/2018 – 29/6/2020; EUR 397.582,04
Abstract	The action aims at developing a tool prototype to detect anomalies in firms' ownership structure that can flag high risks of collusion, corruption and laundering of corruption proceeds. The "DATACROS" tool will help detecting: Ownership links among a set of firms (e.g. bidders in a procurement) to detect collusion patterns; Ownership links between firms and politically exposed persons, including also low-rank and local PEPs not covered by the EU regulation; Complex cross-border firms' ownership structures and ownership links to off-shore and risky jurisdictions.

EACN	
Title	Supporting the activities of the European Contact-Point Network Against Corruption
Objective	Support the European Contact-Point Network Against Corruption
Contract details	ISFP-2016-AG-IBA-EACN; 1/4/2017 – 31/3/2020; 47.368,42
Abstract	The European contact-point network against corruption (EACN) was formally established by a Council Decision in 2008, to be based on the existing structures of the European Partners against Corruption (EPAC). It is a formal network comprising close to 80 anti-corruption authorities (ACAs) and police oversight bodies (POBs) from EU Member States. The network was set up to improve cooperation between authorities mandated with the prevention of and fight against corruption in the EU, as well as to foster closer relations between MS and the European institutions. It affords a platform for the exchange of EU-related information on effective measures and experiences, identifying opportunities, and collaboration in developing common strategies and high professional standards. To increase the importance and impact of EACN and thus strengthen the fight against corruption at EU level, efforts strive to, i.a., raise the number of EACN members to a maximum. The bodies responsible for the functioning of the network are, on the one hand, the EACN Board and, on the other hand, the EACN Secretariat. The latter has been handed over to the Austrian Federal Bureau of Anti-Corruption (BAK) after the election of the Director of the BAK as the new President of EPAC/EACN in 2016.

EAT	
Title	Widely Expanding Anonymous Tipping Technology Deployment, Operation, and Trustworthiness to Combat Corruption in Eastern and Southern Europe
Objective	Expand the availability, functionality, and use of tip submission technology to assist in the fight against corruption in both public and private spheres in the 11 EU countries where corruption is most perceived to negatively affect business and government
Contract details	ISFP-2017-AG-CORRUPT; 1/2/2019 – 31/1/2021; 563.381,22
Abstract	EAT will massively expand the availability, functionality, and use of tip submission technology to assist in the fight against corruption in both public and private spheres in the 11 EU countries where corruption is most perceived to negatively affect business and government. EAT will deploy "secure dropbox" instances to service over 100 agencies and companies, help those agencies and companies leverage the opportunities offered by truly anonymous whistleblowing, expand the technology to maximize its potential by enabling tip submission to be monitored by second- and third-tier reporting mechanisms (law enforcement agencies, civil society, and media), and increase tipsters' confidence that (compared to existing tip submission methods) they are insulated from identification and reprisal.

IRM	
Title	Support to the implementation of the second review cycle of the United Nations Convention against Corruption
Objective	Support States parties to actively and effectively participate in the second review cycle of the Implementation Review Mechanism of the Convention
Contract details	ISFP-2017-AG-IBA-UNCAC; 1/11/2018 – 31/10/2020; 345.031,61
Abstract	The proposal seeks to support States parties to actively and effectively participate in the second review cycle of the Implementation Review Mechanism of the Convention, to use the Review Mechanism for assessing their existing anticorruption frameworks, to prioritize future steps, and to review progress in implementation. The project also enables Least Developed Countries to participate in the sessions of the Implementation Review Group, which oversees the Review Mechanism.

IW Europe	
Title	Integrity Watch: online tools for the fight against political corruption in Europe
Objective	Prevent and reduce political corruption through deploying user-friendly interactive databases on areas with high corruption risks, enabling civil oversight and contributing to significant economic and social impact
Contract details	ISFP-2017-AG-CORRUPT; 1/1/2019 – 31/12/2020; EUR 604.500,78
Abstract	The Action aims to prevent and reduce political corruption through deploying user-friendly interactive databases on areas with high corruption risks, enabling civil oversight and contributing to significant economic and social impact. We will develop a set of online tools tailored to the national contexts in 7 EU Member states (Spain, Italy, Netherlands, Latvia, Lithuania, Greece, Slovenia), and update existing 2 existing ones (France and Integrity Watch EU), allowing for stronger civil oversight in areas with high corruption risks and provide information and data for investigative journalists. Data such as on lobby meetings and registers of lobbyists; declarations of financial interests or assets of politicians; disclosure of political or campaign finance; revolving door cases; business registers; public procurement that is often scattered and difficult to access is scoped for usability, collected, managed, harmonised, triangulated and made easily available on integrated online platforms.

RECORD	
Title	Reducing Corruption Risks with Data
Objective	Create and implement a toolkit to analyse corruption risks in local level public procurement processes, including conclusion of contracts below public procurement thresholds
Contract details	ISFP-2017-AG-CORRUPT; 1/1/2019 – 31/12/2020; 630.251,40
Abstract	This consortium will create and implement a toolkit to analyse corruption risks in local level public procurement processes, including conclusion of contracts below public procurement thresholds. We will undertake assessment of institutional capacities and relevant know-how, evaluating soft regulation, so as to draw a roadmap for increasing integrity, transparency and accountability, and providing public bodies with innovative tech tools for the effective monitoring of procurements.

WOODle	
Title	Whistleblowing open data impact. An implementation and impact assessment. *This project is also relevant for 9.3 Communication systems (interoperability and communication with focus on security).*
Objective	Assess the current implementation and impact of whistleblower protection and open data in seven Member States (Austria, Estonia, France, Ireland, Italy, Romania, and Slovenia) to develop an ICT tool for the public administrations (from local authorities to public companies).
Contract details	ISFP-2017-AG-CORRUPT; 21/1/2019 – 20/1/2021; EUR: 467.117,06
Abstract	Whistleblower protection and open data are unanimously recognised as key measures to deter and detect corruption in public procurement. This project will assess the current implementation and impact of these measures in seven Member States (Austria, Estonia, France, Ireland, Italy, Romania, and Slovenia) in order to develop an ICT tool for the public administrations (from local authorities to public companies). The long-term objective is to increase transparency and integrity in public procurement that contributes obtaining more efficient public expenditure, higher quality of goods, services and public work and more trust in government from the citizens. After reviewing the legislation and policy on whistleblower and open data in the seven partner countries, the main activities of the project are: 1) an assessment of the implementation of the two measures, by identifying how they are applied and how they function, their strengths and shortcoming; 2) an assessment of the impact of these measures, by highlighting if, how and how much they are contributing to enhance transparent and integrity in public procurement; 3) the development of an assessment model grounded on the result of the two previous activities; 4) the development of an ICT tool that allows the public administration to assess their policy on whistleblowing and open data.

SceMaps	
Title	State Capture Estimation and Monitoring of Anti-Corruption Policies at the Sectoral level
Objective	Tackle anti-corruption deficiencies in high-risk EU member states (MSs) by developing and implementing an integrated risk assessment tool for estimating state capture and monitoring of anti-corruption policies at the sectoral level (SceMaps)
Contract details	ISFP-2017-AG-CORRUPT; 1/1/2019 – 31/10/2020; EUR: 391.247,64
Abstract	SceMaps is designed to contribute to the fight against corruption in the EU by delivering impact on multiple levels and providing for long-term sustainability. The project aims at tackling anti-corruption deficiencies in high-risk EU member states (MSs) by developing and implementing an integrated risk assessment tool for estimating state capture and monitoring of anti-corruption policies at the sectoral level (SceMaps). SceMaps addresses the most serious corruption threat - state capture, by assessing high-risk economic sectors though a combination of qualitative and quantitative methods, big data analysis and media content alert system. Designed for easy replication and take-up by EU MSs' public administrations, SceMaps will allow EU authorities to build evolving, risk-responsive instruments to assess and tackle corruption and capture risks in regulatory heavy areas and industries, such as public procurement, pharmaceuticals (healthcare), and construction.

The overview is complemented by a Erasmus+ project.

Fighting corruption - expanding the Union	
Title	Fighting corruption - expanding the Union
Objective	Educate youth workers (from the EU and WB), design a toolkit and develop non-formal education methods, through which youth workers from partner countries will empower youth to address cases of corruption in the Western Balkans
Contract details	602533-EPP-1-2018-1-ME-EPPKA2-CBY-WB; 15/12/2018 - 14/12/2020; EUR: 85.599,96
Abstract	The last months were marked by a renewed European focus on the Western Balkan (WB) region accompanied by a new EU strategy and the visit of the Jean-Claude Juncker to the region in early March 2018. Among many obstacles on the path of WB countries joining the Union is also corruption. The latest Special Eurobarometer 470 shows that more than 60% of EU citizens think that corruption is present in their country; the corruption perception index shows a far bleaker picture for WB. Not only is corruption an impediment to joining the EU, it also has considerable impact on the economic sector, society and individuals. Thus the consortium designed "Fighting Corruption — Expanding the Union" — a project that uses a bottom-up approach to tackling corruption through educating youth workers (from the EU and WB), designing a toolkit and developing non-formal education methods, through which youth workers from partner countries will empower youth to address cases of corruption. The consortium includes 11 organisations from 10 countries (5 from the EU and 5 from WB)Fighting corruption is a crucial priority both in EU28 and WB countries. The majority of initiatives targeting corruption are aimed at decision makers and are thus distinctly top-down in character. While these initiatives are crucial in establishing rule of law, they often overlook the fact that corruption is entrenched in culture and the most effective long-term strategy for fighting it is to make it culturally unacceptable. And in this young people are the key target group — they are the future leaders, entrepreneurs and civil society actors.
Consortium	Coordinator: Nvo Naucno - Istrazivacko Udruzenje Za Umjetnost, Kulturno-Obrazovne Programe I Tehnologiju Epeka (ME)

The overview is complemented by a relevant H2020 project.

BIT-ACT	
Title	Bottom-up initiatives and anti-corruption technologies: how citizens use ICTs to fight corruption *This project is also relevant for 6.3.1 Cyber Security Management (for SMEs/business, local public authorities).*
Objective	Investigate anti-corruption technologies in Algeria, Bangladesh, Brazil, Estonia, India, Italy, Spain, Ukraine, and Uruguay
Contract details	ERC-2018-STG; 1/7/2019 - 30/6/2024; EUR: 1.489.115
Abstract	Corruption is a global challenge that affects the lives of millions of citizens. In the past decade, Information and Communication Technologies (ICTs) have become indispensable tools in the fight to reduce corruption, especially when employed from the bottom-up by civil society organizations. While pioneering initiatives in this direction have flourished, to date we only have unsystematic and descriptive evidence regarding how they work and the associated consequences. With the objective of significantly advancing knowledge on this topic, BIT-ACT will open a new line of inquiry by investigating what I call anti-corruption technologies (ACTs) to: (1) assess how civil society organizations engage with ACTs to counter corruption, (2) appraise how ACTs enable intersections between bottom-up and top-down efforts against corruption, and (3) evaluate how ACTs blend with the transnational dimension in the struggle against corruption. Based on an interdisciplinary framework that combines corruption studies, science and technology studies and social movement studies, BIT-ACT will use the constructivist grounded theory method to analyze a combination of textual and visual data in a comparative and transnational research design including nine countries – Algeria, Bangladesh, Brazil, Estonia, India, Italy, Spain, Ukraine, Uruguay. BIT-ACT will be groundbreaking in three ways. At the theoretical level, it will expand the debate on anti-corruption providing grounded concepts and models to explain ACTs; at the empirical level, it will advance knowledge on how the usage of ACTs is changing the relationship between citizens and democratic institutions; at the methodological level, it will innovate in the use of grounded theory assessing a new standard for cross-national comparative grounded theory. Finally, BIT-ACT will produce sound and useful knowledge for the stakeholders involved in the fight against corruption worldwide by suggesting how to best employ ICTs from the bottom-up.
Consortium	Coordinator: Alma Mater Studiorum - Universita Di Bologna (IT)

6.4.3 Drug detection

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Drug detection	CSW: Cross Border Surveillance on Drugs and Firearms CUSTOM DIRAC DOGGIES DRUGSTOP Joint investigation to fight trafficking in drugs and firearms with the main focus on international airports within and also into the EU LINKSCH LOTUS MicroMOLE NarcoScan No for Drugs ROSFEN SALIANT SNIFFER SNIFFLES SNOOPY Turning

This overview is complemented by ISF projects.

CO3DIL	
Title	Collaboration for Dismantling Drugs Distribution and Illicit Laboratories - CO3DIL
Objective	Dismantle illegal drug meth labs in the EU and criminal activities overlapping the supply of precursors and other active chemical substances for the production of methamphetamine-crystal
Contract details	ISFP-2017-AG-DRUGS; 1/2/2019 – 31/1/2021; 548.166,35
Abstract	The Czech Drug Enforcement Unit is leading a 24-month proposal aiming at the dismantling of illegal drug meth labs in the EU and criminal activities overlapping the supply of precursors and other active chemical substances for the production of methamphetamine-crystal. The proposal will join efforts of 5 anti-drug police bureaus in Slovakia, The Czech Republic, Poland, Serbia and Bulgaria, and one security NGO. However, EU MS and international organisations(Interpol, Europol, EMCDDA, SELEC, DEA, etc.) will be involved. Objectives: (SO1) Dismantling storage and production facilities for illicit drugs (SO2): Development of methodological, notably statistical, tools and methods and common indicators, (SO3) Enhance the collaborative EU and third country law-enforcement capacity to target drug trafficking

CSI-PP	
Title	Combatting suspects dealing in drugs on the Internet – prosecution and prevention
Objective	Deanonymise letters and parcels containing illegal drugs ordered and sent via virtual platforms on the Internet/Darknet as well as the identification of the drug dealer
Contract details	ISFP-2017-AG-DRUGS; 1/2/2019 – 31/1/2021; 748.868,39
Abstract	The main objective is the deanonymisation of letters and parcels containing illegal drugs ordered and sent via virtual platforms on the Internet/Darknet as well as the identification of the drug dealer. Suspects shall be identified by forensic examinations of the postal items by means of fingerprint, DNA and skin particles analyses. The forensic data shall be stored in a central database and therefore be available for all EU member countries. The operational measures shall be strengthened by ways of a multinational judicial cooperation. Further objectives are the detection and seizure of illegal drugs and drug money as well as the distribution of the Best Practice Model Look@your.Life in the field of prevention to all EU member states. With this prevention program especially youths shall be reached who are also present in forums of the Internet/Darknet. The intended objectives shall be achieved by means of a kick-off meeting, a fact-finding mission including the preparation of the meeting, 8 operational/forensic meetings to coordinate the operational criminal tactic and investigative measures, 8 quarterly meetings for quality control, risk management and management of the project course, 8 prevention meetings and a closing conference (including its preliminary meeting) in order to elaborate conclusions and to spread the findings gained to all EU member states, candidate and third countries, Europol, Eurojust, EMCDDA, EC, UNODC and Interpol. Finally the evaluation meeting shall serve to evaluate the project and to point the way forward. The expected results are the strengthening of the multinational judicial and criminal police cooperation, the EU-wide presentation of the Best Practice Model Model Look@your.Life in the field of prevention, deanonymised postal items containing illegal drugs as well as secured traces in databases (fingerprints and DNA) which will be available for all EU countries, arrested suspect, seized drugs and drug money.

Drug combat	
Title	Enhancing capacity of services to combat drug trafficking at the European level *This proejct is also relevant for 6.4.5 Support to law enforcement*
Objective	Enhance capacity of project partners to combat drug trafficking at the European level
Contract details	ISFP-2017-AG-DRUGS; 1/1/2019 – 31/3/2020; 396.726,04
Abstract	The main objective of the project is to enhance capacity of project partners: Regional Police Headquarters in Lublin, Nadbużański Regional Border Guard Unit represented for the purpose of the grant agreement by Komenda Główna Straży Granicznej, Polish Police Central Bureau of Investigation, Berlin Police, National Police General Directorate in Bulgaria, National Spanish Police, Satu Mare County Police Inspectorate, General Inspectorate of the Romanian Police and Estonian Police and Border Guard to prevent and fight drug related crime by targeting drug trafficking, facilitating exchange of information on technical possibilities and dismantling storage and production facilities for illicit drugs . The project activities are: Project Management Team meeting, study visits to Bulgaria, Estonia, Germany, Romania and Spain, two training workshops: first will include simulation exercise of drug smuggling via green border with Ukraine, and second will be taken in International Center for Combating Clandestine Laboratories. Short term project beneficiaries will be participants of study visits and training workshops. Medium term beneficiaries are representatives of police and border guards from EU member countries dealing with drug crime and dismantling lab for illicit drugs. Long term beneficiaries are inhabitants in partner countries, as increased capacity of combating drug-related crime will strengthen society confidence in effective work of these services. The main outcomes of project will be: increased experts capacity in fighting drug crime, elaboration of best practices on preventing and fighting smuggling of drugs, description of technical capacity equipment and software) and guidelines on methods and procedures during dismantling facilities for illicit drugs, contact list of staff project management staff, built mutual confidence and understanding between authorities, film on the course of the training workshops. Within project there will be also purchased the equipment crucial for operational-reconnaissance work of police officers/border guards.

Lion DC	
Title	Law Enforcement Technological Innovation Consolidation for Fight Against Online Drug Crimes *This project is also relevant for 6.4.5 Support to law enforcement*
Objective	Provide Law Enforcement Agencies (LEA) with new skills, methodologies and tools in the fight against drug trafficking, given major discernible shifts in the utilisation of digital environments
Contract details	ISFP-2017-AG-DRUGS; 10/12/2018 – 9/12/2020; EUR 1.102.158,85
Abstract	The Lion DC project aims to provide Law Enforcement Agencies (LEA) with new skills, methodologies and tools in the fight against drug trafficking, given major discernible shifts in the utilisation of digital environments (eg. traditional social media) regarding distribution and sale of drugs such as the increasingly widespread use of cryptocurrencies and blockchain technologies by organized crime. In order to enhance LEA capacity to identify the flow of drugs and key players involved, either to thwart criminal activity or to determine guilt after the fact, the project will: test the efficiency, unique capabilities, and shortfalls in the use of various forms of technology, as well as Open Source Intelligence Tools (OSINT); penetrate the Dark Web; develop novel ways of going beyond the widely used "follow the money" principle; and augment the identification and description of criminals by collating a wide range of sources, both open and closed. The key activity of the Lion DC initiative is real, case based, cross border exercising in drug criminality, which will be enacted by LEA practitioners, providing opportunities for LEA together with academia to share expertise, methodologies and analytical capabilities; and to identify available tools and rank them on their feasibility and usefulness. In addition, specific train-the-trainer modules in the fight against drug trafficking on the Dark Web will be developed and piloted, and an OSINT sandbox will be created that will integrate promising technologies, innovations and research projects such as a Dark Web simulator, and frameworks for tracing illegal use of cryptocurrencies. The cooperation of Networks (eg. ENLETS SENTER i-LEAD) will facilitate the co-creation process between LEA and academia; and open up wide opportunities to disseminate results across all Member State, Law Enforcement organizations (initially in NL, LT, PL, BG, GR, Gibraltar), as well as EU and International security agencies (CEPOL, EUROPOL, etc.).

SYNDEC 9	
Title	Synthetic Drugs Enforcement Conference 9
Objective	Support delivery of the Synthetic Drugs Enforcement Conference 9
Contract details	ISFP-2017-AG-DRUGS; 1/1/2019 – 31/12/2020; EUR: 414.097,49
Abstract	SYNDEC has grown into one of the most important meetings in the synthetic drugs and precursors area and is organized by specialists for specialists. For SYNDEC 9 we have the focus on Precursors , not registered chemicals, the NPS (amongst them the dangerous fentanyl derivatives which cause so many victims worldwide) and the dismantling of these labs. We pay attention to the synthetic drugs in the Middle East which is related to financing terror. We want to organize courses on new technical developments, new identification methods such as drones and mobile detector systems. Also the use of social media to influence users of pills and make them aware of the world of crime behind the pills. We want to pay attention to the increase of export to South America and Australia. We want to know about the role the African countries play in smuggling chemicals and the end product. And we want to pay attention to the so called barriermodel (the whole chain of producing and where to intervene) and we want to share this knowledge, how to investigate and how to prosecute; we work together in small interactive workshops and use demonstration labs to show the 'real' material. We will refer to the results of previous SYNDECs. Besides the SYNDEC conference, the project group and partners want to organize three national (one day) synthetic drugs courses/meetings for members of Law Enforcement and local Government in the partner countries. The objectives of these meeting are to share the knowledge, latest trends and developments regarding synthetic drugs and precursors(amongst 470 participants).The results and recommendations of both SYNDEC, national and strategic meetings may lead to(inter)national projects, change of legislation and cooperation in investigations. We expect from our participants to share and disseminate the lesson learnt in their own organizations in their countries.

SNOW WHITE	
Title	Coordinated tackling of new trends in drug trafficking
Objective	Strengthen the cooperation capacity of antidrug Law Enforcement Agencies (LEA) from Romania, Belgium and Lithuania by actively responding to emerging trends in illicit drug trafficking
Contract details	ISFP-2017-AG-DRUGS; 1/12/2018 – 30/11/2020; EUR: 419.059,08
Abstract	The general objective of the project "Coordinated tackling of new trends in drug trafficking" SNOW WHITE is to strengthen the capacity of antidrug Law Enforcement Agencies (LEA) from European Union member states of Romania, Belgium and Lithuania to improve their cooperation by actively responding to emerging trends in illicit drug trafficking. The project will seek to relaunch an informal network among EU MS covering the whole area of drug trafficking capable of assisting operational needs in fighting drug trafficking. Specific training will be provided in the use of dark net and cryptocurrency for trafficking drugs across EU with a potential for transferability to other MS. (90 prosecutors, police, border police, and customs officers) The exchange of good practices and methods of cooperation in disrupting heroin and cocaine trafficking networks that use harbours as main entry point in EU will be achieve with 2 study visits (30 participants). A risk assessment study on three major European harbours will provide a better understanding among EU LEA of the trafficking networks.

6.4.4 Firearms

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Firearms	Turning

In this iteration of the CoU Mapping Document, no new projects related to firearms were identified.

6.4.5 Support to law enforcement

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Support to law enforcement	CCI CONNEXIONs COPKIT I-LEAD ILEANET IMPRODOVA LAW-TRAIN MAGNETO NOSY

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

CREST	
Title	CREST *This project is also relevant for 9.3 Communication systems (Interoperability and communication with focus on security)*
Objective	Equip LEAs with an advanced prediction, prevention, operation, and investigation platform by leveraging the IoT ecosystem, autonomous systems, and targeted technologies
Contract details	H2020-SU-SEC-2024; Topic code: SU-FCT02-2018-2019-2020; 1/9/2019 - 31/8/2022; € 6 999 078,75
Abstract	CREST aims to equip LEAs with an advanced prediction, prevention, operation, and investigation platform by leveraging the IoT ecosystem, autonomous systems, and targeted technologies and building upon the concept of multidimensional integration and correlation of heterogeneous multimodal data streams (ranging from online content to IoT-enabled sensors) for a) threat detection and assessment, b) dynamic mission planning and adaptive navigation for improved surveillance based on autonomous systems, c) distributed command and control of law enforcement missions, d) sharing of information and exchange of digital evidence based on blockchain, and e) delivery of pertinent information to different stakeholders in an interactive manner tailored to their needs. CREST will also provide chain-of-custody, and path-to-court for digital evidence. Human factors and societal aspects will also be comprehensively addressed, while information packages for educating the wider public on identifying threats and protecting themselves will be prepared and distributed.The platform development will adopt ethics and privacy by-design principles and will be customisable to the legislation of each member state. CREST will be validated in field tests and demonstrations in three operational uses cases: 1) protection of public figures in motorcades and public spaces, 2) counter terrorism security in crowded areas, and 3) Cross-border fight against organised crime (e.g. firearms trafficking). Extensive training of LEAs' personnel, hands-on experience, joint exercises, and training material, will boost the uptake of CREST tools and technologies.
Consortium	Coordinator: 1. Serviciul De Protectie Si Paza (RO) Consortium: 2. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 3. Motorola Solutions Israel Ltd (IL) 4. Sheffield Hallam University (UK) 5. Everis Spain Sl (ES) 6. Wojskowa Akademia Techniczna Im.Jaroslawa Dabrowskiego (PL) 7. Siveco Romania Sa (RO) 8. National University Of Ireland Maynooth (IE) 9. Copting Gmbh (DE) 10. Cyberlens Bv (NL) 11. Ethniko Kai Kapodistriako Panepistimio Athinon (EL) 12. Robotnik Automation Sll (ES) 13. Universitat Wien (AT) 14. In Mm Srl (IT) 15. Police Service Of Northern Ireland (UK) 16. Kentro Meleton Asfaleias (EL) 17. Hochschule Fur Den Offentlichen Dienst In Bayern (DE) 18. Serviciul De Protectie Si Paza De Stat (MD) 19. Ministério Da Justiça (PT) 20. Hellenic Police (EL) 21. Politsei- Ja Piirivalveamet (Ee) 22. Institut Po Otbrana (BU) 23. Victim Support Europe Aisbl (BE)

PREVISION	
Title	PREVISION
Objective	Empower the analysts and investigators of LEAs with tools and solutions not commercially available today, to handle and capitalize on the massive heterogeneous data streams that must be processed during complex crime investigations and threat risk assessments
Contract details	H2020-SU-SEC-2025; Topic code: SU-FCT03-2018-2019-2020; 1/9/2019 - 31/8/2021; € 8 001 180
Abstract	The mission of PREVISION is to empower the analysts and investigators of LEAs with tools and solutions not commercially available today, to handle and capitalize on the massive heterogeneous data streams that must be processed during complex crime investigations and threat risk assessments. With criminals being ever more determined to use new and advanced technology for their cause, the aim is to establish PREVISION as an open and future-proof platform for providing cutting-edge practical support to LEAs in their fight against terrorism, organised crime and cybercrime, which represent three major cross-border security challenges that are often interlinked. PREVISION provides advanced near-real-time analytical support for multiple big data streams (coming from online social networks, the open web, the Darknet, CCTV and video surveillance systems, traffic and financial data sources, and many more), subsequently allowing their semantic integration into dynamic and self-learning knowledge graphs that capture the structure, interrelations and trends of terrorist groups and individuals, cybercriminal organisations and organised crime groups, giving rise to enhanced situational awareness in these fields. PREVISION has a pan-European engagement and support agenda for LEAs: ten (10) different LEAs and practitioners take part in its consortium, while additional ones (including Europol) have joined its external advisory board. A strong inter-disciplinary dimension, combining technological expertise with sociological, psychological, linguistic and data science models, will lead to a common strategic approach for predicting abnormal and deviant behaviour, radicalisation potential, threat risks for soft targets, and cybercrime trends at different timescales. PREVISION will conduct demonstrations on five representative and complementary use cases, under real-life operational conditions, in full compliance with fundamental rights and applicable legislation.
Consortium	Coordinator: 1. Institute Of Communication And Computer Systems (EL) Consortium: 2. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 3. Etra Investigacion Y Desarrollo Sa (ES) 4. Itti Sp Zoo (PL) 5. Ifmpt Institut Fur Prognosetechnik Vertriebs Gmbh (DE) 6. Baltijos Pazangiu Technologiju Institutas (LT) 7. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 8. Universitat Politecnica De Valencia (ES) 9. Siveco Romania Sa (RO) 10. Centre National De La Recherche Scientifique Cnrs (FR) 11. Space Hellas Anonymi Etaireia Systimata Kai Ypiresies Tilepikoinonionpliroforikis Asfaleias - Idiotiki Epicheirisi Parochis Yperision Asfa (EL) 12. Stichting Cuing Foundation (NL) 13. Michael Culture (BE) 14. Parcs (FR) 15. Trilateral Research Limited (IE) 16. Universiteit Maastricht (NL) 17. Catalink Limited (CY) 18. Toulon Var Technologies (FR) 19. Ecole Nationale Superieure De La Police (FR) 20. Gobierno Vasco - Departamento Seguridad (ES) 21. Finansiniu Nusikaltimu Tyrimo Tarnyba Prie Vidaus Reikalu Ministerijos (LT) 22. Hellenic Police (EL) 23. Hochschule Fur Den Offentlichen Dienst In Bayern (DE) 24. Kentro Meleton Asfaleias (EL) 25. Serviciul De Protectie Si Paza De Stat (MD) 26. Bayerisches Staatsministerium Des Innern (DE) 27. Police Service Of Northern Ireland (UK) 28. Serviciul De Protectie Si Paza (RO)

SHOTPROS	
Title	SHOTPROS *This project is also relevant for 8.3.5 Training and Networking*
Objective	Investigate the influence of psychological and contextual human factors (HFs) on the behaviour of decision-making and acting (DMA) of police officers under stress and in high-risk operational situations, in order to design better trainings
Contract details	H2020-SU-SEC-2032; Topic code: SU-FCT01-2018-2019-2020; 1/5/2019 - 30/4/2022; EUR 5 059 843,75
Abstract	So the SHOTPROS project aims to investigate the influence of psychological and contextual human factors (HFs) on the behaviour of decision-making and acting (DMA) of police officers under stress and in high-risk operational situations in order to design better training for police officers to improve DMA Performance. SHOTPROS will develop a Virtual Reality (VR) solution to experimentally assess the degree to which these factors influence DMA behaviour. Subsequently the project will develop a HF-rooted training curriculum and a corresponding VR training solution to provide a comprehensive framework for practical training for decision-making and acting under stress and in high-risk (DMA-SR) situations in order to improve performance. The training will increase DMA-SR performance which will lead to better and more correct decisions (from several perspectives, e.g. law, ethic, etc.), to keep the guidance in threatened situations, to minimise use of force occurrences, and accordingly, to maximise the avoidance of casualties and collateral damage, such as panic and cascading or escalating effects.
Consortium	Coordinator: 1. Usecon The Usability Consultants Gmbh (AT) Consortium: 2. Ait Austrian Institute Of Technology Gmbh (AT) 3. Katholieke Universiteit Leuven (BE) 4. Stichting Vu (NL) 5. Autonoom Provinciebedrijf Campus Vesta (BE) 6. Re-Lion Group B.V. (NL) 7. Ministerul Afacerilor Interne (RO) 8. Polismyndigheten Swedish Police Authority (SE) 9. Der Polizeiprasident In Berlin (DE) 10. Ruprecht-Karls-Universitaet Heidelberg (DE) 11. The National Police Of The Netherlands (NL) 12. Service Public Federal Interieur (BE) 13. Landesamt Fur Ausbildung, Fortbildung Und Personalangelegenheiten Der Polizei (DE)

INSPECTr	
Title	INSPECTr *This project is also relevant for 9.3 Communication systems (Interoperability and communication with focus on security)*
Objective	Develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level
Contract details	H2020-SU-SEC-2033; topic code: SU-FCT02-2018-2019-2020; 1/9/2019 - 31/8/2022; € 6 997 910
Abstract	Intelligence Network & Secure Platform for Evidence Correlation and Transfer (INSPECTr). The principal objective of INSPECTr will be to develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level. This data will originate from the outputs of free and commercial digital forensic tools complemented by online resource gathering. Using both structured and unstructured data as input, the developed platform will facilitate the ingestion and homogenisation of this data with increased levels of automisation, allowing for interoperability between outputs from multiple data formats. Various knowledge discovery techniques will allow the investigator to visualise and bookmark important evidential material and export it to an investigative report. In addition to providing basic and advanced (cognitive) cross-correlation analysis with existing case data, this technique will aim to improve knowledge discovery across exhibit analysis within a case, between separate cases and ultimately, between interjurisdictional investigations. INSPECTr will deploy big data analytics, cognitive machine learning and blockchain approaches to significantly improve digital and forensics capabilities for pan-European LEAs. INSPECTr intends to reduce the complexity and the costs in law enforcement agencies and related actors to use leading edge analytical tools proportionally and in line with relevant legislation (including fundamental rights), with extended options for multi-level and cross-border collaboration for both reactive and preventive policing and facilitate the detection/prediction of cybercrime operations/trends. The final developed platform will be freely available to all LEAs
Consortium	Coordinator: 1. University College Dublin, National University Of Ireland, Dublin (IE) Consortium: 2. An Garda Siochana (IE) 3. Consiglio Nazionale Delle Ricerche (IT) 4. Ebos Technologies Limited (CY) 5. European Cybercrime Training And Education Group (BE) 6. Politsei- Ja Piirivalveamet (EE) 7. Ministere De L'interieur (FR) 8. Ibm Ireland Limited (IE) 9. Inlecom Group (BE) 10. Iekslietu Ministrijas Valsts Policija State Police Of The Ministry Of Interior (LV) 11. Ministerie Van Justitie En Veiligheid (NL) 12. Norwegian Ministry Of Justice And Public Safety (NO) 13. Police Service Of Northern Ireland (UK) 14. Inspectoratul General Al Politiei Romane (RO) 15. Rijksuniversiteit Groningen (NL) 16. Sindice Limited (IE) 17. Trilateral Research Ltd (UK) 18. Universite De Lausanne (CH) 19. Vltn Gcv (BE)

This overview is complemented by ISF projects.

DIVERT	
Title	Diversion of live-firing firearms in the EU: from research to the combat against trafficking
Objective	Address the current lack of a good intelligence picture on the diversion of live-firing firearms from the legal market and possession through a high-quality in-depth study and enhanced information-sharing
Contract details	ISFP-2017-AG-FIRE; 1/1/2019 – 31/8/2020; 632.233,04
Abstract	Project DIVERT addresses the current lack of a good intelligence picture on the diversion of live-firing firearms from the legal market and possession by executing a high-quality in-depth study on this topic and by enhancing information-sharing. This project involves extensive collaboration between LEA and specialized researchers as an innovative approach to increasing expertise on illicit firearms trafficking (IFT).It will contribute to policy and operational initiatives to tackle IFT in the EU by (a) increasing our understanding of the scale, characteristics and dynamics of the main diversion methods, (b) identifying good practices and developing policy recommendations to more effectively combat such diversion; and (c) enhancing information sharing between relevant entities within MS (LEA, judicial entities and administrative agencies), between MS and with EU agencies. The project consists of an explorative mapping of the scale and nature of diversion of live-firing firearms across all EU MS, followed by an in-depth analysis of (the responses to combat) the diversion dynamics in 9 selected MS (3 MS for each of the 3 main diversion methods). In the final part of the project, the identified problems and good practices will be discussed with representatives from relevant EU agencies to develop policy recommendations.

UNODC-DTA-GFP	
Title	Supporting Global Data Collection and Analysis on Firearms Trafficking and Fostering Cooperation and Information Sharing, in particular Among Countries along Major Trafficking Routes to/from the EU
Objective	Establish a regular collection mechanism of statistical data and information on firearms seizures and trafficking based on an internationally agreed methodology and best practices
Contract details	ISFP-2016-AG-IBA-UNODC; 1/4/2017 – 31/10/2019; EUR: 1.576.968,00
Abstract	The project aims at supporting data collection and analysis on firearms trafficking at national, regional and global levels with a view to monitoring and mapping illicit firearms trafficking flows, fostering effective international cooperation in tracing and information sharing, and combating illicit trafficking and related crimes. The project seeks to establish a regular collection mechanism of statistical data and information on firearms seizures and trafficking based on an internationally agreed methodology and best practices (incl. efforts lead by INTERPOL and EUROPOL) and on previous data collection efforts by UNODC, such as the 2015 Firearms Study. The project also contributes to collect and produce statistical data to monitor target 16.4 of the 2030 Sustainable Development Agenda, which calls for a reduction of illicit arms flows and combating all forms of organized crime.

COOPERANT	
Title	Developing A Tool to Assess Corruption Risk factors in firms' Ownership Structure
Objective	Strengthen the police cooperation in the Baltic sea region by providing a training platform
Contract details	ISFP-2017-AG-CORRUPT; 1/3/2019 – 28/2/2021; 375.293,94
Abstract	The project aims at strengthening the police cooperation in the Baltic sea region by providing the platform to train to make best use the existing cross-border cooperation tools, to fill the gaps in the existing bilateral agreements and other arrangements and to create innovative analysis and e-learning tools.

ENFAST SIENA	
Title	SIENA as communication tool for ENFAST *This project is also relevant for 9.3 Communication systems (Interoperability and communication with focus on security)*
Objective	Establish the connectivity between national FAST teams by using SIENA as standard secure and rapid information exchange tool and to further strengthen the existing network
Contract details	ISFP-2016-AG-IBA-SIENA-FAST; 1/11/2017 – 30/4/2019; 735.109,26

ENFAST SIENA	
Abstract	The ENFAST SIENA project aims to establish the connectivity between national FAST teams by using SIENA as standard secure and rapid information exchange tool and to further strengthen the existing network. All EU member states are already connected to SIENA. However this connection is often only available at the headquarters. The consequence is that many FAST teams use alternative ways of communication, which are not secure. The aim of this project is to increase the coverage of SIENA in the EU member states, so that the FAST teams can use SIENA as the standard communication tool of ENFAST, independent of time and place. The objectives of this ENFAST SIENA project are: Increasing the coverage of SIENA in the EU member states, Training on the use of SIENA, The use of SIENA as standard communication tool for exchanging operational information among the ENFAST members, Strengthening of and closer cooperation within the ENFAST network, Further expansion of joint investigations by national FAST teams, Improvement of the cooperation and information exchange between ENFAST and police teams which are concerned with the investigation of persons of interest regarding terrorist activities. At the end of the project at least six, but preferably all, national FAST teams have access to SIENA independent of time and place and use it as standard communication tool. All teams are trained on the use of SIENA. Due to the strengthening of and closer cooperation within the ENFAST network - while using SIENA as standard communication tool - the number of arrests of criminals will increase, which in turn will increase the security within the EU. The main activities will be open to all 28 EU member States and they are all given the opportunity to prepare a project plan before the start of the project. The project plans will be evaluated by the Core Group before the start of the project. The project plans that are mature and of high quality will be executed during the project.

ENLETS ETP	
Title	ENLETS ETP *This project is also relevant for 9.3 Communication systems (Interoperability and communication with focus on security) and 6.3.3 Cyber crime.*
Objective	Support the Core group of the European Network of Law Enforcement Technology Services (ENLETS) in its further efforts to execute the Council Conclusions on ENLETS
Contract details	ISFP-2017-AG-IBA-ENLETS; 1/9/2018 – 31/8/2021; 842.106,05
Abstract	The European Technology Program (ETP) will support the Core group of the European Network of Law Enforcement Technology Services (ENLETS) in its further efforts to execute the Council Conclusions on ENLETS. ENLETS holds 25 member states, Norway and Switzerland. ENLETS is driven by a Core group that consists out 10 members. The Netherlands, Belgium, United Kingdom, France, Spain, Italy, Bulgaria, Romania, Estonia, Germany and Finland. ENLETS is a working group of the Law Enforcement Working Party and reports to the Standing Committee on operational coordination and Internal Security (COSI).

EPRIS-ADEP	
Title	ADEP Pilot Implementation and Evaluation by MS
Objective	Optimize information flow for Law enforcement information exchange to enable searches within other MS LEA and EIS, in order to facilitate cross border access to information held in national law enforcement databases
Contract details	ISFP-2016-AG-IBA-EPRIS; 1/7/2017 – 31/12/2018; 1.578.801,05
Abstract	Optimize information flow for Law enforcement information exchange to enable searches within other MS LEA and EIS, in order to facilitate cross border access to information held in national law enforcement databases

EUCPN Secretariat	
Title	The further implementation of the MAS of the EUCPN and the Informal Network on the Administrative Approach
Objective	Support the EUCPN and Informal Network of Contact Points on the administrative approach to prevent and fight organised crime (Informal Network) in their implementation of their Multiannual Strategies
Contract details	ISFP-2017-AG-IBA-EUCPN; 1/4/2018 – 31/3/2020; 2.000.000,13
Abstract	The EUCPN Secretariat is linked to two European networks which were constructed through a Council Decision and Conclusion. Namely: the European Crime Prevention Network (hereafter EUCPN) and the Informal Network of Contact Points on the administrative approach to prevent and fight organised crime (hereafter Informal Network). The purpose of this project is to support both networks in their implementation of their Multiannual Strategies. The main tasks for the project members will be to support the boards and chairs and to create the output of the networks. The expected impact should be to put crime prevention more on the agenda in the EU and to increase the knowledge on crime prevention and the administrative approach in Europe. The actions will resolve around the increase of visibility, increasing the contributions to the EU policy and Strategy on crime prevention, to develop outputs and good practice materials.

EUCPN Secretariat	
Title	The implementation of the MAS of the EUCPN and the Informal Network on the Administrative Approach
Objective	Support the EUCPN and Informal Network of Contact Points on the administrative approach to prevent and fight organised crime (Informal Network) in their implementation of their Multiannual Strategies
Contract details	ISFP-2016-AG-IBA-EUCPN; 1/10/2016 – 31/3/2018; 1.000.000,00
Abstract	The EUCPN Secretariat is linked to two European networks which were constructed through a Council Decision and Conclusion. Namely: the European Crime Prevention Network (hereafter EUCPN) and the Informal Network of Contact Points on the administrative approach to prevent and fight organised crime (hereafter Informal Network). The purpose of this project is to support both networks in their implementation of their Multiannual Strategies. The main tasks for the project members will be to support the boards and chairs and to create the output of the networks. The expected impact should be to put crime prevention more on the agenda in the EU and to increase the knowledge on crime prevention and the administrative approach in Europe. The actions will resolve around the increase of visibility, increasing the contributions to the EU policy and Strategy on crime prevention, to develop outputs and good practice materials.

EuNAT	
Title	European Network of Advisory Teams *This project is also relevant for 6.4.1 Organised crime*
Objective	Establish a European network of law enforcement advisory teams, to provide a mechanism for immediate international co-operation when responding to the threat or crisis of kidnap, hostage taking and extortion
Contract details	ISFP-2017-AG-IBA-STU; 1/9/2018 – 31/8/2020; 526.097,60
Abstract	The European Network of Advisory Teams (EuNAT) is an informal expert group of advisory teams. The primary purpose of EuNAT is to have a European network of law enforcement advisory teams, to provide a mechanism for immediate international co-operation when responding to the threat or crisis of kidnap, hostage taking and extortion. The network is a platform for sharing good practice in this specific field throughout the EU and within member's respective countries within the constraints of each State's legal framework. The objective of the action is to improve EU Member States' preparedness in cases of kidnapping, hostage taking and extortion as well as attacks related to these types of crimes using the existing European Network of Advisory Teams (EuNAT). The action will improve Member States' ability to prepare for and handle national and international cases and promote, if relevant, the establishment of dedicated Advisory Teams. It will contribute to enhanced cooperation and increased ability to work together on cross-border cases with a multi-national dimension (e.g. when Europeans of different nationalities become victim of a kidnapping or extortion case in a third country). It will provide opportunities for the EU law enforcement agencies to share up-to-date knowledge, expertise and best practices in the above mentioned fields of crime and react to the new emerging threats such as mass hostage taking and cyber enabled extortion. Mass hostage takings can become an (inter-) national crisis, numerous lives are at risk, law enforcement and other institutions are challenged to their limits both regarding the quality and the quantity of the tasks at hand, while the world is watching. The action aims to compile recommendations for law enforcement agencies to improve preparedness for their management of mass hostage takings and cyber enabled extortion; as well as to deliver and facilitate trainings that address the specific challenges of these types of crimes.

PIU.net	
Title	PIU.net: Advancement and Enhancement of Information Exchange *This project is also relevant for 9.3 Communication systems (Interoperability and communication with focus on security*
Objective	Support and enable highly efficient, privacy compliant queries and exchange, as an operational tool that meets operational needs and high data protection safeguards in line with the PNR-Directive
Contract details	ISFP-2016-AG-PNR; 1/11/2017 – 30/9/2019; 4.199.903,12
Abstract	In line with the requirements and objectives of the PNR-Directive, efficient information exchange between PIUs, PIUs and Europol and with third countries, will be ensured through PIU.net. PIU.net supports and enables highly efficient, privacy compliant queries and exchange, as an operational tool that meets operational needs and high data protection safeguards in line with the PNR-Directive. The project will offer a ready to use PIU.net providing a solid foundation for cooperation between PIUs. The project will contribute to enhanced and more efficient international information exchange, improving identification, detection and countering of criminals, terrorists and their travel movements. It will also benefit the relationship between the PIUs and the competent authorities, whom operate within their own law enforcement cooperation framework. The project will work on making operational utility and data protection mutually reinforcing. PIU.net is a secure and auditable real-time communication and exchange solution, supported by commonly. The project will jointly further develop, enhance and deploy the technical solution based on existing and proven solutions and develop data formats, operational guidelines and advise on the governance structure. It is supported by an agile development of the tool for partners developing PIU capabilities. The results of the project - being PIU.net and its supporting materials - will be delivered to the European Commission as guardian of the PNR-Directive and its functioning within the objectives set out by it.

Polish-German JPS	
Title	Strengthening the Polish-German Joint Police Stations / JPS *This project is also relevant for 7.3 Land border security.*
Objective	Enhance the effectiveness of combatting cross-border crime and illegal migration at the PL-DE land border and improve the subjective feeling of security of the population in the border region
Contract details	ISFP-2017-AG-SCHEN; 1/11/2018 – 30/4/2020; 678.985,62
Abstract	The project aims at enhancing the effectiveness of combatting cross-border crime and illegal migration at the PL-DE land border and improving the subjective feeling of security of the population in the border region. To this end, the capacity of the three PL-DE joint police stations at the border shall be strengthened. Thus, the quantity and quality of patrols shall be stepped up, resulting in a higher number of SIS II hits, seizures and arrests. At the same time, the visibility of police cooperation shall be increased. This shall be achieved by increasing the number of patrol cars available to the joint police stations by 6 vehicles. Each car shall be equipped with dedicated search equipment, document verification devices and equipment improving radio communication with the control centre. Additionally, one vehicle will be equipped with an automated number plate recognition system. The operational capacity of the officers will be strengthened by joint trainings, continuous language training and a staff exchange. Situational awareness will be enhanced. Visibility of cooperation shall be stepped up by marking the patrol cars and by a media strategy focused at the local and regional press. The activities carried out will be procurement of vehicles and technical equipment, nine joint trainings, continuous language trainings, staff exchange within the border region and the creation of a new joint risk analysis product based on a best practice example developed at the PCCC Padborg. On the short term, the project will benefit the PL Border Guard and the DE Federal Police. On a medium- and long-basis, the increased security will benefit the citizens living in the area as they are particularly affected by cross-border crime. The manufacturing and service industry involved in cross-border trade and services will benefit both from the protection of their businesses from crime as well as from unhindered traffic across the border. This project is also relevant for 7.4 Multi-modal security, risk management, including migration

UMF3plus	
Title	Universal Message Format 3 plus *This project is also relevant to 9.3 Communication systems (interoperability and communication with focus on security).*
Objective	Enhance the UMF standard (operational and technical model) in the context of the agreed governance, and illustrate its added value through practical implementation in select areas
Contract details	ISFP-2017-AG-IBA-UMF; 3/9/2018 – 2/9/2021; EUR: 3.216.903,64
Abstract	The UMF3plus project consists of two parts: Work stream 1: Working on enhancing the UMF standard (operational and technical model) in the context of the agreed governance. Work stream 2: Practical use of the UMF in select areas. Regarding work stream 1: A coordinated further development of the UMF is intended on the basis of existing requirements (e.g. biometrics, narcotics). The UMF project team will centrally coordinate the maintenance of the model. The governance structure will be handed over to the EU Commission during the course of the project; this task will be finished at the end of the project at the latest. Regarding Work stream 2: This second part of the project serves the purpose of extending UMF use. It is intended to use the UMF in productive implementations to illustrate its added value for individual users as well as in the context of national and European systems.

SIENA for CT	
Title	Extending the use of SIENA as a communication tool for Counter Terrorism *This project is also relevant for 9.3 Communication systems (interoperability and communication with focus on security).*
Objective	Establish connectivity between Member States's competent CT agencies/units and Europol, using an already upgraded version of SIENA, allowing the exchange of classified data up to a security level of EU Confidential
Contract details	ISFP-2016-AG-IBA-SIENA-CT 1/9/2017 – 31/12/2018; EUR: 1.366.060,44
Abstract	13 EU Member States will be partners in the proposal which will involve 3 work packages. An Garda Siochana, Ireland's National Police Service, as a representative of the European CT Centre, was invited by the European Commission to submit a project proposal supporting the activities defined in the ISF Annual Work Programme 2016. The objective is to establish connectivity between Member States's competent CT agencies/units and Europol, using an already upgraded version of SIENA, allowing the exchange of classified data up to a security level of EU Confidential. It is intended that at least one CT per MS will be able to communicate peer-to-peer and with Europol via SIENA.

This overview is complemented by a relevant H2020 project.

SLIPPED	
Title	Maintenance and relapse in long-term desistance from crime and recovery from addiction *This project is also relevant for 6.4.1 Organised Crime*
Objective	Investigate the dual processes of desistance from crime and recovery from addiction within the same population
Contract details	H2020-MSCA-IF-2018 1/7/2019 - 30/6/2021; EUR: 224.933,76
Abstract	The primary objective of this research is to investigate the dual processes of desistance from crime and recovery from addiction within the same population. The research therefore targets a thus far neglected area of scholarly study. Specifically, the aims of the Fellowship are twofold, i) to understand the personal, social, and structural factors that contribute towards 'long-term' desistance and recovery, and ii) to explore why individuals who had achieved more than three years success in both processes then experience relapse and recidivism. The research process will have three avenues of investigation, i) an interdisciplinary review of relevant literature and studies from the disciplines of Criminology and Addiction Studies, ii) an analysis of relevant legislature, and iii) sixty semi-structured qualitative interviews to uncover the nuances and complexities of maintenance and relapse in long-term desistance and recovery. Research data will be collected in Belfast, Northern Ireland, and Dublin, Republic of Ireland. The researcher will work out of the host institution, Queens University Belfast, under the supervision of a world leader in the field, Prof. Shadd Maruna. Participants will be recruited through a careful and determined process, overseen by the research supervisor, which will engage with statutory and non-statutory supervision and support services for former offenders and recovering substance misusers. The project will generate new knowledge relevant for the H2020 societal challenges 1 (Health, Demographic Change and Wellbeing) and 7 (Secure Societies). Further, the European Union Drugs Strategy 2013-20 identifies achieving a better understanding of addiction recovery and rehabilitation as central to the task of 'Demand Reduction'.
Consortium	Coordinator: The Queen's University Of Belfast (UK)

WEIRD WITNESSES	
Title	Beyond WEIRD Witnesses: Eyewitness Memory in Cross-Cultural Contexts
Objective	Develop culturally modulated theory of eyewitness memory and design and test evidence-based interview guidelines
Contract details	ERC-2018-STG; 1/8/2019 - 31/7/2021; EUR: 1.496.770
Abstract	Our increasingly international society demands that eyewitnesses of serious crimes regularly provide testimony in cross-cultural settings, such as international criminal tribunals. This poses significant challenges for investigators and legal decision-makers. Errors in fact-finding may result in wrongful convictions and unjust acquittals. Yet, eyewitness memory research has predominantly focused on Western, Educated, Industrialized, Rich, and Democratic (WEIRD) witnesses. The project addresses two key objectives: (1) develop culturally modulated theory of eyewitness memory and (2) design and test evidence-based interview guidelines. The project integrates analyses of video, document and experimental data to provide insight into culture-dependent variables in eyewitness memory. The new theory will enable researchers and practitioners to steer away from the present WEIRD bias in legal psychology.
Consortium	Coordinator: Stichting VU (NL

6.5 Radicalisation

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Radicalisation	CONTRA CPR DARE FIRST LINE GRIEVANCE IMPACT EUROPE INSIKT Local institutions against extremism LIAISE II MINDb4ACT Pericles PRACTICIES PROPHETS RED-Alert SAFFRON SSCAT STRESAVIORA II TRIVALENT

This overview is complemented by ISF projects.

ARMOuR	
Title	A RADICAL MODEL OF RESILIENCE FOR YOUNG MINDS
Objective	Address societal polarization caused by the adoption and spread of extremist ideologies by creating an interdisciplinary model of learning helping individual and mainstream communities build resilience to ideologies and behaviours specific to violent extremism
Contract details	ISFP-2017-AG-RAD; 1/1/2019 – 31/12/2019; 822.054,25
Abstract	The ARMoUR project aims to address societal polarization caused by the adoption and spread of extremist ideologies by creating an interdisciplinary model of learning helping individual and mainstream communities build resilience to ideologies and behaviours specific to violent extremism. The project will help both existing and potential influencers to model opinions by integrating skills on how to: create a message that deals with common concerns and interests of the middle ground society, develop critical thinking so as to delineate propaganda from solution oriented discourse, capitalise assertiveness and emotional intelligence into mediating speech that engages and connects with the diverse categories of the silent majority, use anger management and conflict resolution so as to contain and push back the discourse of the radical pushers and joiners

BRIDGE	
Title	Building Resillence to reDuce polarisation and Growing Extremism
Objective	Build local actors' awareness and capacities to reduce individual and collective vulnerability to radicalisation by mitigation polarisation
Contract details	ISFP-2017-AG-RAD; 1/1/2019 – 31/1/2021; 701.000,87
Abstract	BRIDGE's general objective is to build local actors' awareness and capacities to reduce individual and collective vulnerability to radicalisation by mitigation polarisation. In this sense, the project specific objectives are: to strengthen local polarisation detection and management tools, to assist local authorities in the development of actions to tackle tensions and social unrest trends; to promote community-based initiatives that imply cooperation between different public services and private actors; to bring together European local authorities and experts willing to address polarisation at the local level.

CHAMPIONs	
Title	Cooperative Harmonized Action Model to stop Polarisation in Our Nations
Objective	Establish permanent offline working groups – 'CHAMPIONs Roundtables' – combining FLPs of different disciplines, professions and institutions / agencies, to jointly develop effective detection & response solutions to counter polarisation, build resilience and protect vulnerable groups in their local communities
Contract details	ISFP-2017-AG-RAD; 1/1/2019 – 31/3/2021; 833.011,05
Abstract	CHAMPIONs' central action is to establish permanent offline working groups – 'CHAMPIONs Roundtables' – combining FLPs of different disciplines, professions and institutions / agencies, to jointly develop effective detection & response solutions to counter polarisation, build resilience and protect vulnerable groups in their local communities. FLPs will be trained to build capacity to design solutions and programmes to most effectively address the drivers of polarisation, and to collaborate most efficiently by breaking down institutional barriers. Medium term: their actions not only directly affect vulnerable individuals, but also the wider community – who will be engaged in awareness-raising events – as well as local and national policy-makers. To facilitate these processes of offline joined-up solution development, an online platform will be produced combining three central instruments: (i) 'Alert' – a collation of tools and services developed under other EU-funded projects that enable FLPs to bring attention to key focal issues to address in their community (e.g. social media monitoring tools); (ii) 'Arena' – a communication & cooperation mechanism that enables instantaneous information exchange either privately, between collaborating FLPs, and publicly through sharing good practice and highlighting strengths / weaknesses of certain actions; (iii) 'Training Yard' – a capacity-building resource centre which FLPs can engage with either individually or as a group, complete with learning materials, video-tutorials, good practice guidelines / handbooks and case study simulation exercises developed through the project action. The long-term aim of the project is to transfer this pilot model to other communities across the EU where other FLP Roundtables are established and become users of the developed platform. To achieve this, synergies with related EU-funded projects, platforms and networks will be harnessed throughout the project and after its implementation period.

CICERO	
Title	CounternarratIve Campaign for prEventing RadicalisatiOn *This project is also relevant for 8.2.2 Civil society engagement.*
Objective	Develop and implement a counter-narrative communication campaign aimed at preventing radicalisation leading to violent extremism, accompanied by a methodology for evaluating the campaign's effectiveness
Contract details	ISFP-2017-AG-CSEP; 1/2/2019 – 31/1/2021; 1.058.765,00
Abstract	The goal of the CICERO project is to develop and implement a counter-narrative communication campaign aimed at preventing radicalisation leading to violent extremism, accompanied by a methodology for evaluating the campaign's effectiveness. The CICERO consortium will, at first, identify the target audiences that are considered particularly susceptible to extremist propaganda. The most prominent radicalisation narratives circulating across the EU will then be collected and analysed. The campaign will rely on both online and offline communication channels for disseminating a wide range of multimedia contents, produced by the consortium, to the different audiences. CICERO will deal with different kinds of radicalisation narratives, ranging from those related to politico-religious extremism (e.g. jihadist), to left-wing, right-wing and single-issue extremism. The aim is to undermine the appeal of the extremist propaganda, while also providing credible and positive alternatives to the related narratives. Additional purpose of the campaign is to empower relevant civil society actors in challenging extremist narratives. To this end, online communication efforts will be designed to promote messages that encourage civic engagement and the assimilation of democratic fundamental rights and values embedded in EU society, supported by off-line activities dedicated to amplifying the CICERO counter-narrative message. Civil society engagement efforts, including the organisation of "train-the-trainers" workshops directed at specific stakeholders, will be undertaken to further enhance the ability of civil society to detect and cope with radicalisation leading to violent extremism.

Counteract	
Title	Preventing and combating online radicalisation *This project is also relevant for 8.2.2 Civil society engagement.*
Objective	Contribute to behavioural changes which dissuade societal groups susceptible and vulnerable to radicalisation and terrorist content online by providing positive, alternative and credible narratives
Contract details	ISFP-2017-AG-CSEP; 1/1/2019 – 31/12/2020; 358.863,02
Abstract	Preventing radicalisation has been identified as one of the main goals of the European Agenda on Security (EAS). In addition, the role of civil society engagement and the input that civil society organisations can add in achieving such goal has been recognised. In light of these developments, we intend to contribute to behavioural changes which dissuade societal groups susceptible and vulnerable to radicalisation and terrorist content online by providing positive, alternative and credible narratives. It is our goal to study how these groups behave online, develop a communication campaign which delivers these alternative or counter narratives, and thoroughly assess its impact.

D.O.B.T.	
Title	DO ONE BRAVE THING *This project is also relevant for 8.2.2 Civil society engagement.*
Objective	Counter extremist narratives
Contract details	ISFP-2017-AG-CSEP; 15/1/2019 – 14/1/2021; 744.238,50
Abstract	Objectives: (1) Empower young people to challenge extremist narratives they experience in their daily lives. (2) Provide young people with media literacy skills and software tools to investigate online sources of information and think more critically (3) enable young people to develop counter-narrative campaigns to challenge hate speech and extremist rhetoric online (4) Encourage young people to non-violently address their political grievances through policy-advocacy.

DECOUNT	
Title	Promoting democracy and fighting extremism through an online counter-narratives and alternative narratives campaign *This project is also relevant for 8.2.2 Civil society engagement*
Objective	Design and disseminate an online campaign including deradicalization and prevention online resources (majorly online counter-narratives, such as the stories of formers); videos produced by vulnerable youth (alternative narratives) and a video game structured along binary decisions leading to radicalization or maintaining resilience (both)
Contract details	ISFP-2017-AG-CSEP; 1/11/2018 – 31/10/2020; 791.687,65
Abstract	The project aims to design and disseminate an online campaign including deradicalization and prevention online resources (majorly online counter-narratives, such as the stories of formers); videos produced by vulnerable youth (alternative narratives) and a video game structured along binary decisions leading to radicalization or maintaining resilience (both). The action focuses on frames and individual roles and decisions in a sophisticated and modular way by: de-constructing extremist frames and challenging extremist roles in achieving these in videos of formers; illustrating the consequences of extremist choices and the possibilities of alternatives in the video game; producing actual alternative frames, alternative solutions to everyday and socio-political problems and alternative roles in vulnerable youth videos. The outcomes of the action are: bringing about behavior change dissuading target audience from promoting terrorism and violent extremism and/or using violence; growing civic engagement and take active stance in democratic processes by target audiences; halting radicalisation and recruitment processes; enhancing (digital) resilience and critical thinking of the target audience against terrorist and extremist propaganda on-and offline. The beneficiaries are vulnerable individuals and on the brink of radicalization: short term immediate contact with the online products through the screenings and the interviews; medium term as audience of the full scale online campaign, and radicalized individuals in offline deradicalization work, CSOs and institutions in the field in Europe. Long term beneficiaries are additionally the broader population interested in credible and authentic sources of information. The action will contribute in the long term to deradicalisation and preventing radicalization, by: empowering young alternative voices and creating a domino effect; lay bare and combat by showing the consequences of, and offer alternative narratives.

EUROTOPIA	
Title	EUROTOPIA *This project is also relevant for 8.2.2 Civil society engagement.*
Contract details	Create counter narratives by a international video campaign and a "call to action" campaign- to counteract right wing and Islamic extremism propaganda on social media
Abstract	ISFP-2017-AG-CSEP; 1/11/2018 – 30/4/2020; 395.525,50
Website	The aim of this project is to create counter narratives by a international video campaign and a "call to action" campaign- to counteract right wing and Islamic extremism propaganda on social media. The project will be a three country cooperation between Sweden, Italy and Belgium. Belgium and Sweden have faced horrific terrorist attacks and we wish to counter further attacks and act proactively concerning the case of Italy. The aim is to challenge the definition of who the hero and villain is in the narrative that is formatted by the extremist propaganda and promote visions of co-existence and tolerance. The fundamental thing we want to do is to change the story by changing the image, to be able to halt recruitment and foster behavior change. The aim is to create a 21 video package consisting of 3 minutes per video that will portray victims, former extremists and key against working against extremism. we wish to personalise the stories behind extremist violence from a holistic experience and also bring forth young voices and how they see us co-existing in the EU in the future.They will all get the opportunity to also discuss what they see as important qualities for a positive coexistence and this will be a part of a "call to action campaign" named Eurotopia- to promote positive visions of co-existence to engage the public. Our target group is at-risk teens and the public with the aim to boost civic engagement in projects for at-risk teens through the call to action campaign. The videos will be divided into 7 from Sweden, 7 from Belgium and 7 from Italy and disseminated through social media such as Facebook, Twitter and Youtube. During the final phase of the project, we will showcase the campaign at the Google Centre (or other suitable venue) in Brussels, and in the context of the events linked to Cannes Film Festival in France and the Oscars in United States - to enhance exposure and dissemination. This project has the potential to spread to all European countries.

EXIT EUROPE	
Title	EXIT EUROPE
Objective	Create counter narratives by a international video campaign and a "call to action" campaign to counteract right wing and Islamic extremism propaganda on social media
Contract details	ISFP-2017-AG-RAD; 1/1/2019 – 31/12/2020; 800.474,49
Abstract	The aim of this project is to create counter narratives by a international video campaign and a "call to action" campaign- to counteract right wing and Islamic extremism propaganda on social media. The project will be a three country cooperation between Sweden, Italy and Belgium. Belgium and Sweden have faced horrific terrorist attacks and we wish to counter further attacks and act proactively concerning the case of Italy. The aim is to challenge the definition of who the hero and villain is in the narrative that is formatted by the extremist propaganda and promote visions of co-existence and tolerance. The fundamental thing we want to do is to change the story by changing the image, to be able to halt recruitment and foster behavior change. The aim is to create a 21 video package consisting of 3 minutes per video that will portray victims, former extremists and key against working against extremism. we wish to personalise the stories behind extremist violence from a holistic experience and also bring forth young voices and how they see us co-existing in the EU in the future.They will all get the opportunity to also discuss what they see as important qualities for a positive coexistence and this will be a part of a "call to action campaign" named Eurotopia- to promote positive visions of co-existence to engage the public. Our target group is at-risk teens and the public with the aim to boost civic engagement in projects for at-risk teens through the call to action campaign. The videos will be divided into 7 from Sweden, 7 from Belgium and 7 from Italy and disseminated through social media such as Facebook, Twitter and Youtube. During the final phase of the project, we will showcase the campaign at the Google Centre (or other suitable venue) in Brussels, and in the context of the events linked to Cannes Film Festival in France and the Oscars in United States - to enhance exposure and dissemination. This project has the potential to spread to all European countries.

OLTRE	
Title	Oltre l'orizzonte. Contro narrazioni dai margini al centro *This project is also relevant for 8.2.2 Civil society engagement.*
Objective	Counter religious radicalisation of Muslim youth in Italy through an interdisciplinary approach to mobilise CSOs, academia, companies and direct target groups in a co-designed communication campaign throughout Italy
Contract details	ISFP-2017-AG-CSEP; 15/11/2018 – 14/1/2020; 1.068.011,94
Abstract	The Action, to be developed in 24 months, considers the relational context-specific nature of religious radicalisation of Muslim youth, adopting multi-situated approaches, co-design and participatory practices. Empirical studies show that participative collaborative campaigns involving mixed target groups (young people with Muslim and non-Muslim backgrounds, second/"new" generations) allow to limit stigmatisation and related backlashes. This is where the present project intends to intervene with an interdisciplinary approach to mobilise CSOs, academia, companies and direct target groups in a co-designed communication campaign throughout Italy.

Project Grey	
Title	Project Grey: Building the Middle Ground *This project is also relevant for 8.2.2 Civil society engagement.*
Objective	Empower the middle ground of society by bringing social media campaigners, big data analysts, and social workers together under the banner of the 'Grey Narrative', focused on the promotion of values such as nuance, diversity, and empathy
Contract details	ISFP-2017-AG-CSEP; 1/11/2018 – 31/10/2020; 857.777,27
Abstract	Project Grey aims to empower the middle ground of society by bringing social media campaigners, big data analysts, and social workers together under the banner of the 'Grey Narrative': a narrative focused on the promotion of values such as nuance, diversity, and empathy. The project will use big data applications to identify local & polarised hot topics and personas, after which a coalition of social workers and social media campaigners will use their expertise to intervene in a holistic approach: infiltrating filter bubbles, 1-on-1 interventions, and, last but not least, promoting nuanced views through social media campaigns. By combining these efforts, the consortium of Project Grey aims to counter polarisation across the EU in a new, innovative, and continuously adapting approach, making sure that, in the long run, our society will be more resilient to the powers of division and the processes of radicalisation that spring from them.

RAGE	
Title	Radical Awareness Game Engagement *This project is also relevant for 8.2.2 Civil society engagement*
Objective	Design, implement and evaluate professional counter and alternative- narrative campaigns adapted to 15 to 24 years old vulnerable to the radicalisation process
Contract details	ISFP-2017-AG-CSEP; 1/3/2019 – 28/2/2021; 1.108.532,56
Abstract	The main objectives of RAGE are to design and implement professional counter and alternative- narrative campaigns adapted to 15 to 24 years old vulnerable to the radicalisation process, evaluate and improve their effectiveness, prove the positive impact of such actions to build legitimacy for their financial support. RAGE is a multi-dimensional project: it consists of research, training, an on-line social campaign and an off-line social activity (social city game). It builds on previous training (CSEP1) and EU research projects as it is an intermediary project of a 3-phase CSE Progamme.

RaP	
Title	Rhizome against Polarisation
Objective	Prevent polarisation and radicalisation in 3 European countries (Austria, Italy and Spain) at grass-root level through a participative approach (Living Lab methodology).
Contract details	ISFP-2017-AG-RAD; 1/1/2019 – 31/1/2021; 606.403,24
Abstract	Prevention of polarisation and radicalisation in 3 European countries (Austria, Italy and Spain) at grass-root level through a participative approach (Living Lab methodology).

Resilient and united	
Title	PREVENTING AND COUNTERING EXTREMISM AND RADICALISATION: AN ACTION PLAN FOR PORTUGAL *This project is also relevant for 8.2.2. Civil Society Engagement*
Objective	Prevent and counter extremism and radicalization in Portugal by combining communication technology with a more coordinated and knowledge-based prevention effort.
Contract details	ISFP-2017-AG-CSEP; 1/1/2019 – 30/6/2020; 419.660,42
Abstract	Despite Portugal's peaceful environment and generous reception policies, it's not immune to borderless invisible threat that is violent extremism, radicalization and terrorism. Destructive forces from extremist groups – within our country and abroad – currently poses a threat to the security and social cohesion of the Portuguese society. This proposal aims to prevent and counter extremism and radicalization in PT, by combining communication technology with a more coordinated and knowledge-based prevention effort.

RETHINK	
Title	(Re)think Before Act – Alternative Narratives to Violent Extremism *This project is also relevant for 8.2.2. Civil Society Engagement*
Objective	Prevent vulnerable audiences of starting a process of radicalisation by offering them resilience and critical thinking mechanisms to provide an alternative narrative that deconstructs the extremist rhetoric
Contract details	ISFP-2017-AG-CSEP; 1/11/2018 – 31/10/2020; 992.464,59
Abstract	Objectives: to prevent vulnerable audiences of starting a process of radicalisation by offering them resilience and critical thinking mechanisms to provide an alternative narrative that deconstructs the extremist rhetoric to those already engaged within a process of radicalisation, in order to change violent behavior

YouthRightOn	
Title	Resilient Youth against Far-Right Extremist Messaging Online *This project is also relevant for 8.2.2 Civil Society Engagement*
Objective	Address the problem of far right influence over youth in Bulgaria by development of alternative narratives to confront extremist messages and ideas propagated online
Contract details	ISFP-2017-AG-CSEP 1/1/2019 – 31/12/2020; EUR: 343.677,58
Abstract	This project aims to address the problem of far right influence over youth in Bulgaria by development of alternative narratives to confront extremist messages and ideas propagated online. The expected impact of the project involves enhanced resilience and critical thinking as well as increased civic engagement among youth in Bulgaria susceptible to extremist content online. The central outcome of the project involves development of targeted online campaign supported by offline activities to aid prevention of processes of far right radicalisation among vulnerable youth.

YoungRes	
Title	Strengthening European Youngsters Resilience through Serious Games *This project is also relevant for 6.1 Terrorist threats*
Objective	Implement a new innovative approach based on digital technologies to overcome the difficulty of efficient interaction with youth and vulnerable population at risk of radicalization or polarization
Contract details	ISFP-2017-AG-RAD 1/1/2019 – 31/3/2021; EUR: 540.350,00
Abstract	Objectives: This project aims to overcome the acknowledged difficulty of efficient interaction with youth and vulnerable population at risk of radicalization or polarization. To do so, YoungRES advocates a new innovative approach based on digital technologies to overcome this barrier, built on previous achievements by project partners in game technology, social media analytics, and eLearning (e.g.: SAVEit, RiskTrack, CrisisTracker, Clutler, E-genius, SmaCC).

WayOut	
Title	Integrated Exit Programme for Prison and Probation *This project is also relevant for 6.1 Terrorist threats.*
Objective	Improve and facilitate the implementation of prison and probation exit programmes (EPs) by building a common framework to evaluate them and creating an innovative and integrated one based on approaches with proven effectiveness
Contract details	ISFP-2017-AG-RAD 1/12/2018 – 30/11/2020; EUR: 697.520,16
Abstract	The WayOut - Integrated Exit Programme for Prison and Probation project aims to improve and facilitate the implementation of exit programmes (EPs) by building a common framework to evaluate them and creating an innovative and integrated one based on approaches with proven effectiveness. It desires to generate impacts such as an increased understanding about EPs among judicial, prison, probation and community organisations (religious) staff; improved knowledge about the efficacy of EPs and 'what works'; enhanced staff capacity to deal with radicalised (or at risk) detainees; promote quality training and learning for prison staff. Consequently, its main outcomes will be a framework of EPs evaluation, an integrated EP based on approaches with proven effectiveness, a training course on exit strategies (ES) to practitioners, and law enforcement officials' awareness enhancement.

RVIEU	
Title	Resonant Voices Initiative in the EU *This project is also relevant for 8.2.2 Civil Society Engagement and 7.4 Multi-modal security, risk management, including migration*
Objective	Strengthen the influence of credible and resonant voices challenging extremist propaganda targeted at audiences vulnerable to radicalisation and recruitment within the Western Balkans diaspora in the EU
Contract details	ISFP-2017-AG-CSEP 1/11/2018 – 31/10/2020; EUR: 1.030.007,68
Abstract	The Resonant Voices Initiative in the EU initiative pursues objectives closely linked to the nexus of the security, migration and preventing radicalisation leading to violent extremism agendas of the European Union. It aims to strengthen the influence of credible and resonant voices challenging extremist propaganda targeted at audiences vulnerable to radicalisation and recruitment within the Western Balkans diaspora in the EU. The vulnerability and resilience of this overlooked cohort is a crucial factor impacting, not only the security situation, but also community cohesion within the EU, democratic developments outside of the EU, and EU enlargement. Through a positive and alternative narrative campaign, 20 in-depth investigative articles will be published by 20 Resonant Voices Fellows, and 200 diverse campaign materials collaboratively produced by 140 community influencers from three diaspora communities in three different EU countries. The capacity and commitment of this core group to push back against polarising, inflammatory, and radicalising discourse will be strengthened through formal training and hands-on assistance. In sum, behavioral change consistent with increased resilience to violent extremism will be created through information campaigns in challenging, politically charged contexts and by effectively combining technology with a deep understanding of the community to disseminate compelling content.

This overview is complemented by relevant Erasmus+ projects.

Cooperation and Tools Against Youth Radicalization	
Title	Cooperation and Tools Against Youth Radicalization
Objective	Foster cooperation and exchanges in the field of youth on the prevention of violent radicalization, xenophobia and racism between 5 partners in EU countries and 2 Partner from region 11 ACP
Contract details	602654-EPP-1-2018-1-SE-EPPKA2-CBY-ACPALA 15/12/2018 - 16/8/2020; EUR: 149.615,44
Abstract	The project is finalized to foster cooperation and exchanges in the field of youth between 5 Partners EU Countries:Eu Diaspora Council, Sweden,Soma Forengin Rf Finland,London Placement Academy UK, Cooperazione Sud per l'Europa Italy, Asociacion Cultural Integra,Spain and 2 Partner from region 11 ACP :Soma View Kenya, Kenya and Putland Network Forum Somalia on the prevention of violent radicalization, xenophobia and racism.The project contributes to promoting the development of social and civic and intercultural competences and critical thinking in young people and also to face radicalization, discrimination, racism and violence.Helps to fill these gaps through the dissemination of knowledge and the construction of these tools will take place through the collection of experiences, needs and proposals of young workers working in different countries (Finland, Sweden, Italy, Spain, Kenya and Somalia) and in various areas that concern the world of young people (schools, cultural associations, NGOs, youth centers, reception centers for young migrants, etc The project intends to create a tool "Brochure Youth worker against radicalization" for useful to youth work, develop and convey messages aimed at deconstructing extremist propaganda in frontline work with young people (new migrants, immigrants and young natives) and fostering integration through inter-religious dialogue and intercultural knowledge based on the knowledge of the other.
Consortium	Coordinator: EU Diaspora Council (SE)

Media and Critical Thinking Against Radicalisation	
Title	Media and Critical Thinking Against Radicalisation
Objective	Develop tools and resources to prevent radicalisation and fight hate speech in media
Contract details	602623-EPP-1-2018-1-TN-EPPKA2-CBY-SMED; 15/12/2018 - 14/12/2020; EUR: 137.753,12
Abstract	"Media and Critical Thinking Against Radicalisation" (MCTAR) is a youth project coordinated by Euro- Med Eve (Tunisia) in partnership with EN.O Greece, URI Mena (Jordan) and Freeminds in Action (Italy). It aims to develop tools and resources to prevent radicalisation and fight hate speech in media.MCTAR is thought to be a project to develop further different methodologies and approaches in youth work as a way to prevent and identify radicalisation processes amongst youngsters. On the other hand, we aim to foster youth understanding on current topics and foster their critical thinking as a way to become mindful citizens who are able to discern hate speech in and negative messages in media and online.The project is divided in two main phases. The first one is devoted to provide youth workers with tools and resources in order to identify risk behaviours and patterns in youngsters that could lead to radicalisation. The second phase objective is to engage youth into critical thinking and debate over different topics spinning around the concept of intercultural dialogue and tolerance. On the other hand, youth will get the opportunity to get an insight into creative processes such as photography and videomaking as an alternative way to express themselves and oppose to hate speech messages. By sharing these experiences with youth from different countries and cultural background, youngsters will get the chance to share diverse perspectives and learn from each other. In addition, they will engage into the production of several short films that will be presented at a local festival in Nabeul.Throughout the project several intellectual outputs are to be produced, highlighting, an antiradicalisation toolkit, a field research report on the four communities , OER's related to the project content and training sessions, photographies and videos made during the youth exchanges and several short films co-produced by the youngsters. All the learning outcomes will be available through our website under creative commons license for free use.The main goals to be achieved can be divided in three points: 1. Raising awareness about radicalisation and hate speech in media. 2. Developing tailored methods for youth workers to address prevention on radicalisation and provide them with tools and resources adapted to each specific context.3. Foster critical thinking amongst youngsters while providing them with skills and creative tools as a way to develop counter narratives.With MCTAR we aim to provide tools for change, a different approach to youth work, focused on the prevention and identification of youth radicalisation processes by promoting the intercultural dialogue and the creation of alternative messages through media tools. MCTAR is a project to overcome mental walls, and build up new narratives in contraposition to hate speech.
Consortium	Coordinator: L Association Euro-Mediterraneenne Des Echanges, Volontariats, Evenements (FR)

H(Youth) manity	
Title	H(Youth) manity
Objective	Raise awareness of European citizenship and European values, against Euro scepticism, radicalization and violence
Contract details	602682-EPP-1-2018-1-AL-EPPKA2-CBY-WB 15/12/2018- 29/2/2020; EUR: 80.492,65
Abstract	H(Youth)MANITY aims to raise awareness of European citizenship and European values, against Euro scepticism, radicalization and violence, by promoting solidarity towards crisis immigration in the EU; by empowering youth workers and youth leaders in the field of prevention of radicalization and extremism among young people by analyzing local realities, exchanging practices and developing sustainable activities aimed at promotion of culture of peace.
Consortium	Coordinator: Agjencia Per Zhvilim Rinor (AL)

This overview is complemented by relevant H2020 projects.

MPP	
Title	Jihad Or Re-Integration: Pathways Of Foreign Fighters After War
Objective	Enhance understanding of pathways of foreign fighters after war
Contract details	H2020-MSCA-IF-2017 2/9/2019 - 1/9/2021; EUR: 177.598,80
Abstract	Foreign fighters pose a serious threat to Europe. Western intelligence agencies believe that approximately 400 foreign fighters have returned to the EU from Syria and Iraq, and that at least 250 radicalized individuals have been smuggled to Europe from 2014 until 2016. The major hotbeds of foreign fighters smuggling and recruitment are located in Europe itself, in Bosnia and Kosovo, both of which underwent civil wars that featured foreign fighters. We know little about how foreign fighters behave in the aftermath of such civil wars: why some continue fighting in other wars while others go back to civilian life. This is an unfortunate shortcoming because numerous studies have shown that some foreign fighters have demobilized in the aftermath of wars in Afghanistan and Bosnia, while others left for Chechnya, Iraq and Syria to continue jihad. Those who continued fighting built networks with terrorists who are responsible for recent attacks in Europe. It is, therefore, imperative to understand these dynamics in order to make sound decisions that can prevent terrorism in Europe. This project will remedy this shortcoming by pursuing three goals. First, the project will adopt a fresh theoretical framework for the study of foreign fighters. Drawing on organizational theory, career transition and political violence literature, the project aims to explain post-war pathways of foreign fighters as a function of their role in previous war(s). Such an approach goes beyond standard focus on motivations and will help elicit why foreign fighters demobilize or turn violent in a long-term perspective. Second, the project will obtain new empirical insights into how foreign fighters pursued different paths in two similar, post-conflict contexts (Bosnia-Herzegovina and Kosovo). The third objective of the project is to develop a set of policy recommendations that will assist future policy makers in dealing with returning foreign fighters." This project is also relevant for 6.1 Terrorist threats.
Consortium	Coordinator: Universiteit Leiden (NL)

BRaVE	
Title	Building Resilience Against Violent Extremism and Polarisation
Objective	Develop better analytical and policy tools for the design of more efficient resilience policies that counteract polarization and prevent violent extremism
Contract details	H2020-SC6-GOVERNANCE-2018;1/1/2019 - 30/6/2021; EUR: 1.483.750
Abstract	Far Right and Islamist groups seeking to recruit people to their particular political cause promote 'black and white' ideologies that lead to polarization, hatred, intolerance and violence. Often cherry-picking from religious doctrines, they rely on superficial understanding and interpretation of such doctrines. The activities of such groups can lead to disruption of social cohesion, diminished civic capacity, social tensions, hate speech, intolerance, discrimination and even violence. This project builds on existing knowledge and policy experience with a view of developing better analytical and policy tools for the design of more efficient resilience policies that counteract polarization and prevent violent extremism. The project starts with a critical reading of existing scholarly literature and with a critical mapping of existing policy approaches to develop a preliminary impact assessment of these approaches. It continues with a further survey of good practices in counteracting polarization and violent extremism and builds an integrated database of such practices. The project develops a Resilience Hub that engages with three types of factors that can promote or mitigate polarization and violent extremism in society: notably historical and cultural factors; socio-economic conditions; the role of the social media and networking. We develop stakeholder workshops in relation to these three sets of factors that affect radicalization in society, and follow up with digital forums with the participation of a large number of stakeholders. Each stakeholder dialogue builds a tool of resilience in their field: notably inter-faith education training for secondary school teachers; a proposal for a basic income policy that mitigates socio-economic inequalities; a guide to responsible social media design. The Resilience Hub further develops a Resilience Fair where arts-based community interventions to stop polarization and build resilience will be presented
Consortium	Coordinator: 1. European University Institute (IT) Consortium: 2. "University Of Lancaster (UK) 3. Ceji (BE) 4. Dublin City University (IE) 5. Cultures Interactive E.V. - Verein Zur Interkulturellen Bildung Und Gewaltpravention (DE) 6. Itti Sp Zoo (PL) 7. Kozep-Europai Egyetem (HU)"

DESIGN	
Title	Design Thinking in Defence Organisations: The Promises and Dangers of Intellectual Emancipation in the Management of Violence
Objective	Study the relationship between radical ideas, change, and violence in defence organisations based on the ongoing transnational diffusion of second generation design across four NATO member and partner organisations: NATO Defence College, the Royal Danish Defence College, the Design Centre for Excellence (Poland) and Swedish Defence University
Contract details	H2020-MSCA-IF-2017 1/4/2019 - 31/3/202; EUR: 212.194,80
Abstract	The DESIGN project will conduct sociological study of the relationship between radical ideas, change, and violence in defence organisations based on the ongoing transnational diffusion of second generation design across four NATO member and partner organisations: NATO Defence College, the Royal Danish Defence College, the Design Centre for Excellence (Poland) and Swedish Defence University. Design means the art of transforming reality into a preferred one by opening conceptual possibilities that were unthinkable before. This add-on to defence planning is paradoxical as it seeks to leverage the critical and creative capacities of officers at the expense of the very principles sustaining modern defence organisations. The project will investigate what made this development possible and what differences, if any, design is making to those managing violence and to those being managed by violence? To provide unique answers to these questions, UCPH Centre for Experimental Economics (CEE) will provide training to adapt field experiment methods to sociological approaches to better observe design in practice. Using this new method promises data challenging deeply held assumptions on the relationships between ideas, change and violence in International Relations and Design Studies. A broader impact can also be expected by exposing the promises and dangers of design thinking to both users and stakeholders. I will significantly benefit from undertaking the action at UCPH as it is uniquely equipped to develop the interdisciplinary assemblage required. The project will benefit from being located at the intersection of three leading research centres in the Department of Political Science: the Centre for Military Studies (CMS), the Centre for Advanced Security Theory (CAST) and the Centre for Resolution of International Conflicts (CRIC). Beyond the University, Copenhagen is an ideal location to learn from its avant-garde design movement in private, public and education sectors.
Consortium	Coordinator: Kobenhavns Universitet (DK)

TRANSJIHAD	
Title	Explaining Transnational Jihad - Patterns of Escalation and Containment
Objective	Advancing our understanding of the ability of transnational jihadist movements to tap into local conflicts, hence escalating violence
Contract details	ERC-2018-STG; 1/9/2019 - 31/8/2024; EUR: 1.499.056
Abstract	TRANSJIHAD aims at advancing our understanding of one of the greatest contemporary challenges on the international agenda for peace and security, namely the ability of transnational jihadist movements to tap into local conflicts, hence escalating violence. TRANSJIHAD specifically investigates the questions of how jihadist conflicts become transnational and under what circumstances they can be contained. The project also aims at developing an interdisciplinary analytical framework, which combines micro- and macro level approaches to jihadism, drawing from both Religious Studies, Security Studies and Peace & Conflict Studies. Methodologically, TRANSJIHAD dissolves the scientific dichotomy between inside- and outside-oriented approaches to the study of transnational jihadist conflicts, widening prevailing scientific understandings of transnationalization processes. The project uniquely combines i) a quantitative examination of transnationalization processes drawing from the Religion and Armed Conflicts (RELAC) dataset based at Uppsala University, ii) comparative case studies of the mechanisms of escalation and de-escalation of jihadist conflicts across Asia, the Middle East, the Arab Peninsula and Africa focusing on the movements of Islamic State, Al-Qaeda, the Taleban, and Boko Haram, iii) securitization analyses of the macro-level conflict structures that transnational jihadist movements tap into, and finally iv) sociotheological worldview analyses of potential changes in jihadist conflict imagery during transnationalization processes. With its focus on macro-level conflict structures, TRANSJIHAD also contributes to developing a new framework for thinking about containment, providing an alternative to both the micro-level countering discourses embraced by much of the radicalization research, and the containment thinking that stems from the treatment of jihadist conflicts as civil wars in the peace and conflict literature.
Consortium	Coordinator: Dansk Institut For Internationale Studier (DK)

6.6 Supply Chain

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Supply Chain	BABBLER CASSANDRA CORE DNA TRUSTAG IPATCH ISTIMES LOGSEC LowCostTracking MITIGATE OSMOSIS SAFEPOST SECURECHAINS

In this iteration of the CoU Mapping Document, no new projects related to supply chains were identified.

6.7 Financial crime

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Financial crime	COFFERS COMFIN DANTE DEVTAXNET EUSECON FORENSICS HEMOLIA INVENTORY, OUTLOOK, AND ASSESSMENT OF EMERGING ENVIRONMENTAL CRIMES AGAINST WATER IN EUROPE LocationWise PARSIFAL PROTAX QuardCard TITANIUM VALUESEC

This overview is complemented by the following ISF projects.

EBOCS II	
Title	European Business Ownership and Control Structures - Phase II
Objective	Extend and further develop the initial pilot of the EBOCS, in which four funded business registers (Estonia, Italy, Latvia, Romania), and a number of Financial Intelligence Units and business registry domain organisations participated
Contract details	ISFP-2016-AG-IBA-EBOCS; 1/7/2017 30/6/2018; 368.420,26
Abstract	The ultimate deliverable for the project is to extend and further develop the initial pilot of the EBOCS, in which four funded business registers (Estonia, Italy, Latvia, Romania), and a number of Financial Intelligence Units and business registry domain organisations participated. The extended pilot phase covered by the grant will enable the participating users to immediately analyse at an operational level the information that will be furnished to them by the extended range of business registers. The project will deliver on the ambition of the funding body and FIUs that in due course this will translate into substantial time savings in the intelligence and investigation activities. It will significantly reduce the need for FIUs and other authorities to consult foreign registers directly, or to ask foreign counterparts for source information which holds up the analysis or investigation until the information is received.

SANS	
Title	AMON 2018-2019
Objective	Strengthen and further develop the anti-money laundering operational expert network AMON established in 2012
Contract details	ISFP-2017-AG-IBA-AMON; 1/9/2018 – 31/8/2020; EUR: 398.875,67
Abstract	The objective of this project is to strengthen and further develop the established in 2012 anti-money laundering operational expert network AMON. For this purpose the current and future Presidency of the network - Bulgaria and the Netherlands are joining their efforts in order to plan and carry out the necessary activities. For the 24-month period 7 meeting of the network's Steering group (SG) are scheduled to take place as well as 2 Annual General Meetings (AGM). These meetings with bring together the SG members (7 EU countries) and the AMON Secretariat (Europol). During these meetings the managing body of the network - the SG will discuss the most relevant topics in the field of anti-money laundering and the most pressing needs of the investigators working in this area. The agenda for the network's largest venue - the AGM will be set, the topics chosen and the speakers selected. During their meetings the SG will discuss also the plans for the enlargement of the network and developing it as an international center for knowledge and excellence in all matters related to anti-money laundering. The AGMs bring together all the members of the network - currently 38 countries, as well as observers and guests. During this major venue presentations are delivered by experts working in the field and also the participants have the chance to brainstorm and discuss in the working groups. In multinational surroundings the participants have the unique opportunity to meet and connect with fellow practitioners in an open and informal environment and benefit from the contacts and the additional knowledge.

This overview is complemented by the following H2020 project.

COBAFRA	
Title	Combatting Banking Fraud with SiS-id: A unique solution for preventing corporate payments fraud using AI and blockchain
Objective	Further develop SiS-id, a highly secure, innovative platform helps guarantee that payments go to the right company and keeps the banking identity of companies safe online
Contract details	H2020-SMEInst-2018-2020-1; 1/1/2019 - 30/6/2019; EUR: 50.000
Abstract	My SiS-id, a highly secure, innovative platform helps guarantee that payments go to the right company and keeps the banking identity of companies safe online. My SiS-id is different because: It is not a payment system but an interface that addresses the identity part of the payment process. It integrates with customer and supplier existing systems, SiS-id has integrated AI and blockchain into its solution to reinvent and enhance the traditional data-pooling and enrolment models, My SiS-id benefits both customers and suppliers. Information has to be acquired and authenticated one time only to be made available to all, It is a viral business model: customers invite their suppliers onto the platform, suppliers in turn invite their suppliers and also their customers, The solution was co-developed with 13 pioneer customers (CFOs and Treasurers) to ensure it solves the business need, not technology for technology sake, My SiS-id is blue ocean strategy. No other such solution currently exists. The other solutions on the market only tackle parts of the problem.
Consortium	Coordinator: SIS (FR)

6.8 Civil-military cooperation

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Civil-military cooperation	CivilNext

In this iteration of the CoU Mapping Document, one project categorised under another theme is also relevant for civil-military cooperation: ECCOFEX.

6.9 External security threat

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
External security threat	EU-LISTCO

In this iteration of the CoU Mapping Document, no new projects related to external security threat were identified.

7. Border security and customs

7.1 Aviation security

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Aviation security	Aerobits AIRPOL III COPRA EUNADICS-AV EUROSKY FLYSAFE GAMMA INVENTORY, OUTLOOK, AND ASSESSMENT OF EMERGING ENVIRONMENTAL CRIMES AGAINST WATER IN EUROPE OPTICS2 SUBITO SARAH SAPIENT Smart-Trust TASS XP-DITE

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

SATIE	
Title	SATIE *This project is also relevant for 4.1.2 Detection of potential CBRN-E threats at urban soft targets / urban critical infrastructures*
Objective	Develop an interoperable toolkit which improves cyber-physical correlations, forensics investigations and dynamic impact assessment at airports
Contract details	H2020-SU-SEC-2047; Topic code: SU-INFRA01-2018-2019-2020; 1/5/2019 - 30/4/2021; EUR 7 989 264
Abstract	SATIE adopts a holistic approach about threat prevention, detection, response and mitigation in the airports, while guaranteeing the protection of critical systems, sensitive data and passengers. Critical assets are usually protected against individual physical or cyber threats, but not against complex scenarios combining both categories of threats. In order to handle it, SATIE develops an interoperable toolkit which improves cyber-physical correlations, forensics investigations and dynamic impact assessment at airports. Having a shared situational awareness, security practitioners and airport managers collaborate more efficiently to the crisis resolution. Emergency procedures can be triggered simultaneously through an alerting system in order to reschedule airside/landside operations, notify first responders, cybersecurity and maintenance teams towards a fast recovery. Innovative solutions will be integrated on a simulation platform in order to improve their interoperability and to validate their efficiency. Three demonstrations will be conducted at different corners of Europe (Croatia, Italy and Greece) in order to evaluate the solutions in operational conditions (TRL≥7). Results and best practises will be widely disseminated to the scientific community, standardization bodies, security stakeholders and the aeronautic community. Finally, SATIE paves the way to a new generation of Security Operation Centre that will be included in a comprehensive airport security policy.
Consortium	Coordinator: 1. Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (DE) Consortium: 2. Airbus Cybersecurity Sas (FR) 3. Idemia Identity & Security France (FR) 4. Frequentis Ag (AT) 5. Network Integration And Solutions Srl (IT) 6. Alstef Automation (FR) 7. Teclib Spain S.L. (ES) 8. Itti Sp Zoo (PL) 9. Satways - Proionta Kai Ypiresies Tilematikis Diktyakon Kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis Epe (EL) 10. Eticas Research And Innovation (ES) 11. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (DE) 12. Instituto Superior De Engenharia Do Porto (PT) 13. Inov Inesc Inovacao - Instituto De Novas Tecnologias (PT) 14. Ustav Informatiky, Slovenska Akademia Vied (SK) 15. Athens International Airport S.A. (EL) 16. Medunarodna Zracna Luka Zagreb Dd (HR) 17. Societa Per Azioni Esercizi Aeroportuali Sea Spa (IT) 18. Kentro Meleton Asfaleias (EL)

This overview is complemented by relevant ISF projects.

Airpol IV	
Title	Airpol IV *This project is also relevant for 6.4.5 Support to law enforcement*
Objective	Continuation of Airpol network, with a focus on means to detect security risks from various phenomena such as lone suicide bomber, foreign fighters, to Insider Threats and persons committing crimes at the airports
Contract details	ISFP-2017-AG-IBA-AIRPOL; 16/1/2018 – 15/1/2020; 746.734,81
Abstract	The mission of the Airpol network (HOME/2015/ISFP/AG/AIRP/0001) is to enhance the overall security in the European airports & civil aviation domain by optimizing the effectiveness and efficiency of airport and aviation related law enforcement and border guard issues in the EU. The network aims at contributing to a more harmonized approach of enforcement in this domain and the networks scope encompasses the three aviation related themes: Airport Policing, Aviation Security and Air Border Security. The present focus for development of Airpol, as a complement to the use of technology is looking into irregular and unwanted behaviour, in a wider sense as a mean to detect security risks from various phenomena such as lone suicide bomber, foreign fighters, to Insider Threats and persons committing crimes at the airports. For that purpose Airpol will continue working with expert groups on relevant topics e.g. Insider Threats in a wider sense including preventing radicalization and other specifics generating risks in the Airport Community such as badge management, access control etc. Airpol will also continue developing Behaviour Detection as well as work with the concept Securing the Airport Community. The activities in this application focuses on continuing working with expert groups in order to establish best practise and further develop the concept on how to secure the Airport Community.

Airpol Trainin	
Title	Airpol Trainin
Objective	Continuation of Airpol network, with a focus on means to detect security risks from various phenomena such as lone suicide bomber, foreign fighters, to Insider Threats and persons committing crimes at the airports
Contract details	ISFP-2016-AG-IBA-AIRPOL; 1/1/2017 - 31/12/2017; 245.344,50
Abstract	The mission of the Airpol network (HOME/2015/ISPF/AIRP/0001) is to enhance the overall security in the European airports and civil aviation domain by optimizing the effectivness and efficiency of airports and aviation related law enforcement and border guard issues in the EU. The network aims at contributing to a more harmonized approach of enforcement in this domain and the networks scope encompasses the three aviation related themes: Airport Policing, Aviation Security and Air Border Security. The present focus for development as a compliment to the use of technology is looking into irregular and unwanted behaviour, in a wider sense as a mean to detect security risks from various phenomena such as lone suicide bomber, foreign fighters, to Insider Threats and persons committing crimes at the airports. For that purpose expert groups are working on e.g Insider Threaths moving on from the previous Airpol work on Community Policing Preventing Radicalization and Terrorism at European Airports (COPPRA). There are also expert groups on developing a Behaviour Detection model and one on Securing Airport Community.The activitites in this application focuses on the outcome of these expert groups and to secure that this outcome is taken care of in training sessions and a conference on Behaviour Detection where the result of the expert group will be discussed with all possible actors at European Airports within Law Enforcement Agencies (LEA) as well as with participants from other relevant organizations outside this group. The third area is creating a Secure Airport Community where the expert group will come up with a document on how to organize the work to create a secure airport community, including all steps from booking a ticket to departure i.e both landside and airside security.

EIFS	
Title	Enhancing In-Flight Security *This project is also relevant for 9.2 Standardisation, Testing & Certification*
Objective	Augment the operational capabilities of the seven active European In-Flight Security Officer (IFSO) units and their operatives
Contract details	ISFP-2017-AG-IBA-EUIFSO; 1/9/2018 – 31/8/2020; 523.152,96
Abstract	This project aims to enhance European in flight security by augmenting the operational capabilities of the seven active European In-Flight Security Officer (IFSO) units and their operatives. Therefore the project Enhancing In-Flight Security (EIFS) has formulated four objectives: Define a standard for Behavior Observation Analysis (BOA) for IFSO, Create standards and best practices for Tactical First Aid (TFA) for IFSO, Produce a recommendation for the procedural and tactical framework to achieve interoperability among European In-Flight Security (IFS) units, Identify and analyze emerging and future threats to IFS, and provide recommendations regarding IFSO training, equipment and operations to address these threats.

This overview is complemented by a H2020 project.

XSPERINSE	
Title	X-ray SPEctral detectors for Reliable, Intelligent and INnovative SEcurity
Objective	Revise the design of a prototype for hand luggage scanners, to comply with the new performance requirements (EDSCB C3)
Contract details	H2020-EIC-FTI-2018-2020; 1/6/2019 - 30/11/2021; EUR: 2.619.440,25
Abstract	We have created a prototype scanning solution which complies with the new performance requirements (EDSCB C3) for hand luggage scanners. It consists of a novel multi-view, multi-spectral, CT type luggage scanner based on a new multi-energy (ME) X-ray scanner system and uses a dedicated intelligent trolley into which passengers place their hand luggage without having to unpack it. The entire trolley is then scanned, and any suspicious items automatically flagged for checking by security personnel. This provides a more relaxed security screening experience and minimises queuing. Our scanner solution increases the total passenger throughput from 150 to 600 per hour, while increasing the surface efficiency (passenger screened per sq m) with 362% and requiring 35% fewer operators. The solution also reduces the screening cost (luggage scanning cost per passenger) from EUR 5 to EUR 2.8 compared to current solutions, resulting in cost savings of EUR 55,000,000 per year. In XSPERINSE we will revise the design of the prototype scanner to produce a version that incorporates an upgraded version of the currently used ME detector tailored to the specific requirements of the scanner and implement new data analysis algorithms and reduce the scanner's power consumption. These activities will result in demonstrating our solutions competitive advantages through a large-scale testing and prepare it for commercialisation.
Consortium	Coordinator: 1. Danmarks Tekniske Universitet (DK) Consortium: 2. "Point Fwd Bv (NL) 3. Exruptive A/S (DK) 4. Detection Technology SAS (FR)"

7.2 Maritime security

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Maritime security	AEROCEPTOR ALFA AMASS CLOSEYE CONTAIN Emergency assistance covering staff related costs in order to ensure a high level domain awareness of the severely affected Eastern Aegean EU external borders and to minimize the losses of human lives at sea Emergency assistance for the procurement of Search & Rescue Equipment to avert losses of migrants' life at sea EU-CISE 2020 I2C LINCOLN MARINE-EO MARISA MASS New Arrivals Intervention – phase II OPERAMAR PERSEUS PROMERC RANGER SafeShore SAR OPERATIONS III SAR OPERATIONS IV SEABILLA SECRONIC SUPPORT TRITON WIMAAS

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

COMPASS2020	
Title	COMPASS2020 *This project is also relevant for 7.4 Multi-modal security, risk management, including migration*
Objective	Demonstrate the combined use and seamless coordination of manned and unmanned assets to achieve greater coverage, better quality of information and shorter response times in maritime surveillance operations
Contract details	H2020-SU-SEC-2036; Topic code SU-BES03-2018-2019-2020; 1/5/2019 - 31/10/2020; € 4 838 489,61
Abstract	The external borders of the EU have historically been under great pressure, subject to a variety of threats, which include irregular migration and trafficking of narcotics. Within this context, authorities in charge of border and maritime patrol are faced with different challenges that include the heterogeneity of the traffic that undertakes illegal activities in European waters, limitations in the ability to collect and share timely available data among institutional organizations, as well as a lack of assets by the relevant authorities to cover the wide maritime areas under their mandate. Although there has been an expressive investment done in the domain of surveillance technologies and tools, the intake by the competent authorities has been slow, due to lack of uniformity in the integration of such systems with existing surveillance infrastructures. In order to address these challenges, project COMPASS2020 aims to demonstrate the combined use and seamless coordination of manned and unmanned assets to achieve greater coverage, better quality of information and shorter response times in maritime surveillance operations. The proposed solution will be based on an innovative CONOPS that makes use of multiple aerial and underwater unmanned vehicles with improved capabilities, deployed from OPVs or from land, and will be supported by a central, multi-domain and interoperable Mission System (MS) that enables the operation of these platforms from both locations. UxVs may act as deported ship sensors, providing critical mission data to the MS that can then be exploited through dedicated services to be developed in the scope of the project (e.g. Data Fusion and Threat Risk Analysis). The major goal of COMPASS2020 is to demonstrate an operational solution to ensure long range and persistent surveillance, increasing the situational awareness of coast guards and maritime authorities, and, thus, increasing the cost-effectiveness, availability and reliability of the operations.
Consortium	Coordinator: 1. Direccao Geral Da Autoridade Maritima (PT) Consortium 2. Tekever Asds (PT) 3. Naval Group (FR) 4. Airbus Defence And Space Gmbh (DE) 5. Edisoft-Empresa De Servicos E Desenvolvimento De Software Sa (PT) 6. Eca Robotics (FR) 7. Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (NL) 8. "Institutul National De Cercetare-Dezvoltare Aerospatiala ""Elie Carafoli""- Incas Bucuresti" (RO) 9. Isd Lyseis Olokriromenon Systimatonanonymos Etaireia (EL) 10. Stichting Nationaal Lucht- En Ruimtevaartlaboratorium (NL) 11. Centro De Analise E Operacoes Maritimas-Narcoticos (PT) 12. Nato Science And Technology Organisation (BE) 13. Home Office (UK) 14. Ministarstvo Saobracaja I Pomorstva (ME)

This overview is complemented by ISF projects.

BEST Surveillance	
Title	Baltic External Borders Surveillance Technology Performance Enhancement project to strengthen the European Border Surveillance System
Objective	Enhance technical border surveillance means in the area of Gulf of Finland at the EU's external maritime border
Contract details	ISFB-2017-AG-ESUR; 1/1/2019 – 31/12/2020; 2.672.860,00
Abstract	In the frame of ISFB-2017-AG-ESUR Call, Finnish Border Guard (FBG) and Estonian Police and Border Guard Board (EPBGB) are applying funding to enhance their technical border surveillance means in the area of Gulf of Finland at the EU's external maritime border. With these actions taken, FBG's and EPBGB's operational reaction capabilities will be enhanced through improved situational awareness in the framework of Baltic Sea Region Border Control Cooperation (BSRBCC) and European border surveillance system (EUROSUR).

PRIORITY	
Title	Improvement of the Security at the EU External Borders and Enhance the Cooperation with Turkey for Addressing the Migratory Pressure *This project is also relevant for 7.3 Land border security and 7.4 Multi-modal security, risk management, including migration*
Objective	enhance the development of functional, effective and integrated systems in border management between Greece, Turkey and Bulgaria
Contract details	ISFB-2016-AG-ESUR; 1/1/2018 – 31/12/2019; 707.550,34
Abstract	The project objective is to enhance the development of functional, effective and integrated systems in border management between Greece,rperation for border management related tasks, structured border coordination mechanisms among three countries. Improvement of the Security at the EU External Borders and Enhance the Cooperation with Turkey for Addressing the Migratory Pressure. Another objective is to support Turkey's border management efforts in line with the EU Acquis and good practices via enhancing the regional cooperation on border management among Turkey, Greece and Bulgaria at central and local level. This project will continue the activities from the previous GA HOME/2014/ ISFB/AG/REGI/0001 between the EU and Chief Directorate Border Police (CDBP), Bulgaria. The new moment in this project proposal is envisaged equipment which CDBP want to purchase in the framework of EUROSUR.

CERETAB	
Title	CoopERation for incrEased siTuational Awareness estaBlishment
Objective	Support the improvement of border surveillance by enhancing cooperation between Greece and Cyprus
Contract details	ISFB-2017-AG-ESUR; 1/12/2018 – 30/11/2020; 1.023.990,00
Abstract	CERETAB aims to support the improvement of border surveillance by enhancing cooperation between 2 EU Member States, Greece (EL) & Cyprus (CY), which over the recent years suffer from heavy irregular migration attempts via the Mediterranean sea, as well as cross-border crime. The unique geographical position of both countries in the South Eastern end of the EU renders them as significant targets for smuggling groups, using small maritime vessels. The overall objective is to increase the situational awareness within the broad area defined by the Greek-Cypriot sea borders, by the improvement of the cooperation and the information exchange of the Greek-Cypriot National Coordination Centres (NCCs). More specifically, the area between Cyprus and Greece is considered a sea route for suspected vessels moving from Turkey, Syria & Lebanon towards Europe and it is widely acknowledged that it lacks proper monitoring. Thus, timely effective and secure exchange of information & coordination between the relevant authorities of the 2 countries is of utmost importance. The latter will be implemented within CERETAB project through the utilization of new, state-of-the-art border surveillance technologies, such as the deployment of Unmanned Aircraft Systems (UASs), that facilitate information exchange, in order to prevent cross border crime & irregular migration, while optimizing the common efforts for saving lives of people in distress at sea, e.g., in Search And Rescue (SAR) incidents.

This overview is complemented by a relevant H2020 project.

LASH FIRE	
Title	Legislative Assessment for Safety Hazards of Fire and Innovations in Ro-ro ship Environment
Objective	Provide a recognized technical basis for the revision of international IMO regulations regarding fire prevention and management on ro-ro ships without recourse to external intervention
Contract details	H2020-MG-2018-TwoStages; 1/9/2019 - 31/8/2023; EUR: 12.209.148,33
Abstract	Ro-ro ships are an important component of the global transportation system, but an increasing trend of ro-ro ship fires in recent years call for improved fire protection. From comprehensive ship operators' experience and by participation in ongoing work for the European Maritime Safety Agency and the International Maritime Organization (IMO), critical aspects of ro-ro ship fire safety have been identified to form the scope of the project LASH FIRE. It aims to provide a recognized technical basis for the revision of international IMO regulations, which greatly enhances fire prevention and ensures management of fires on ro-ro ships without recourse to external intervention. This is done by developing and demonstrating operational and design solutions which strengthen the fire protection of ro-ro ships in all stages of a fire and which address current and future challenges, including regulatory issues. Twenty specific challenges have been identified, which will be addressed by new solutions developed and demonstrated with regards to performance and ship integration feasibility by system suppliers, researchers, ship owners and shipyards. For the solutions to be considered for regulatory uptake, their impact on risk reduction and cost will be assessed and advisory groups with operators and flag states will be established. Thereby, the project is expected to significantly strengthen the independent fire protection of ro-ro ships and to reduce the frequency of ro-ro ship fires by 35% and the number of fatalities by 45%.
Consortium	Coordinator: 1. Rise Research Institutes Of Sweden Ab (SE) Consortium: 2. "Teknologian Tutkimuskeskus Vtt Oy (FI) 3. Rise Fire Research As (NO) 4. Flow Ship Design Doo Za Projektiranje, Konzalting I Inzenjering U Brodogradnji (HE) 5. Marioff Corporation Oy (FI) 6. Unifire Aktiebolag (SE) 7. Center Of Maritime Technologies Ev (DE) 8. Bureau Veritas Marine & Offshore Registre International De Classification De Navires Et De Plateformes Offshore (FR) 9. Ap Sensing Gmbh (DE) 10. Stena Rederi Ab (SE) 11. European Ferry Company (BE) 12. Shipyards And Maritime Equipment Association Of Europe (BE) 13. Sick Ag (DE) 14. Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO) 15. Sociedad De Salvamento Y Seguridad Maritima (ES) 16. Centre Internacional De Metodes Numerics En Enginyeria (ES) 17. Magellan-Associacao Para A Representacao Dos Interesses Portugueses No Exterior (PT) 18. Universite De Lorraine (FR) 19. Ntnu Samfunnsforskning As (NO) 20. Fike Safety Technlogy Limited (UK) 21. Rs2n (FR) 22. Uniaccess (FR) 23. University Of Cyprus (CY) 24. Dfds As (DK) 25. Fifi4marine Bv (NL) 26. Hoegh Autoliners As (NO)"

7.3 Land border security

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Land border security	EWISA iBorderCtrl MOBILEPASS OPARUS SMILE SUNNY TALOS

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

ANDROMEDA	
Title	ANDROMEDA *This project is also relevant for 7.2 Maritime security and 6.4.5 Support to law enforcement*
Objective	Further enhance, validate and demonstrate CISE by extending its scope for land borders and adapting relevant C2 solutions and associated services
Contract details	H2020-SU-SEC-2027; Topic code SU-BES03-2018-2019-2020; 1/9/2019 - 28/2/2021; € 4 999 462,50
Abstract	The project aims to unlock the full potential of CISE, by validating in a long period of time CISE-compatible command, control and coordination systems from several Coast and Border Agencies. At the same time it is envisaged to further enhance, validate and demonstrate CISE by extending its scope for land borders and adapting relevant C2 solutions and associated services. This will be accomplished by extending the CISE data model based on the use cases and requirements and adapting state-of-the-art command & control systems for full compliancy with the enhanced model and CISE message exchange patterns. The project architecture will follow a hybrid scheme in order to allow the usage of the End User CISE Nodes/Gateways and at the same time to allow the testing and validation of the extended data model. The project will leverage on the developments, results and experience of the consortium from current and previous research projects (PERSEUS, CloseEye, MARISA, RANGER), from National Procurement projects of CISE Nodes and Adaptors and on the CISE infrastructure of the End Users.
Consortium	Coordinator: 1. Ministry Of Maritime Affairs And Insular Policy (EL) Consortium: 2. Gmv Aerospace And Defence Sa (ES) 3. Satways - Proionta Kai Ypiresies Tilematikis Diktyakon Kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis Epe (EL) 4. Institute Of Communication And Computer Systems (EL) 5. Exus Software Ltd (UK) 6. Inovaworks Ii, Command And Control,Sa (PT) 7. Fondazione Centro Euro-Mediterraneosui Cambiamenti Climatici (IT) 8. Laurea-Ammattikorkeakoulu Oy (FI) 9. Codin - Societa Per Azioni (IT) 10. Stemo Ood (BU) 11. Kentro Meleton Asfaleias (EL) 12. Engineering - Ingegneria Informatica Spa (IT) 13. Hellenic Police (EL) 14. Ministero Della Difesa (IT) 15. Ministerio Da Defesa Nacional (PT) 16. Ministry Of Public Security (IL) 17. Executive Agency Maritime Administration (BU) 18. Ministry Of National Defence, Greece (EL) 19. Ministarstvo Saobracaja I Pomorstva (ME)

This overview is complemented by ISF projects.

BSIEG 2	
Title	Development of Information Exchange Gear of Baltic states
Objective	increase reaction capabilities of LCCs and to develop the possibility of direct communication (with support of NCCs) among units of Estonia, Latvia and Lithuania Border guard authorities
Contract details	ISFB-2016-AG-ESUR; 1/1/2018 – 31/12/2019; 1.641.320,61
Abstract	The main objectives of this project is to increase reaction capabilities of LCCs and to develop the possibility of direct communication (with support of NCCs) among units of Estonia, Latvia and Lithuania Border guard authorities) at local and regional level in the border areas with neighbouring states.

RAILPOL	
Title	RAILPOL *This project is also relevant for 4.2.2 Critical Transport / Transportation Infrastructure*
Objective	Support RAILPOL network
Contract details	ISFP-2017-AG-IBA-RAILPOL; 1/7/2018 – 31/12/2019; 525.566,88
Abstract	The RAILPOL Strategy 2014-2019, composed from those from EU-ISS/DG HOME, National Authorities and RAILPOL-member organisations gives RAILPOL's priorities. RAILPOL strives for a safe and secure rail-transport by establishing effective cross-border law-enforcement cooperation on the main EU railway-corridors. RAILPOL is an EU network of (governmental controlled) Railway Police organizations, established in 2004, and has 19 (associated) members from 13 EU M.S, U.K., Switzerland and USA. The network is expanding. RAILPOL is connected to EUROPOL, FRONTEX, ERA, DG HOME, DG MOVE, etc. and to private stakeholder organisations like UIC, CER, Colpofer and EIM. RAILPOL aims at long-term development of cross-border law-enforcement in the EU dealing with actual threats. RAILPOL has developed to more complex forms of cooperation, which include external partners (EU agencies and others), which are intelligence-led and which enhance the cooperation between various law-enforcement disciplines. RAILPOL has a strong operational focus. The RAILPOL members are connected via a network of "Single Points of Contact". Gradually RAILPOL reinforces its systems and processes and connects these more to the EU programs (like EMPACT) and the EU policies, such as interdisciplinary law-enforcement cooperation, cooperation with- and between EU agencies and cooperation with private partners. The added value of RAILPOL is beyond doubt, as concluded by a DG-HOME audit on the network (E&Y report 2012).

SARA	
Title	Security Activities RAILPOL – SARA *This project is also relevant for 4.2.2 Critical Transport / Transportation Infrastructure*
Objective	Facilitate RAILPOL, an EU network of (governmental controlled) Railway Police organizations
Contract details	ISFP-2016-AG-IBA-RAILPOL; 1/7/2017 – 30/6/2018; EUR: 472.137,50
Abstract	The RAILPOL Strategy 2014-2019, composed from those from EU-ISS/DG HOME, National Authorities and RAILPOL-member organisations gives RAILPOL's priorities. RAILPOL strives for a safe and secure rail-transport by establishing effective cross-border law-enforcement cooperation on the main EU railway-corridors. RAILPOL is an EU network of (governmental controlled) Railway Police organizations, established in 2004, and has 19 (associated) members from 13 EU M.S, U.K., Switzerland and USA. The network is expanding. RAILPOL is connected to EUROPOL, FRONTEX, ERA, DG HOME, DG MOVE, etc. and to private stakeholder organisations like UIC, CER and EIM. RAILPOL aims at long-term development of cross-border law-enforcement in the EU dealing with actual threats. RAILPOL has developed to more complex forms of cooperation, which include external partners (EU agencies and others), which are intelligence-led and which enhance the cooperation between various law-enforcement disciplines. RAILPOL has a strong operational focus. The RAILPOL members are connected via a network of "Single Points of Contact". Gradually RAILPOL reinforces its systems and processes and connects these more to the EU programs (like EMPACT) and the EU policies, such as interdisciplinary law-enforcement cooperation, cooperation with- and between EU agencies and cooperation with private partners. The added value of RAILPOL is beyond doubt, as concluded by a DG-HOME audit on the network (E&Y report 2012). RAILPOL has become a strong network with a strong commitment of its members. Like the RSA-projects (ISEC) also this one will build on the proven RAILPOL instruments: meetings Heads of Service; working groups for experts; training seminars for experts; exchange of experts; further enhancement of the RAILPOL website (www.railpol.eu).

7.4 Multi-modal security, risk management, including migration

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Multi-modal security, risk management, including migration	ABC4EU ACXIS BAPS BODEGA CAMELOT C-BORD CUSTOM DIRAC DOGGIES EFFISEC FASTPASS FIDELITY FOLDOUT GLOBE INGRESS MESMERISE ORIGINS RefBorder RESPOND ROBORDER SNIFFER SNIFFLES SNOOPY PERSONA PROFILE PROTECT TERASCREEN VIRTUOSO ZONESEC Cooperation on Border Management among Turkey, Bulgaria and Greece Development of the next generation uniform format EU visa sticker Emergency assistance in support of the organisation, provision of legal information and interpretation for the effective management of immigration flows in the Eastern External Borders Humane and EU conform handling of extreme migratory pressure on Hungary Linguistic and Intercultural Mediation for Emergency action Strengthening external border protection in relation to the irregular mass arrival of third country nationals Strengthening of the first reception response to new arrivals in mixed migratory movements on the Aegean islands

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

PERCEPTIONS	
Title	PERCEPTIONS
Objective	Identify and understand the narratives and (mis-)perceptions of the EU abroad, assess potential issues related with the border and external security in order to allow better planning and outline reactions and countermeasures
Contract details	H2020-SU-SEC-2026; Topic code SU-BES01-2018-2019-2020; 1/9/2019 - 31/8/2022; € 4 994 652,50
Abstract	Narratives on a "better life" that can become reality elsewhere have always been shaping human migration. The image or idea of a "promised land", however, might not be real, and newcomers are often faced with obstacles and challenges. Certain narratives and perceptions of Europe influence migration aspirations and false images can not only lead to problems when the image does not hold true, but it might also even lead to security threats, risks or radicalisation. It is, therefore, of the utmost importance to understand and investigate narratives about Europe, how these can lead to problems and threats, how they are distributed, and, in a next step, find ways to react and counteract on them. Perceptions on Europe are formed in the country of residence, and they are based on a multitude of sources. Social media and new communication networks, in addition, have increased the scope and the intensity of distribution of such narratives; and furthermore, so-called filter bubbles and echo chambers can lead to isolated misperceptions that are not corrected. Due to new communication technologies, false or incorrect claims become life on their own, raise expectations or disapproval. At the same time, however, these technologies and communication networks might also provide a channel to set an exaggerated image straight and to promote a more realistic narrative. It is, therefore, the aim of the PERCEPTIONS project to identify and understand the narratives and (mis-) perceptions of the EU abroad, assess potential issues related with the border and external security in order to allow better planning and outline reactions and countermeasures. For that purpose, the project will conduct research on the narratives and the myths that are circulating about the EU in countries West- and Central Mediterranean area. Based on the research insights, the consortium will develop a PERCEPTIONS framework model including policy recommendations and action plans.
Consortium	Coordinator: 1. Synyo Gmbh (AT) Consortium: 2. Sheffield Hallam University (UK) 3. Alma Mater Studiorum - Universita Di Bologna (IT) 4. Universidad De Granada (ES) 5. Universidad Rey Juan Carlos (ES) 6. University Of Northumbria At Newcastle (UK) 7. Swansea University (UK) 8. Universita Degli Studi Di Roma La Sapienza (IT) 9. Erasmus Universiteit Rotterdam (NL) 10. Universiteit Antwerpen (BE) 11. International Centre For Migration Policy Development (AT) 12. Kentro Meleton Asfaleias (EL) 13. Center For The Study Of Democracy (BU) 14. Sinus Markt- Und Sozialforschung Gmbh (DE) 15. Centre De Recherche En Economie Appliquee Pour Le Developpement (DZ) 16. Egyptian Center For Innovation And Technology Development (EG) 17. Aditess Advanced Integrated Technology Solutions & Services Ltd (CY) 18. Association Des Agences De La Democratie Locale (FR) 19. Kosovar Centre For Security Studies (XK) 20. Fundacion Euroarabe De Altos Estudios (ES) 21. Koinonia Caritas Cyprus (CY) 22. Fondazione Bruno Kessler (IT) 23. Hellenic Police (EL) 24. Ministry Of Public Security (IL) 25. Glavna Direktsia Granichna Politsia (BU)

D4FLY	
Title	D4FLY
Objective	Augment the current capabilities and capacities of border authorities in countering emerging threats in document and identity verification at manual and highly automated border control points and in the issuance process of genuine documents
Contract details	H2020-SU-SEC-2037; Topic code: SU-BES02-2018-2019-2020; 1/9/2019 - 31/8/2022; € 6 984 727,50
Abstract	The D4FLY project will augment the current capabilities and capacities of border authorities in countering emerging threats in document and identity verification (e.g., forged documents, impostor fraud, morphed faces) at manual and highly automated border control points and in the issuance process of genuine documents. The confluence of D4FLY set of tools and systems will improve the quality of verification and reduce major time sinks in the processes thus enabling real on-the-move border crossing experience for travelers. Novel sensor hardware based on advanced lightfield cameras and novel algorithms developed in the project will enhance verification accuracy and robustness via the combined usage of 2D+thermal face, 3D face, iris and somatotype biometrics. Analytical means to identify known criminals based on somatotype and 3D face data generated from mugshots and observation data will be developed. Various operational needs of end-users with different threat landscapes constitute the backbone of D4FLY development efforts. D4FLY will create a resilient document verification system that can verify a multitude of physical and electronic security features (e.g. Kinegrams®, MLIs, CLIs), detect complex forms of electronic fraud and advanced morphing, and identify fraud in breeder documents. The potential benefit of blockchain technology in identity verification will also be investigated. The D4FLY solution will consist of a border control kiosk geared with enhanced enrolment, verification and detection capabilities; smartphones applications for improved performance and verification capabilities; and a non-stop on-the-move system for biometric verification. The innovation will be validated against European societal values, fundamental rights, privacy, data protection and applicable legislation. Four different border control points and one document fraud expertise center will form the project's testing and demonstration ground.
Consortium	Coordinator: 1. VERIDOS GMBH (DE) Consortium: 2. Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (NL) 3. "National Center For Scientific Research ""Demokritos""" (EL) 4. Norges Teknisk-Naturvitenskapelige Universitet Ntnu (NO) 5. Teknologian Tutkimuskeskus Vtt Oy (FI) 6. Trilateral Research Limited (IE) 7. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 8. The University Of Reading (UK) 9. Wojskowa Akademia Techniczna Im.Jaroslawa Dabrowskiego (PL) 10. Regula Baltija Sia (LV) 11. Raytrix Gmbh (DE) 12. Ovd Kinegram Ag (CH) 13. Ministry Of Citizens Protection (EL) 14. Piraeus Port Authority Sa (EL) 15. Ministerie Van Justitie En Veiligheid (NL) 16. Ministry Of Defense (NL) 17. Home Office (UK) 18. Baltijos Pazangiu Technologiju Institutas (LT) 19. Valstybes Sienos Apsaugos Tarnyba Prie Vidaus Reikalu Ministerijos (LT)

MIRROR	
Title	MIRROR *This project is also relevant for 9.1 Foresight studies on security threats & Roadmaps*
Objective	Develop an integrated platform, a set of tools and a systematic methodology for comprehensive intermedia analysis of the perception of Europe, the detection of discrepancies between perception of and reality in Europe, and the creation of awareness for the impact of such misconceptions and the resulting threats, including hybrid threats
Contract details	H2020-SU-SEC-2041; Topic code: SU-BES01-2018-2019-2020; 1/6/2019 - 31/5/2022; € 5 181 997,50
Abstract	The goal of the MIRROR project is to develop an integrated platform, a set of tools on top of this platform, as well as a systematic methodology for the comprehensive intermedia analysis of the perception of Europe, the detection of discrepancies between perception of and reality in Europe, and the creation of awareness for the impact of such misconceptions and the resulting threats, including hybrid threats. In a process driven by perception-specific threat analysis, the MIRROR project will combine methods of automated text, multimedia and social network analysis for various types of media (including social media) with empirical studies for creating a substantiated picture of the perception of Europe and for combining evidences from different sources. Solutions developed in the project, including technology and actionable insights, will be thoroughly validated with border agencies and policy makers, e.g. via pilots. For achieving its goals, MIRROR brings together a strong multidisciplinary consortium combining research excellence experts in text and multimedia analysis, social network analysis, security research, social science, in particular communication science, law and ethics, gender research with commercial partners and border agencies as well as civil society organizations.
Consortium	Coordinator: 1. Gottfried Wilhelm Leibniz Universitaet Hannover (DE) Consortium: 2. Bundesministerium Fuer Landesverteidigung Und Sport (AT) 3. Malta Police Force (MT) 4. Polismyndigheten Swedish Police Authority (SE) 5. Sail Labs Technology Gmbh (AT) 6. Eurix Srl (IT) 7. Rijksuniversiteit Groningen (NL) 8. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 9. Totalforsvarets Forskningsinstitut (SE) 10. Universitat Wien (AT) 11. Universita Ta Malta (MT) 12. Conoscenza E Innovazione Societa Aresponsabilita Limitata Semplificata (IT) 13. Fremde Werden Freunde (AT) 14. Fondazione Agenfor International (IT)

ARESIBO	
Title	ARESIBO *This project is also relevant for 7.2 Maritime security*
Objective	Develop the ARESIBO system to enhance tactical command and control of land and maritime borders
Contract details	H2020-SU-SEC-2043; Topic code: SU-BES02-2018-2019-2020; 1/5/2019 - 30/4/2022; € 6 999 882,50
Abstract	ARESIBO aims at improving the efficiency of the border surveillance systems by providing the operational teams and the tactical command and control level with an accurate and comprehensive information. The pillars of research in ARESIBO are three-fold: 1. Set-up a complete configuration at tactical and execution level to optimise the collaboration between human and sensors (fixed and mobile), 2. Improve situation awareness by enhancing the understanding of the situation through adapted processing of sensor data, correlation between heterogeneous data and information and creation of knowledge through deep learning techniques and 3. Create a situation awareness capability at C2 level that will combine reports on previous missions, real time situation understanding and threat analysis for future actions. This capability will be used to optimise the operations (teams deployment and sensor positioning) as well as an online briefing tool for the teams that will be able to access to the results of the previous missions while in the field. ARESIBO integrates research activities in the domain of 1. surveillance platforms (air, ground, surface, underwater) to optimise the collaborative capabilities of the platforms and their positioning (between themselves and with the teams), 2. Sensor processing to interpret, fuse and correlate all the data to produce information and knowledge and 3. Augmented reality techniques to elaborate and provide to the operators a situation awareness picture which is fit for their missions (minimum information for maximal understanding) both as team level and tactical C2 level. The ARESIBO system will be developed incrementally during the 3 years with two major versions that will lead to sub-versions for land and maritime borders. The system will be tested and assessed in 1. a controlled environment enabling testing at any time without pre-requisite authorisations and 2. in real conditions in Finland, Greece, Romania and Portugal for the 2 versions.
Consortium	Coordinator: 1. Airbus Defence And Space Sas (FR) Consortium: 2. Ethniko Kai Kapodistriako Panepistimio Athinon (EL) 3. Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (DE) 4. Intelligence For Environment And Security Srl Ies Solutions Srl (IT) 5. Ubimax Gmbh (DE) 6. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (EL) 7. Tekever Asds (PT) 8. Robotnik Automation Sll (ES) 9. Ministry Of National Defence, Greece (EL) 10. Teknologian Tutkimuskeskus Vtt Oy (FI) 11. Institut Po Otbrana (BU) 12. Oceanscan - Marine Systems & Technology Lda (PT) 13. Rajavartiolaitos (FI) 14. Ministerio Da Defesa Nacional (PT) 15. Viasat Antenna Systems Sa (CH) 16. Nato Science And Technology Organisation (BE) 17. Cross-Border Research Association (CH) 18. Istituto Di Sociologia Internazionale Di Gorizia Isig (IT) 19. Serviciul De Protectie Si Paza (RO) 20. Admes Monoprosopi Idiotiki Kefelaiouchiki Etaireia (EL)

This overview is complemented by ISF projects.

NUNIRESPER	
Title	DEVELOPMENT OF A NEW MODEL OF UNIFORM FORMAT FOR RESIDENCE PERMITS FOR THIRD-COUNTRY NATIONALS
Objective	Develop a new uniform format for residence permits for third-country nationals
Contract details	ISFB-2016-AG-IBA-RESI; 1/10/2017 – 30/6/2018; 598.367,00
Abstract	The main reason behind the amending proposal lies in the fact that the design of the current uniform format for the Residence Permit was adopted back in 1997. In 2009 new security features were introduced in order to improve the security of the Residence Permit. However, the high quality of counterfeited EU Residence Permits found in recent years forced Member States to start working on a new design for the uniform format. The selected design proposal, presented by Spain, has been developed so far in a subgroup set up under Article 6 of Regulation (EC) No 1683/95 ("Article 6 committee").EU Member States and Schengen Associated Countries will benefit from the new design of the EU Residence Permit, designed with the goal of raising the current level of counterfeit deterrence to that of a state-of-the-art high security document. The new design introduces a more harmonised format, ensuring the highest possible security level, and helping border guards and other officials recognise Residence Permits at first sight. Also the list of national security features has been significantly reduced, improving the present situation in which the quality and appearance of residence permits among Member States differs greatly.

PCCC network	
Title	Strengthening of PCCC Activities in Europe *This project is also relevant for 6.4.5 Support to law enforcement*
Objective	Develop a more secure, detailed and standardised as well higher interoperable information exchange between Police and Customs Cooperations Centers (PCCC), Central National Authorities (CNA/ENU) and Europol
Contract details	ISFP-2017-AG-IBA-PCCC; 1/9/2018 – 31/8/2021; 525.477,00
Abstract	The aim of the project is to harmonize procedures on information exchange at each Police and Customs Cooperations Centers (PCCC). To Intensify the information exchange of national PCCC delegations with their respective Central National Authorities (CNA) via the use of SIENA, and additionally the exchange via CNA or directly with Europol, in accordance with the respective national law of the participants,.Moreover a tool for automatied data transfer between PCCC Case Management Systems (CMS) and SIENA will be developped and tested in a realtime environment. This poject will also support the further role out of SIENA at PCCCs, The specific knowledge available in PCCC´s in the field of crime analyzes and risk assessment at the regional level will contribute to a wider picture about the fight against border related crime. Working out harmonised and standardised work flow procedures, implementing joint trainings and exchanges will support the PCCC´s staff in their daily work. The project will support the implementation of all possible working areas at PCCC as defined by the EU PCCC guidelines. PCCC, CNA/ENU and Europol will benefit from these activities via a more secure, detailed and standardised as well higher interoperable information exchange.

This overview is complemented by relevant Erasmus+ projects.

Citizenship, migration and security in the EU	
Title	Citizenship, migration and security in the EU
Objective	Foster better knowledge and understanding of the Europeanization of citizenship, migration, asylum and security in relation to a) teaching and research and b) the quality of professional training on EU subjects
Contract details	599736-EPP-1-2018-1-NL-EPPJMO-CoE 1/9/2018 - 31/8/2021; EUR: 80.000,00
Abstract	CIMIS aims to foster better knowledge and understanding of the Europeanization of citizenship, migration, asylum and security in relation to a) teaching and research and b) the quality of professional training on EU subjects. CIMIS seeks to examine how the interplay between migration and security shapes the legal landscape of EU migration law and the rights and experiences of those subjected to these laws: nationals, EU citizens, migrants, asylum seekers, travellers etc. The events that have taken place since 2015 in the field of migration require a much more rigorous academic engagement and scrutiny of the interphase between citizenship, migration, asylum and security with a view to help a critical reflection on EU's actions in these fields and their consequences. Our proposal is designed to reach out to students, legal professionals, policy makers, academics and civil society actors. The project outputs are linked to our objectives concerning teaching, research and dissemination. They include: a summer course; a specialized course for EU judges; three quarterly newsletters; three specialized seminars; three publications linked to these seminars; a monitoring report on EU citizens' rights and two academic publications. CIMIS activities focus on selected EU legislative measures concerning citizenship, migration, asylum and security in order to improve knowledge about their implementation, application at the national level and their interpretation by the European Court of Justice. CIMIS aims to ensure that individuals supposed to enjoy EU rights do not have their rights ignored or violated due to poor knowledge of those rights or misunderstanding concerning their content. This is why our activities reach out to students, legal professionals and civil society actors who all need to keep up to date with new developments in the field. By providing accurate and up to date knowledge on EU rights, CIMIS hopes to contribute towards social cohesion in the EU.
Consortium	Coordinator: Stichting Katholieke Universiteit (NL)

Boosting European Security Law and Policy	
Title	Boosting European Security Law and Policy: Focus on flows of migrants, data security and movement of capitals
Objective	Support dissemination of knowledge and skills with regard to security and its role in the process of European integration, involving public and private actors who can play a role in the different areas linked to the subject of security
Contract details	599763-EPP-1-2018-1-IT-EPPJMO-PROJECT 1/9/2018 - 31/8/2021; EUR: 60.000,00
Abstract	The subject of security is a central aspect of the process of European integration. After the Lisbon Treaty, security constitutes a key aspect of the Common Foreign and Security Policy (including a Common Security and Defence Policy) and of a the European Area of Freedom, Security and Justice. In light of these dynamics, this Project intends to support activities of information and dissemination of knowledge and skills with regard to the subject of security and its role in the process of European integration, involving public and private actors who can play a role in the different areas linked to the subject of security, such as policy-makers, business representatives, staff of public administration and, in general, stakeholders in the field of European security. The project consists of one opening event, three general conferences, three thematic workshops and one final event. The opening event is intended as a presentation of the project to the broader academic community in Siena as well as to local public and private stakeholders.
Consortium	Coordinator: Universita' Degli Studi Di Siena (IT)

This overview is complemented by H2020 projects.

Silent Flyer	
Title	Solving the greatest problem of surveillance: To see without being seen
Objective	Develop a small UAV (or small unmanned air system, SUAS), which is an autonomous flapping wing bird-like robot for 1) Civil use and surveillance, 2) wildlife photography & research
Contract details	H2020-SMEInst-2018-2020-1; 1/5/2019 - 31/8/2019; EUR: 50.000
Abstract	Flygildi developed SILENT FLYER: "An entirely new drone design solving the greatest problem of surveillance -to see without being seen". SILENT FLYER is a Small UAV (or small unmanned air system, SUAS), which is an autonomous flapping wing bird-like robot. It looks like a bird and flies like a bird: It uses flapping flight for lift and propulsion instead of propellers. It will revolutionize the drone's market by introducing the first UAV that combines silent flight (<70dB of noise emission) and bird-like appearance while incorporating accurate vertical take-off and landing (VTOL) capabilities to operate in turbulent weather conditions. SILENT FLYER can fly for >40 mins under favorable conditions (due to the ability to utilize wind currents during soaring, like a bird) and >300m maximum altitude of operation and do accurate landings relative to the ground. This makes it the perfect solution for 1) Civil use and surveillance, 2) wildlife photography & research. Moreover, SILENT FLYER will also represent a great boost for our company, not only regarding revenues, but also for our staff, since we plan to increase our staff a 120% from 8 to 18 people, in order to reach our production needs.
Consortium	Coordinator: Flygildi Ehf (IS)

SECURITY FLOWS	
Title	Enacting border security in the digital age: political worlds of data forms, flows and frictions. *This project is also relevant for 6.3.1 Cyber Security Management (for SMEs/business, local public authorities) Digital borders.*
Objective	Develop a novel interdisciplinary framework to understand how data is generated, exchanged and contested in border encounters, and to investigate the complex epistemic, practical, political and ethical implications of these transformations
Contract details	ERC-2018-COG; 1/6/2019 - 31/5/2024; EUR: 1.897.826
Abstract	Datafication, the process transforming our everyday lives into quantifiable digital data, is also transforming borders today. Data collection, exchange and interoperability have become key for EU border security. How does data enact border security in the digital age? What are the political and ethical implications of these processes of datafication? This project proposes to develop a novel interdisciplinary framework to understand how data is generated, exchanged and contested in border encounters, and to investigate the complex epistemic, practical, political and ethical implications of these transformations. Starting from a socio-material reconceptualisation of datafication as the production of data forms, flows and frictions, the project advances an innovative theorisation of the (i)epistemic effects of datafication as producing both knowledge and ignorance. It will shed light on how data forms make things intelligible or unintelligible, and how digital data flows and frictions redistribute knowledge and ignorance among border security actors, NGOs and irregular migrants. To trace the (ii)practical implications of datafication, the project will devise a multi-modal methodology for 'following the data' along the Eastern, Central and Mediterranean routes as well as the routes leading to these from Morocco, Niger and Turkey, and finally along return routes. (iii)Politically, the project investigates how data reconfigures the worlds of actors involved in the governance of border security by enacting new power relations between these actors and reshaping decision-making. Finally, the project also advances a socio-material approach to (iv)ethics to account for how data protection and the rights of both citizens and non-citizens are transformed by datafication. Through its ambitious theoretical and methodological innovations, which will shape an emergent field of research, the project will have long-lasting impact for border and security studies.
Consortium	Coordinator: King's College London (UK)

8. Societal resilience and civil protection

8.1 Socio-economic and ethical implications

8.1.1 Ethics, Societal implications

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Ethics, societal implications	ADDPRIV ALTERNATIVE COMRADES CUIDAR EDUCEN e-SIDES EVIDENCE EUNPACK ICT4COP MARGIN IMPACT INEX PACT PARIS PRISMS PS RESPECT SAPIENT SECONOMICS SECILE SLANDAIL SOURCE SURPRISE SURVEILLE TRANSSOL VIDEOSENSE

In this iteration of the CoU Mapping Document, no new projects related to Ethics, societal implications were identified.

8.1.2 Post-crisis societal and psychological support

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Post-crisis societal and psychological support	BESECU NDTERROR OPSIC PFA-CE PSYCRIS SUPER

In this iteration of the CoU Mapping Document, no new projects related to Post-crisis societal and psychological support were identified.

8.1.3 Societal resilience to disasters

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
External security threat	ALTER BRTE SCALAR SMR

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

BuildERS	
Title	BuildERS
Objective	Develop knowledge and insights that will devise recommendations for policies, plans, strategies, and competencies for building partnerships, networks and trust for progressively fortifying the social capital and resilience against future threats, be they natural or man-induced
Contract details	H2020-SU-SEC-2035; topic code SU-DRS01-2018-2019-2020; 1/5/2019 - 30/4/2022; € 4 946 900
Abstract	The Sendai Framework for Disaster Reduction 2015-2030 points out that global evidence indicates that in all countries the exposure of people and assets to disasters has increased faster than attempts to decrease vulnerability. The Framework underlines an all-society engagement, which addresses the most vulnerable groups, whilst accounting for contextual and cultural differences. It also calls for a more explicit focus on people, their health and livelihoods, and the local level, since individuals and local communities possess their own capabilities, networks, methods, tools and means to absorb impacts and bounce back. Thus, the 'capital' that is available at the root-level deserves to be recognised and incorporated in the policies and strategies for disaster risk reduction and enhancing of resilience. To improve the overall resilience of people, communities and thereby the whole society, the BuildERS project focuses on the most vulnerable individuals, groups and communities. Strengthening the social capital, risk awareness and preparedness of the most vulnerable segments of the societies and communities will increase understanding on what societal resilience comprises. BuildERS will develop knowledge and insights that will device recommendations for policies, plans, strategies, and competencies for building partnerships, networks and trust for progressively fortifying the social capital and resilience against future threats, be they natural or man-induced. The special focus on communities and in particular on the most vulnerable groups answers to the so-far unfulfilled needs of these communities.BuildERS uses several research methods such as i) Stakeholder engagement with co-design and co-creation processes, ii) Field surveying and questionnaires, iii) Comparative research, iv) Multiple case analysis.
Consortium	Coordinator: 1. Teknologian Tutkimuskeskus Vtt Oy (FI) Consortium: 2. Stockholms Universitet (SE) 3. Universitetet I Stavanger (NO) 4. Transportokonomisk Institutt (NO) 5. Tartu Ulikool (EE) 6. Universita Degli Studi Di Trento (IT) 7. Poliisiammattikorkeakoulu (FI) 8. Estonian Rescue Board (EE) 9. Stiftelsen The Stockholm Environment Institute (SE) 10. Ou Positium Lbs (EE) 11. Geonardo Environmental Technologies Ltd (HU) 12. Armee Du Salut (BE) 13. Eberhard Karls Universitaet Tuebingen (DE) 14. Deutsches Rotes Kreuz Ev (DE) 15. Provincia Autonoma Di Trento (IT) 16. University Of Indonesia (ID) 17. George Mason Research Foundation, Inc (US)

8.2 Public involvement / engagement in research and use of social media

8.2.1 Enhanced communication in crisis management

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Enhanced communication in crisis management	COSMIC EMERGENT EVACUATION HELP ISAR+ MEDIA4SEC PEP SOTERIA TRILLION UCPM SOPs

In this iteration of the CoU Mapping Document, no new projects related to Enhanced communication in crisis management were identified.

8.2.2 Civil society engagement

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Civil society engagement	ARCHIMEDES ASSERT ATHENA City.Risks CityCop INSPEC2T NITIMSER LIFE Legal Actions PANDORA SECUREPART UNITY

In this iteration of the CoU Mapping Document, one project categorised under another theme is deemed related to civil society engagement: DECOUNT.

8.3 Population alert, civil protection (in case of emergencies) and practitioners' involvement

8.3.1 Civil Protection Operations, including volunteer involvement

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Civil Protection Operations, including volunteer management	HELI4RESCUE LYNCEUS2MARKET MOBNET JET ANTI-FIRE GRIMASSE POLG SARA SINSIN SWIFTERS MERCI PROVOICE Best practices in rescuing and threats elimination DiveSmartBaltic F.E.M.R.Z. EESM Cooperation between PL and LT in Promoting volunteer fire and rescue services

This overview is complemented by H2020 projects.

PALAEMON	
Title	PALAEMON – A holistic passenger ship evacuation and rescue ecosystem *This project is also relevant for 7.2 Maritime Security*
Objective	Develop and evaluate a sophisticated mass centralised evacuation system, based on a radical re-thinking of Mass Evacuation Vessels (MEVs) combined with an intelligent ecosystem of critical components providing real-time access to and representation of data
Contract details	H2020-MG-2018-TwoStages; 1/6/2019 - 31/5/2022; EUR: 8.943.775
Abstract	PALAEMON proposes the development and evaluation of a sophisticated mass centralised evacuation system, based on a radical re-thinking of Mass Evacuation Vessels (MEVs) combined with an intelligent ecosystem of critical components providing real-time access to and representation of data to establish appropriate evacuation strategies for optimizing the operational planning of the evacuation process on damaged or flooded vessels. The intelligent ecosystem of PALAEMON incorporates innovative technologies for sensing, people monitoring and counting and localisation services as well as real-time data during accident time. These will be integrated into an independent, smart situation-awareness and guidance system for sustaining an active evacuation route for large crowds, making emergency response in EU passenger ships more efficient. Continuous monitoring and permanent control will enhance the capacity to detect, prevent and mitigate any issue and potential harm arising from physical and/or man-made accidents and disasters. The proposed ecosystem will include the new IMO standard for data exchange-VDES.
Consortium	Coordinator: 1. Airbus Defence And Space Sas (FR) Consortium: 2. "Atos Spain Sa (ES) 3. Konnekt Able Technologies Limited (IE) 4. Engitec Systems International Limited (CY) 5. Internet Of Things Applications Andmulti Layer Development Ltd (CY) 6. Johanniter Osterreich Ausbildung Und Forschung Gemeinnutzige Gmbh (AT) 7. National Technical University Of Athens - Ntua (GR) 8. Advantic Sistemas Y Servicios Sl (ES) 9. Siveco Romania Sa (RO) 10. Dsb Deutsche Schlauchboot Gmbh (DE) 11. Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth (DE) 12. Ericsson Hellas Sa Tilepikoinoniakoy Ilinox (GR) 13. Autoritatea Navala Romana (RO) 14. Danaos Shipping Company Limited (CY) 15. Engineers For Business Ipiresies Technologias Kai Michanikis Anonimi Etairia (GR) 16. Astilleros De Santander Sa (ES) 17. Dnv Gl Hellas Sa (GR) 18. Admes Monoprosopi Idiotiki Kefelaiouchiki Etaireia (GR) 19. Thales Italia Spa (IT) 20. Universidad De Alcala (ES) 21. Panepistimio Aigaiou (GR) 22. Wiser Srl (IT) 23. Anonimi Naftiliaki Eteria Kritis (Anek) S.A. (GR) 24. Oesterreichischer Lloyd Seereederei (Cyprus) Ltd (CY)"

SafePASS	
Title	Next generation of life Saving appliances and systems for saFE and swift evacuation operations on high capacity PASSenger ships in extreme scenarios and conditions *This project is also relevant for 7.2 Maritime Security.*
Objective	Develop an integrated system that will collectively monitor, process and inform during emergencies both crew and passengers of the optimal evacuation routes, coupled with advanced, intuitive and easy to use LSA, resulting to a significant reduction of the total time required for ship evacuation and increased safety
Contract details	H2020-MG-2018-TwoStages; 1/9/2019 - 31/8/2022; EUR: 8.270.366,25
Abstract	Evacuating a large passenger ship is a safety-critical and strictly time-bound task and a complex decision-making process based on the evolving situation and the information available. Timely evacuation requires fast and accurate evaluation of ship's condition and estimation of remaining evacuation time. The assumption that all passengers will be able to comprehend and follow instructions or even that the crew will be able to communicate verbally during a crisis is very optimistic. In response, a system that will provide clear instructions and guide passengers safely on how to react in an emergency situation without reliance on any passenger skills or experience is of paramount importance for any large passenger ship. SafePASS will radically redefine the evacuation processes, evacuation systems/equipment and international regulations for passenger ships in all environments, hazards and weather conditions, independently of the demographic factor, by developing an integrated system that will collectively monitor, process and inform during emergencies both crew and passengers of the optimal evacuation routes, coupled with advanced, intuitive and easy to use LSA, resulting to a significant reduction of the total time required for ship evacuation and increased safety. SafePASS is an integrated solution that provides passengers tailored evacuation assistance, assists the crew by enhancing their situational awareness and ability to handle de-skilled equipment, while incorporating fail-safe processes for the evacuation procedure. SafePASS prototypes will be validated in real environment, on a cruise ship and in LSA manufacturers testbeds and towing tanks. The consortium, consisting of 15 partners, amongst which academic institutions, classification societies, innovative SMEs, shipyard, LSA manufacturers and a cruise operator, safeguards both the high impact and implementation of the project results, through the preparation of a set of recommendations for IMO submission.
Consortium	Coordinator: 1. National Technical University Of Athens - Ntua (GR) Consortium: 2. "Exus Software Ltd (UK) 3. University Of Strathclyde (UK) 4. Telesto Technologies Pliroforikis Kai Epikoinonion Epe (GR) 5. Crowd Dynamics International Limited (UK) 6. Diginext (FR) 7. The Provost, Fellows, Foundation Scholars & The Other Members Of Board Of The College Of The Holy & Undivided Trinity Of Queen Elizabeth Near Dublin (IE) 8. Survitec Group Limited (UK) 9. Chantiers De L'atlantique (FR) 10. Rina Hellas Etairia Periorismenis Evthinis Niognomonas (GR) 11. Rina Services Spa (IT) 12. Seability (Cyprus) Ltd (CY) 13. Rcl Cruises Ltd (UK) 14. Dnv Gl Se (DE) 15. Viking Life-Saving Equipment As (DK)"

8.3.2 Population alerting

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Population alerting	POP-ALERT ZOOVEL-UC Joint Initiatives and Solutions (INTERREG)

In this iteration of the CoU Mapping Document, one project categorised under another theme is also deemed relevant for population alerting, this is PROACTIVE.

8.3.3 Public Protection

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Public Protection	PPDR-TC SAFECITI CUBETTO LetsCrowd MASC II

In this iteration of the CoU Mapping Document, two projects categorised under another theme are also deemed relevant for public protection, namely: PROACTIVE and BioWatchID.

8.3.4 International cooperation / Humanitarian aid

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
International cooperation / Humanitarian aid	EU-CIVCAP IECEU GAP iTRACK PeaceTraining.eu WOSCAP

In this iteration of the CoU Mapping Document, no new projects related to international cooperation/humanitarian aid were identified.

8.3.5 Training and Networking

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
External security threat	AUGGMED CAST CRISIS ELITE ESENET GARTNET-E HYRESPONSE INDIGO L4S SEREN 3 SEREN 4 TARGET ESSENTIAL TEAMS 2.0 TEAMS Prepare Prodidge SERIOR SSN EU LIFE IP C2C CC

In this iteration of the CoU Mapping Document, no new projects related to training and networking were identified.

8.3.6 Protective equipment

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Protective equipment	FRESP IF REACT SMART@FIRE SMARTPRO Hazijax

In this iteration of the CoU Mapping Document, one project categorised under another theme is also relevant for protective equipment: INDIGENOUS.

9. Horizontal issues

9.1 Foresight studies on security threats & Roadmaps

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Foresight studies on security threats & Roadmaps	ANVIL CBRNEMAP ETTIS EVOCS FESTOS FOCUS FORCE EU-DRONES

This overview is complemented by Erasmus+ projects.

The European Union and Peace-Building in East Asia	
Title	The European Union and Peace-Building in East Asia
Objective	Fund Jean Monnet Chair programme, "The European Union and Peace-Building in East Asia (EUPBEA), which focuses on the security relations between EU and East Asia and analyses the ways to build a constructive tie to deal with mutual security agenda such as crisis management, human security and sustainable development
Contract details	600165-EPP-1-2018-1-KR-EPPJMO-CHAIR 1/9/2018 – 31/8/2021; EUR: 49985,1
Abstract	The Jean Monnet Chair programme, "The European Union and Peace-Building in East Asia (EUPBEA)," focuses on the security relations between EU and East Asia and analyses the ways to build a constructive tie to deal with mutual security agenda such as crisis management, human security and sustainable development. It assumes that the EU can function as an important security actor in East Asia. While regional cooperation among China, Japan and Korea has long been suggested, the tension still remains in East Asia, especially on the Korean Peninsula. The European model of peace-building through dialogue needs to be explored as an alternative.
Consortium	Coordinator: Korea University (KR)

Peace, War and the World in European Security Challenges	
Title	Peace, War and the World in European Security Challenges
Objective	Contribute to overcoming contradictions in international security perception by key international actors (EU, Middle East, Turkey, Russia), to provide multilateral approach to responses to European security challenges, to foster policy dialogue on their political, geopolitical and religious issues
Contract details	599962-EPP-1-2018-1-RU-EPPJMO-NETWORK 1/9/2018 - 31/8/2021; EUR: 293.803,46
Abstract	European security challenges have become that very Bell that "tolls for thee" and its ring is echoed in each region, each country, each community. Urgency of the present moment is to give responses to actual menaces in security. However to manage this we have to come to common vision what poses thereat and how they are understood by different international players. The strategic aims of the project are to contribute to overcoming contradictions in international security perception by key international actors (EU, Middle East, Turkey, Russia), to provide multilateral approach to responses to European security challenges, to foster policy dialogue on their political, geopolitical and religious issues.The main objectives are to create a network with aim to facilitate space for a constructive dialogue about diverse visions to European security challenges, to generate modern understandings of security beyond the state-of-the-art by applying multi-disciplinary approach.
Consortium	Coordinator: Voronezh State University (RU)

Building Resilient States and Societies	
Title	Building Resilient States and Societies: EU's Response to New Security Challenges in the European Neighbourhood Area
Objective	Enhance understanding of current and new threats in Europe's strategic orbit and contribute to development of research-led teaching and evidence-based policy making in European Security Studies by considering theoretical and practical issues relating to security cooperation between the EU and its neighbourhood
Contract details	599312-EPP-1-2018-1-UA-EPPJMO-PROJECT 1/9/2018 - 31/8/2020; EUR: 60.000,00
Abstract	The project 'Building Resilient States and Societies: EU's Response to New Security Challenges in the European Neighbourhood Area' aims to bridge a major gap in knowledge and understanding of current and new threats in Eu-rope's strategic orbit and contribute to development of research-led teaching and evidence-based policy making in European Security Studies by considering theoretical and practical issues relating to security cooperation between the EU and its neighbourhood.
Consortium	Coordinator: Public Organisation Ukrainian Institute Of Crisis Management And Conflict Solution (UA)

Jean Monnet Chair EU and the World	
Title	Jean Monnet Chair EU and the World
Objective	Fund the Jean Monnet Chair "EU and the World", which addresses some of the challenges the union is currently facing in three different ways: by conducting excellent cutting-edge research;developing and providing in-depth teaching in european union studies; and by reaching out to various target groups
Contract details	600350-EPP-1-2018-1-NL-EPPJMO-CHAIR 1/9/2018 - 31/8/2020; EUR: 50.000,00
Abstract	European Union's external policies have received increased attention due to the multiple security crises at Union's doorstep both at the East and the South. While the transatlantic relationship has entered into a new phase and Brexit is about to happen, the Union started looking for ways to shore up its resilience, to provide security to its citizens and to make sure it remains a global player. This involves creating synergies between multiple policies such as security, foreign policy, development, trade, migration but also environmental policies or health. This project addresses some of the challenges the union is currently facing in three different ways: by conducting excellent cutting-edge research;developing and providing in-depth teaching in european union studies; and by reaching out to various target groups.
Consortium	Coordinator: Universiteit Leiden (NL)

9.2 Standardisation, Testing & Certification

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Standardisation, Testing & Certification	CREATIF CRISP SLAM HECTOS RESISTAND CBRNE STNDS 2017 SAYSO ALBINA GDP Bad Nieuweschans 2017+

These projects were complemented in the H2020 framework by the following project funded by the Secure Societies programme:

iProcureNet	
Title	iProcureNet
Objective	Build an EU network of organisations centred on the procurement of security solutions through the appointed iProcureNet National Contacts (IPNCs), together with a larger community of people composed of individuals and experts interested in procurement
Contract details	H2020-SU-SEC-2034; topic code SU-GM01-2018-2019-2020; 1/5/2019 - 30/4/2024; € 1 588 262,50
Abstract	The iProcureNet project aims to build an EU network of organisations centred on the procurement of security solutions through the appointed iProcureNet National Contacts (IPNCs), together with a larger community of people composed of individuals and experts interested in procurement. Via the established Network+Community, iProcureNet will facilitate collaboration and dialogue among procurers, enabling: i) coordinated sharing and analysis of procurement trends included in the investment plans, ii) development of common and standardised practices from the technical, legal and financial perspectives, and iii) establishing pathways for joint procurement (JP) of innovative and new to market solutions, research services, and commercial off-the-shelf (COTS) products in the field of security. iProcureNet will develop the iProcureNet Toolbox including a comprehensive methodology, guidelines and a knowledge database of current procurement practices and processes in Europe; and will create a firm foundation for the set-up of Established Buyers Groups (EBGs) – countries which, using the iProcureNet Toolbox, have found common ground and are ready to procure. Close collaboration with related PCP and PPI actions and the practitioner innovation networks will be a key component of the project. Ultimately, iProcureNet, will aim to create a stepping stone to future collaboration in the form of a future investment plan for collaborative procurement actions, and to develop detailed pro-innovation procurement strategies. The Network+Community will be supported by i) the iProcureNet Online Platform (IPOP) enabling professional social networking and online dialogue on good practices and procurers' needs; ii) a sustainable organisational set-up composed of well organised bodies and processes, and iii) appropriate communication and dissemination activities including Annual Conferences, trainings and workshops. The consortium includes 15 partners, out of which 10 are procurement agencies.
Consortium	Coordinator: 1. Ministere De L'interieur (FR) Consortium: 2. Arttic (FR) 3. Inspectoratul General Al Politiei De Frontiera (RO) 4. Institut Po Otbrana (BU) 5. Isem-Institut Pre Medzinarodnu Bezpecnost A Krizove Riadenie, No (SK) 6. Jera Consulting Limited (UK) 7. Ministerio Del Interior (ES) 8. Ministerstvo Vnutra Slovenskej Republiky (SK) 9. Ministerul Afacerilor Interne (RO) 10. Ministry Of Interior (CY) 11. Mokslo Inovaciju Ir Technologiju Agentura (LT) 12. Ministério Da Justiça (PT) 13. Orszagos Rendor - Fokapitanysag (HU) 14. Politsei- Ja Piirivalveamet (EE) 15. Tartu Ulikool (EE)

This overview is complemented by a DG ECHO project.

BELICE	
Title	Building Experience to Lead Initial Assessment in Challenging Emergency
Objective	Provide a methodology and train on it to perform the initial wide assessment (ASR1) as INSARAG Guidelines/ training (i.e.First Responders Training) does not cover specifically this aspect of emergency intervention
Contract details	2018/PREP/826208; 3-6-2019 - 2-2-202; € 702.813,92
Abstract	BELICE is aimed at providing a methodology and train on it to perform the initial wide assessment (ASR1) as INSARAG Guidelines/training (i.e.First Responders Training) does not cover specifically this aspect of emergency intervention. BELICE brings together operational (USAR teams) and non-operation actors (LLAA, disaster managers) who will be trained on a standard methodology (mirrored in a Manual on ASR1)
Consortium	Coordinator: 1. Ministero Dell'interno - Corpo Nazionale Dei Vigili Del Fuoco (IT) Consortium: 2. Bundesministerium Des Innern (DE) 3. Ministere De L'interieur (FR) 4. Timesis Srl (IT) 5. Presidenza Del Consiglio Dei Ministri - Dipartimento Della Protezione Civile (IT)

This overview is complemented by a H2020 project.

STAIR4SECURITY	
Title	Stair4security- Standards, Innovation And Research For Security *This project is also relevant for 5.7 CBRNE (Cross-cutting) and 9.4.2 Information/communication systems for Disaster Management.*
Objective	Propose a collaborative platform as single entry point of information on the security sector coming mostly from research activities allowing a better governance of standardization needs in the Disaster Resilience and Chemical Biological Radiological Nuclear and Explosive (CBRN-E) sectors
Contract details	H2020-IBA-SC7-PSM-2018; 1/1/2019 - 31/12/2020; EUR: 900.000
Abstract	The main objective of this proposal is to propose a collaborative platform as single entry point of information on the security sector coming mostly from research activities allowing a better governance of standardization needs in the Disaster Resilience and Chemical Biological Radiological Nuclear and Explosive (CBRN-E) sectors. The aim of the platform is to permit a better overview of current and new projects being at, national, European or International level; ensuring more coordination between all stakeholders and responding more efficiently and timely to the critical needs following an agreed strategic vision and identified priorities. Besides ensuring the necessary partnering network, the project will review the necessary tools and mechanisms including the CEN and CENELEC Workshop Agreement (CWA) process and a fast-track procedure to adopt, if market relevant, a CWA or any other deliverable or reference document e.g. TS and TR into a consensus standard (EN). Possibilities and conditions to include classified information in a non-consensus standard (CWA, TS or TR) will also be explored.
Consortium	Coordinator: Comite Europeen De Normalisation (BE)

9.3 Communication systems (Interoperability and communication with focus on security)

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Communication systems (Interoperability and communication with focus on security)	CRISYS DARIUS DESTRIERO EPISECC FREESIC SALUS SECTOR CIVILEX BroadWay OpSec

9.4 Information / Communication systems for Disaster Management

9.4.1 Communication systems / response coordination for first responders

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Communication systems / response coordination for first responders	DITSEF E-SPONDER ESS GERYON INFRA OD REDIRNET SECRIROM SPARTACUS

In this iteration of the CoU Mapping Document, no new projects related to Communication systems / respone coordination for first responders were identified.

9.4.2 Communication systems with focus on disaster management (general)

As a cross-reference to projects funded previously under FP7 and H2020 (see acronyms in the table below), the reader is invited to consult the CoU Mapping Documents published in 2016 and 2018 in which the following projects are described.

Research sub-category	Project Acronyms
Communication systems with focus on disaster management (general)	C2-SENSE CRISCOMSCORE ISITEP SECINORE BROADMAP EMYNOS NEXES ShamRock GICA IPCOM

In this iteration of the CoU Mapping Document, three projects categorised in another theme are also deemed relevant for Communication systems with focus on disaster management (general), these include REMESH, STAIR4SECURITY and DRONECOP.

10. WAY AHEAD

Most policies dealing with Disaster Risk and Crisis Management have established operational links with research. For example, the CBRN and Explosive Action Plans include the goal to strengthen and prioritise research. Furthermore, an engagement in further research cooperation with international partners is promoted with a view to enhancing synergies and avoiding duplications, using existing scientific networks, taking into account the research work performed by EDA, JRC and ESRIF (expired in 2009), organisation of periodic meetings by the Commission. While interactions among research and policies are high on the policy agenda, much remains to be done to improve the way information flows from the different communities involved in implementation of both research outputs and policies. This includes capitalizing on past research and enhancing cooperation among EU Member States organisations. The complexity of the security sector stems from the wide variety of actors involved and the lack of coordination mechanism at EU and national level regarding the transfer of information and their actual use by implementers and decision-makers. The need for enhanced coordination and information sharing form the basis of the Community of Users on Safe, Secure and Resilient Societies described in this paper.

Prior to developing a Community of Users (based on existing communities which are presently fragmented) with the view of improving science-policy-industry-operator's links in the context of Horizon2020, it was essential to understand the architecture of the research framework and how it interacted with various policy technical/scientific challenges. This was the subject of the previous mapping iterations as well as the of the present document. These should not be regarded as an impact assessment (i.e. no analysis was done about the actual impact and use of research outputs on policies) but rather as a means to better understand the complex science-policy working environment at EU and national levels and propose a mechanism to streamline information flows and transfer in the future. The analytical value of the document stands for the "matrix" established between research and science, i.e. a factual image of the present situation. For the time being, it does not go as far as analysing the real outputs of research regarding policy implementation but complements the work of the Commission's Disaster Risk Management Knowledge Centre (DRMKC) which intends to improve science-based services and analysis, the use and uptake of research and operational knowledge as well as to advance science and technology in DRM.

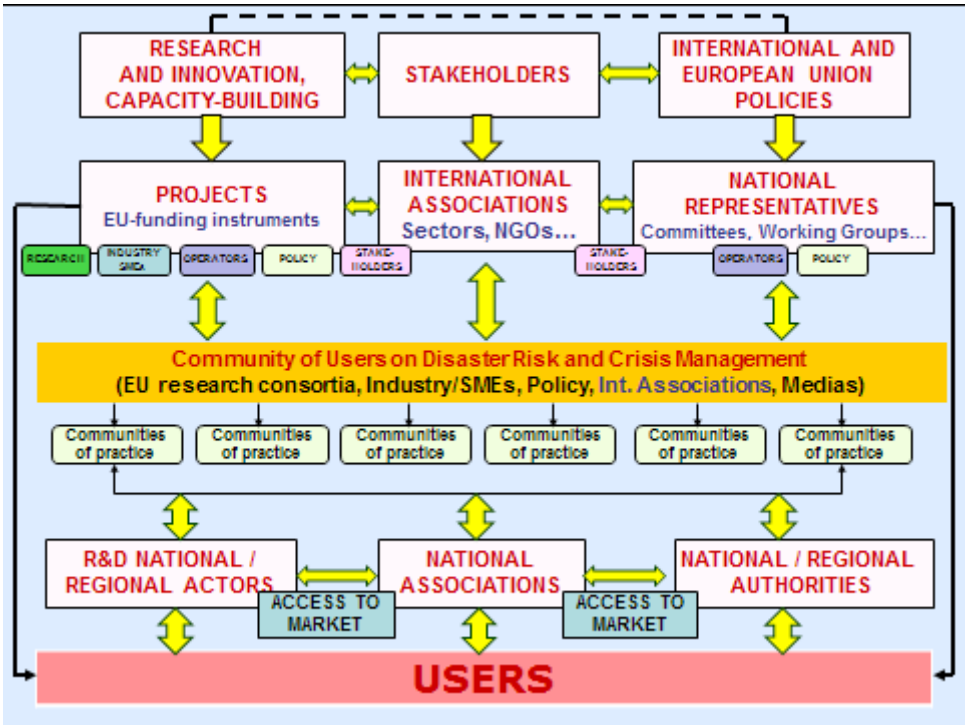
Based on this report CoU objectives will be pursued, from the short to the long term, as described in details in Section 2 "Tasks and objectives". Besides the technical objectives and the coordination of a better information exchange system, the Community of Users on the long term has the capacity to rise sharing of experiences among different actors involved in disaster risk and crisis management, with possible initiatives leading to synergies in the EU and beyond.

What is at stake here is to create a mechanism involving different levels (EU, national and regional) by which the different actors, and primarily the "users", will be able to rapidly trace back information and experiences issued from research, capacity-building and training projects, giving them the possibility to identify and contact right persons at the right time to get the feedback that they are looking for via the CoU dedicated website. Regular information exchanges and debates orchestrated by the Community of Users have readily enabled to better channel the information to the "users", which will have a direct effect on research programming, policy implementation and update. It will also have an effect on the involvement of end-users at various levels, e.g. in steering committees of Horizon 2020 projects, consortia, and cater links between research projects and capacity-building / training initiatives, e.g. making links with training programmes and centres, modules exercises, etc.

The Community of Users has the potential to become a useful complementary supporting group on research related activities to EU security policies (not duplicating existing advisory groups dealing with policy implementation but rather channelling information about research outputs) in the framework of which the European Commission with the EU Member States (through the policy and programme committees), EU Agencies, Intergovernmental Agencies, International Organisations and the wide range of sectors concerned (research, industry, operators) will cooperate for boosting implementation of research outputs, including their usability for policy implementation in the Member States (through information given to relevant existing committees and advisory groups). This will in addition have the capacity of returns of experiences from Industry and practitioners to the EU level, and enable to identify the most potential technologies, tools and methods in order to support their access to the market.

The Community of Users, along with the DRMKC, now enable to better visualise / identify research (and on the long term capacity-building and education) projects related to different themes relevant to safety, security and resilience. While this network is progressively establishing "horizontal" dialogues and helping interactions among different disciplines and actors, it will not have the capacity to create operational links with users at large without dedicated thematic networks (referred to as "Communities of practice").

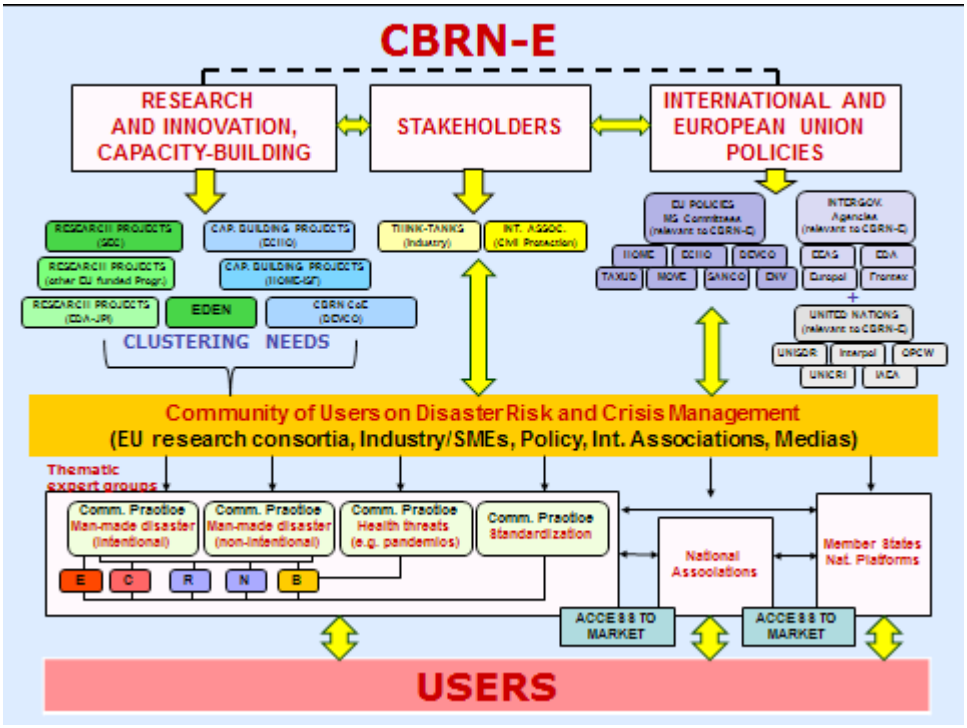
Linking CoU to Communities of practice



This need for "vertical" transfer of information from the EU to the national and the regional levels could be fulfilled by connecting the CoU to appropriate expert networks or communities, either existing or to be developed, that would play the role of knowledge integrating and "translating" bodies at European levels, with the mission – in support and in connexion with MS authorities – to effectively relays research outputs (e.g. new tools or technologies, methods etc.) to appropriate users at national, regional and even local levels. This process of pulling EU research outputs to users, i.e. transforming these outputs into outcome, can only be possible through an effective partnership with users. In other words, if the CoU provides on a regular basis information on new tools / technologies or other research information, different "communities of practice" might format this information to address different categories of users (policy-makers, scientists, industry/SMEs, practitioners, civil society) and undertake ad-hoc actions to ensure that potentials of EU research developments are known and possibly applied by them. This flow of information would enable that we do not miss opportunities (or duplicate work) and would also create effective bridges among the EU down to the citizen's level with possible feedback received and contributing to further research programming.

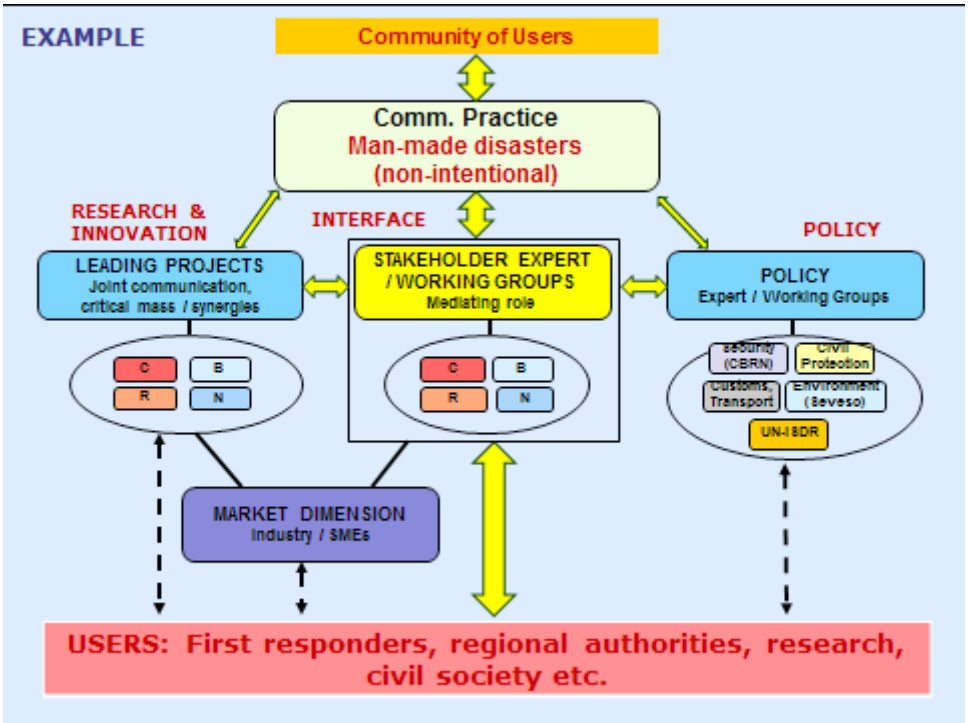
Two examples are given below to illustrate this purpose. In the CBRN-E area, the CoU will continue its efforts in identifying relevant projects funded by different (research, capacity-building) programmes with the aims to propose clustering initiatives through platforms of information exchanges. Stakeholders will continue to interact with these programmes to help interfacing with relevant policies. The CoU is naturally not interfering with policy development and implementation, but contacts are readily established with different policy bodies, enabling to inform users about possible updates and helping research information to be efficiently disseminated to policy actors. The "Community of practice" need to be activated to relay ad-hoc information to users as shown below.

Main actors in the CBRN-E area



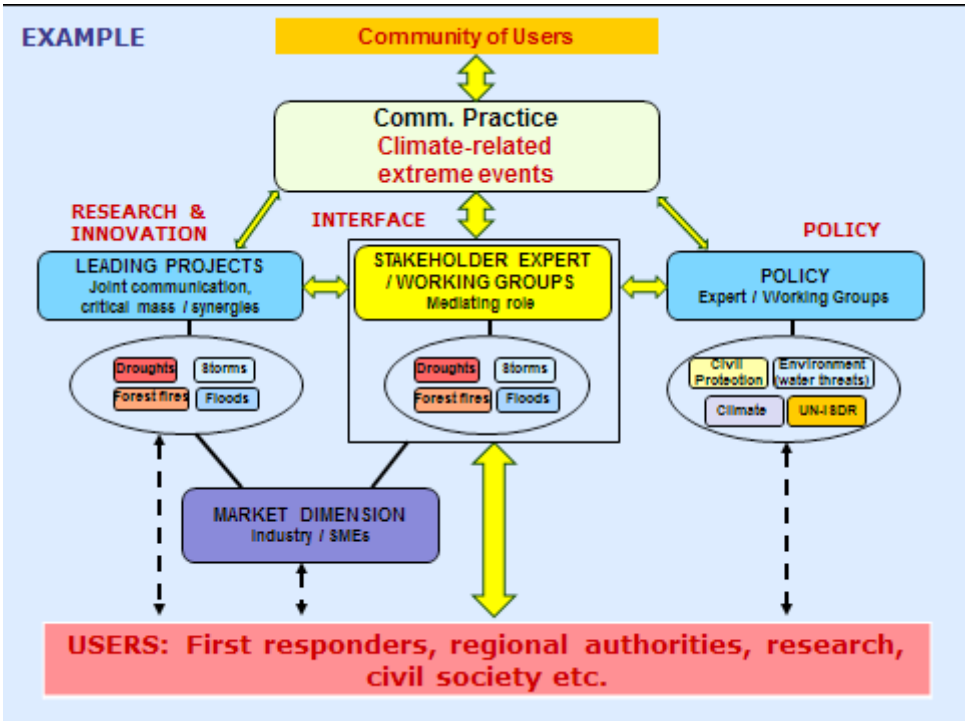
Zooming into the CBRN picture, this would imply that each Community of practice gets a comprehensive overview of leading projects in their area (research, capacity-building, training / education), help bringing these projects together if and when possible so that synergies and a critical mass may be built-up. Interfacing among research & innovation and other actors in the industry and policy areas should be facilitated by stakeholder expert / working groups with a mediating role, i.e. able to translate / format the information to target speciticially different users (e.g. specific technology information addressed to industry, support to a specific policy action with reference to the appropriate regulation ect.). In bridging the different "worlds", there is a greater chance that users will get better channelled information as the knowledge base would in principle become consolidated and made known to a wide range of different actors.

Channelling information in the CBRN

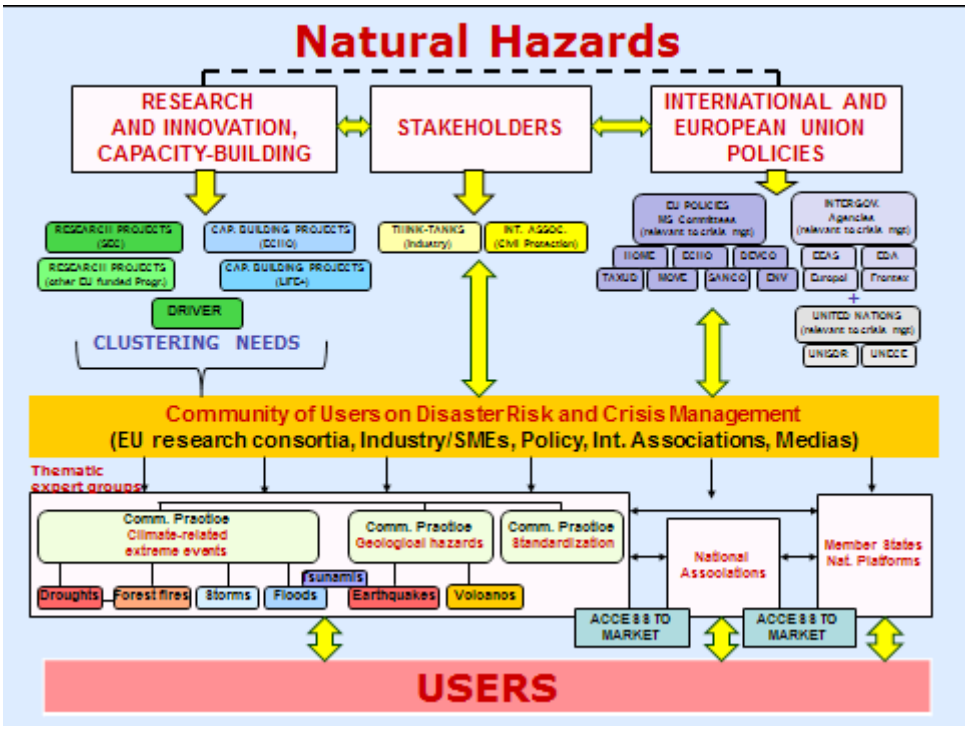


The same can be examplified in the area of natural hazards, taking into consideration the different "communities" and hazards.

Main actors in the Natural Hazards



Channelling information in the Natural Hazards



In conclusion, the Community of Users has the vocation to act as a facilitating platform, creating links and dialogues among different actors / disciplines (the "horizontal level") and among different levels (from EU to local). Based on the present mapping, a similar architecture has been used to develop a website which will facilitate information searches (not repeating what is readily in place but rather providing paths helping users to more easily find information per themes / areas). This mapping will be complemented on a regular basis (annually) for H2020 and other projects, and the CoU will pursue the organisation of gathering events to consolidate a culture of exchanges at EU level for the sake of improved safety, security and resilience of our societies

Getting in touch with the EU

In person
All over the European Union there are hundreds of Europe Direct Information Centres.
You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by e-mail
Europe Direct is a service that answers your questions about the European Union.
You can contact this service

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by electronic mail via: http://europa.eu/contact

Finding information about the EU

Online
Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU Publications
You can download or order free and priced EU publications from EU Bookshop at: http://bookshop.europa.eu. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact)

EU law and related documents
For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU
The EU Open Data Portal (http://data.europa.eu/euodp/en/data) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

DR-03-19-812-EN-N

Publications Office