EN

Horizon Europe

First draft Work Programme 2021-2022

Cluster 3: CIVIL SECURITY FOR SOCIETY

Version 23 September 2020

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions.

Please note that **budget figures are not included in this draft** because the actual overall budget of Horizon Europe, the budget of Cluster 3 and the consequent budget that could be allocated to the different *Destinations* are still unknown. The proposed draft topics can only be kept in the HE 2021-22 Work Programme if sufficient budget will be available

Table of Contents

INTRODUCTION

Supporting EU policy priorities

This Cluster 3 Work Programme will support the implementation of EU policy priorities relating to security, including cybersecurity, and disaster risk reduction and resilience. In addition, it will build on lessons learnt from the COVID-19 crisis in terms of prevention, mitigation, preparedness and capacity building for crises (including health crises) and in improving cross-sectoral aspects of such crises. In this respect, this Work Programme will therefore also ensure synergies and coordination of actions with other parts of Pillar 2.

It will support the Commission policy priority '*Promoting the European way of life*', as well as '*European Green Deal*' and '*Europe fit for the digital age*'. It will in particular support the implementation of the **EU Security Union Strategy**[1], the border management and security dimensions of the **New Pact on Migration and Asylum**, **EU Disaster Risk Reduction policies, the EU Maritime Security Strategy** and the future **EU Cybersecurity Strategy**.

Within the framework of the Horizon Europe Strategic Plan, the Cluster 3 expected impacts are of particular relevance to the Key Strategic Orientation D "*Creating a more resilient, inclusive and democratic European society*" and to Key Strategic Orientation A "*Promoting an open strategic autonomy by leading the development of key digital and enabling technologies, sectors and value chains*".

Meeting capability requirements

Projects will develop new knowledge, technologies and/or other solutions to the identified requirements. Projects will involve practitioner end-users (usually relevant national authorities) alongside researchers and industry. Such involvement has shown its worth in ensuring that the results of R&I are targeted to practitioner needs[2]. Relevant requirements are specified for the different topics.

Projects will need to show awareness of a project being only one stage in a wider needs-driven capability development cycle that triggers research, steers its implementation and capitalises on its outcomes. This means that projects should, on the one hand, show an understanding of the capability requirement that has led to the R&I need, and, on the other hand, include a strategy for ensuring the uptake of the outcomes including opportunities for using relevant EU funds for funding deployment.

[1] COM(2020) 605 final.

[2] Such as capability gaps identified by IFAFRI – International Forum to Advance First Responder Innovation www.internationalresponderforum.org

Ensuring ethical outcomes that are supported by society

In the field of security research it is particularly important that projects take into account human factors and the societal context, and ensure the respect of fundamental rights, including privacy and protection of personal data. Citizens and communities should be engaged, for example in assessing the societal impact of security technologies, so as to improve the quality of results and to build public trust. SSH (social sciences and humanities) disciplines need to be better integrated into security research. Again, relevant requirements are specified for the different topics.

The six Destinations

This Work Programme comprises the following six Destinations that (i) respond to the expected impacts of Cluster 3 presented in the Strategic Plan and (ii) build on the structure of the Horizon 2020 work programmes for security research:

1. **Destination – Better protect the EU and its citizens against Crime and Terrorism**

   Expected Impact: *"Crime and terrorism are more effectively tackled, while respecting fundamental rights, thanks to more powerful prevention, preparedness and response, a better understanding of human, societal and technological aspects of crime, and the development of cutting-edge capabilities for law enforcement agencies, including measures against cybercrime."*

2. **Destination – Effective management of EU external borders**

   Expected Impact: *"Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors."*

3. **Destination – Protected infrastructure**

   Expected Impact: *"Resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured with the help of knowledge, effective solutions and state-of-the-art technologies, as well as better cooperation between stakeholders."*

4. **Destination – Increased Cybersecurity**

   Expected impact: "*Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.*"

5. **Destination - A Disaster-Resilient Society for Europe**

   Expected Impact: *"Losses from natural, accidental and man-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness, and resilience and improved disaster risk management in a systemic way."*

6. **Destination – SSRI (Strengthened Security Research and Innovation)**

   Expected Impact: *"Security threats are more effectively addressed thanks to better cross-cutting knowledge across different areas of security and diverse disciplines, included social sciences and humanities, enhanced implementation of the research and innovation cycle and improved uptake at all levels of society."*

Under each Destination, before the texts of the topics themselves, there is an important introductory part that explains the relevant policy objectives, that specifies any elements to be taken into account for all the topics of the Destination -including international cooperation- and that identifies specific expected impacts. Proposals should set out a credible pathway to contributing to those specific expected impacts.

International cooperation

Security research under Cluster 3 requires a specific approach towards international cooperation to achieve the right balance between the need to exchange with key international partners (including with relevant international organisations) while at the same time ensuring the protection of the EU security interest and respecting the need for open strategic autonomy in critical sectors.

Within the Destination 'A Disaster-Resilient Society for Europe' there is an established culture of comprehensive collaboration with third countries under the different security research programmes, taking due account of the trans-national dimension of different natural and man-made hazards and their drivers (such as climate change). Cooperation can include sharing knowledge, experiences, expertise and mutual learning on disaster-risk management.

As for the Destinations relating to protecting against crime and terrorism, to border management, to infrastructure protection and to cybersecurity, international cooperation is explicitly encouraged only where appropriate and specifically supporting ongoing collaborative activities. Due to the sensitive nature of most projects in those areas and the obvious interest of the EU to ensure confidentiality of projects results, as well as maintaining the ability to maintain strategic autonomy in critical domains of security, such explicit cooperation will need to be assessed at the level of topics and limited to selected international partners only. In line with the overall strategic approach to Research and Innovation policy, cooperation would need to be based on reciprocity and contribute to wider strategic goals of the EU.

Destination – Better protect the EU and its citizens against Crime and Terrorism

Relevant Cluster 3 Expected Impact:

"Crime and terrorism are more effectively tackled, while respecting fundamental rights, thanks to more powerful prevention, preparedness and response, a better understanding of human, societal and technological aspects of crime, and the development of cutting-edge capabilities for law enforcement agencies, including measures against cybercrime."

The main purpose of this destination is, among other, to significantly contribute to the implementation of the **Security Union Strategy** that is to explicitly include Research and Innovation as one of the main building blocks enabling the achievement of the overall policy objectives. As such, the topics in this destination aim at fully addressing all the key issues underlined in the Strategy. In addition, this destination touches upon the security dimension of the **New Pact on Migration and Asylum**, notably the issues related to criminal networks. More specifically, this destination includes research topics aiming at fighting crime and terrorism more effectively, particularly through better prevention of crime and enhanced investigation capabilities notably as concerns cybercrime, as well as at a better protection of citizens from violent attacks in public spaces, through more effective prevention, preparedness and response while preserving the open nature of such spaces. This destination will develop the knowledge and technologies to be taken up by the Internal Security Fund, as a complementary instrument that will enable exploitation of research results and final delivery of the required tools to security practitioners.

The goal of this destination is to bring improved prevention, investigation and mitigation of impacts of crime, including of new/emerging criminal modi operandi (such as those exploiting digitisation and other technologies). This needs to be based on a deeper knowledge of human and social aspects of relevant societal challenges, such as child sexual exploitation, violent radicalisation, trafficking of human beings, disinformation and fake news, corruption and cyber criminality, including support to victims. Research can further help to transpose such knowledge into the operational activities of European Law Enforcement Agencies (LEAs), i.e. European public agencies responsible for the enforcement of the law, as well as civil society organisations.

Research and innovation will support LEAs in better tackling crime, including cybercrime, and terrorism as well as different forms of serious and organised crime (such as smuggling, money laundering, identity theft, counterfeiting of products, trafficking of illicit drugs and of falsified/substandard medicines, environmental crime or illicit trafficking of cultural goods) by developing new technologies, tools and systems (including digital tools, e.g. artificial intelligence, interoperability solutions, etc.). This refers especially to capabilities to analyse in near-real-time large volumes of data to forestall criminal activities, or to combat disinformation and fake news with implications for security.

In addition to improved knowledge, preparedness, prevention and response, projects within this destination will deliver operational tools for enhanced criminal investigation capabilities for

LEAs. This covers a broad range of activities from forensics, big data management to the investigation of cybercriminal activities, improved cross-border cooperation and exchange of evidence.

With regards to CBRN-E threats, research and innovation within this destination allows, among others, to generate knowledge for counterterrorism on the continuously evolving methods related to dangerous chemicals, contaminants and unknown substances, and the development of technologies to counter and respond to related incidents.

Furthermore, this destination aims at improved security of public spaces and public safety, while at the same time preserving the open nature of urban public spaces. All measures to be explored by research and innovation in this area should ensure that citizens can continue their daily lives without major intrusions. To achieve higher security for public space, research in this destination will identify concepts for prevention, preparedness and response of urban actors (city authorities, law enforcement authorities, public/private service providers, first responders and citizens) in response to threats of terrorist attacks in public spaces. Technological innovations can be used to design/improve public spaces to be more secure, also with the help of advanced vulnerability assessments. They can increase the capacity to protect spaces against attacks with manned or unmanned vehicles and can help to detect firearms and other weapons, as well as CBRN-E materials being brought into public spaces. In case attacks cannot be prevented, enhanced effectiveness of mitigation measures including through strategies to reduce vulnerability and strengthening the resilience of possible targets have the potential to reduce the potential impacts of such attacks. Advanced data analysis in real time can critically reduce the time-to-react for first responders.

This destination will also promote, whenever appropriate and applicable, the proposals with:

- the involvement of the LEAs in their core,
- a clear strategy on how they will adapt to the fast-evolving environment in the area of fight against crime and terrorism (evolution of related technologies, evolution of criminal modi operandi and business models related to these technologies, etc.),a minimum-needed platform, i.e. tools that are modular and can be easily plugged into another platform (in order to avoid platform multiplication),
- tools that are developed and validated against practitioners' needs and requirements,
- a robust plan on how they will build on the relevant predecessor projects,
- the (active) involvement of citizens, voluntary organisations and communities,
- education and training aspects, especially for LEAs and other relevant practitioners, as well as information sharing and awareness raising of the citizens,
- a clear strategy on the uptake of the outcomes, defined in consultation with the involved stakeholders,

- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

The destination will also create opportunities for collaboration on research and innovation among different communities of practitioners operating in the area of fighting crime and terrorism, such as police, border and coast guard authorities, and customs authorities. International cooperation is also encouraged where appropriate and relevant.

Proposals for topics under this destination should set out a credible pathway to contributing to better protect the EU and its citizens against crime and terrorism, and more specifically to one or several of the following impacts:

- Modern information analysis for Law Enforcement, allowing them to efficiently fight criminals and terrorists who use novel technologies;
- Improved forensics and lawful evidence collection, increasing the capabilities to apprehend criminals and terrorists and bring them to the court;
- Enhanced prevention, detection and deterrence of societal issues related to various forms of crime, including cybercrime, and terrorism, such as violent radicalisation, domestic and sexual violence, or juvenile offenders;
- Increased security of citizens against terrorism, including in public spaces (while preserving their quality and openness);
- Improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime;
- More secure cyberspace for citizens, especially children, through a robust prevention, detection, and protection from cybercriminal activities.

The following call(s) in this Work Programme contribute to this Destination:

CALL FCT 2021:

Proposals are invited against the following topic(s):

Area FCT01 - Modern information analysis for Law Enforcement

FCT01-1.2021 (RIA) – Terrorism and other forms of serious crime countered using travel intelligence

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- European Law Enforcement Agencies benefit from better, modern and validated tools and training curricula on the use of travel intelligence to prevent, detect and investigate terrorism and other forms of serious crime (e.g., child sexual exploitation, drugs, human trafficking);
- European common approaches are made available to policy-makers and security practitioners for analysing risks/threats, and identifying and deploying relevant security measures while exploiting travel intelligence information, which take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy, protection of personal data and free movement of persons;
- Improved support in shaping and tuning of regulation on travel intelligence by security policy-makers;
- Improved understanding of the capacity and usefulness of travel intelligence in tackling terrorism and other forms of serious crime, and of the key challenges related to it.

Scope:

Travel intelligence is intended here as all the information available in different systems and databases related to travellers. In particular, the research should focus on Passenger Name Record (PNR) and Advance Passenger Information (API) data, but the use of other data available in the context of the interoperability should also be envisaged.

PNR is information provided by passengers and collected by airlines, for enabling reservations and carrying out the check-in process. It may contain, for example, dates of travel, travel itinerary, ticket information, contact details, travel agent, means of payment, seat number and baggage information. As such, PNR is an important law enforcement tool allowing to prevent, detect and investigate terrorism and other forms of serious crime, such as drugs, human trafficking, child sexual exploitation and others.

API is commonly understood as the information of a passenger collected at check-in or at the time of online check-in. API information includes biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their travel.

Research is needed on methods to facilitate the data collection and their quality check as well as to combine different data sets, to sift through (and learn from) vast amounts of data for risk analysis, and to streamline the identity management of passengers, while taking care of the data protection and fundamental rights. Whereas, for instance, the blockchain technology is already being used in the logistics and supply chain management processes with promising results, there is little or no knowledge and or evidence whether this technology could significantly improve customs/law enforcement passenger targeting capacity. The issue of having representative data sets for training and testing should be addressed as well. Namely, proposals should take into account the sensitivity of the travel intelligence data and which competent authorities are entitled to request or receive these data. An added value of the proposals would be to have some of these authorities actively involved in their consortia. Research and innovation activities could be conducted utilizing various technological approaches (such as - but not limited to - Artificial Intelligence, neural networks, Big Data analysis, blockchain technology, etc.) as long as the developed solutions deliver the expected improved capabilities. The use of pseudonymisation techniques, rendering personal data unreadable yet searchable, should also be envisaged. Synergies with successful proposals from topic FCT01-4.2021 (on training and testing data issue as well as on pseudonymisation techniques) should be envisaged. Proposed research that could also link with security research for border management (for example, border checks) would be an asset.

FCT01-2.2021 (RIA) – Lawful interception using new and emerging technologies (5G & beyond, quantum computing and encryption)

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

- European Law Enforcement Agencies benefit from better, modern and validated tools and training curricula to anticipate and cope with new and emerging technologies (notably 5G and beyond, as well as application-level communication*,* quantum computers and potential of quantum technology to encrypt communications) and facilitate their (specialised) daily work on prevention, detection and investigation of criminal and terrorist offences;
- European common approaches are made available to policy-makers and security practitioners for analysing risks/threats, and identifying and deploying relevant security measures while performing lawful interception in this new age, which take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy, protection of personal data and free movement of persons;
- Improved support in shaping and tuning of regulation by security policy-makers on lawful interception in case of new communication capabilities abused by criminals and terrorists, including on procedures and rules for the exchange of data retrieved from the lawful interception between Member States and on international scale, taking into account the court-proof nature of the evidence;
- Increased law enforcement contribution to standardisation activity in relation with lawful interception and access to digital evidences, by fostering a European approach to the challenges posed by new technologies in the field of communication for the police and the judiciary;

- Improved understanding of the capacity and usefulness of lawful interception in tackling terrorism and other forms of crime, and of the key challenges related to its capability to cope with new and emerging technologies.

Scope:

Software-based communication technologies such as 5G and beyond will bring many benefits but also pose a number of new challenges for the police and the judiciary. In particular, lawful interception systems will have to adapt to the increased use of encryption including end-to-end encryption, to edge computing that might limit the availability and accessibility to relevant data and to slicing technology that will multiply the number of virtual operators. In addition, high bandwidth access networks pose the challenge for law enforcement and the judiciary to be able to cope with tremendous amount of data and will accelerate the switch to application level communication that are commonly used by criminals. Finally, quantum computers could break current encryption standards, as well as be used to develop new ways of encrypting communications for illicit purposes, making them impenetrable to interception. Thus, there is a strong need to adequately tackle challenges for law enforcement stemming from all these emerging developments as well as to make sure that lawful interception keeps track with these evolutions, respecting applicable legislation and fundamental rights such as personal data protection and privacy. Activities proposed within this topic should address LEAs' lawful interception challenges related to both software based technologies of communication including 5G (and beyond) and quantum computers in a balanced way.

FCT01-3.2021 (RIA) – Disinformation and fake news are combated and trust in the digital world is raised

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- European Law Enforcement Agencies, other relevant practitioners and (social) media organisations are provided with better, modern and validated tools and training materials to tackle those activities related to disinformation and fake news that are considered as crime or could lead to a crime and that are supported by advanced digital technologies;
- European common approaches are made available to policy-makers and security practitioners for analysing risks/threats, and identifying and deploying relevant security measures related to disinformation and fake news, which take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data;

- Improved support in shaping and tuning of regulation on disinformation and fake news by security policy-makers, including on standardising evidence collection and harmonising procedures in the investigation of cross-border crimes;

- Improved understanding of the cultural and societal aspects of disinformation and fake news, as well as on the key challenges related to combating it;

- Strengthened key personnel's knowledge regarding disinformation campaigns;

- Enhanced perception of security thanks to an increased awareness of the citizens about the value of verified and trustworthy data sources and their content, obtained through education and training materials on trustable sources of information.

Scope:

Combating disinformation and fake news with implications for security is an important aspect where modern information analysis is needed. Bots are increasingly used to manipulate the public opinion and spread fake news on the internet. Causing a mass panic by spreading fake news is one example. Dimensions of this problem increase even more in crisis situations, such as the COVID-19 lockdown, where spreading disinformation and fake news, by infusing uncertainty and fear, aims at harming people's life, intensifying the crisis situations, weakening the European societies and aggravating the divisions. This topic asks for an interdisciplinary research both on societal capabilities to withstand such a threat (e.g., education on trustable sources of information, research on the impact of uncertainties caused by disinformation on public crisis management and society overall) and on technological means of fighting against it. Regarding the latter, for a more effective early detection of criminal activities, LEAs and (social) media organisations need tools and (forensic) capabilities that, e.g., enable the assessment of the origin, veracity and trustworthiness of digital content by identifying altered or fake generated information. In the European context, this also implies that the tools should have various functionalities such as: identification of non-human originated content via origin and activity, detection of machine-generated text in various languages, verification of the authenticity of data with a high accuracy (better than human), fast analysis of large amounts of data to pre-filter for faked and/or manipulated content, which can be presented to investigators, etc. Activities proposed within this topic should address both technological and societal dimensions of fighting against disinformation and fake news in a balanced way, including also knowledge about cultural aspects and perception of disinformation (including trustworthiness of sources) among citizens.

Synergies with the topic in Cluster 2 on democratic processes are welcome.

FCT01-4.2021 (IA) – Improved access to fighting crime and terrorism research data

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- The relevant community (researchers, practitioners, industry, policy makers) is made aware of the legal, ethical and technical pre-requisites that a European common research training and testing data repository in the area of fighting crime and terrorism should fulfil (e.g. by defining, e.g. how it should be organised, which characteristics it should have) while taking into account ethical rules of operation and fundamental rights (including privacy and data protection) as well as cost-benefit considerations which must be made in the context of proportionality in strict sense (as a step to assess the lawfulness of a measure interfering with the fundamental rights);
- Improved anonymisation and pseudonymisation technologies, including other security measures, such as masking and unmasking technologies to facilitate data management in this context, ensuring full access to the data actually needed (in line with the necessity and proportionality principle), taking into account all applicable legislation and fundamental rights.

Scope:

The lack of realistic, up-to-date and sufficient training and testing data for research purposes has been regularly raised by the projects working in the area of fighting crime and terrorism (FCT), to the extent that such data are necessary instead of dummy and synthetic data. Namely, the accuracy of tools, notably (but not only) digital ones, depends heavily on the quantity and on the quality of the training and testing data, including the quality of their structure and labelling, and how well these data represent the problem to be tackled.

This issue is generally present in any research area, but it gets more emphasized in the, e.g., security, health or defence domain due to the special categories of data involved and the sensitivity of the domain, which calls for additional requirements to access to real datasets or the creation of representative datasets at a national level.

In EU-funded projects, in the area of FCT, the problem of having a scientifically satisfactory amount of up-to-date high-quality and realistic data needed to develop reliable (digital and non-digital -e.g., detection and/or qualification of explosives, drugs, DNA traces) tools in support of Law Enforcement Agencies (LEAs) becomes even more complex. Namely, training and testing data sets considered legal and used in one Member State have to be shared and accepted in other Member States, while simultaneously observing fundamental rights and substantial or procedural safeguards.

Another problem that is often encountered is a lack of trust between researchers and law enforcement community, as well as between different projects when it comes to data sharing. To this end, it is important to break down barriers between projects and keep on passing the message that the projects should not be competing to outperform each other, but working together to provide the EU with the best possible solutions. As a pre-requisite for all the above, there is a need to have a common research data repository.

The aim of this topic is to tackle this multi-layered issue and set the basis for such a common data repository by creating a roadmap consisting of a clear set of rules, conditions and characteristics that such a repository should have, be it the variety of the data in function of the type and of the problem at hand, legal issues, accessibility levels related to the sensitivity of various data sets, harmonisation of data formats, solutions for annotation as well as for the aging of the data, etc.

As an integral part of proposed activities, apart from the above sets of requirements, technical solutions should be developed that could help research activities comply with privacy and data protection requirements when handling data, while being able to extract information if needed. Namely, as learnt from the previous research activities, standard pseudonymisation and anonymisation methods are not satisfactory in this domain, as they, e.g., either break the links between different pieces of evidence or take a lot of time and effort. Thus, new and/or improved anonymisation and pseudonymisation technologies, including other security measures, such as masking and unmasking technologies should be developed to facilitate data management ensuring full access to the data actually needed (in line with the necessity and proportionality principle), in full respect of fundamental rights and applicable legislation.

Although proposed activities should focus on the research data for fighting crime and terrorism within the remits of Horizon Europe regulation (including ethics), a broader view of data interoperability related to other security research areas would be an added value.

Synergies with the successful proposals from topic SU-AI02-2020 (on AI research datasets) and future successful proposals in FCT01-1. 2021 (on travel intelligence training and testing data for research purposes as well as on pseudonymisation techniques), FCT02-2.2022 (on ground-truth data sets for conventional forensics) and FCT02-3.2022 (on common data formats) should be foreseen.

Area FCT02 - Improved forensics and lawful evidence collection

FCT02-1.2021 (RIA) – Modern biometrics used in forensic science and law enforcement

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

- Use of modern, robust, validated and reliable biometric technologies by forensic institutes and law enforcement, improving European investigation capabilities to fight terrorism and other forms of serious and organised crime;

- Shorter court cases due to the availability of more solid (cross-border) forensic evidence that is acceptable in court;

- Policy-makers and security practitioners benefit from European common approaches for analysing risks/threats, and identifying and deploying relevant security measures while exploiting biometric information, which take into account legal and ethical rules of operation, the procedural differences in the creation of biometric information, cost-benefit considerations, as well as fundamental rights such as privacy, protection of personal data and free movement of persons;

- Improved support to policy-making on the use of biometric technologies by forensics institutes and LEAs;

- Improved understanding of the capacity and usefulness of biometric technologies information in tackling terrorism and other forms of serious and organised crime, and of the key challenges related to it, such as harmonisation/standardisation of data and processes;

- Contribution to the development of European standards for the handling and processing of biometrics in the context of judicial investigation;

- Forensic practitioners active in biometrics are provided with modern education and training curricula.

Scope:

Biometric technologies allow for a person to be recognised to a certain degree based on a set of features. These features can be more (e.g., fingermarks) or less (e.g., shoemarks) distinctive. In many cases, biometric technologies provide a crucial support to forensic investigation and as well as evidence in court. However, the full extent of their potential is not yet exploited. A wider use of these technologies by forensic institutes and LEAs in the European context and in harmonised way is needed, respecting applicable legislation and fundamental rights such as personal data protection and privacy. Thus, biometrics deserves a special research attention, which should include some of the following: 1) automation and scalability of the identification, identity verification, intelligence, investigation and evaluation processes; 2) robustness and validation of biometrics in forensic conditions; 3) biometric data protection and privacy; 4) harmonisation/standardisation of data and processes and conversion of existing biometric tool for use in the judicial system; 5) usage of biometrics in smartphones and other devices, including the possibility to unlock criminal’s devices using biometric data; 6) exchange of biometric data and interoperability of the systems, and risk of direct adoption of existing biometric tool for use in the judicial system.

The issue of training and testing data has to be tackled as well. One of the key priorities here consists in the need for forensic tools to combat organised crime and smuggling, with the aim of increasing crime investigation through more efficient detection, as well as intensifying prosecutions and convictions. Cooperation with the European Network of Forensic Science

Institutes (ENFSI) should be foreseen. Proposed research that could also link with security research for border management (for example, border checks) would be an asset.

Area FCT03 - Enhanced prevention, detection and deterrence of societal issues related to various forms of crime

FCT03-1.2021 (RIA) – Domestic and sexual violence are prevented and combated

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved prevention, detection and investigation of domestic violence and sexual assaults, including collection of court-proof crime evidence, which take into account European multicultural dimension, legal and ethical rules of operation, as well as fundamental rights such as privacy, protection of personal data and anonymity of victims;
- Enriched European common approaches applied by LEAs to fight domestic and sexual violence relying on the synergy of technology, the latest socio-psychological knowledge learned from cases and the field experience of LEAs and entities dealing with victims;
- Novel, safe, lawful and efficient solutions applied by security practitioners and policy-makers to protect victims of domestic or sexual violence, along with a proper assessment methodology to validate the approach;
- Increased awareness of citizens regarding domestic and sexual violence;
- Improved support in shaping and tuning of regulation on domestic violence and on sexual violence by security policy-makers, which also includes GDPR-compliant IT tools in the procedures;
- Improved skills, tools and training curricula for LEAs and civil society organisations to prevent and combat domestic and sexual violence;
- Identification and development of new concepts, innovative approaches and pioneering practices pertaining to alternatives to imprisonment for offenders to reduce recidivism and, therefore, support the fight against crime.

Scope:

Domestic violence keeps on being a persistent crime throughout Europe. However, the ratio of cases that are effectively reported to LEAs is very low. One of the causes of this lack of reporting is the limited protection offered to victims, fear, reluctance of neighbours to intervene by informing the LEAs, lack of awareness whom to turn to, which mechanisms exist, etc. In addition to domestic violence, women are also exposed to the threat of sexual abuse and aggression in many situations off-home. Moreover, the increase of cases of multiple abuse by groups of offenders that record their crimes using mobile devices and then share them by phone or online is a growing concern with a high social impact. In addition, rates of domestic and sexual violence rise when societies are under stress, during, e.g., food shortages, economic crisis, natural disasters, and epidemics.

The COVID-19 lockdown showed that in such a crisis situation the problem of domestic violence gets even more emphasized, both because victims are trapped in their homes with violent partners who are even more stressed than usually, and because the ability of services to help becomes even more limited. Similarly, women who are displaced, refugees, and living in affected areas are particularly vulnerable and exposed to sexual violence; the closure of establishments offering legal sex work because of e.g., epidemics, brings further dangers.

Needs from research, to be performed in a lawful and ethical manner while protecting fundamental rights, such as privacy and protection of personal data, are as follows. Firstly, there is a need to improve current European approaches to fight domestic and sexual violence (prevent, locate, report and collect evidence) using innovative technological solutions, such as by enriching existing risk analysis tools with real-time data obtained through technological means, that will reduce both the amount of human resources to be committed and the response time.

In addition, specifically related to the cases of multiple abuse by groups of offenders that share their crimes through mobile devices or via social media, research is needed to develop innovative technological solutions to find the source of these videos, identify offenders, and find victims.

Moreover, modern and effective awareness raising campaigns need to be developed for LEAs and relevant civil society organisations to pass key messages to potential victims, as well as wide communities, while taking into account European multicultural dimension.

Last but not the least, research efforts are needed to modernise and develop novel approaches to support victim assistance services of LEAs and relevant civil society organisations in providing efficient protection and help to victims. As both technological and societal developments are expected, the consortia should consist in IT specialists, LEAs, relevant civil society organisations, sociologists, social workers and psychologists. If possible, taking into account their right to anonymity, their dignity and rights, victims could be involved as well, through relevant civil society organisations that have the safeguards in place to protect them.

Evolutions in domestic and sexual violence, such as their increase during any type of emergency, e.g., epidemics, should be taken into account too. Methods for evaluating proposed solutions should be developed as well. All developed solutions should be accompanied by corresponding training curricula for LEAs and relevant civil society organisations. Proposals are expected to address both identified sub-topics, domestic violence and sexual violence, in a balanced way.

Area FCT04 - Increased security of citizens against terrorism, including in public spaces

FCT04-1.2021 (RIA) – Improved preparedness on attacks to public spaces

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved vulnerability assessments by law enforcement and local managers of public spaces with a specific focus on countering and/ or preventing terrorist attacks or other forms of severe violence (amok, mass-riots), including attacks with explosives;
- Better identification of specific vulnerabilities and elaboration of mitigation strategies by security practitioners and policy-makers due to the possibility to simulate attack-scenarios in any public space in realistic conditions and to test and train different prevention and response measures;
- Improved training of Law Enforcement Agencies in collaboration with different public and private actors (e. g., crisis management and civil protection authorities, fire brigades, regulatory agencies, emergency health services, private security companies, etc.) to enhance their preparedness to attacks on public spaces;
- Enhanced planning capabilities of security practitioners and policy-makers due to the identification of potential vulnerabilities connected to the design/refurbishment and construction/improvement of different public spaces and measures to reduce them by implementing a comprehensive security-by-design approach in urban planning (also including aspects of social inclusion).
- Enhanced modelling capabilities of security practitioners, policy-makers and research institutions due to the identification of potential vulnerabilities connected to the different public spaces, analysis of crowd behaviour and possible emergence of various threats to security in order to minimize possible threats and vulnerabilities and supporting planning of respective resources and activities.

Scope:

Public spaces such as squares, sport venues, shopping districts, places of worship or touristic attractions have been the target of numerous terrorist and other violent attacks causing significant loss of lives and causing societal insecurity as well as economic losses. The means to carry out such attacks from one or several attackers range from sophisticated and well-planned scenarios including several attackers using explosives and firearms, up to so called low-cost attacks making use of everyday goods such as cars, axes and kitchen knives. Such attacks have proven to be very difficult to prevent and quick-reaction and preparedness to respond are the crucial elements in reducing their impact.

The EU and its Member States have reacted to this challenge in the framework of its Action plan to support the protection of public spaces and the respective staff working document Good practices to support the protection of public spaces[3]. Vulnerability Assessments (VA) are an established tool for example in the area of the protection of critical infrastructures. Their aim is to identify the inherent vulnerabilities of a specific target and thus to be able to put in place appropriate mitigation measures. Such assessments are used in public spaces already by Law Enforcement Agencies in case of large-scale events, official visits or as part of forward-looking city planning activities. The impact on the quality and openness of public spaces should however be minimised as much as possible.

What is missing so far is a capability for security authorities, private security organisations and local authorities to conduct VA with the help of most advanced technological means. Tools for large-scale urban VA should be able to simulate realistic scenarios in any public space of different urban areas and give the users the possibility to test different prevention and response measures. They should further give the possibility for cooperation of the main public and private actors (e. g., crisis management and civil protection authorities, fire brigades, regulatory agencies, emergency health services, private security companies, etc.), and the development of tailor-made trainings. Continuing updates of the tools with the data of new urban areas, new modes of attacks and different scenarios would ensure that such capability is of long-term use and able to adapt to new developments. At the same time, such platforms could provide support in planning processes of public spaces in case of new constructions, or re-design in order to avoid creating vulnerabilities and supporting a security-by-design approach, similar to what exist already for safety.

Area FCT05 - Organised crime prevented and combated

FCT05-1.2021 (RIA) – Fight against trafficking in cultural goods

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved intelligence picture and understanding of mechanisms behind organised crime activities related to trafficking of cultural goods both offline and online, modus operandi, possible nexus with terrorist financing;
- Enhanced ability of security practitioners to identify organised crime networks involved in trafficking in cultural goods and to detect their illicit business models, including financial aspects and money laundering activities in this sector;

[3] Reference to be added

- Enhanced ability of security practitioners to detect and prevent the emergence of organised crime networks involved in trafficking in cultural goods, and to respond to the threat of existing organisations;

- Improved and validated tools, skills and training materials (including the lawful court-proof collection of crime evidence) for European LEAs and Border Guards and customs Authorities to tackle criminal activities related to trafficking of cultural goods;

- Improved cooperation between European LEAs and Border Guards and customs Authorities, as well as with specialised researchers and international actors, in tackling this form of crime;

- Improved databases on stolen/trafficked cultural goods;

- Improved evidence-based policy-making against trafficking of cultural goods.

Scope:

Trafficking in cultural goods has become one of the most profitable criminal activities for organised crime groups and the booming art market is creating new business models for organised crime. The art market is at the same time also one of the least regulated markets in Europe, characterised by a lack of traceability and speculative pricing of the objects, rendering it an ideal place also for money laundering, tax evasion, etc.

Building on the results of recently completed projects, the nexus between terrorism and serious and organised crime (including cyber) deserve to be analysed further. The involvement in serious and organised crime may as well allow terrorists to generate funds to finance terrorism-related activities, as it is the case in trafficking of cultural goods. "Blood antiquities" are, unfortunately, nothing new: works of art are looted in war zones as well as in regions not experiencing conflict, and then sold to wealthy collectors and antiquities dealers in Europe. Research has shown that crimes related to cultural goods may be conducted by organised crime groups in order to generate profit or to launder illegally acquired funds. Despite the seriousness of this issue, fundamental questions remain: How are these precious items secretly transported and what facilitates their illicit movement? What are the relations with other types of crime? How much does the trafficking of cultural goods bring in? What is the role and extension of online markets and social networks in supporting trafficking (e.g., discussion groups where looters and intermediaries exchange tips and tricks to circumvent police checks)? How can a stolen work be identified? How should the information be stored in accessible databases? What are reliable and ethical ways to gather and share information about this type of crime? What is the relationship between organized crime and the open market for cultural goods (the “grey” market)? What roles do museums and other cultural institutions (unwittingly) play in this trade? And - who defines what is an antiquity and to whom it should belong? Evidence-based research is needed to answer these questions, and to support the development of targeted and effective anti-trafficking policy.

The proposals in this topic should shed a light on these issues through robust research methodologies that prioritise new data collection and analysis, and applications towards the development of evidence-based policy. Proposals should support the gathering of intelligence and the development of tools that law enforcement needs to fight this crime and to collect actionable (cross-border) evidence acceptable in court, with the ultimate goal of disrupting the illicit trade and of mitigating its harmful effects in Europe and beyond.

Activities proposed within this topic should address the issue from various angles, combining both social research with technological development and applications in a logical manner. Proposals should also include research into the international dimensions of the trafficking of cultural goods, as well an as investigation of the possible connections between this and other forms of crime. LEAs, Border Guards and customs Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime.

Synergies with projects funded under FCT05-2.2021, FCT05-3.2021, FCT05-4.2022, FCT05-5.2022, FCT05-6.2022 and FCT05-7.2022 should be envisaged. Proposed research that could also link with security research for border management (for example, border checks) would be an asset. If relevant, the proposed activities should attempt to complement the objectives and activities of the EU Policy Cycle (EMPACT) – Priority Organised Property Crime.

FCT05-2.2021 (RIA) – Fight against organised environmental crime

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved intelligence picture of organised environmental crime in Europe, modus operandi of such criminal organisations, both offline and online;
- Improved tools and innovative training curricula for European LEAs and Border Guards Authorities, validated against practitioners' needs and requirements, to help them tackle criminal activities related to environmental crime, supported by advanced digital technologies and including the lawful court-proof collection of crime evidence as well as environmental crime statistics;
- Improved cooperation between European LEAs, Border Guards Authorities and other national Authorities involved in tackling this form of crime, including on goods not released for free circulation (e.g. in transit, warehousing etc.);
- Improved cooperation with third countries and international actors involved in the fight against environmental crime;
- Enhanced ability of security practitioners to identify and prevent emergent and existing organised crime networks involved in environmental crime;

- Increased ability of public services to detect places of illegal waste storage;
- Improved shaping and tuning of regulation related to the fight against environmental crime by security policy.

Scope:

Environmental crime breaches environmental legislation and causes significant harm or risk to the environment, climate and/or human health. Environmental crime is highly lucrative, but the sanctions are low, and it is often harder to detect than more traditional forms of organised crime. These factors also make it highly attractive for organised crime groups. These crimes present a high risk for the environment, climate and health, and are very harmful to society as a whole. The extent of the problem is clearly demonstrated by waste trafficking, which is characterised by the clear interconnection between criminal actors and legal businesses.

Nowadays waste traffickers operate along the entire waste-processing chain, rely on the use of fraudulent documents and group with other types of organised criminal activities. LEAs need new means, both technological and intelligence-based, to prevent and combat illegal environment-related activities, such as illegal waste dumping, waste trafficking and the illegal trade of refrigerants including ozone depleting gases and hydrofluorocarbons (HFCs). Research activities are needed to support LEAs in finding polluting substances intentionally dumped in land and water (by, e.g., developing or improving existing technologies able to differentiate such substances from non-pollutant components, possibly involving remote sensing approaches), in detecting hazardous waste (e.g., fuel or electronic equipment), and in having a complete intelligence picture of this type of crime (such as modus operandi of the crime organisations involved in this type of crime, both offline and online).

The illegal trade of ozone depleting gases and HFCs also remains a significant obstacle to international efforts seeking to limit the worst impacts of climate change. Here, smuggling activities using in particular the custom transit procedures need to be addressed. Furthermore, one of the main issues with understanding the scale and specific issues are problems in developing comparable EU crime statistics. Therefore, activities proposed within this topic should address both the technological and societal dimensions of environmental crime in a balanced way, as well as the needs of LEAs. Connections with other forms of crime should be tackled too, as well as with other forms of environmental crime which, similarly to illegal waste, pose a risk to health and society and are also reflected in Commission regulations – illicit wildlife trafficking, forest fires, illegal timber trade etc.

The International dimension, a crucial element in certain environmental crimes, should be analysed as well, including but not limited to the smuggling processes of illegal waste and refrigerants. Thus, both LEAs and Border Guards Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime. A particularity with environmental crime is the variety of actors involved at national level (inspection authorities, sanitary bodies etc.), so their participation would be welcome in the consortia.

Synergies with projects funded under FCT05-1.2021, FCT05-3.2021, FCT05-4.2022, FCT05-5.2022, FCT05-6.2022 and FCT05-7.2022 should be envisaged. Proposed research that could also link with security research for border management (e.g., border checks) would be an asset. If relevant, the proposed activities should attempt to complement the objectives and activities of the EU Policy Cycle (EMPACT).

FCT05-3.2021 (RIA) – Fight against firearms trafficking

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Contribution to the implementation of the 2020-2024 EU Action Plan on firearms trafficking;
- Improved intelligence picture of firearms trafficking in Europe, modus operandi of such criminal organisations, both offline and online;
- European LEAs, customs and Border Guards Authorities, as well as forensics specialists and prosecutors benefit from modern and validated tools, skills and training curricula (including on the lawful court-proof collection of crime evidence) to tackle criminal activities related to firearms trafficking;
- Harmonised procedures in the investigation of trans-border crimes in full compliance with applicable legislation on protection of personal data;
- Improved cooperation between European LEAs and Border Guards Authorities, as well as with international actors, in tackling this form of crime;
- Strengthened ability of security practitioners to identify organised crime networks involved in firearms trafficking in an early stage;
- Reduced diversion of firearms into criminal hands in Europe;
- Enhanced ability of security practitioners to prevent the emergence of organised crime networks involved in firearms trafficking, and respond to the threat of existing organisations;
- Improved shaping and tuning of regulation related to the fight against firearms trafficking by security policy-makers;

Scope:

Firearms are the lifeblood of organised crime in Europe as well as worldwide. Firearms trafficking is a big enabler of organised crime and terrorism. It is a high-time to fix a new agenda, involving research, by:

1) analysing possibilities for safeguarding the legal market and preventing diversion, notably by developing technological solutions for addressing new threats such as 3D printed firearms, including distribution of blueprints for 3D printing of firearms, clamping of 3D printing machines and of blueprints, and their sale both offline and online (including darknet);

2) improving the intelligence picture in firearms trafficking, in particular by developing technological solutions to enable simultaneous searches/input in the Schengen Information System and Interpol's iArms database, developing solutions to facilitate and approximate a systematic collection on data on all firearms seizures, and developing a European-level tool tracking in real-time all firearms-related incidents or shootings and extracting continuously updated data;

3) increasing knowledge on the legal limitations and room for improvement in police and judicial cooperation in the field of firearms trafficking, developing tools to enable automated cross-border exchange of ballistics information, and exploring how new and emerging approaches (such as, but not limited to Artificial Intelligence) could help improve automated detection of firearms and firearms components through scanning of parcels and containers;

4) improving international cooperation by supporting operational cooperation between the LEAs of the EU and of third countries.

Activities proposed within this topic should address both technological and societal dimensions of the firearms trafficking in a balanced way. Connections with other forms of crime should be tackled too. The international dimension should be analysed as well, including but not limited to the firearms smuggling processes. Thus, both LEAs and Border Guards/customs Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime. Synergies with projects funded under FCT05-1.2021, FCT05-2.2021, FCT05-4.2022, FCT05-5.2022, FCT05-6.2022 and FCT05-7.2022 should be envisaged. Proposed research that could also link with security research for border management (for example, border checks or detection of concealed objects) would be an asset. If relevant, the proposed activities should attempt to complement the objectives and activities of the EU Policy Cycle (EMPACT) – Firearms.

Area FCT06 – Citizens are protected against cybercrime

FCT06-1.2021 (RIA) – Child sexual exploitation prevented

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Increased understanding of security practitioners and policy-makers of the prevalence and of the process leading to child sexual abuse and child sexual exploitation;

- Enhanced understanding of the characteristics and key differences between offending and non-offending Minor Attracted Persons;

- Innovative and effective solutions, including training curricula, are validated and adopted by European LEAs and relevant civil society organisations to prevent, detect and effectively act on child sexual exploitation, both offline and online, by providing necessary assistance to potential offenders, as well as by providing adequate preventative campaigns to reach vulnerable groups;

- Developed cross-culturally validated risk assessment tools for child sexual offenders; Enhanced perception by the citizens that Europe is an area of freedom, justice and security thanks to increased security of children;Improved cooperation between European LEAs and relevant civil society organisations in preventing this form of crime, taking into account fundamental rights;

- Improved evidence-based policy-making related to the prevention of child sexual exploitation.

Scope:

Child Sexual Exploitation (CSE), including the increasing amount of child sexual abuse material (CSAM) detected online as well as the online solicitation of children for sexual purposes, remains a serious threat. During the first wave of the global pandemic of COVID-19 there was an increased online activity in dedicated forums by offenders exploiting opportunities to engage with children who were more vulnerable due to isolation, greater online exposure and less supervision. This further highlighted the importance of CSE prevention, early detection and effective actions, both online and offline. Research is needed to better understand the process leading to offending in all its various forms (e.g. from watching CSAM to sexually abusing a child), i.e. what triggers the behaviour of potential offenders, which approaches in addressing their behaviour work and which not, which profiles of offenders can be generated, etc.

Research is also needed to provide a deeper understanding of the prevalence of these crimes as well as the prevalence of persons with a sexual interest in children. Early or weak signals should be further researched in combination with effective countermeasures and interventions. The solutions should be accompanied by corresponding training curricula for LEAs and civil society organisations when necessary (e.g. when they involve providing assistance to potential offenders or victims). Methods for evaluating proposed solutions should be developed as well. Special care needs to be given to ethics and fundamental rights protection throughout the research and the solutions proposed. The evolving character of the CSE modus operandi should be taken into account in all activities proposed under this topic. The societal dimension should be in the core of proposed activities. In addition to the mandatory involvement of LEAs, the involvement of other relevant practitioners in the consortia - e.g. from civil society organisations, health professionals (psychologists, psychiatrics…), forensic psychologists, criminologists and sociologists - is requested as well.

FCT06-2.2021 (RIA) – Online identity theft is countered

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- European LEAs are provided with modern, innovative and validated tools and training curricula, which take into account legal and ethical rules of operation as well as fundamental rights such as privacy and protection of personal data to prevent, detect and investigate online identity theft, and lawfully collect crime evidence across borders for its use in court proceedings;
- Strengthened ability of security practitioners to identify (new forms of) online identity theft at an early stage thanks to improved knowledge on the modus operandi and new trends in identity theft, including but not limited to deepfakes, and innovative solutions for LEAs to tackle them in lawful manner;
- Improved understanding on the societal aspects and impacts of identity theft, as well as on the key challenges related to it;
- Enhanced perception by the citizens that Europe is an area of freedom, justice and security thanks to innovative awareness-raising campaigns explaining to citizens the key and evolving mechanisms of identity theft and how to protect against them;
- Improved shaping and implementation of regulation related to the fight against identity theft by security policy-makers.

Scope:

The "classical" form of identity theft has been a big business for years and consists in personal and financial data stolen online, sold in the underground economy and misused by criminal organisations all over the world, usually for financial gain. With the technological evolution, identity theft evolves as well. Personal details can be found by hacking computers, but identity thieves are increasingly getting citizens' personal information from social media sites. Furthermore, an on-going improvement of technologies to create deepfake audio and video material may result in novel forms of identity theft. This relatively new but rapidly evolving technology superimposes audio, images or videos over another video or creates new ones. For instance, it can be used among others, to generate new "personalised" child abuse material, to create fake social media accounts in the name of the target person (to harness or stalk them), to place the faces of celebrities on existing pornographic videos, to spread misinformation about a company (leading to financial losses) or a politician or an expert (reputational damage).

Research is needed to develop new technological means of detecting deepfakes in support of LEAs' work, as it may only be a matter of time before deepfakes are used more often in online identity theft cases. In addition, this can have serious implications for law enforcement, since it might complicate investigations and raise questions about the authenticity of evidence. The issue of collecting (cross-border) evidence for its use in courts of law, i.e. in a lawful manner and respecting fundamental rights such as privacy and protection of personal data, should be tackled in proposed activities as well. Other evolving modus operandi and new trends in online identity thefts should be analysed too, and corresponding innovative lawful societal means of preventing as well as innovative lawful technological means of detecting and investigating them should be developed. Thus, activities proposed within this topic should address both the technological and societal dimensions of online identity theft in a balanced way. With the aim of developing effective awareness raising campaigns, involvement of relevant civil society organisations, sociologists and psychologists who can shed a light on the phenomenon of identity theft from the side of victims and how to support them, would be an added value of proposals submitted under this topic.

CALL FCT 2022:

Proposals are invited against the following topic(s):

Area FCT02 - Improved forensics and lawful evidence collection

FCT02-2.2022 (IA) - Improved crime scene investigations related to transfer, persistence and background abundance

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved European common investigation capabilities thanks to modern, robust, validated and reliable solutions, used by forensic institutes and law enforcement for analysing complex crime scenes with various types of trace evidence items;
- Shorter court case thanks to the availability of more solid forensic (cross-border) evidence that is acceptable in court, respecting fair trial requirements;
- Common European approaches are made available to policy-makers and security practitioners for analysing risks/threats, and identifying and deploying relevant security measures while inspecting, gathering and analysing trace substances collected in complex crime scenes, which take into account legal and ethical rules of operation, the traceability of forensic evidence, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data;
- Improved shaping and tuning by security policy-makers of regulation on using innovative solutions in crime scene investigations by forensic institutes and LEAs;
- Improved understanding of the underlying phenomena governing the transfer of material from a surface to another, persistence of material once transferred, recovery process of the material as well as characterisation and expectations regarding the background noise;
- Ground truth datasets accessible to the scientific community to support interpretation at the activity level of transfer of microtraces, biological traces, biometric traces and chemical traces;
- Enhanced evidence collection on crime scene due to an increased use of novel technologies;
- LEAs and Forensic Institutes are provided with innovative methods of biological fluid identification for forensic applications;
- Forensic practitioners and police authorities active in crime scene investigations are provided with modern and innovative training curricula.

Scope:

Nowadays, law enforcement deals with a growing complexity of crime scenes containing various types of trace evidence items that can also present safety hazards for the forensic experts and crime scene investigators. Traditional forensic crime scene analysis typically involves several techniques to inspect, gather and analyse collected trace substances. There is a need to improve these processes and make them more accurate, effective and sensitive in such a complex scenario, by employing modern approaches, for instance (but not limited to) nanotechnology, next generation sequencing or Artificial Intelligence.

A way to modernise forensic science for the professionalisation of crime scene investigations is through improving the understanding of the underlying phenomena governing the transfer of material from a surface to another, persistence of material once transferred, recovery process of the material as well as characterisation and expectations regarding the background noise.

Regarding transfer, persistence and background abundance, two different types of developments are needed: 1) of ground truth datasets accessible to the scientific community to support interpretation at the activity level for transfer of microtraces (paint, glass, soil), biological traces (body fluids, DNA), biometric traces (fingermarks, shoemarks), chemical traces (drugs, explosives, ignitable liquids); and 2) of methods of biological fluid (blood, semen, saliva, urine, etc.) identification for advanced forensic applications. The proposed activities should take into account the European dimension regarding harmonisation of the approach and cross-border acceptance of the collected evidence. A special attention has to be given to applicable legislation, ethics and fundamental rights, as well as to the well-documented use of scientific method to enhance transparency in the establishing of forensic evidence.

Synergies with the successful proposals from topic SU-AI02-2020 (on AI research datasets) and future successful proposals in FCT01-4.2021 (on ground-truth data sets for conventional forensics) and FCT02-3.2022 (on common data formats) should be foreseen. Cooperation with the European Network of Forensic Science Institutes (ENFSI) should be foreseen too.

FCT02-3.2022 (CSA) – Common lexicon and mechanisms for data transfer, storage and security, as well as harmonized data formats

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved European common forensics investigation capabilities and cross-border exchanges thanks to a common, modern lexicon that is used by forensic institutes and law enforcement, validated against practitioners' needs and requirements, to facilitate their (specialized) daily work on investigating terrorism and other forms of serious crime;

- Shorter court cases due to the availability of more solid court-proof (cross-border) forensic evidence;
- Fortified European common approaches for data transfer, storage and security, which would include latest technology developments and allow for adaptations as technologies progress, and which would take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data;
- LEAs and Forensic Institutes are provided with an increased interoperability and improved (cross-border) exchange of data thanks to harmonised data file formats across Europe and data access procedures, which would easily take into account technological evolutions, i.e. be adaptable in time;
- Modern education and training curricula for forensic practitioners and police authorities active in crime scene investigations.

Scope:

With continuous and fast technological improvements, including but not limited to the Internet of Things, new data formats and mechanisms for data transfer, storage and security are and will be developed. In addition, data formats are often not harmonized amongst similar research projects, thus hampering potential interoperability requirements.

Furthermore, in the European context, a critical enabler for an improved collaboration and communication between forensic practitioners is the use of a clear, consistent vocabulary. Such a shared vocabulary would, among others, allow for a common understanding of forensics, improve structured (cross-border) data sharing, and amplify the (cross-border) acceptance of evidence in court. The same applies for mechanisms of data transfer, storage and security. In order to allow for data and evidence exchanges, there is hence a need for a development of a common lexicon, common mechanisms of data transfer, storage and security, and data file format harmonisation within the justice ecosystem.

The activities proposed under this topic should take into account the evolving aspect of forensic technologies, i.e. propose solutions that would be able to adapt to the corresponding changes in time. This topic addresses both digital and non-digital forensics.

Synergies with the successful proposals from topic FCT01-4.2021 (on common data formats), FCT02-2.2022 (on ground-truth data sets for conventional forensics) and FCT02-4.2022 should be foreseen. In addition, where relevant, synergies should be foreseen with actions and results of projects under Justice Programme (2014-2020) under Call JUST-AG-2016-01, Topic JUST-JCOO-CRIM-AG-2016 "Action grants to support transnational projects to promote judicial cooperation in criminal matters", including project EVIDENCE2e-CODEX and The JUD-IT Project (Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring

Efficient Cross-Border Cooperation and Mutual Trust). Operational examples should also be considered, where relevant in line with activities of the Europol SIRIUS Project that has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under grant agreement No PI/2017/391-896. Cooperation with the European Network of Forensic Science Institutes (ENFSI) should be foreseen too.

FCT02-4.2022 (RIA) – Better understanding the influence of organizational cultures and human interactions in the forensic context

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Increased European common forensic investigation capabilities and cross-border exchanges thanks to a better understanding of main organisational cultures and of human interactions in the forensic context, and of the main causes of biases in interpretation and reasoning;
- Strengthened bridges between different actors in an investigative process through an improved non-ambiguous communication and enhanced communication mechanisms at all levels;
- Development of safer justice outcomes through an increased understanding of how human interactions impacts on decisions at all levels of an investigative process;
- Modern and robust methods of reasoning and of experts' decision making in forensic practice, overcoming various types of biases;
- Forensic Institutes and LEAs active in crime scene investigations benefit from innovation education and training curricula.

Scope:

Security research projects related to forensics typically focus only on technologies and data, while the process by which forensic experts evaluate and interpret the evidence is often put aside. However, cognitive methods and human judgement play a significant role as forensic experts observe and interpret the data. By doing this, forensic experts are almost inevitably exposed to irrelevant contextual information (such as suspect's criminal record or ethnicity, a type of the information that can be obtained due to a liaison between a forensic expert and investigators, police and the prosecution), which can potentially cause bias. In contexts where digital technologies are involved in creating forensic outcomes, biases and loss of transparency can also arise from different roles and disciplinary backgrounds of the different actors working on and with the digital tools. Communication between practitioners within the same institute can introduce a bias as well. When exchanging the information cross-border, both organisational cultures and languages can also cause a bias.

Understanding how human interaction, both internally and in the European context, impacts on decisions at all levels of an investigative process is critical for the development of safe justice outcomes. In forensic practice, it is crucial to understand the impacts of various types of biases on interpretation and reasoning, and to develop methods to increase the robustness of reasoning and of experts' decision making. Research is needed to evaluate, develop and enhance methods and cognitive techniques to communicate non-ambiguously in the forensic and legal context, as well as to develop, improve and enhance communication mechanisms between the actors of the criminal justice chain. Synergies with the successful proposal from topic FCT02-3.2022 should be foreseen. In addition, cooperation with the European Network of Forensic Science Institutes (ENFSI) should be foreseen too. For aspects related to digital forensics, cooperation with the European Cybercrime Training and Education Group (ECTEG) should be foreseen.

Area FCT03 - Enhanced prevention, detection and deterrence of societal issues related to various forms of crime

FCT03-2.2022 (RIA) – Enhanced fight against the abuse of online gaming culture by extremists

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Enhanced knowledge on the use of online gaming culture and structure by violent extremists as well as their modus operandi through video game chatrooms, used as their recruitment tools;
- European LEAs benefit from better, innovative and validated tools and training curricula (which take into account legal and ethical rules of operation, as well as fundamental rights such as privacy and protection of personal data) to tackle violent radicalisation through online gaming culture;
- Increased awareness of citizens about online radicalisation through gaming culture;
- Enhanced protection of youth in the gaming environment against recruitment into violent radicalisation;
- Improved shared understanding and cooperation between different actors involved, including security practitioners, gaming industry, social media, video game hosting services and civil society;
- Improved shaping and tuning by security policy-makers of regulation on preventing abuse of online gaming culture by violent extremists.

Scope:

A highly increasingly influencing societal issue related to radicalisation is the online gaming culture. Earlier studies have shown no link between video games and violence. However, terrorism and gaming experts claim that forums and chatrooms are used as recruitment tools. Research is needed to analyse the use of online gaming culture and structure by violent extremists as well as their modus operandi through video game chatrooms and forums.

Regarding video games themselves, an in-depth analysis is needed on how the type of the video game, of its theme, design, aesthetics etc. plays a role in the choice of the chatroom to be used as a recruitment area. As far as video game chatrooms, including social media platforms discussing video games, are concerned, dissemination strategies of violent extremists through them as well as their ways of grooming should be analysed.

Based on the results of these analyses, innovative (societal) means of fighting this type of crime, both online and offline, should be developed. The role of LEAs in this respect should be analysed. Possibilities of detecting and investigating this type of crime should be discussed as well, with a focus on legal and ethical aspects. Modern and effective awareness raising campaigns should be developed, that would target young people, parents, school teachers, video-gaming industry and wide communities, and that take into account the European multicultural dimension. Methods for evaluating proposed solutions should be developed as well. Suggestions to gaming industry on which traps to avoid when designing and upgrading a video game should be provided too.

Proposed activities should take into account the evolving nature of this type of crime and of technology, and be performed while respecting the applicable legislation and fundamental rights, such as privacy and protection of personal data. Societal dimension should be in the core of proposed activities, with a support of technologies. The consortia should consist in LEAs, representatives of gaming industry, gaming experts, IT specialists, (cyber) psychologists and sociologists. Participation of relevant civil society organisations or gaming communities would be an added value.

Area FCT04 -Increased security of citizens against terrorism, including in public spaces

FCT04-3.2022 (CSA) – Public spaces are protected while respecting privacy and avoiding mass surveillance

Expected Outcomes: Projects’ results are expected to contribute to the following outcomes:

- Improved understanding by local authorities, operators and policy makers of the effect of large-scale surveillance of public spaces on the behaviour of citizens and possible negative effects on local communities;

- Enhanced transparency for citizens on different forms of surveillance by law enforcement, local authorities and private actors in public spaces, and increased awareness of applicable rights towards operators of such systems;

- Improved protection of public spaces without the need for 24/7 data collection and storage;

- Set of common standards and good practices by local authorities, operators and policy makers for internal access restriction, anonymization and data minimization allowing a proportionate use of already installed surveillance-systems (such as CCTV) in public spaces, reducing the risk of misuse of collected data and respecting fundamental rights, especially the protection of personal data.

Scope:

In recent years, the number of different tools for the surveillance of public spaces has been growing at massive pace in most European cities. CCTV-systems in public spaces are the most evident examples. They have been expanded in terms of quantity (number of CCTV in public spaces, such as squares, streets or touristic sites), quality (improved solution of images, possibility of tracking and automatic pattern-recognition) and also scope (CCTV present in areas like parks, 24/7 recording as standard due to higher data storage capacities).

CCTV-systems are the most evident and visible, although by far not the only ones. Acoustic sensors, Automatic Number Plate Recognition (ANPR) and in the future possibly widespread facial recognition add to a system of sensors that cover large parts of public spaces in many European cities.

While evidence suggests that such tools can help to combat certain forms of crime an increase the perceived security of citizens, the significant expansion of areas that are monitored risks to create negative effects for the right for privacy. Scientific studies indicate that also legal forms of behaviour are adapted by persons, which are aware that they are monitored by surveillance systems. Furthermore, there is evidence that such systems are often concentrated in socially deprived districts, creating the risks of stigmatisation of its residents.

In terms of crime prevention there are indications that for many settings, sensors like CCTV are in the best case only part of a solution and they can create a tendency of reducing personnel on the ground, thus limiting the possibilities for classical policing and reducing the direct interaction between local police and public order services and the citizens. Such interaction is however key to address crime prevention and response to criminal threats in a holistic manner.

The quantitative growth of both public and private surveillance has led to the fact that nowadays, citizens are hardly able to keep track of where their data has been captured and thus not able to make us of their rights as guaranteed by applicable legislation, such as the GDPR. While citizens as subjects of the surveillance are becoming transparent towards public and private operators of surveillance, the operators themselves remain in many cases inaccessible and few technological innovations are used to make sure only relevant data is stored and processed.

While significant industry and research resources are invested in the design of new and the upgrading of existing surveillance systems for public spaces, innovation could be stimulated to look for alternatives. Such alternative could identify means to protect public spaces though enhanced interaction with local communities, re-design sensors as to ensure they capture data in the most proportionate way, increase transparency for citizens towards public and private operators o surveillance systems and finally explore privacy-friendly technological features to ensure that only relevant data is kept, processed and accessible by authorised actors. Synergies with the topic in Cluster 2 on trust in democracy being restored are welcome.

Area FCT05 - Organised crime prevented and combated

FCT05-4.2022 (RIA) – Effective fight against organised cargo crime

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved and complete intelligence picture of security practitioners and policy-makers on organised cargo crime, such as modus operandi, both offline and online, including cross-border dimension, trade of stolen goods, new trends;
- Enhanced ability of security practitioners to identify organised crime networks involved in cargo theft;
- Fortified ability of security practitioners to detect and prevent the emergence of organised crime networks involved cargo theft, and respond to the threat of existing organisations;
- Improved policy-making related to the fight against cargo theft;
- European LEAs and Border Guards and customs Authorities are provided with better, modern and validated tools (including the lawful court-proof collection of crime evidence) and training materials to tackle criminal activities related to organised cargo crime;
- Enhanced ability of security practitioners to curtail the fencing of stolen property;

- Improved strategies of cooperation between transport and logistic operators, European LEAs and Border Guards Authorities in fighting organised cargo crime and dismantling these criminal networks.

Scope:

Organised property crimes, as a highly visible category of crime, most often committed by cross-border organised criminal groups, cause feelings of insecurity among citizens. These crimes are typically conducted by mobile organised crime groups that exploit diaspora communities in Member States to create networks of contacts, typically carry out a significant number of offences in a region over a short period and then move on to another region. They still mostly operate offline while preparing the crime, but the trade of stolen goods is increasingly taking place on online marketplaces.

Cargo crime, a type of the organised property crimes, hits record levels in Europe. The organised criminal groups involved in cargo crime typically target high-value products (e.g., tobacco, alcohol, electronics, and pharmaceutical products). These crimes range from thefts from trucks at parking sites to violent crimes such as high-jacking and robberies. European industry loses billions to cargo theft each year.

Thus, there is an urgent need to have a complete intelligence picture, such as the modus operandi, cross-border dimension, new trends etc., as well as to analyse existing and propose innovative societal and technological measures and approaches to tackle this type of crime, including prevention, detection, disruption of the business model, as well as lawful investigation of both offline and online trade of stolen goods, together with the collection of cross-border court-proof evidence. Relations with other types of crime should be explored too.

Activities proposed within this topic should address both technological and societal dimensions of organised cargo crime in a balanced way, taking care of the applicable legislation. International dimension should be analysed as well, such as networking and smuggling processes. Thus, both LEAs and Border Guards Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime.

Synergies with projects funded under FCT05-1.2021, FCT05-2.2021, FCT05-3.2021, FCT05-5.2022, FCT05-6.2022 and FCT05-7.2022 should be envisaged. Proposed research that could also link with security research for border management (for example, border checks, detection of concealed objects or security controls in cargos) would be an asset. If relevant, the proposed activities should attempt to complement the objectives and activities of the EU Policy Cycle (EMPACT) – Priority Organised Property Crime.

FCT05-5.2022 (RIA) – Effective fight against corruption

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Security practitioners and policy-makers are provided with improved and complete intelligence picture of corruption, such as modus operandi, both offline and online, including cross-border dimension, new trends, its social and economic impact, its role in enabling other types of crime, as well as its close links with money laundering;
- A comprehensive risk analysis is provided to security practitioners and policy makers on the new opportunities offered by the COVID-19 pandemic in terms of corruptive practices, cross-border dimension, its social and economic impact and sectors at high risk;
- European LEAs, Border Guards Authorities and Financial Supervisory Authorities benefit from better, modern and validated tools (including the lawful court-proof collection of crime evidence) and training materials to tackle criminal activities related to corruption and improve resilience for corruption acts;
- Improved strategies of cooperation between European LEAs and Border Guards Authorities in fighting corruption and dismantling related criminal networks;
- Improved policy-making related to the fight against corruption.

Scope:

Corruption, a criminal category that ranges from bribery of public officials via sports to abuse of power and money laundering of proceeds from crime, is a strong enabler for crime and terrorism, and, as such, it constitutes a threat to security. By creating business uncertainty, slowing processes, and imposing additional costs, it has a negative impact on economic growth.

Although the nature and scope of corruption may differ from one Member State to another, it harms the whole Europe by lowering investment levels, hampering the fair operation of the Internal Market and reducing public finances.

The points where research can help are threefold. Firstly, there is a need to estimate the impact of corruption. It refers to social impact, factors that promote or hinder it, impact on vulnerable groups, economic, as well as fiscal and development costs.

Secondly, the role of corruption as an enabler of other crimes deserves analysis as well. Namely, corruption, increasingly facilitated by online services, is a fertile ground for organized criminal activities (human trafficking, smuggling…) and terrorism. For some criminal activities, corruption is an integral part of their modus operandi. Thus, relations with other types of crime should be explored too. Money laundering, closely linked to corruption, deserves special attention.

Thirdly, innovative societal and technological solutions for prevention, detection and investigation of this type of crime are needed, including also the collection of cross-border court-proof evidence. Therefore, activities proposed within this topic should address both societal and technological dimensions of corruption in a balanced way, taking care of the applicable legislation and fundamental rights. The international dimension should be analysed as well, hence both LEAs and Border Guards Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime.

Synergies with projects funded under FCT05-1.2021, FCT05-2.2021, FCT05-3.2021, FCT05-4.2022, FCT05-6.2022 and FCT05-7.2022 should be envisaged.

FCT05-6.2022 (RIA) – Effective fight against illicit drugs production and trafficking

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved and complete intelligence picture of security practitioners and policy-makers on drug production and trafficking, such as modus operandi, both offline and online, including the whole chain of trade, cross-border dimension, new trends, prevention of illicit drug market, new drugs, internet, including darknet, monitoring of drugs, financial flows of the related profits, etc.;
- European LEAs and Border Guards Authorities benefit from better, modern and validated tools (including the lawful court-proof collection of crime evidence) and training materials to tackle criminal activities related to drugs, such as monitoring of internet, including darknet;
- Enhanced ability of security practitioners to identify organised criminal groups involved in drug production and trafficking at an early stage;
- Enhanced ability of security practitioners and policy-makers to prevent the emergence of organised crime networks related to drugs, and respond to the threat of existing organisations, while respecting fundamental rights;
- Improved monitoring of dual-use chemicals used to drugs production;
- European LEAs and Border Guards Authorities benefit from improved strategies of cooperation in fighting drug trafficking and dismantling related criminal networks;
- Security policy makers are better supported in analysing the features of the drug trade and the business models underlying it, and the policy regulation related to the fight against drug production and trafficking is enhanced.

Scope:

Drug trafficking and drug production are the most profitable criminal activity of organised crime groups active in Europe. According to the 2019 EU Drug Markets Report, the total value of the retail market for illicit drugs in the EU was estimated at EUR 30 billion. There is a need for a comprehensive complete intelligence picture of this type of crime.

In the following, two main priorities in security research in this area are indicated. Firstly, innovative methods are needed to research developments in the illicit drug market, especially on prevention and new drugs (their production, marketing and distribution). Secondly, internet, including darknet, monitoring as regards drugs has not been sufficiently addressed by research until now. As stated by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), it is worth mentioning that over 100 global darknet markets are known to have existed for varying lengths of time since 2010 when the phenomenon emerged, that illicit drugs have been and continue to be the backbone of most darknet markets (drugs are important, but they share space with other illicit goods), and that two thirds of darknet markets content is known to be drug-related.

While vendor and customer interactions are relatively well researched and understood, there is limited knowledge regarding the actors and mechanisms involved in this trade beyond the distribution/sales phase in the drug trafficking chain. Knowledge gaps also remain in relation to the extent of involvement of traditional organised crime in the darknet trade in illicit drugs. Then, gaps exist in the knowledge of the financial flows related to the profits from darknet market platforms.

Activities proposed within this topic should address both societal and technological dimensions of drug trafficking and drug production in a balanced way, taking care of the applicable legislation and fundamental rights. As the organised crime groups involved are practically fully interconnected, the international dimension should be analysed as well, hence both LEAs and Border Guards Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime, such as cross-border drugs smuggling.

Synergies with projects funded under FCT05-1.2021, FCT05-2.2021, FCT05-3.2021, FCT05-4.2022, FCT05-5.2022 and FCT05-7.2022 should be envisaged. Proposed research that could also link with security research for border management (e.g., border checks or detection of concealed objects) would be an asset.

FCT05-7.2022 (RIA) – Effective fight against trafficking in human beings

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Security practitioners and policy makers are provided with an improved and more complete intelligence picture of trafficking in human beings, such as modus operandi, both offline and online, including the whole trafficking chain, cross-border dimension, new trends, relations with other types of crime, financial flows of the related profits, etc.;

- European LEAs and Border Guards Authorities benefit from better, modern and validated tools (including the lawful court-proof collection of crime evidence) and training materials to tackle criminal activities related to trafficking in human beings;
- Enhanced ability of security practitioners to detect and identify organised criminal groups involved in trafficking in human beings, in collaboration with citizens or NGOs when applicable;
- Enhanced ability of security practitioners to detect victims of all forms of exploitation, taking into account consistent patterns, and identify victims at an early stage;
- Enhanced ability of security practitioners to prevent the emergence of organised crime networks related to trafficking in human beings, to disrupt the trafficking chain at an early stage, deter organised crime groups related to trafficking in human beings and respond to the threat of existing organisations, as well as their potential expansion via de use of social media;
- Improved strategies of cooperation applied by European LEAs and Border Guards Authorities in fighting trafficking in human beings and dismantling related criminal networks, while respecting fundamental rights such as the protection of personal data, and improved cooperation between European and origin and transit countries authorities;
- Better policy-making related to the fight against trafficking in human beings.

Scope:

Trafficking in human beings is a serious and organised form of crime that involves the criminal exploitation of vulnerable people, the goal of which is the economic gain. This crime is often cross-border and consistently the vast majority of its victims are women and girls, around one fourth of all victims being children. Around half of the victims are EU nationals within the EU.

Trafficking can take place for various exploitation purposes, including sexual exploitation, forced labour, servitude, removal of organs, forced criminality (e.g., pickpocketing or drug trafficking). Trafficking in human beings is a grave violation of people's fundamental rights and dignity, and is explicitly prohibited by the EU Charter of Fundamental Rights. Understanding the nature, scale and costs of the crime is key to ensuring appropriate action at the European level to prevent the phenomenon. The 2017 Communication (COM(2017) 728 final) identifies as key priorities: to address the culture of impunity via disrupting the business model of criminals and untangling the trafficking chain; to provide a better access to and realize the rights of victims; to intensify a coordinated and consolidate response within and outside the EU.

Research, reliable and comprehensive statistics are crucial in obtaining a complete intelligence picture of this crime, the modus operandi of the related criminal groups, identifying and addressing trends, developing evidence-based policy, and measuring the impact of individual initiatives. Innovative intelligence-based technological means of detecting, tracking and disrupting the online activities related to trafficking in human beings (including darknet) should be developed as well. The research would also aim to contribute to countering the culture of impunity by increasing LE capacity to detect the trafficking crime, the suspected perpetrators and the victims and to disrupt the business model and/or establish responsibility of all those involved in the trafficking chain.

Activities proposed within this topic should address both societal and technological dimensions of trafficking in human beings in a balanced way, taking care of the applicable EU legal and policy framework including fundamental rights. Since the international dimension of this crime should be analysed as well, both LEAs and Border Guards Authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime, such as finding together means of disrupting the human traffickers’' business model. Collaboration with LEAs, security practitioners and Border Guards Authorities from countries or origin or transit of criminal networks would be an added value.

Synergies with projects funded under FCT05-1.2021, FCT05-2.2021, FCT05-3.2021, FCT05-4.2022, FCT05-5.2022 and FCT05-6.2022 should be envisaged. Proposed research that could also link with security research for border management (e.g., border checks or security controls) would be an asset.

Destination – Effective management of EU external borders

Relevant Cluster 3 Expected Impact:

"Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors."

This destination addresses, among other, objectives identified by the EU Security Union Strategy 2020-2025 as well as the border management and security dimension of the New Pact on Migration and Asylum. As such, topics included under the destination are aimed at ensuring strong European land, air and sea external borders –including by developing strong capabilities for checks at external borders hence safeguarding the integrity and functioning of the Schengen area without controls at the internal borders, by compensating the absence of intra-EU border checks; being capable to carry out systematic border checks, including identity, health and security checks as necessary, while facilitating travels of bona fide travellers and respecting rights and possible vulnerabilities of individuals; providing integrated and continuous border surveillance, situational awareness and analysis support; combating identity and document frauds; supporting future technology for the European Border and Coast Guard; supporting the interoperability and performance of EU data exchange and analysis IT systems; supporting better risk detection, incident response and crime prevention; improving European preparedness to, and management of, future rapidly evolving changes; and updating our maritime security management including migration, trafficking as well as search and rescue capabilities.

The European Border and Coast Guard Agency (Frontex) will be closely associated with, and will assist the Commission on drawing up and implementing, relevant research and innovation activities, taking into account its central role in defining capability requirements for the European Border and Coast Guard. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) could also assist the Commission on relevant research and innovation activities and specific topics. Research should also consider how future management of borders can develop protection of human rights, and facilitate protection of refugees.

This research will also contribute to the implementation of the European Border Surveillance System (EUROSUR) and the development of tools and methods for Integrated Border Management.

Regarding maritime security, the topics under this destination will also support the implementation of the relevant actions under the Capability development, research and innovation area of the EU Maritime Security Action Plan[4] and of the Civil-Military Research Agenda for Maritime Security[5]. Research activities will therefore enable better security and management of EU maritime borders, maritime critical infrastructures, maritime activities and transport, contributing as well to a better performance and cooperation on coast guard functions. Research and innovation in the area of maritime security will also support the development of future capabilities for the protection of sea harbours and related sea lines of communication including entry/exit lines. The objective of maritime security research activities in this regard covers prevention, preparedness and response to, expected and unexpected events including among others, anthropogenic and natural disasters, accidents, climate change as well as threats such as terrorism and piracy, cyber, hybrid and chemical, biological, radiological and nuclear (CBRN) ones. The EU Maritime Security Research Agenda lays down in this regard specific areas to address, including cybersecurity, interoperability and information sharing, autonomous systems, networking and communication systems and multi-purpose platforms. Specific EU maritime security legislation[6] also emphasises maritime passenger transport, and the threats to passengers. Considering that, innovative and more efficient capabilities for the security of maritime passenger transport could also be a useful area of research.

Regarding security in the cross-border movements of goods, research will address requirements identified by the Commission and EU customs authorities and should contribute to capabilities for detecting illegal activities both at external border crossing points and through the supply chain. EU customs authorities face increasing volumes of commerce, trade and traffic of goods, as well as having a range of tasks to fulfil besides security. International smuggling has the potential to become more sophisticated and/or increase in the next years and decades, and could be facilitated by cybercrime. Criminal networks may exploit potential weaknesses of global supply chains, transport and logistics to pursue illicit trade and other crimes. At the same time, threats and hazards that may need to be detected in the flow of goods are very diverse and often needing different sensors and technologies to be detected (from chemical, biological, nuclear, radiological and explosive material to drugs, firearms, money, waste, trafficked wildlife, cultural goods etc.). Hence, customs need innovation to enable detection, and ensure security without at the same time disrupting or unnecessarily hampering the trade flow. Capabilities built through research will contribute to the implementation of the new EU Customs Union action plan to reinforce customs risk management and effective controls. Capabilities include those on threat detection in the postal flows, automated controls and detection that reduce the need to open or stop containers, packages, baggage or cargo, decision support, portability of control solutions, and technologies to track cross-border illicit trade.

[4] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf

[5] WK 15068/2017 INIT

[6] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security

Research projects should be complementary and not overlap with relevant actions funded by other EU instruments, including projects funded by the European Defence Fund and the European Defence Industrial Development Programme, while maintaining a focus on civilian applications only.

Proposals submitted under this Destination should demonstrate how they plan to build on relevant predecessor projects; to consider the citizens' and societal perspectives; to include education, training and awareness raising for practitioners and citizens; to measure he achieved TRL; and to prepare the uptake of the research outcomes.

This destination will develop knowledge and technologies that may be taken up by other instruments, such as the Integrated Border Management Fund, that will enable exploitation of research results and final delivery of the required tools to security practitioners.

Expected impact

Proposals for topics under this Destination should set out a credible pathway to contributing to effective management of EU external borders, and more specifically to one or several of the following impacts:

- Improved security of EU land and air borders, as well as sea borders and maritime environment, infrastructures and activities, against accidents, natural disasters and security challenges such as illegal trafficking, piracy and potential terrorist attacks, cyber and hybrid threats;
- Improved border crossing experience for travellers and border authorities staff, while maintaining security, supporting the Schengen space, and protecting fundamental rights of travellers;
- Better monitoring of movements across air, land and sea EU external borders and reduction of illegal movements of people and goods across those borders, without detriment to those people and/or the flow of goods;
- Improved customs and supply chain security though better prevention, detection, deterrence and fight of illegal activities involving flows of goods across EU external border crossing points and through the supply chain, minimising disruption to trade flows.

The following call(s) in this Work Programme contribute to this destination:

CALL BM 2021:

Proposals are invited against the following topic(s):

Area BM01 – Efficient border surveillance and maritime security

BM01-1.2021 (IA) - Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Increased surveillance capability compared to the state of the art, including longer endurance, better reliability, lower maintenance requirements, longer permanence and wider coverage;
- Improved performance and/or safety, including better detection, classification and tracking capabilities, cyber and physical security, better cost-efficiency, better autonomy, lower visual and acoustic signatures;
- Improved multi-tasking capabilities to respond to a variety of needs and situations in the surveillance of border and maritime environment, including enhanced multi-authority collaboration.

Scope:

Border and coast guards, as well as other security practitioners, require capabilities to monitor wider areas beyond the EU external borders in order to prevent, detect and react to crime, including that crossing external borders, illegal border crossings and/or smuggling at the border regions of the EU and of the Schengen area. This applies to all border contexts – land, sea and air – but it may be specifically useful in the maritime domain, and these capabilities could also have a strong impact on other maritime security-related tasks beyond border control and for key dimensions identified by the EU maritime strategy Action Plan, including the civil-military research agenda. These capabilities should include monitoring for challenges and threats to maritime activities, including transport, maritime infrastructures and environments; contribute to measures to support vessels in distress and search and rescue missions; and scanning of coastal and border areas.

The solutions proposed by project proposals should reach advanced capability levels concerning detection, identification and tracking, including long endurance, persistence, reliability, and wide coverage. These platforms would be expected to have multi-tasking capabilities and be able to respond to a variety of needs and situations, including but not limited to environmental incidents, search and rescue needs, illegal migration and cross-border crimes. Platforms should offer cyber and physical security, be able to operate in groups/clusters, be highly autonomous, and offer increased endurance, taking into account better energy efficiency and cost-efficiency (including lower maintenance requirements) for security practitioners, low visual and acoustic signatures, and/or improved safety compared to the state of the art.

Solutions should be able to share their information products and integrate with existing and upcoming border and maritime surveillance systems in the EU, including EUROSUR.

Research and innovation activities could be conducted utilizing a range of technological approaches (including but not limited to UAVs, balloon, blimps, High Altitude Platforms (HAPs), Lighter-Than-Air (LTA) solutions, etc) as long as the specific platform delivers the expected improved capabilities.

The specific platform should be brought at least to the level of validation, by European border and coast guard authorities, in an operational or real environment. Proposals should be convincing in explaining the frameworks they intend to use for demonstrating, testing and validating the systems; these frameworks will also include assessments of manufacturability, cost-effectiveness, efficiency and demonstrated integration with existing systems, and legal and ethical issues.

While some components studied could be more innovative and brought to mid-TRL, most components of the envisaged solutions are expected to arrive at high TRL and be demonstrated by projects in actual environments with operations and exercises for validation by practitioners. Proposals should also delineate the plans for further uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, after the research project and should it deliver on its goals, of the solutions that they will demonstrate in the research project. Projects are also recommended to integrate impact assessments, including leveraging insights from previous research, in investigating and developing the solutions they propose.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals will need to ensure the key role of Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Research and Innovation Framework Programmes projects.

Research projects should be complementary and not overlap with relevant actions funded by other EU instruments, including projects funded by the European Defence Fund and the

European Defence Industrial Development Programme[7], while maintaining a focus on civilian applications only.

Area BM02 - Secured and facilitated crossing of external borders

BM02-1.2021 (CSA) – Increased safety, security, performance of the European Border and Coast Guard and of European custom authorities

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved safety, security, performance and user experience (including personal safety and security) of operational staff of European border and coast guards and customs authorities;
- Better situational awareness supporting decision-making systems of European border, maritime and customs authorities, including better communication, preparedness and preparation.

Scope:

Research should investigate and define future capability needs for increasing the safety, security, performance and user experience of the operational staff of border and coast guards and of customs authorities. This also in view of the reinforcement of the standing corps of the European Border and Coast Guard Agency. Research should analyse capabilities to facilitate and/or protect the work of the operational staff, including their safety and security. Technological components may include security and safety solutions and protective equipment for deployed staff, advanced communication systems, advanced human interface devices and sensors. Capability needs and possible solutions should also be explored on increased situational awareness for border and coast guards and customs, including how to prepare for and manage changing situations; or analytics support solutions for managing border and coast guards or customs staff, response and operations, taking into account legal and ethical, including data protection, requirements.

Complementarity with other security research streams, such as those that developed critical business continuity and safety and security solutions for security practitioners and first responders should be explored, while ensuring tailoring to the user needs in the specific operational context.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage

[7] With particular care to synergies with projects funded by call EDIDP-ISR-EHAPS-2019 "European High Altitude Platform Station (Euro-HAPS) solution for Union defence (surveillance of maritime zones, land borders or critical assets)"

with the Agency in the development of the project. Proposals will need to ensure the key role of Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Research projects should consider, build on if appropriate and not duplicate previous research, including but not limiting to research by other Framework Programmes' projects such as those on human factors and/or on situational awareness capabilities for border security and border management, as well as European stud(-ies) on potential applications of technologies to the improvement of border management capabilities.

BM02-2.2021 (IA) – Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Validation of innovative solutions for border crossing facilitation systems at European level for near-seamless and improved border crossing experience for travellers

- Increased security and reliability of border checks, including identification of people and goods crossing external borders, with stronger protection of their fundamental rights and personal data;

- Better organisation, flexibility and planning of border checks by European border authorities.

Scope:

Research should develop and systematically test and validate solutions to fasten and facilitate the border crossing experience for both travellers and staff of border authorities. Systems for easier border crossings, while maintaining security and reliability, would further advance one or more capabilities including the capabilities of border guards to do checks in mobility; of identifying and/or controlling passengers (and their vehicles and/or luggage) without stopping them; and/or of temporarily setting or scaling up the capacity of certain border crossing points within a relatively short notice. Systems should integrate solutions being able to offer these capabilities in a flexible way and at the same time process border checks for a range of cases and types of passengers (for example EU nationals, third country nationals, ETIAS/non-ETIAS eligible, persons recorded in a national facilitation programme, etc.).

For one aspect of the border crossing system, mobile or transportable technologies would enable authorities to quickly react to actual situations at the borders. In some scenarios, border checks are not only carried out in fixed crossing points, but also exceptionally in temporary points. New technologies can support authorities on document and information checks and verification (e.g. scanning passports, biometric verification, customs declarations, etc.), including health or security checks as necessary, establishing a secure and reliable communication channel to a backend service and providing immediate feedback to the field officer. Special considerations should be given to situations where officers operate in limited space areas (e.g. inside a train, on the road, on board of a ship in a port area). Equipment should not be heavy or bulky and should not restrict their freedom of movement. Solutions should have the potential to contribute to better border crossing experience for travellers, operators and authorities, improving throughput at border crossing points while maintaining or improving reliability and security of checks.

For another aspect of the border crossing system, research should advance the capabilities to capture and use biometrics of travellers without them having to stop and in natural contexts for border checks, in full respect of fundamental rights and considerations to safeguard data and integrity. Proposed research that could also link with innovation for fighting crime and terrorism beyond just the border checks (for example, biometrics capabilities that could help law enforcement to fight trafficking of human beings) would be an asset.

Projects should address the various components of an integrated system, test and validate it in real operational environment. Proposals should be convincing in explaining the frameworks (tools, methods, procedures, resources and criteria) they intend to use for demonstrating, testing and validating the operational performance of the systems; these frameworks will also include assessments of manufacturability, cost-effectiveness, efficiency and integration with existing systems.

While some components studied could be more innovative and brought to mid-TRL, most components are expected to arrive at high TRL and be demonstrated by projects in relevant, operational or real environments with operations and exercises for validation by practitioners. Proposals should also delineate the plans for further uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, after the research project and should it deliver on its goals, of the border crossing facilitation systems that they will demonstrate in the research project. Projects are also recommended to integrate impact assessments, including leveraging insights from previous research, in investigating and developing the solutions they propose.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals will need to ensure the key role of Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Research projects should consider, build on if appropriate and not duplicate previous research, including but not limiting to research by other Framework Programmes' projects such as those on border checks capabilities, risk-based integrated border control systems, travel facilitation, biometrics and document security, as well as and EU stud(-ies) on potential applications of technologies to the improvement of border management capabilities.

Area BM03 – Better customs and supply chain security

BM03-1.2021 (RIA) – Advanced detection of threats and illicit goods in the postal and express courier flows

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved detection of threats and dangerous and illicit goods by practitioners and operators within the post and parcel flows, without disruption to the flow;
- Improved capacity of practitioners and operators to deny the misuse of the postal and parcel service by criminal or terrorist group to move items;
- Improved risk assessment, preparedness and reaction capacities in the postal and parcel service.

Scope:

Research under this topic will contribute to build capabilities for more effective detection of threats and of dangerous and illicit goods within the postal and express courier flows, without impeding those flows. Currently there is a lack of technology that allows screening the volumes and at the speed of processing the parcels, making manual intervention necessary. At the same time, organised crime groups think they run a relatively low risk in exploiting postal and parcels supply chains to move a range of illicit and dangerous goods. Successful innovation could hence also have a deterrent effect on criminal organisations to use such channels.

Examples of threats and dangerous and illicit goods include explosives and explosive precursors, CBRN material, drugs, cash, contraband or counterfeit items, including counterfeit identity documents, and fake medicines. Detection capabilities should be built for post and parcels crossing the external borders of the Union, but also for internal shipping, but without introducing additional controls that may disrupt free movement of goods. Cooperation with operators of postal and express courier service in the research project is strongly encouraged. Solutions that could improve data quality, availability, integration among different steps in the flow, and interpretability, would also be welcome of projects.

The active participation in the research consortium of security practitioners from both custom authorities and law enforcement authorities is required by the eligibility conditions.

Research projects should consider, build on if appropriate and not duplicate, previous research, including but not limiting to research by other projects funded by the Framework Programmes for Research and Innovation. Proposed research that could also link with innovation for fighting crime and terrorism would be an asset.

BM03-2.2021 (IA) - Improved detection of concealed objects on, and within the body of, persons

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved capability of customs and border authorities to detect drugs, illicit goods, weapons, explosive and other threats concealed on individuals or within their bodies, in the operational environment of border crossing points;

- Safer, more efficient and more easily deployable solutions for detection compared to the state of the art are used by customs and border authorities , in particular avoiding ionizing radiation and minimizing any safety risk to users and operators and ensuring respect of fundamental rights.

Scope:

Research under this topic will increase the capabilities to detect objects concealed on persons, or hidden inside the body of persons. The proposed technology should be able to detect concealments on moving persons and should be based on non-ionising approaches that provide necessary safety and privacy. Proposed solutions should be harmless for users and operators (avoiding ionizing radiation, and include the assessment of the risk of any kind of toxic substances and/or potentially harmful techniques), provide fast detection and include easily deployable devices.

They should be able to detect weapons (including non-metallic weapons); explosives (combined or not with electronics), including homemade explosives (HMEs) and improvised explosive devices (IEDs); other threats and illicit goods such as drugs, tobacco or currency, concealed under or in the clothes or bags of individuals as well as within the individuals' bodies. The need for such detection capabilities could be increasingly useful especially in contexts such as airports or ferry terminals where people board on foot or in vehicles, where a sufficient and efficient detection capacity will have to cope with substantial growth of passenger volume.

Proposed solutions must maximise respect of fundamental rights, including for dignity and privacy. In this sense, solutions should avoid explicit formation of images, physical contact or intrusive techniques. Solutions should also prove their potential to enable the quick scan of large flows of people, employing a minimum number of operators. Solutions should be systematically tested and validated in operational or real environments.

Research projects should consider, build on if appropriate and not duplicate previous research, including but not limiting to research by other Framework Programmes' projects such as on basic capabilities to detect concealed objects on individuals and in cargo or containers.

CALL BM 2022:

Area BM01 – Efficient border surveillance and maritime security

BM01-1.2022 (RIA) – Improved underwater detection and control capabilities to protect maritime areas and sea harbours

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved security of maritime infrastructures and maritime transport, including sea harbours and their entrance routes;
- Improved detection of illicit and dangerous goods and/or of threats hidden below the water surface, either threatening infrastructures or vessels, or moving alone or connected to vessels.

Scope:

Security of maritime infrastructures and transport is key to support the movement of people and trade to, from, and within Europe. Furthermore, it is important to strengthen capabilities for security in and of sea harbours and of their entrance routes, and detection, prevention and response to illicit activities in and near sea harbours, including in the underwater sea space. Both legal and illegal activities in the maritime domain increase and become more sophisticated and this presses on security practitioners to build and improve their capabilities to keep up and fulfil their tasks in the future.

A particularly critical environment would include the abilities to detect and act below the water surface. Possible threats concealed below the water surface should be detected. Criminal organizations for example have the modus operandi of hiding narcotic cargos under the water surface of large and medium sized vessels. Detection and response capabilities against active threats below the surface (such as terrorist attacks against ships or harbour infrastructures) should also be developed. Security controls and fiscal manifest verifications on closed containers and cargo should be supported by information gathered below water surface.

Research could develop solutions to detect and identify anomalies below the water surface and/or automatically assess for below the water surface threats to a ship at harbour entrance and/or a pier. Projects should demonstrate, test and validate solutions working from detection to minimisation of threats from below the water surface. Research and innovation activities should focus on the delivering advanced autonomous or semi-autonomous vessel screening capabilities (detection of underwater smuggling – for example in cylindrical containers). Capabilities could also result impactful for key dimensions identified by the EU maritime security research agenda.

Research projects can include harbour authorities and operators, border and coast guards, and custom authorities. Research projects should consider, build on if appropriate and not duplicate, previous research, including but not limiting to research by other projects funded by the Framework Programmes for Research and Innovation.

Area BM02 - Secured and facilitated crossing of external borders

BM02-1.2022 (IA) - Enhanced security of, and combating the frauds on, identity management and identity and travel documents

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved capabilities of border management and law enforcement practitioners to identify citizens and the use of identity and travel documents and credentials in the context of border and police checks, for a better, more reliable and more secure experience for citizens and security practitioners, including in connection to optimised e-Government settings;
- Improved capabilities of border management and law enforcement practitioners to defend identity and document/credential management against attacks to their security and attempts to falsify biometrics, identity thefts and online frauds;
- Improved knowledge for European approaches to future identity management systems and document and credential security, building on and integrating with existing tools and respecting the privacy of European citizens.

Research will build capabilities to prevent, detect and respond to challenges to the security and reliability of identity management and identity and travel documents, in the context of border and police checks. Research should also address solutions for integrated secure identity creation, protection and management in the context of future increasingly "digitalized" borders; and contribute to improve the performance and the comfort of the border and police checks experience for both security authorities' operators and the users.

New challenges for secure identity management and secure identity and travel documents could emerge in the next years and decades. Solutions will hence have to enable new capabilities while at the same time ensuring both privacy and security of identity and identity documents. Future electronic identification systems will have to safeguard key parameters of identity management, such as security, efficiency, user friendliness, trust, privacy and protection of data. Electronic identifications (eIDs) can be carried on mobile devices, to respond to security requirements, ease of use and range of applications. In addition, it is necessary to ensure the reliability and link among the information contained on identity supports and their owner, to avoid the possibility of having authentic documents with false information. Research can focus on security and privacy enhancing features in new eID ecosystems and/or on innovative identity lifecycle processes.

Areas of research could include exploring solutions against morphing attacks to the security of identity and travel documents, including robust algorithms to detect morphing, as well as against other possible future attempts and techniques to falsify biometrics; methods to validate and verify identity at borders or police checks; or advanced and privacy-enhanced technologies for the security of identity, breeder and travel documents. Research should explore novel solutions for document verification and fraud detection, including Manipulation Attack Detection (MAD) and Presentation Attack Detection (PAD) at border checks.

The proposed solutions should act not only at technological level, but should also propose new approaches to the traditional central authority architecture. The solutions must take into account that the management of sensitive information and imply assessment of legal and ethical issues.

Solutions have the potential to contribute to future evolutions of European identity strategies based on eIDAS (Electronic Identification, Authentication and Trust Services), and could explore synergies with tools offered by the eIDAS Regulation.

The active participation in the research consortium of security practitioners from both border authorities and law enforcement authorities is required by the eligibility conditions. Research projects should consider, build on if appropriate and not duplicate previous research, including but not limiting to research by other Framework Programmes' projects such as those on capabilities for document security, as well as EU stud(-ies) on potential applications of technologies to the improvement of border management capabilities.

Area BM03 – Better customs and supply chain security

BM03-1.2022 (RIA) - Integrated, automated security controls and fiscal manifest verification in closed baggage, containers and/or cargo

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved capabilities for security controls and fiscal manifest verifications at customs;
- Integrated systems used by customs authorities for scanning, non-intrusive inspection, detection, analysis and decision support, minimizing disruption to the goods flow.

Scope:

Research will contribute to build capacities for quicker and more efficient security controls and fiscal manifest verifications of items and materials enclosed in baggage, containers or cargo, minimizing the need to open them. Capacities should be improved for automatically detect threats and illicit or dangerous goods, both in terms of sensors and in terms of data (including image) interpretation and anomaly detection.

Border and custom authorities control selected baggage, containers and/or cargo using technology-enabled and physical inspection. This process is often manual and time consuming, and it suffers from large numbers of false-positive results. Possible false-negative results could also limit the mitigation of risks to the society. This becomes even more relevant with increasing trade flows, or higher risk scenarios.

At the same time, there is limited automation also in the other parts of the process, needing not only human inspection but also human interpretation and decision, which currently leads to an inefficient use of the largest limiting factor of the whole process, i.e. time.

Wider application of technology not only for security checks but also for declaration verification also for fiscal purposes, further increases the value of automation. Solutions should also allow to better and more automatically interpret images from baggage, containers and/or cargo and identify anomalies that support the detection of threats, smuggling and illicit trade, while eliminating or minimizing disruption to the flow. This may include, but not limit to, development of Artificial Intelligence and semantic object tagging solutions to support and facilitate image interpretation and anomaly detection. Any proposed technology (or combinations thereof) should demonstrate how it will integrate well with supply chains.

This technology shall also allow for an automatic collection of relevant data on the conditions and outcomes of the controls, as to allow measuring the efficiency of the measures and feeding the analysis for risk management and security at the borders. Solutions that would improve data quality and availability from a variety of possible sources; integration among different phases of transactions, shipments and border crossings; and data interpretability, would also be welcome of projects.

Border and custom authorities physically and administratively inspect shipments out of a wide range of needs. Limited availability of restricted internal information along with relevant open source information, and on-site analysis of goods and data causes inefficient work. The lack of automated real-time evaluation of derived information against available information, suggesting the next question for inspection, leads to inefficiencies. Physical and administrative inspections therefore are time and labor intensive processes that are paused often to acquire knowledge support. A swift technology-supported inspection decision support system should help solving questions in first line, along with a clear reduction of the burden of inefficiently preparing, acquiring, analyzing and reporting and using information.

Research should hence develop solutions that integrate tracing capabilities (including tampering, condition or intrusion detection) before arriving at the external borders; advanced sensing and detection capabilities without opening baggage, containers or cargo; automated interpretation and anomaly detection; risk-based and knowledge-informed analytics, assessment and decision support system; and user interfacing. Research can also explore alternatives to, and/or limitations of, the use of ionizing radiation.

Threats and illicit and dangerous goods that should be targeted include but do not limit to weapons and parts of weapons; explosives and precursors; drugs; alcohol, tobacco, potentially dangerous and/or counterfeit medicines and pharmaceuticals; other illicit goods including counterfeit luxury goods and contraband cultural goods; illicit wildlife; raw materials; and oil.

The active participation in the research consortium of security practitioners from both border authorities and custom authorities is required by the eligibility conditions.

Projects should plan to integrate in the proposed solutions intelligence information and data that can inform risk-based screening choices and decisions, in particular regarding terrorism and organised crime, in recognition of the involvements of criminal or terrorist organisations with illicit trade. The relevant involvement of law enforcement and intelligence security practitioners is hence encouraged, as well as consideration of relevant innovation from the Fight against Crime and Terrorism research area, especially regarding cargo crimes.

Research projects should consider, build on if appropriate and not duplicate previous research, including but not limiting to research by other Framework Programmes' projects such as those on capabilities for inspection, detection and analysis in the border and customs context.

BM03-2.2022 (IA) -Better, more portable and quicker analysis and detection for customs

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Portable or easily deployable solutions used in customs inspections for detecting threat agents such as drugs, including new psychoactive substances;
- Improved capacities of customs authorities to acquire, analyse, share drugs spectra, and detect new drugs in the context of customs inspections.

Scope:

Research will further develop capabilities for portable and quicker testing, analysis and detection of threats at customs checks sites. Example of target substances include drugs, with a focus on new psychoactive substances, but also gems or precious metals and other threats or illicit goods.

These capabilities would allow customs to deploy detection capacity where and when more appropriate and efficient and to carry out inspections "on the move" and more quickly. This would allow detection of threats in the flow of goods directly at the customs inspection site, without having to divert the scanned object(s) to a different site, like a more distant dedicated detection laboratory. This would provide better response capability for customs in an ever-changing operational environment. It would allow for a faster detection and verification capability in the field.

The improved capability includes being more easily and quickly updated on references for the targets goods and substances, to be able to detect them. This includes updated spectra of drugs as new psychoactive substances, which would allow detecting them. There is room for innovation to improve customs' access to updated spectra of substances when they appear; easily make spectra available to customs' devices; and improve data for spectra libraries.

This technology shall also allow for an automatic collection of relevant data on the conditions and outcomes of the controls, as to allow measuring the efficiency of the measures and feeding the analysis for risk management and security at the borders.

The involvement of law enforcement practitioners is encouraged, as well as synergies with relevant topics of the Fight against Crime and Terrorism destination, to ensure operational scenarios are best identified for detection capabilities by customs. Research projects should consider, build on if appropriate and not duplicate previous research, including but is not limited to research by other Framework Programmes' projects.

Destination – Protected Infrastructure

Relevant Cluster 3 Expected Impact:

"Resilience and autonomy of physical, social and digital infrastructures are enhanced and vital societal functions are ensured with the help of knowledge, effective solutions and state-of-the-art technologies, as well as better cooperation between stakeholders."

The reliable, robust and resilient operation of infrastructures is vital for the security, well-being and economic prosperity of people in Europe. They provide the basis for our daily lives, connect people to each other and guarantee different kinds of social and economic interactions. To be able to allow for such interactions, be it in transport, communications or services, infrastructures has grown more complex to keep up with the development of modern societies, while at the same time ensuring their resilience against disasters and the impacts of climate change and other factors that affect society e.g. demographic changes. Infrastructures operate in a rapidly evolving technological and threat environment with increasingly interconnected networks highly reliant upon one another, which presents both risks and opportunities for their protection. They must be resilient towards different expected and unexpected events, emerging risks, be they natural or man-made, unintentional, accidental or with malicious intent.

The new Security Union Strategy list the protection of critical infrastructures as one of the main priorities for the EU and its Member States for the upcoming years. Specific reference is established to growing interconnectivity as well as emerging and complex threats: technological trends like the use of Artificial Intelligence and the rapid development of sophisticated unmanned vehicles, the impact of natural and man-made disasters, as well as major crisis scenarios like the COVID-19 pandemic and unexpected events. Infrastructure preparedness and protection is a technologically complex domain, affected by various global developments and thus needs to be supported by targeted security research. This work programme aims at supporting the protection of European infrastructures with relevant projects, enabling public and private actors to meet current and emerging challenges.

Technologically complex applications offer the possibility for better prevention and preparedness, can allow for efficient response to different threats and faster recovery. But at the same time, they create new vulnerabilities. The potential damage resulting from their disruption can escalate rapidly and negatively affect wider parts of vital societal functions. This is typically the case of satellite-based positioning and timing systems, which provide a wealth of high quality Positioning, Navigation and Timing (PNT) services that are exploited by critical infrastructures such as transport and logistics, energy grids, drinking water network, dams, telecom networks or financial markets. GNSS disruption or denial of services is recognised as an important economic and societal threat.

Infrastructures in the European Union are a high-value target for terrorist groups as well as agencies of third countries. With the *Directive on identification and designation of European critical infrastructures and assessment of the need to improve their protection (*2008/114) the EU and its Member States have created a basis for a common approach towards protection.

Under the umbrella of the new Security Union Strategy, the regulatory framework for critical infrastructure protection is currently under revision. The Proposal for additional measures on Critical Infrastructure Protection which is part of the Commission work programme for 2020 is also making use of the significant results that security research has produced in the last decade.

Especially in the cyber-domain, the risks have been constantly growing in recent years, with both more frequent and more sophisticated attacks. In addition, criminals attack infrastructures with the help of cyber-tools for extortion or blackmailing with the help of ransomware. The EU has acknowledged the strong role of the cyber dimension in infrastructure protection, most notably in the *Directive on security of network and information systems* (2016).[8] /1148). Large-scale data mining of cross-sectoral information should be supported by targeted research on appropriate AI techniques and infrastructure. It is very important to be able to react quickly to different scenarios and make decisions based on sufficient available data.

Physical attacks are less frequent, but cases in the EUs neighbourhood have shown the destructive potential of new technologies used for attacks such as Unmanned Aerial Vehicles (UAVs), which can also be used for intentional disruptions that pose danger to safe operations of infrastructures and create significant economic losses.

Hybrid threats are of particular relevance in the overall risk scenarios, since they are designed to target vulnerabilities and aim in many cases disrupting infrastructure, making use of different methods. Hybrid threats and means encompass a combination of physical and cyber-attacks or disruptions, diplomatic, military and political as well as economic means. The effects of cyber-instruments and disinformation are crucial elements of such malevolent strategies and create the need for comprehensive preparedness to avoid large scale disruptions. As such, both the *Joint Framework on Countering Hybrid Threats* (2016)[9] and the *Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* (2018)[10] pay special attention to the role of infrastructures and research should provide better means to counter hybrid threats.

Europe is exposed to a wide range of natural hazards and the vulnerabilities of infrastructures need to be addressed also from that perspective. With certain disasters striking more frequent and more severe, as well as long-term challenges such as climate change, there is a need to deploy innovative solutions to ensure the continuous functionality of European infrastructures exposed to such natural extremes. Security research should in this regard support the regulatory and cooperation measures on European level, such as the *EU Civil Protection Mechanism established by the amended Decision 1313/2013/EU* and the *EU Adaptation Strategy*. On the other hand, new Infrastructures technologies themselves (for example energy production and storages, new materials, water protection, etc.) can pose a potential risks for society due to

[8] Directive (EU) 2016/1148

[9] JOIN/2016/018 final

[10] JOIN/2018/16 final

accidents. Therefore, the role of fire and rescue services needs to be reflected in targeted research to the same level as it is the case for different security authorities.

The COVID-19 crisis presents a challenge that is unprecedented in recent European history and it concerns infrastructures in two main dimensions. Pandemics are an extreme stress-test for the function of certain infrastructures (most notably: health, transport and supply-chains) by disrupting established procedures, threatening the function due to infection of workforces and massively scaling up the need for resources. In addition, infrastructures themselves can increase pandemic risk if unsuited to different mitigation measures and promoting virus transmission. This area will build on lessons learnt from the COVID-19 crisis. It will be for certain topics essential also to ensure synergies and coordination of actions with the Health Programme [final name to be agreed following the adoption which is due by 20 May].

Increased complexity in the area of infrastructure protection is not only related to the amplified role of the cyber dimension, but also by the mix of man-made and natural hazards and the growing interdependence. The development of European cities into smart cities has opened up a new domain in infrastructure protection, expanding the perspective beyond classical sectors of (critical) infrastructure since more complex, connected and vulnerable assets are deployed in urban areas. This consideration unveils the still fragile building blocks of smart cities' technological features and underlines the need to put a stronger emphasis on broader societal challenges and needs. Security research can help to make use of the knowledge acquired in other sectors and to make it usable for local authorities to protect and empowers people and assets in cities and urban areas.

Expected impact

Proposals for topics under this Destination should set out a credible pathway to contributing to the protection of infrastructure, and more specifically to one or several of the following expected impacts:

- Ensured resilience of large-scale interconnected systems infrastructures in case of complex attacks, pandemics or natural and man-made disasters
- Upgraded infrastructure protection systems that respond quickly and without substantial human intervention to complex threats and challenges, and better assess risks ensuring resilience and strategic autonomy of European infrastructures
- Resilient and secure smart cities are protected using the knowledge derived from the protection of critical infrastructures and systems that are characterised by growing complexity.

The following call(s) in this Work Programme contribute to this Destination:

CALL INFRA 2021:

Proposals are invited against the following topic(s):

Area INFRA01 – Improved preparedness and response for large-scale disruptions of European infrastructures

INFRA01-1-2021 (RIA) –European infrastructures and their autonomy safeguarded against systemic risks

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved large-scale vulnerability assessments of EU Member States' (MS) or Associated Countries' (AC) key infrastructures covering one or more types of infrastructure (energy, water, communications, transport, finance etc.) in more than two MS/AC

- Improved cooperation to counter Hybrid Threats and subsequent large-scale disruptions of infrastructures in Europe, allowing for operational testing in real scenarios or realistic simulations of scenarios with specific regard to the cross-border dimension (intra-EU as well as non-EU)

- Improved concepts and instruments for the anticipation of systemic risks to European infrastructure, allowing for comprehensive long-term risk assessments, with regards to climate change, technological trends, foreign direct investment (FDI) and dependence on critical supplies from non-EU countries

- Improved risk, vulnerability and complexity related assessments for interconnected physical-digital European infrastructures aiming to increase security, resilience and design effective preventive, mitigating and preparedness measures and protect against and respond to cascading effects

- Terrestrial back-up/alternative PNT solutions used by to ensure continuous operation of Critical Infrastructure in case of the disruption of GNSS services or other essential services

- Enhanced preparedness and response by definition of operational procedures of both private and public infrastructure operators as well as public authorities considering citizens involvement (needs and vulnerabilities) in case of large scale infrastructure disruptions also with a view of assessing the combined physical and cyber resilience

Scope:

Security research related to infrastructure protection has been traditionally following a sectorial approach. With more and more infrastructure systems being interconnected, a stronger focus on the systemic dimension and complexity of attacks and disruptions by cyber or physical means needs to be applied. As such, not only interdependencies within one type of infrastructure (or closely related types) can be taken into account, but large-scale disruptions also with a view of the specific challenges of the cross-border dimension. Also, there is a need for a comprehensive strategy that takes into account different forms of interdependence (e.g. physical, geographic, cyber and logical).

In order to raise the awareness and preparedness for emerging risks, research should enhance the capabilities for foresight and risk management on a systemic level. As such, large-scale Vulnerability Assessments and risks management capabilities, as well as forecasting of emerging risks should be developed with a view of preparing for attacks or disruptions on the whole infrastructure of one or several EU Member States and Associated Countries' (AC).. To allow for rapid and adequate response, simulations to prepare for systemic disruption of several key infrastructures are necessary. Since especially physical attacks on infrastructures in the EU are less frequent compared to other scenarios there is less empirical data available that can be used to improve protection. Furthermore, there is a lack of capabilities for testing protective equipment and training manuals. Security research can help to develop tools for operational testing in real-scenarios or simulated scenarios. Specific attention should be dedicated to Hybrid Threat scenarios, as defined by the European Centre of Excellence for Countering Hybrid Threats. The same is true for extreme natural disasters, which have the potential to disrupt several key infrastructures and whose subsequent effects are difficult to predict. Security research should in this regard support and complement EU Member States and Associated Countries' (AC) legal obligations to better prevent, prepare for crisis situation set *by the amended Decision 1313/2013/EU*, establishing a Union Civil Protection Mechanism.

Some essential sectors of the economy need uninterrupted access to the high-quality position and timing information provided for free by satellite navigation systems. Despite the fact that satellite navigation systems such as Galileo are made ever more robust towards risks and disruptions both in terms of ground segments as well as space assets, there remain residual vulnerabilities that cannot not be coped with when facing the emergence of new challenges. These critical sectors shall therefore develop complementary positioning and/or timing solutions that are able to sustain a sudden disruption of GNSS service. This would make the vital functions of the society more resilient.

Infrastructure security research is in many cases transnational. While there has always been a strong European dimension in the conducted research, there has been less of a focus on cross-border scenarios with third-countries. Security research should therefore stimulate knowledge generation and cooperation with relevant third countries, which are vital for the functioning of European infrastructure. Examples could include energy, but also critical supplies, digital services or transport.

The means to attack infrastructure on a large scale have been rapidly enhanced by malevolent actors. Nevertheless, risks do not only emerge from intentional acts or disruptions, they can also grow over time based on other factors such as climate change, or lack of independence in critical technologies. Thus, better anticipation of systemic risks including forward-looking technological risk assessment and advanced screening of private interests related to ownership and operations (licensing), and FDI should be a key area of security research in the future. On a constant basis, information about the functioning and vulnerabilities of European infrastructures is unlawfully gathered for economic reasons, as well as with a view of preparing possible intentional disruptions. With the aim of safeguarding autonomy, more sophisticated tools against unlawful gathering of information on infrastructures need to be developed.

INFRA01-2-2021 (RIA) – Ensured infrastructure resilience in case of Pandemics

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Strategies for the resilience of infrastructure networks and services, and their interaction and vulnerabilities in a context of rapidly changing volumes and patterns of use
- Understanding of inter-dependencies and strategies to overcome disruptions at local – regional – national and European (cross-border) level
- Better understanding of the cascading effects of pandemics for different infrastructures and the services they provide
- Improved mitigation strategies in case of the infrastructure disruptions caused by the absence of large parts of critical workforce, or disruptions of critical supplies

Scope:

Pandemics such as the COVID-19 crisis and other health risks have the potential to massively disrupt the functioning of infrastructures and vital societal functions. While this is most evident for the health system, the negative impacts reach much further. Resilient infrastructure systems particularly 'lifeline' services such as electric power, water and health care are critical for minimizing the societal impact of extreme events. It is essential to develop targeted solutions to ensure continuity of operations of different services and supplies, which are also critical to allow for prevention, preparedness and response to pandemics. This preparedness must also account for climate change as a "threat multiplier", for example with heatwaves, forest fires or flooding either accelerating the spread of a pandemic or rendering countermeasures like confinement less effective.

Member States remain the primary actors in preventing and responding to the outbreaks of infectious diseases. Enhanced European coordination into capacity-building, improved prevention, preparedness and coordinated response can support their efforts. In order to improve the EU-wide prevention and response to the specific challenges for the functioning of infrastructure in case of a severe infectious disease crises requires targeted security research which can deliver better knowledge, security risk assessment as well preparedness and response emergency planning tools. Public-private cooperation is absolutely essential in order to respond to a crisis as far reaching as a pandemic. Any comprehensive European approach to infrastructure resilience in case of a disruption caused by it, will need to take due account of this cooperation.

In infrastructure protection research, it is of high importance to understand the impact of the pandemic beyond the directly affected health system. The availability of specialised work force and vulnerability assessment of health capacities constitute the essential elements in this regard, as disruption of infrastructures due to the infection of large parts of a specific work force poses the immediate risk of cascading effects. The same is the case for integrated supply-chains for both critical goods, as well as non-essential ones. As such, understanding interdependencies and identifying truly critical activities is key for enhancing overall societal resilience against pandemics.

A situation like the COVID-19 crisis, also puts the capacities of different infrastructures under exceptional stress, due to the rapidly increased demand for certain supplies and services and the ensuring change of load stress of different networks (as for example sudden increase in communication, decrease in transport, ensuring essential resources). Such changes in use-patterns open vulnerabilities, as for example increased cyber-risks in the event of teleworking or less physical protection due to staff contingency measures. Design of some critical infrastructure components, such as transport networks and critical manufacturing may in themselves be resilient to the pandemic threat, but put overall societal resilience at risk by promoting disease transmission and being unsuited to different mitigation measures.

Area INFRA03 - Resilient and secure smart cities

INFRA03-1-2021 (RIA) – Advanced security and resilience across urban mobility systems

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved physical and cyber protection for smart bridges, tunnels and roads including corridors for unmanned vehicles (land, air, sea) from unlawful interference, manipulation and attacks

- Security-by-design concept implemented as part of integrated urban planning processes (which also include measures on safety, environmental protection etc.) and the design or maintenance of urban mobility infrastructures to avoid the creation of vulnerabilities at the earliest stages

- Comprehensive processes and systems for the protection of physical and digital infrastructures and in vehicle anti-hacking systems for unmanned and autonomous vehicles like the U-Space, vehicle-to-vehicle communication and charging facilities

- Enhanced urban mobility systems' resilience to natural and man-made disasters, as well as system successful performance and failures

- Cybersecurity solutions to detect and mitigate associated safety risks caused by hacking attempts to vehicle.
- Cost-efficient security upgrades of urban infrastructures and possibilities of pooling and sharing of complex security systems, taking into account limited budgets of local authorities and citizens (needs and capabilities)

Scope:

European cities are developing into more connected and complex systems of different services and infrastructures empowered by technologies and growing digitisation. As one of the essential services of every city, transport in particular is affected by this transformation. Connected transport solutions require a stable infrastructure able to connect with different vehicles and exchange data in a secure environment. Such *mobility systems* of interaction between users, vehicles and infrastructure pose specific challenges in terms of prevention, protection from and response to cyber- and physical threats.

As such, advanced protection of (smart) tunnels, bridges and roads including corridors for autonomous vehicles should be a priority for research in the coming years. Connected to the above mentioned area is the necessary preparation for safeguarding new forms of transport and the multiple-use of infrastructure. Consequently, the protection of physical and digital infrastructures for unmanned and autonomous vehicles needs to be enhanced with new tools, processes and practices. Security research on such infrastructures needs to be closely aligned with other projects funded under the domain of smart cities and transport, most notably the ***European Partnership on Connected, Cooperative and Automated Mobility (CCAM)***.

The classical large-scale infrastructures have a long tradition of implementing the principles of Safety by design and Security by design when planning their assets. However, with more and more infrastructures on the local level becoming vulnerable, security research can support their protection with new approaches in 'Security-by-design'**.** Many transport infrastructures have been equipped with protective tools in the past, but these are sometimes not fit for current threats scenarios. Also in view of limited budgets of many local administrations, improved knowledge as well as innovative security upgrades and processes for existing urban infrastructures equipped with advanced connectivity technologies and cooperative systems could be explored with the help of research.

Other Actions – Infrastructure Protection

Study – Research on Infrastructure Protection and Resilience in Europe - lessons learned, trends and challenges (2021)

(Critical) Infrastructure protection has been a long existing priority for EU-funded security research, most notably in the European Programme for Critical Infrastructure Protection (EPCIP). As such, a significant amount of relevant results have been achieved under the different framework programmes for research and innovation, national research initiatives , as well as by the work of the European Reference Network for Critical Infrastructure Protection (ERNCIP). A particular focus was put on the sectorial approach, aiming at enhancing the level of protection for the different domains (such as energy, transport, communication etc.). EU-funded research has covered the majority of infrastructures with at least one project and identified synergies in terms of improved knowledge, processes and technologies.

The aim of the proposed study is to take stock of the results achieved so far and provide a comprehensive analysis of at least the following items:

- Identifying sectors that have not yet been (adequately) covered by EU-funded security research on infrastructures, or where technological developments or an anticipation of more severe natural disasters require new projects to be funded in order to keep up with the related risks
- Define cross-cutting technologies and methodologies that have the potential to be deployed for the protection of several different types of infrastructures
- Identify existing good practices for the incorporation of future risk modelling to enhance infrastructure resilience, including cross-border and/or cascading risks
- Explore potential for the market-uptake of these solutions and thus provide input for the future work of the European Networks for Innovation in Security focussing on infrastructure protection , including exploration of rapid innovation and implementation of existing or high TRL technologies from other sectors
- Provide an overview of the possibilities to cooperate with different international partners on selected infrastructures, taking into account the specific sensitivity of the area

The results of the study should provide the basis for the definition of priority areas to be covered under INFRA in the calls as of 2023.

CALL INFRA 2022:

Proposals are invited against the following topic(s):

Area INFRA02 - Upgraded infrastructure prevention, protection and response systems

INFRA02-1-2022 (IA) – Autonomous systems used for infrastructure protection

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Autonomous surveillance, detection and fast and coordinated response based on updated integrated contingency plans to threats against different types of infrastructures in order to support existing security measures, reduce the risk to human personnel and allowing for mitigation in locations that are hard to reach (underwater, underground, high altitude, etc.) and without or just limited telecoms-connection

- Long term deployment of autonomous solutions for the decontamination of large scale infrastructures (including in public urban areas) in case of the release of CBRN-materials, or with specific regard to support efforts to reduce the spread of infectious diseases, preventing and responding to pandemics

- Long term deployment of autonomous solutions/systems/devices to detect CBRN threats in a fast, secure and forensic way

- Consideration of system performance, interdependencies, new failure modes and conditions that need to be in place for this to work as intended

- Concepts for the use of advanced materials, smart technologies and built-in monitoring and repair capabilities to reduce the destructive potential of natural disasters and (terrorist) attacks on infrastructures

- Improved knowledge and solutions for the protection and response against large-scale attacks or intentional disruptions with (fast moving) unmanned vehicles or other moving objects reducing critically the time to react also close to residential areas

- Enhanced knowledge on the ethical and legal impact on individuals and society as a whole of the use of robotics in order to maintain the vital functions of society

Scope:

Time is critical to prepare and react to disruptions of infrastructures. Faster and coordinated interventions can significantly reduce the impact, avoid negative cascading effects or in the best case prevent disruptions. The increasing interconnectivity of infrastructures has also led to bigger complexity in regards to the detection and response to incidents and certain technologies can be misused to conduct attacks or targeted disruptions of infrastructures. As underlined in the Security Union Strategy this is for example the case for scenarios involving unmanned aircraft systems (UAS). It could however also be relevant for possible incidents with land- or sea borne devices approaching at very high speed.

In order to allow for the best possible detection of threats and quick response and restoration of performance levels (e. g. through decontamination of the affected material/person; detection as well as mitigation of a risk), autonomous systems for infrastructure protection are a promising field of research. Many state-of-the art technologies used in other areas (for example: advanced robots or other autonomous detection and repair capabilities based on artificial intelligence) combined with user centred approaches, have the potential to significantly reduce the reaction time and can provide therefore an added value also for security solutions. Besides a reduced reaction time, the use of autonomous systems can reduce the risk for human responders, which is important for dangerous operations as for example in gas or chemical plants, or CBRN contaminated areas. At the same time, such systems can access challenging locations, such as underground cables, underwater pipes or assets in high altitude. Those features do not only present an advantage in responding to intentional acts, but also allow for faster and more efficient response to natural disasters and subsequent cascading effects. On the other hand, automated systems do create new vulnerabilities and its use raises ethical concerns that would need to be taken into account in any research. Solutions and measures must take into account legal and ethical rules of operation, as well as fundamental rights such as privacy and protection of personal data. Cost-benefit analysis not compromising ethics and privacy should also be considered.

Results achieved so far in the area of robots and autonomous systems (RAS), also under Horizon 2020, have led to applications making use of Unmanned Vehicles for example in the area of infrastructure maintenance and the detection and response to safety risks. Other concepts have been including self-healing materials, smart technologies and built-in tools as well as associated processes. For security incidents, there are so far less solutions available which would take into account the specific challenges of intentional disruptions as compared to accidents or material failure.

INFRA02-2-2022 (RIA) – Advanced real-time data analysis used for infrastructure protection

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved capabilities for risk identification in infrastructure networks through real-time analysis (including big data) by public and private actors via secured and trusted platforms and interconnected systems where the collaboration follows clear legal and political frameworks

- Tools and processes for facilitating stakeholders efforts to identify, analyse, assess and continuously monitor risks and boost adaptive capacity to unexpected events risks in advance by allowing for the analysis of various data sources (e.g. audio, video, social media, web-content, sensor or machine generated data)

- Fast and continuous real-time identification, classification and tracking of hazardous agents, contaminants or anomalies in infrastructure networks and supply-chains

- Interoperable interfaces and improved collaboration between infrastructure operation detection and response systems, national/EU risk management/coordination centres and first responder equipment in order to allow for remote on-scene operations considering citizen knowledge
- Increased cyber-resilience of industrial 5G networks and cloud data covering specific infrastructure domains
- Ability to map in real-time the source(s) of risk factors that could endanger the networked infrastructure.

Scope:

Today's society is more interconnected than ever before. Telecommunication networks, transport networks, aviation, the energy grid, finance are the backbone of today's society. Due to their exceptional complexity and size, infrastructure networks pose a specific challenge when it comes to identifying different risks either cyber- or physical. Especially in the cyber-domain, many intrusions or attacks remain unnoticed or are detected relatively late. Technological developments in areas like machine-learning for analytics, user interfaces as well as storage applications have the potential to improve related capabilities.

Modern and interconnected infrastructures create constantly big amounts of data. In addition, other sources can be exploited to support the identification and analysis of risks to infrastructures. Therefore, research on enhanced **risk anticipation through real-time data analysis** has the potential to lead to useful tools to enhance preparedness (contingency plans, scenario based exercises, allocation of resources, etc.).

In addition to general cybersecurity issues of digital systems - as covered in this work programme for example under CS1.1.2021 or 2022 (IA) - infrastructure protection is marked by a set of specific requirements taking into account most notably aspects from the integration considering user centre approaches as well as social and ethical aspects of Industrial Internet of Things (IIoT), Supervisory Control and Data Acquisition (SCADA), and AI/ Machine Learning approaches for real-time data analytics, ensuring transparency, sufficient knowledge and their operational challenges in this area.

While the availability of larger amounts of data from different sources offers potential to improve the identification of possible risks to infrastructures, it increases also the demand for fast and resilient analytical tools. There is a need to filter information to identify data that is relevant as an indicator for risks and - given the large number of different forms of cyber-attacks or intrusions - also a need to prioritise and decide according to the degree of danger they present. This implies the need for matching data in the appropriate context and verifying the source with a view of ensuring that only relevant data is analysed, thus avoiding false results.

Faster identification of hazardous agents and contaminants inside the infrastructure networks is a key to allow for quick response, inform and involve citizens and to avoid large-scale damage of any incident. Such identification capabilities can be deployed as part of the infrastructure and integrate with the systems public authorities use to make sure information is available as soon as possible. Furthermore, it is crucial to develop methods for better cooperation between different actors to ensure a common understanding and interpretation of data and to provide interactive tools for exchange and visualisation for decision support. Cooperation between different public and private actors is essential in this regard.

Area INFRA03 - Resilient and secure smart cities

INFRA03-2-2022 (IA) – Nature-based Solutions integrated to protect local infrastructure

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

- Integrated Nature-based solutions **(NBS)** into overall concepts for the protection of infrastructures and existing integrated risk management plans for cities and urban areas with a view of complementing existing methods for protection and resilience
- Adaptation and mitigation strategies for infrastructure protection applied by local authorities and operators, including lessons learned from studying reactions of natural eco-systems to different external shocks
- Resilience of local infrastructures enhanced by integrating local knowledge from population and historical documents, as well as natural components in their physical assets preventing potential damages from different types of hazards, including storms, floods and heatwaves.
- Full potential of Nature-based Solutions exploited by local authorities and operators to mitigate the risks related to multiple hazards manifesting at the same time, while also taking into account social empowerment and environmental co-benefits like leisure, clean air, and immunity and response to cyberattacks etc.

<u>Scope</u>:

The aim of the topic is to expand the knowledge on Nature-based Solutions (NBS) and their ability to enhance infrastructure resilience in cities and urban areas against natural and man-made hazards. Thus complementing other traditional security measures.

Cities are undergoing a rapid transformation most notably due to their digitisation. Besides this, the need for solutions to make them more sustainable and environmentally friendly has been addressed in many research projects, mainly from the perspective of climate change adaptation. In this regard, **nature-based solution**s **combined with local knowledge** offer a potential also for security research on infrastructures. Such solutions can help and provide business opportunities to make cities more resilient against natural disasters and possibly other security challenges. Under Horizon 2020, the Commission has brought together several experts to deliver a recommendation on ‘Nature-Based Solutions and Re-Naturing Cities[11]’ in form of a comprehensive report. They delivered the definition of NBS as: ‘*actions which are inspired by, supported by or copied from nature. Some involve using and enhancing existing natural solutions to challenges, while others are exploring more novel solutions, for example mimicking how non-human organisms and communities cope with environmental extremes.’*

EU-funded and national research activities have demonstrated the significant opportunities of NBS with regard to for example improved resilience, climate adaptation and the reduction of pollution in cities. What concerns security, projects have been focussing on the effects that NBS can have for prevention (for example flood-plains and mangroves for flood protection, natural source water protection, green roofs and pavements for heat and water absorption). The reduction of disaster risks and the potential for enhanced resilience of cities against different natural hazards are a priority to be put in place when applying NBS. Besides man-made hazards, Europe is facing increasingly frequent and intense natural hazards, including epidemics, droughts, heat waves, storms, floods and wildfires, which trigger needs for constant innovation when it comes to the protection of people. With the continuing increase of population concentrated in cities and urban areas and increasing impacts of climate change, such risks present a significant challenge in this regard.

NBS can offer the tools to address the potential to improve risk management and resilience using approaches that can provide greater benefit than conventional tools at the same time, like for example heat waves and wildfires, or storms and floods. The detailed understanding of ecosystems and how nature responds to different external shocks can help to strengthen existing strategies for urban resilience and deliver new approaches in protection, for example by integrating natural components in the different infrastructure assets.

Applicants are required to demonstrate strategies for the projects to build synergies with the expected ***European partnership to coordinate R&I efforts on land management and climate related disasters*** under DRS02-5.2021.

[11] https://ec.europa.eu/newsroom/horizon2020/document.cfm?doc_id=10195

Destination – Increased Cybersecurity

Relevant Cluster 3 Expected Impact:

"Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats."

Europe is in the midst of a digital transformation. Digital technologies are profoundly changing our daily life, our way of working and doing business, and the way people travel, communicate and relate with each other. Digital communication, social media interaction, artificial intelligence e-commerce, and digital enterprises are steadily transforming our world. They are generating an ever-increasing amount of data, which, if pooled and used, can lead to a completely new means and levels of value creation. The more interconnected we are, however, the more we are vulnerable to cyber threats.

Digital disruption, notably caused by malicious cyber activities, not only threaten our economies but also our way of life, our freedoms and values, and even try to undermine the cohesion and functioning of our democracy in Europe.

Regardless of the economic, political or personal motivations behind the cyber threats, securing our future wellbeing, freedoms, democratic governance, and prosperity depend on improving our capacity to shield the EU from malicious attacks and to address digital security weaknesses in general. The digital transformation requires improving cybersecurity substantially, so as to ensure the protection of the increasing number of connected devices and the safe operation of network and information systems, including power grids, drinking water supply and distribution services, vehicles and transport systems, hospitals and the overall health system, finances, public institutions, factories, and homes. Europe must build resilience to cyber-attacks and create effective cyber deterrence, while making sure that data protection and freedom of citizens are strengthened. These efforts should include considerations for particularly vulnerable organisations and citizens.

The technological tools of cybersecurity are strategic assets, as well as being key growth technologies for the future. It is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy, to protect critical hardware and software and to provide key cybersecurity services.

Cybersecurity research and innovation activities will support a Europe fit for the digital age, enabling and supporting digital innovation while highly preserving privacy, security, safety and ethical standards. They will contribute to the implementation of the digital and privacy policy of the Union, in particular the NIS Directive, the EU Cybersecurity Act, the GDPR, and the future e-Privacy Regulation.

Research and innovation will build on the results of Horizon 2020. The activities will be aligned as relevant with the future objectives of the Cybersecurity Competence Centre and Network of National Coordination Centres (Commission proposal COM(2018) 630). They will be complementary to actions under the Digital Europe Programme, for example actions relevant to Cybersecurity and digital skills will be addressed by support to innovative approaches and tools to raise awareness and skills of end-users on digital security. Research and innovation results may feed into the operational work on preparedness and response in the Joint Cyber Unit.

<u>Expected impact:</u>

Proposals for topics under this Destination should set out a credible pathway contributing to increased cybersecurity and a secure online environment, and more specifically to one or several of the following impacts:

- Strengthened EU cybersecurity capacities and European sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across Europe
- Reinforced awareness and a common cyber security culture

The following call(s) in this Work Programme contribute to this Destination:

CALL Increased cybersecurity 2021 or 2022[12]:

Proposals are invited against the following topic(s):

Area 1: Secure and resilient digital infrastructures and interconnected systems

CS1.1.2022 (IA) – Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

[12] Budget and specific call title and call year to be decided

- Improved disruption preparedness and resilience of digital infrastructure in Europe
- Improved capacity building in digital infrastructure security including organizational capabilities
- Robust evidence used in cybersecurity decisions and tools
- Better prediction of cybersecurity threats and related risks
- Improved response capabilities based on collaboration with other relevant national or EU bodies in charge of Cybersecurity, including holistic incident reporting.

Scope: Digital infrastructures together with their connected devices are characterised by complex interdependencies involving various physical and logical layers and connecting a wide range of legacy IT solutions and innovative technologies. Application scenarios include but are not limited to cybersecurity of communication systems and networks and their components, e.g. 5G networks, Internet of Things (IoT) devices, medical devices, supervisory control and data acquisition (SCADA) systems, and their services, e.g. cloud-based ICT solutions. Their availability, controlled performance and reliability need to be guaranteed at every moment serving the needs, sometimes critical and safety-related e.g. in transportation, energy, healthcare, of millions of citizens, enterprises and society. Therefore, they need to be protected in real-time against ever-evolving cybersecurity threats.

Building on research and innovation in the area of cybersecurity of digital infrastructures for example projects funded from H2020 SU-DS01-2018[13], SU-DS04-2018-2020[14], SU-DS05-2018-2019[15] and SU-TDS-02-2018[16] , state of the art technologies should support the logging, categorisation, data aggregation from different sources, automatic information extraction and analysis of cybersecurity incidents. Proposals should develop and validate demonstration prototypes of tools and technologies to monitor and analyse cybersecurity incidents in an operational environment in line with the NIS directive and the General Data Protection Regulation. They should contribute to improved penetration testing methods and their automation by using machine learning and other AI technologies as appropriate. Moreover, proposals should support effective network traffic analysis applying detection techniques in network operations based on advanced security information management and threat intelligence. Proposed solutions should also include validation or piloting of cyber threat

[13] Cybersecurity preparedness - cyber range, simulation and economics

[14] Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches

[15] Digital security, privacy, data protection and accountability in critical sectors

[16] Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures

intelligence with early-stage detection, prediction and contributions towards response capability using predictive analytics, and as relevant, with efficient and user-friendly interaction methods, e.g. visual analytics. Furthermore, solutions deployed by this action should validate their approach to intrusion detection and incident monitoring with real end-users and their needs. A strong culture awareness of data protection should be fostered. The proposals should also appropriately address concerns about mass surveillance and protection of personal spaces.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side. Participation of SMEs is strongly encouraged. For these grants, beneficiaries may strengthen the activities by providing financial support to third parties in line with the conditions set out in General Annex [X] of the Work Programme.

The proposal should provide appropriate indicators to measure its progress and specific impact.

CS1.2.2021 (RIA) – Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Advanced self-healing disaster recovery and effective business continuity in critical sectors (e.g. energy, transportation, health).
- Better disaster preparedness against possible disruptions, attacks and cascading effects
- Better business continuity covering two or more sectors

Scope: This action aims at developing new methodologies, services and tools for accelerating the self-recovery and possible adaption of the infrastructures and supply chains after an attack. In line with the NIS Directive the focus should be on critical sectors (e.g. energy, transportation, health) as well as telecommunication networks. The proposal should go beyond the state-of-the-art in developing and validating AI-based self-healing, effective business continuity and disaster recovery in real-world scenarios covering two or more business sectors and supporting their private and public actors.

Cyber threat intelligence and situational awareness need to be developed from the current research level towards strategic considerations, and down to real-time events. This requires collaboration and data sharing between different security actors and should be based on a collection of heterogeneous data, models and predictions for multi-level security. Cyber incidents are likely to require the efforts from a heterogeneous network of organisations, both when it comes to prevention, detection and response. Thus, an organisational perspective should be included.

The proposed solutions should include dynamic execution of disruption recovery and business continuity processes. They should dynamically extract all relevant digital evidence, information and digital traces, provide real-time personalised technical assistance, share information and real-time alerts with relevant stakeholders.

Human factors (e.g. behavioural, psychological, and cultural) need to be considered appropriately in all aspects of the proposed solution. Proposals should build on existing research and projects[17], clearly identify the state-of-the-art and explain the strengths of the new solution in the context of the chosen sectors.

Research should address the risks and impact of a cyber-incident on the business itself, using appropriate KPIs, but also possible cascading effects of cyber incidents for critical infrastructure and society overall.

The research should include a proof of concept in order to validate the claimed progress and show the benefits in an adequate testing environment involving real end-users. End-users should be involved in all steps of the cycle from design to development and testing. Participation of SMEs is encouraged.

The proposal should provide appropriate indicators to measure its progress and specific impact.

Area 2: Hardware, software and supply chain security

CS2.1.2022 (RIA) – Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components

Expected Outcomes: Projects' results are expected to contribute to one or more of the following outcomes:

- Effective access control to system components and management of trustworthy updates
- Modelling of security and privacy properties and frameworks for validating and integration on the testing process
- Integrated process for testing, formal verification, validation and consideration of certification aspects
- Tools providing assurance that third-party and open source components are free from vulnerabilities weakness and/or malware

[17] References to be included.

- Data security “by design” e.g. via secure crypto building blocks
- Instrumentation and secured communication with system components for dynamic testing
- Methods and environments for secured coding by-design and by-default and secure hardware and software construction
- Effective audit procedures for cybersecurity testing
- Introduction of scalable dynamic fuzz-testing methodologies together with symbolic execution
- Methods or procedures to make supply chains secure

Scope: – Trustworthy methodologies and tools for advanced analysis and verification, and dynamic testing of potentially vulnerable, insecure hardware and software components calls for good practices for system security, with a particular focus on software development tools, IT security metric and guidelines for secure products and services throughout their lifetime. A holistic methodology is needed, integrating runtime methods for monitoring and enforcement as well as design-time methods for static analysis and programme synthesis, which allows for the construction of secure systems with the strongest possible formal guarantees. The firmware of devices, implementations of communication protocols and stacks, Operating Systems (OSs), Application Programming Interfaces (APIs) supporting interoperability and connectivity of different services, device drivers, backend cloud and virtualization software, as well as software implementing different service functionalities, are some examples of how software provides the essence of systems and smart (networked) objects. Due consideration to supply chain issues, including integration of software and hardware, should be given.

R&I will be funded to develop hybrid, agile and high-assurance tools capable of automating evaluation gestures; accountability tools for audit results and updates and lightweight, isolated virtualisation environments capable of securely inspecting and orchestrating appliances in heterogeneous hardware and software architectures. Moreover, KPIs, metrics, procedures and tools for dynamic certification of implementation security and scalable security, from chip-level to software-level and service-level, should be developed. It may also include testing methods like coverage guided fuzzing as well as symbolic execution.

CS2.2.2021 (RIA) – Improved security in open-source and open-specification hardware for connected devices

Expected Outcomes: Projects' results are expected to contribute to one or more of the following outcomes:

- Reduced security threats of open source hardware for connected devices.
- Formal verification of open hardware.
- Use of reconfiguration to implement security patches for open hardware.
- Effective management of cybersecurity patches for connected devices in restricted environments such as IoT devices.
- Effective security audits of open source hardware, software and other security-relevant aspects of connected devices.
- Effective mechanisms for inventory management, detection of insecure components and decommissioning.
- Methods for secure authentication and secure communication for connected devices in restricted environments such as IoT devices.

Scope: The quality of hardware and software, notably open source, for IoT and connected devices is improving. However, the restricted environment of many IoT devices does not allow the deployment of more complex protection schemes (e.g. Trusted Platform Modules, Sandboxing applications in managed memory partitions) and other approaches to ensure cybersecurity. Open Source designs are frequently used in IoT technology and become more reliable and efficient with the number of developers that deploy them. The management of this large collaborative development environment that Open Source represents is a real cybersecurity challenge.

The aim is to support European trustworthy platforms by methods, tools and technologies that foster a stronger Cybersecurity, which can serve in a variety of connected devices. The proposed action should integrate formal security models and verified and scalable cryptography that can be used in future key system components (operating systems,…).

Proposals should cover one or more of these research activities:

- development of verifiable implementations of cryptographic solutions, authentication schemes, and, as relevant, software libraries that implement them securely in operating systems;

- develop mechanisms to mitigate hardware-related security vulnerabilities
- development of security auditing for connected devices;
- development and advancing of security testing in restricted environments;
- development and advancing of verification methods for secure software patching in connected devices;
- development of multi-factor authentication hardware and software solutions.
- development of the security upgrading of the connected devices within the life cycle (bootstrapping, commissioning, operational, upgrade etc)

Area 3: Cybersecurity and disruptive technologies

CS3.1.2022 (IA) – Transition towards Quantum-Resistant Cryptography

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Measuring, assessing and standardizing/certifying future-proof cryptography.
- Gaps between the theoretical possibilities offered by quantum resistant cryptography and its practical implementations are addressed.
- Quantum resistant cryptographic primitives and protocols encompassed in security solutions.
- Solutions and methods that could be used to migrate from current cryptography towards future-proof cryptography.
- Preparedness for secure information exchange and processing in the advent of large-scale quantum attacks.

Scope:

During the next decades Europe should seize the opportunities that quantum technologies will bring. However, quantum technologies will also pose a significant risk to the security of our society. The advent of large-scale quantum computers will compromise much of modern cryptography, which is instrumental in ensuring cybersecurity and privacy of the digital transition. Any cryptographic primitive based on the integer factorization and/or the discrete logarithm problems will be vulnerable to large-scale quantum-powered attacks. The digital data/products/systems that derive their security ultimately from the abovementioned primitives will be compromised and must be upgraded -including their replacement when needed- to quantum-resistant cryptography. The massive scale of this foreseen upgrade shows that preparations are needed today in order to widely implement the relevant mitigations in the future. Many companies and governments cannot afford to have their protected communications/data decrypted in the future, even if that future is a few decades away. There is a need to advance in the transition to quantum-resistant cryptography.

Applicants should propose approaches to tackle the abovementioned challenges, with the goal to develop cryptographic systems that are secure against attacks using both quantum or/and classical computers. Proposals may also try to better understand the expected capabilities of quantum computers (e.g. novel relevant quantum algorithms) and to further assess their implications to cybersecurity.

The proposed actions responding to this topic should take stock of and build on the relevant outcomes from other research fields (such as mathematics, physics, electrical engineering) and actions (e.g. H2020 projects, NIST Post-Quantum Cryptography competition, efforts in ETSI), and are encouraged to plan engaging and cooperating with them to the extent possible. For these grants, beneficiaries may strengthen the activities by providing financial support to third parties in line with the conditions set out in General Annex [X] of the Work Programme

Proposers should demonstrate innovative ways to design, build, and deploy the new quantum-resistant infrastructures (including relevant hardware, software and IT processes). This should include switching from nowadays infrastructures to the proposed new ones with practical migration paths, aiming to efficiently manage the total time needed and the total costs associated, while also paying attention to affordable energy consumption.

Applicants should look at the implementation of quantum-resistant algorithms on software as well as specific hardware, such as. resource constrained IoT devices, smart cards, high-speed field-programmable gate arrays.

Proposals should devise, develop and validate metrics, methodologies, conformity assessment tests and tools for assessing and quantifying the security and the privacy of the proposed systems and services. Furthermore, proposals should strive to encompass a thorough comprehensive security evaluation of the engineering and deploying of efficient and secure implementations of the proposed solutions. Due consideration should be given to countermeasures against side channel attacks.

Applicants should strive to use the most promising relevant cryptographic primitives as well as to adapt the used cryptographic protocols accordingly.

Proposals may analyse how to develop combined quantum-classical[18] cryptographic solutions in Europe, for those use cases where these hybrid solutions might bring gains to the overall security. To this end, the analysis should take into account relevant actions in quantum cryptography (e.g. H2020 OpenQKD project, EuroQCI). Furthermore, hybrid solutions may also include a combination of classical and post-quantum-resistant algorithms.

Proposals should validate their concept by exercising and deploying pilot demonstrators in relevant use cases. The demonstrators should include exercises on executing different migration strategies for real use cases and applications that would allow their implementation in large-scale, complex systems. Lessons learned from the exercises should be transformed into practical, multidisciplinary guidelines that support entities to plan and execute their own migration, considering the technical, the economical and legal contexts.

CS3.2.2021 (RIA) – AI for cybersecurity reinforcement

Expected Outcomes: Projects’ results are expected to contribute to at least one of the following outcomes:

- Reinforced cybersecurity using AI technological components and tools in line with relevant EU policy, legal and ethical requirements.
- Increased knowledge about how an attacker might use AI technology in order to attack IT systems.
- Digital processes, products and systems resilient against AI-powered cyberattacks.

Scope:

Artificial intelligence (AI) is present in almost every application area where massive data are involved. Understanding the implications and possible side effects for cybersecurity however requires deep analysis, including further research and innovation. On the one hand, AI can be used to improve response and resilience such us for the early detection of threats and other malicious activities with the aim to more accurately identify, prevent and stop attacks. On the other hand, attackers are increasingly powering their tools by using AI or by manipulating AI systems.

The proposed actions addressing this topic should develop AI-based methods and tools in order to (i) improve systems robustness (i.e. the ability of a system to maintain its initial stable configuration even when it processes erroneous inputs, thanks to self-testing and self-healing);

[18] [18] “classical” is used here with the sense of non-quantum. Hence “post-quantum cryptography” is considered as advanced classical cryptography.

(ii) improve systems resilience (i.e. the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection and allowing security analysts to retrieve information about cyber threats); (iii) improve systems response (i.e. the capacity of a system to respond autonomously to attacks, thanks to identifying vulnerabilities in other machines and operate strategically by deciding which vulnerability to attack and at which point, by deceiving attackers and by being able of launching efficient counterattacks); and to (iv) counter the ways AI can be used for attacking (e.g. adversarial machine learning, manipulating AI-powered cybersecurity systems). Advanced AI-based solutions, including machine learning tools, as well as defensive mechanisms to ensure data integrity should also be included in the proposed actions. Proposals should strive to ultimately facilitate the work of relevant cybersecurity experts (e.g. by reducing the workloads of security operators).

Regarding the manifold links among AI and cybersecurity, privacy and personal data protection, applicants should demonstrate how their proposed solutions comply with and support the EU policy actions and guidelines relevant to AI (e.g. Ethics Guidelines for Trustworthy AI, the AI Whitepaper, and the Data Strategy). Proposals should foresee activities to collaborate with projects stemming from relevant topics included in the Cluster 4 “Digital, Industry and Space” of Horizon Europe. Proposals should also build on the outcomes of and/or foresee actions to collaborate with other relevant projects (e.g. Horizon 2020 projects).

Proposals should strive to use, and contribute to, European relevant data pools (including federations of national and/or regional ones to render their proposed solutions more effective. To this end, applicants should crucially strive to ensure data quality and homogeneity of merged/federated data. Applicants should also identify and document relevant trade-offs between effectiveness of AI and fundamental rights (such as personal data protection). Moreover, privacy in big data should also be addressed.

Key performance indicators (KPI), with baseline targets in order to measure success and error rates, should demonstrate how the proposed work will bring significant progress to the state-of-the-art.

Area 4: Smart and quantifiable security assurance and certification shared across Europe

CS4.1.2022 (IA) – Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

Expected Outcomes: Projects are expected to contribute to at least three of the following outcomes:

- Availability of applicable tools and procedures for partial and continuous assessment and lean re-certification of ICT products, ICT services and ICT processes;
- Reduction of efforts spent for (re-) certifying ICT products, ICT services and ICT processes;
- Improved stakeholder collaboration on cybersecurity certification information, including manufacturers and end users from different Member States;
- Efficient (re-)use of information and evidence relevant to certification and in support of multi-scheme (re-)use;
- Integration of certification on the whole system modelling, verification, testing and verification process
- Increased comparability of assurance statements arising from certification schemes and the standards used therein; avoidance of multi-certification;
- Advancing test and simulation facilities, including incident and threat analysis;
- Increased Digital Twin capabilities for continuous assessment and integration of new solutions.

Scope:

In order to foster the application of security standards, agile certification and continuous assessment of cyber resilience systems, actions will cover the harmonising, packaging and distributing of certification processes for contemporary ICT products, services, and processes but to new and disruptive technologies as well, such as AI and High Performance Computing.

To support cybersecurity autonomy of the EU, approaches concerning a dynamic, real time, collaborative vulnerability testing and information sharing should be developed and build on existing resources. The resources may range from tools, procedures, practices, and information sources, such as checklists, flaw repositories deployment and configuration guidance, and impact assessments posted by European industries, manufacturers, developers, CSIRTs, ISACs (Information Sharing and Analysis Centres), or national and international authorities (e.g. NIST, JVN) and relevant standards.

For these grants, beneficiaries may strengthen the activities by providing financial support to third parties in line with the conditions set out in General Annex [X] of the Work Programme

The actions should aim at improving certification processes, tools, evidence presentation and assurance statements, at least in quantifiable terms, where relevant by relying on a suitable IT security metric and should complement or aid other certifications relevant in other sectors or risk scenarios.

Area 5: Human-centric security, privacy and ethics

CS5.1.2021 (RIA) – Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

<u>Expected Outcomes</u>: Projects' results are expected to contribute to one or more the following outcomes:

- Improved scalable and reliable privacy-preserving technologies for federated processing of personal data and their integration in real-world systems

- More user-friendly solutions for privacy-preserving processing of federated personal data registries by researchers

- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solution

- Contribution to promotion of GDPR compliant European data spaces for digital services and research (in synergy with topic DATA-01-2021 of Horizon Europe Cluster 4)

- Strengthened European ecosystem of open source developers and researchers of privacy-preserving solutions

<u>Scope</u>: Using big data for digital services and scientific research brings about new opportunities and challenges. For example, machine learning methods process medical and behavioural data for finding causes and explanations for diseases or health risks. However, a large amount of this data is personal data. Leakage or abuse of this kind of data and potential privacy infringement (e.g. attribute disclosure or membership inference) risks are a cybersecurity threat to individuals, society and economy and an impediment for further developing data spaces involving personal data. Vice versa, adequate protection of this data according to the GDPR can also prevent its full utilization for society. Advanced privacy-preserving computation techniques such as homomorphic encryption, secure multiparty computation, and differential privacy are being researched and have proven promising to address these challenges. However, further research is required to ensure their applicability in real-world use case scenarios. For example, fully homomorphic encryption is not practically applicable in many cases and secure multi-party computation often imposes special infrastructural requirements.

Building on research and innovation in the area of privacy-preserving computation, proposals should address scalability and reliability of privacy-preserving technologies in realistic problem areas and take integration with existing infrastructures and traditional security measures (e.g. access control) into account. They should respond to users' needs, e.g. for research and digital services in access and data management for citizens geared towards their own profiles (incl. dynamic personalised recommendations for improved cybersecurity) or in personalised medicine. They should further address the legacy variation in personal data types and data models across different organisations in the same business sector and/or across different potential application sectors. A proposed solution should include validation or piloting of privacy-preserving computation in realistic federated data infrastructures and more specifically European data spaces involving personal data (e.g. the EU heath data space). It should be guided by the EU's high standards concerning the right to privacy, protection of personal data, and the protection of fundamental rights in the digital age. It should ensure, by-design, compliance with data regulations and specifically the GDPR.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side, i.e. industry, service providers and end-users. Participation of SMEs is strongly encouraged. . Legal expertise should also be incorporated to assess and ensure compliance of the technical project results with data regulations and the GDPR.

The proposal should provide appropriate indicators to measure its progress and specific impact.

Destination - A Disaster-Resilient Society for Europe

Relevant Cluster 3 Expected Impact:

"Losses from natural, accidental and man-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness and resilience and improved disaster risk management in a systemic way."

This Destination supports the implementation of international policy initiatives (e.g. the Sendai Framework for Disaster Risk Reduction, Green Deal, SDGs), **EU Disaster Risk Reduction** and climate change adaptation policies tackling natural and man-made threats (either accidental or intentional) and the **Security Union Strategy** (in particular for disasters linked to terrorism).

The world and our societies are facing growing risks of anthropogenic and natural hazards, which call for enhanced capacities in risk and resilience management and governance, including instruments for better prevention and preparedness, technologies for first responders and overall societal resilience. The increasing severity and frequency of extreme weather events (e.g. floods, heat and cold waves, storms, forest fires) resulting from anthropogenic climate change compounded vulnerabilities, and exposure requires a specific research focus while geological hazards (earthquakes, tsunamis, volcanic eruptions) and slow-onset hazards (e.g. sea-level rise, glacier melt, droughts) also deserve a continuous attention. Anthropogenic threats also demand strengthened crisis management capacities, as shown by recent industrial accidents and terrorist attacks associated with chemical, biological, radiological, nuclear and explosive materials (CBRN-E). Finally, the COVID-19 crisis has demonstrated how human society has become more exposed and vulnerable to pandemic risks and shown that existing global inequalities often exacerbate both the exposure and vulnerability of communities, infrastructures and economies.

Risk reduction of any kind of disasters is regulated by a number of international, EU and national and local policies and strategies covering various sectors and features such as awareness raising, prevention, mitigation, preparedness, monitoring and detection, response, and recovery. Our societies nowadays have to deal with complex and transboundary crises within which a more systemic approach with strict interconnection between risk reduction and sustainable development is needed. Complex crises affect scientific, governance, policy and social areas and require inter-sectoral cooperation. A wide range of research and technological developments, as well as capacity-building and training projects, has supported the development and implementation of policies and strategies. Integrating needs are, however, overwhelming owing to the complexity of the policy framework and the high level of fragmentation of research and capacity-building initiatives. In addition, enhanced cooperation and involvement of different sectors and actors are essential, including policy-makers, scientists, industry/Small and Medium Enterprises (SMEs), public administration (both at national and regional/local level), scientists, credit /financial institutions, practitioners, Non-Governmental Organisations (NGOs), and Civil-Society Organisations (CSOs), notwithstanding the citizen dimension.

In this respect, the implementation of international policy initiatives (e.g. the Sendai Framework for Disaster Risk Reduction), EU Disaster Risk Reduction and climate change adaptation policies tackling natural and man-made threats (either accidental or intentional) and the Security Union Strategy (in particular for disasters linked to terrorism), requires cross-border cooperation as well as enhanced collaboration among different actors and strengthened knowledge covering the whole disaster management cycle, from prevention and preparedness to response and recovery. Understanding and exploiting the existing linkages and synergies among policy initiatives such as the Paris Agreement, the EU strategy on adaptation to climate change, the EU Green Deal, the Sendai Framework and the Sustainable Development Goals (SDGs) represents in this sense a global priority for future research and innovation actions in the field of natural hazards and man-made disasters.

For the response side, international cooperation on research and innovation with key partners has the potential to identify common solutions and increase the relevance of outcomes. As such, the International Forum to Advance First Responder Innovation (IFAFRI) has provided a detailed, sophisticated overview of existing gaps and offer the possibility to engage in cooperation with partners inside and outside the EU, the results of which can provide a valuable source for identifying most urgent needs concerning disaster management (e.g. knowledge, operational, organizational and technological) of relevance to international cooperation, in particular in support to the implementation of international policies such as the Sendai Framework for Disaster Risk Reduction.

Integrated approaches are essential to bridge different policy areas including civil protection, environment (including water, forestry, biodiversity / nature and Seveso-related policies), climate change adaptation and mitigation, health and consumer protection, and security (in particular in the CBRN-E area). Common resilience pathways emerging from different scientific and operational domains still need to be explored in terms of their implementation potential. It also requires the strengthening of opportunities for transdisciplinary and transboundary joint efforts in order to organise and structure, a new strategy for the Horizon Europe Framework with all the relevant actors. In particular, the paradigm shift from managing “disasters” to managing “risks” and enhancing resilience needs to be supported by research and innovation actions, including innovative methods and solutions addressed to decision-makers, to support complementary education and training needed in all the domains of interventions (from public administration to private companies, citizens, NGOs), complementary procedural and organisational changes that have impact on the overall society as well as on technologies, processes, procedures and various tools in support of first responders operations. A huge body of knowledge and technology has been developed in the Seventh Framework Programme and Horizon2020. This forms a strong legacy that will pave the way for future research in support of an enhanced resilience of European society to disasters of any kind, and previous findings will need to be fully recognized and used in forthcoming research developments.

Expected impact

Taking into account previous findings resulting from FP7 and H2020 developments and other research programmes, proposals for topics under this Destination should set out a credible pathway to contributing to a disaster-resilient society for Europe, more specifically to one or several of the following impacts:

- Enhanced understanding and improved knowledge and situational awareness of disaster-related risks by citizens, empowered to act, thus raising the resilience of European society.

- More efficient cross-sectoral, cross-disciplines, cross-border coordination of the disaster risk management cycle (from prevention, preparedness to mitigation, response, and recovery) from international to local levels.

- Enhanced sharing of knowledge and coordination regarding standardisation in the area of crisis management and CBRN.

- Strengthened capacities of first responders in all operational phases related to any kind of (natural and man-made) disasters so that they can better prepare their operations, have access to enhanced situational awareness, have means to respond to events in a faster, safer and more efficient way, and may more effectively proceed with victim identification, triage and care.

The following call(s) in this Work Programme contribute to this Destination:

CALL DRS 2021:

Area DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens

Topic DRS01-1.2021 (RIA) Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

- Advanced disaster / crisis simulations and impact assessments supporting decision-making processes based on best available knowledge, adaptive strategies and methodologies, including accurate exposure data and adequate vulnerability curves, quantitative hazard information with comparable metrics across different risks (especially addressing multi-hazards situations), including losses and damages data and qualitative information issued from historical testimonies and case studies.

- Risk and resilience assessment studies and outputs in support of long-term multi-hazard management strategies (e.g. climate adaptation, disaster risk reduction and prevention and mitigation strategies) with a focus on vulnerable regions prone to multiple hazard occurrences, involving interdisciplinary teams in different scientific and technological fields (such as geology, climate, man-made hazards, critical infrastructures and assets, history, health sciences, economics and social sciences). This requires novel interdisciplinary risk approaches to assessing human-hazard interactions, and reaching the most vulnerable segments of the community.

- Advanced data management, information update and forecast / early warning systems (including via satellite and in-situ observation) in support of evolving public understanding and decision-making needs in the field of multi-hazard preparedness policy and planning, taking into account data uncertainties and including the determination of baseline scenarios and corresponding risk thresholds, as well as data potentially available (e.g. from surveys, earth observations, historic databases, academic and business/private sector repositories, climate projections, etc.) and near-real-time impact simulations combined with data-farming approaches.

- Communication and dissemination platforms supporting an increased dialogue and cooperation between scientific, technological, practitioners, policy-makers, private sector (e.g. insurers), NGOs, citizens and community-based organisations for sharing and building-up the knowledge of hazards and related risks for a comprehensive awareness (and preparedness) of the risk at all levels (risk memory and implementation of lessons learnt into policy actions), taking into account various uncertainties that may affect decision-making.

Scope:

The awareness of multiple hazards and the understanding and the assessment of risks and their consequences is a critical and fundamental step towards the development of local, national and international policies and strategies within all phases of the disaster risk management cycle, in particular preparedness. The availability of reliable scientific data and information (including historical occurrences and climate projections) to anticipate future disaster events or crisis situations, considering uncertainties inherent to natural systems characterization, and effectively support decision-making processes at all levels represents a global challenge for both the research community and governance institutions.

Actions at national/local and global/regional levels rely on knowledge of risks in all its dimension and changeable nature. A strengthened understanding of risks by the population (and decision-makers) is needed, based on both records of past events and forecasts and projections (with quantified uncertainties) that reflect consideration of evolving trends and dynamics over time and space. This is particularly acute in the case of multi-hazard risks, i.e. occurrences of several disasters either in cascade or at once. Moreover, the work needs to be complemented with improved knowledge on how risk awareness and actions are influenced and shaped by diverse aspects such as past events, cultures and traditions.

The understanding of multiple disaster risks (and related awareness) relies on knowledge gained about historical data and information about past events and related lessons learned as well as the ability to forecast and assess future risks under uncertainty (including impacts of pandemics, as well as global change, including climate trends and earth system and environment dynamics). These complex interactions between human decisions and multiple hazards require novel risk assessment approaches such as agent-based modeling and systems dynamics methods. This will result in improved preparedness actions built upon these analyses (e.g. defining evacuation routes, responsiveness of health services, etc.). Social media also plays a role in disaster analytics. For example, an increasing number of location-based social network services can provide time-stamped, geo-located data that opens new opportunities and solutions to a wide range of challenges by analysing the extracted public behaviour responses from social media before, during and after disaster events. When using social media data, the design for data collection and analysis has to respect fundamental rights, privacy and data protection and analyses have to take related societal effects in online and offline environments into account. Also, risk awareness, understanding and preparedness are unequally distributed along a wide range of variables (socio-economic, cultural, regional etc.) that may generate drawbacks and conflicting issues with respect to groups' vulnerability.

Topic DRS01-2.2021 (IA) - Enhanced citizen preparedness in the event of a disaster or crisis-related emergency –

Expected Outcomes: Projects’ results are expected to contribute to the following outcomes:

- Design of preparedness actions linking together multilevel interventions that need to involve citizens, communities, business organisations, public administrations for empowering citizens and their communities to act by themselves together with emergency services and managing spontaneous volunteers in the case of a disaster or crisis-related emergency of any kind (natural hazards, including pandemics, or man-made including terrorist threats) in the form of best practices and guidelines exploiting local resources (knowledge, networks, tools) developed with practitioners and local decision-makers.

- Development of effective means for communication improving inter-organisational collaborative processes e.g. early warning systems and communication chains, roles, tasks and responsibilities of citizens, communities, local authorities, NGOs, business companies and practitioners, taking into account the legal framework, procedures for normal operation and organizational boundaries.

- Improved early warning systems, forecasts and strategies to reach different public representatives with proper messages in the event of a disaster.

- Demonstration exercises involving citizens, training and educational institutions, local decision-makers, employees in public administrations and in business companies, and practitioners, to identify practices, test guidelines and communication strategies in near-real-case situations in the framework of field exercises, virtual trainings and serious gaming, school / university curricula and professional training.

- Building a ‘culture of disaster preparedness’ for citizens, communities, public administrations, business companies, practitioners: Development of an effective education system and integration of theory and practice of preparedness in school curricula; development of an effective integration of multilevel action in public administration (at local and regional national and international levels) focusing also on responsibility and deliberation issues; development of effective preparedness practices for citizens, communities, business organisations and practitioners (and their associations).

- Deployment of evidence-based assessment methods/models to monitor and strengthen emergency preparedness.

Scope:

Improving societal resilience to disasters or crises relies on various features related to preparedness of citizens, communities, education systems, public administrations, business companies and practitioners. These concern, in particular, ways to react and informed decisions to take in case of an event. Individual, public and multi-level actions are needed in disaster risk management and they have huge implications on potentially reducing losses and increasing the operational capacity of responders, along with significant impacts on the emergency planning and management phases and its relation to continuous operations and existing safety management. In particular, the level of awareness of EU citizens of the risks in their region is an indicator for measuring progress in increasing public awareness and preparedness for disasters and in the implementation of the Union Civil Protection Mechanism legislation.

Besides the required risk understanding dealt with in topic DRS01-1.1.2021, research is needed in several domains. With regard to public administrations, it is relevant to conceptualize how to increase risk awareness by building processes capable of fostering a long-lasting coalition with citizens around the objective of reducing vulnerability. This implies the definition of action protocols and models of responsibility that mobilize the intervention of individual employees of public administrations. With regard to business companies and practitioners, it is relevant to integrate their emergency activities in the local context. With regard to citizens and communities, it is necessary to design preparedness actions enabling an empowerment of citizens (including particularly vulnerable groups), their communities and NGOs through bottom-up participatory and learning processes. This includes school/university curricula and professional training and trust building among local actors, integrating relevant traditional knowledge, incorporating a gender perspective where relevant, best practices, guidelines, and possible changes of regulations, to allow participatory actions. Difficulties in communication to the public in preparedness (and response) phases requires the consideration of legal aspects, along with investigations into innovative practices, forms and tools that will enable the more effective sharing of information. These will support citizens in acting efficiently by themselves, through enhanced collaboration and communication and improving information exchanges between local authorities (including first responders), vulnerable populations (e.g. socio-economic groups, ethnic groups, people with illnesses or disabilities, children, elderly, hospital patients), and the private sector.

Moreover, recent crises have shown that there is a large sense of solidarity among the population during a disaster or crisis situation. Many citizens that were not involved in disaster relief organisations before the crisis want to offer support to their fellow citizens and the broader community in times of crises. These initiatives of “spontaneous volunteers” are however most efficient if they are informed and trained and if their valuable contributions are coordinated with the authorities and first-responders on the ground. Preparedness plans, tests and continued adaption on how best to manage spontaneous volunteers and integrate those into the response are needed.

Area DRS02 - Improved Disaster Risk Management and Governance

Topic DRS02-1.2021 (IA) - Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building

Expected Outcomes: Projects’ results are expected to contribute to the following outcomes:

- Improved dialogue and cooperation among scientific and technical communities, stakeholders, policy-makers and local communities in the field of extreme climate events (e.g. forest fires, droughts, floods, heatwaves and storms) and disaster risk reduction.

- Enhanced community engagement for prevention, preparedness and response to extreme climate events by strengthening knowledge and involvement of volunteers linked to recognised organisations into the planning, design and implementation of prevention, including building with nature, preparedness and emergency response activities.

- Strengthening of disaster risk reduction and resilience building through innovative use of media means, namely by examining the potential of new communication tools and apps for better preparedness and response.

- Overview of existing knowledge, tools and development of new tools (innovative data collection, satellite data, data harmonisation, artificial-intelligence tools, algorithms, sensors and decision-aid approaches) for early warning, response and resilience / adaptation to be demonstrated in the framework of real-case scenarios designed for training addressed to first responders, (national, regional, local) authorities and populations. The overview should document how legal and ethical rules of operation as well as fundamental rights such as privacy and protection of personal data are taken into account.

- Based on the demonstrations, development of new governance strategies and robust decision-support methodologies for integrated risk reduction and improved adaptation to climate extreme events.

- Improved understanding of enablers and barriers to multi-risk governance frameworks and multi-risk thinking, by involving interdisciplinary teams in different fields, particularly the social and behavioural sciences.

- Cost-benefit or cost-effectiveness analyses of investment and regulatory strategies to protect people and nature in vulnerable areas.

- Identification of production/livelihood practices (goods, services, activities etc) at community and national level that contribute to increased local/global climate risks, and explore how these can be adapted so that they are both economically and environmentally sustainable.

Scope:

In contemporary society, the capacity of communities and governments to manage expected and/or unexpected extreme climate events depends heavily on effective governance throughout the entire Disaster Risk Management cycle. This covers operational mechanisms ranging from short-term actions (e.g. early warning and forecast-based actions) to long-term adaptation strategies and resilience building, including nature-based solutions. A coherent integration between Disaster Risk Reduction, Climate Change Adaptation policies and Sustainable Development Goals as fostered by the Green Deal and UN major initiatives should result in a comprehensive resilience framework, while improving synergies and coherence among the institutions and international agencies involved.

The effective implementation of global and European risk governance and policies to enable integrated disaster risk reduction for extreme climate events requires a collaborative involvement in risk assessment and information sharing across involved institutions, including the civil and private sector and the population.

Cross-regional, cross-border and cross-sector agreements covering all phases of Disaster Risk Management can improve the knowledge about extreme climate events such as forest fires, droughts, floods, heatwaves, storms and storm surges. In addition, improving effective prevention, preparedness and response rely upon specific national or local expertise and experience. It is important to overcome silos between technical and political authorities at all levels and advocate integration among involved actors. Multi-risk governance frameworks related to climate extremes, shifting from single to multi-risk thinking in governmental agencies, represents the key challenge for the future, considering how measures to improve the resilience of the built environment and communities may provide effective solutions to strengthen adaptation measures.

Creating an overview of existing knowledge, integrating tools and developing new ones for resilience and emergency management should include careful planning for interoperability amongst many actors. It is important that solutions pay attention to societal side-effects of integrating data about emergencies, for instance Apps, where persons concerned tend to share more willingly, but do not reflect consequences of that. Thus, the development of data management tools for emergencies need to respect fundamental rights, data protection and avoid function creep.

Topic DRS02-2.2021 (RIA) - Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections

<u>Expected Outcomes</u>: Projects’ results are expected to contribute to the following outcomes:

- Innovative exposure and vulnerability analysis methods, including those that take a systemic perspective by integrating sectoral expertise (e.g. social science, human health, cultural heritage, environment and biodiversity, public financial management and key economic sectors) and identifying key vulnerable groups and assets.

- Maximising usability through a service-oriented approach, including through the optimisation and tailoring recommended practices, scientific models and scenarios for the intended users to support technical policy improvements and implementation of actions.

- Enhanced exploitation of monitoring data and satellite/remote sensing information as well as artificial intelligence to improve high-level assessment from international to local levels, identifying the major sources of uncertainty in hazard assessment and ways to reduce them.

- Evaluation of existing disaster risk and resilience assessment and scenarios (at national and local levels), taking into account historical / geological data, monitoring, risk and forecasting data, and based on the evaluation, serious games, modelling of future scenarios accounting for current and future impacts of diverse extreme events and disasters.

Scope:

The assessment of disaster risks requires different types of actions ranging from soft measures to technologies. Simulation-based risk and impact assessments represent an effective approach to make science understandable to decision makers and streamline national to local mitigation/adaptation actions. This is especially the case if they are integrated with evaluation tools for cost-benefit/effectiveness and multi-criteria analyses, data-farming experiments, serious games, and are tailored to meet end-user’s needs, to assess the effectiveness of alternative options in different phases of the Disaster Risk Management cycle.

Specific risk assessments must be decision- or demand-driven and informed by scientific evidence, and there is a clear need to translate the results to ensure they are relevant, usable, legitimate and credible from the perspectives of the users. Co-design, co-development, co-dissemination and co-evaluation engaging the intended end users represent in this sense key features of improved risk, resilience and impact assessments.

In a first place, the acquisition of data is an essential feature and this requires innovative solutions for faster risk assessment and reduction. This includes the identification of precursors for different types of threats, supporting the design or improvement of risk-targeted monitoring programmes. In addition, risk assessments themselves are primarily designed to predict the likelihood of a specific event, whereas what is of primary concern is the impact of that event on society, infrastructure, governance, etc. Numerous experiences gathered in the natural hazards area showed that an enhanced assessment of risks and scenario building may be improved by taking into account reliable data (both quantitative and qualitative) and historical occurrences, when available, including disaster loss data (studies of past events in particular low-probability / long-time recurrence events). This includes for example a higher completeness of the historical-geological records of volcanic eruptions, major earthquakes, tsunamis etc.

In the case of extreme climate events such as storms and related storm surges, or health crises (outbreaks, pandemics) the analysis should take into account the uncertainties brought on by climate change and our state of knowledge of the key processes underpinning the functioning of the Earth system. In cases where there are not be enough historical data and a high level of uncertainty, assessments and decision making will have to rely on qualitative data.

Topic DRS02-3.2021 (IA) - Improved quality assurance / quality control of data used in decision-making related to risk management of natural hazards, accidents and CBRN events

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Evaluation of Quality Assurance / Quality Control (QA/QC) needs in areas not prone to systematic quality checks prior to decision-making in the natural hazards and CBRN areas, for physical, chemical and biological parameters.
- Based on past experience, organised intercomparisons among laboratories and institutes at EU level which are in charge of providing data for risk- and evidence-based decision-making in order to evaluate the comparability of data produced worldwide.
- Production of reference materials and possible certification schemes for the systematic checking of laboratory and method's performance for monitoring data used in risk- and evidence-based decision-making that are not prone to readily established schemes.

Scope:

Risk management of natural hazards and CBRN events closely rely on available data, taking into account uncertainties brought on by climate change and Earth dynamics. The soundness of decisions is based on quality data, which justifies that continuous efforts are made to improve their quality assurance / quality control, in particular in the natural hazards area as well as in the CBRN area. In many instances, measurement data used in decision-making are rarely challenged in the areas of crisis management and/or mechanisms are still underdeveloped to systematically demonstrate their quality (e.g. in the case of substances of criminal nature such as biological toxins).

Quality assurance / Quality control (QA/QC) are prone to standardized procedures such as the EN 45000 Series, which includes requirements related to laboratory settings, analytical techniques, criteria for analytical performances (e.g. accuracy, repeatability, limits of detection etc.) that are well implemented in sectors such as the environment (including water), food and health. In other areas requiring monitoring data of physical, chemical or biological nature related to risk assessment of natural hazards such as climate threats and pandemics, man-made (accidental) risks (e.g. chemical substances in Seveso-type environments) or terrorism threats (e.g. chemical or biological toxins used for criminal purposes), the QA/QC rules are much less known and followed.

In particular, the systematic comparison of measurement techniques related to risk assessment of natural hazards (including health) and CBRN data is not wide-spread and references data or materials are often lacking. Recent developments have led to the testing of proficiency testing schemes for biological toxins of potential bioterrorism risk, but a general framework for checking data quality and controlling laboratory and analytical technique performances (including from measurement data directly gathered in the field) does not yet exist at European level.

There is hence a need to evaluate the needs for QA/QC developments in relevant areas for which physical, chemical and biological measurement data are insufficiently checked for quality, and to develop an appropriate EU-wide approach to improve and demonstrate this quality, thus ensuring a traceability and comparability of data used throughout Europe for sound risk- and evidence-based decision-making.

Topic DRS02-4.2021 (IA) - Innovative concepts to enhance cooperation and use of available knowledge across disaster and crisis management-related disciplines and administrative levels

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Analysis of the influence of operational and organisational structures in disaster risk reduction on knowledge sharing both across different thematic disciplines and administrative levels.

- Development of concrete knowledge-sharing and knowledge management tools and platforms to enhance the situational awareness and foster cooperation across relevant thematic disciplines usable on different administrative levels (local, regional, national as well as European and international), taking into account the specificities of classified information.

- Development and scale-up of innovative solutions to overcome language, cultural and organisational barriers (e. g. in cross-border cooperation) like collaborative platforms for knowledge exchange including a neutral machine translation engine, which uses machine learning to improve and fine-tune its output. This would help the exchange as authorities could easily translate documents using DRR jargon on the platform

- Concepts to mainstream disaster prevention work and knowledge available in prevention into preparedness and response.

Scope:

Innovative solutions are required to use relevant knowledge available across risk reduction-related disciplines and administrative levels for enhancing cooperation in the case of (natural or man-made) disaster and crisis events, taking into account multiple language aspects. This goes along with needs related to the fostering of cross-sectoral cooperation at different levels (from international to local) between different security-related actors in preparedness and response, prevention, and recovery efforts. Possible actions include cross-sectoral / disciplines networking, information exchanges among existing networks, synergy building among different types of research and innovation, capacity-building, education and training programmes, standardization, deployment of innovative disaster risk financing instruments including risk transfer mechanisms and disaster risk insurance.

The importance of prevention as a field of action in security overall and for disaster-resilient societies is still not well enough understood. This is largely because actors in prevention (e.g. administrative departments and offices such as environment, agriculture, marine, health, consumer protection, economy, energy etc.) are often different from actors in preparedness and response (e.g. civil protection units, fire services, law enforcement agencies, emergency health services etc.) as well as in recovery. Organisational or public management research could be undertaken to find innovative solutions for better cooperating and using relevant knowledge available across disciplines and administrative levels. The specificities of working with classified information that cannot be shared easily should also be considered in this context.

Topic DRS02-5.2021 (CSA) - Developing a European partnership to coordinate R&I efforts on risk management of climate-related disasters

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Consolidate platform gathering key actors involved in risk management of climate-related disasters to identify R&I activities including nature-based solutions, to prevent and reduce the damages caused by climate extreme events (e.g. forest fires, floods) and slow-onset events (e.g. sea-level rise, glacier melt, droughts). Discuss the key features and priorities actions (consultation, dissemination, research programming)

- In consultation with key-stakeholders (practitioners and policy-makers) establish research needs and take relevant steps to accommodate those needs including research programming within the National and European R&I programmes.

- Support to the implementation of the Climate Change Adaptation Strategy, the European Green Deal implementation, as well as Member States' National Adaptation Strategies, and local climate adaptation plans.

Scope:

Climate change increases the intensity and frequency of climate extreme events such as, forest fires, floods and storms, as well as slow-onset events such as sea-level rise and droughts. In addition, unsustainable land-use practices, inadequate land-urban planning and demographic changes make the EU even more vulnerable to natural disasters. Ecosystems provide essential services such as food, fresh water and clean air, and shelter and help regulate the climate. They offer solutions to reduce disaster risk and mitigate natural disasters. Resilient ecosystems offer solutions to reduce disaster risk, but the stakeholders responsible for land-management, environmental protection and Disaster Risk Management communities are fragmented.

Therefore, a CSA is needed to bring these communities together to explore the needs of key-stakeholders, exploit local knowledge and how the research programming can contribute to fulfilling these needs with a special focus on nature-based solutions. This action aims at bringing together all key stakeholders responsible for water, land and environmental protection and Disaster Risk Management for the development and implementation of strategies and plans to prevent and reduce the damages caused by for climate extreme events. This will require the collaboration and information sharing across all involved institutions, including the private sector and local communities, where the collaboration follows clear legal and political frameworks.

Existing advisory structures like the Expert Group on Forest Fires, the Coordination Group on Biodiversity and Nature and the Disaster Prevention Expert Group will be used to identify partners and key-stakeholders. The action will be carried out in collaboration with Disaster Risk Management Knowledge Centre (DRMKC), Emergency Response Coordination Centre (ERCC), European Forest Fire Information System (EFFIS) and the European Flood Awareness System (EFAS)

Topic DRS02-6.2021 (CSA) - Developing a prioritisation mechanism for research programming in standardisation related to natural hazards and/or CBRN sectors

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Building up on existing initiatives, development of a consolidated platform in close cooperation with CEN-CENELEC / ETSI gathering key actors involved in DRM for natural hazards and/or CBRN to identify on-going standardisation activities, discuss key features related to them, including classification, and prioritise actions (consultation, dissemination, research programming).
- Setting a two-steps mechanism to (1) evaluate standardisation needs, taking into account existing and running activities, and establish priorities in close consultation with key users (policy-makers and practitioners at all levels, including Commission's DGs, national and regional authorities and relevant actors), and (2) take actions relevant to the identified priorities according to their degree of maturity, including research programming in the Disaster-resilient Societies part of the Horizon Europe programme.

- Establish a standardisation roadmap at international (ISO) and European (EN) levels, leading to improved coordination of activities at EU and international levels and cross-fertilisation among different sectors.

Scope:

Increasing resilience to natural disasters or CBRN events closely relies on management procedures, technologies and tools. An important feature supporting Disaster Risk Management and relevant international and EU policies is standardisation needed to improve the technical, operational and semantic interoperability of command, control and communication systems, or the interoperability of detection equipment and tools in the areas of CBRNE. A range of actions have been undertaken to identify and prioritise standardisation activities, from pre-normative (design of new tools and methods) to co-normative (comparison / validation of existing tools and methods) research to mandate of mature items to European Standardisation Organisations via the CEN-CENELEC and ETSI.

While some research projects delivered tangible CEN Workshop Agreements (CWAs) and made progress in standardisation-related research in the areas of natural hazards and CBRN civil protection and crisis management, no mechanism yet exists to ensure that standardisation is developed in close consultation with key stakeholders such as policy-makers and practitioners at all levels (European, national, regional and local). There is a need to ensure that any standardisation activities where a significant contribution to improve the disaster-resilience through standardisation can be expected are developed in close cooperation with end users and prioritised with them while paying attention to the legal frameworks in place.

In this context it is important to remind that standardisation should support operations and policy-making to supplement it but should by no means substitute it. While standardisation of technology may be more straightforward, the right balance does especially have to be sought for processes. Based on existing or developing platforms linked to CEN-CENELEC, a prioritisation mechanism should hence be established, taking into account classification aspects (in particular in the CBRN sector), leading to decisions related to on-going or new standardisation items that should be directed in an organised way to pre- or co-normative research actions, CWAs or mandates, or to guidelines / Standard Operating Procedures not requiring formal standardisation (corporate voluntary agreements). This mechanism should have a close connection with future research programming and ensure close synergies with standardisation activities on European (e.g. CEN/TC 391) and international level (e.g. ISO/TC 223).

Area DRS03 - Strengthened capacities of first responders

Topic DRS03-1.2021 (IA) - Harmonized or standardized dispersion models for improved decision support in situations with a CBRNE release

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Methodologies to support product developers in designing customized tools for first responder applications.
- Guidelines for model-system interfaces, definition of performance parameters for a better evaluation of models and evaluation of different models using these performance parameters.
- Evaluation system on how improved decision support may be achieved, and mechanism to test effective ways of treating uncertainties in order to improve decision-making.

Scope:

There is a wide range of dispersion models and a need of different decision support tools for first responder applications in case of a CBRN-E release. The development of standardised model-system interfaces would help enhancing decision-support tools more effectively and contribute to the ability to rapidly identify hazardous agents and contaminants. These interfaces concern both parameters and data as well as communication protocols. In addition, there is a need for better understanding uncertainties and how to know which uncertainties influence the result. This relies on a better definition of parameters that should be associated with uncertainties and how these can be described. This uncertainty estimation requires effective and efficient methodologies.

Topic DRS03-2.2021 (IA) - Fast deployed mobile laboratories to enhance situational awareness for pandemics and emerging infectious diseases

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Inventory and comparison of existing mobile laboratories, including heavy structures (both military and civilian) and light self-sustained systems, evaluation of quality management systems for maintenance, validation and testing.
- New (mobile laboratory) solutions for the fast, reliable and unambiguous detection and identification of infectious agents, diagnostic tests, monitoring and mapping of contamination and enhanced field data communication to decision-making authorities.
- Strategies to orchestrate mobile laboratory capacities in the EU, and improvements in the management of trained staff in Europe.

Scope:

The recent COVID-19 crisis has demonstrated that the ability to rapidly identify viruses on scene are crucial to ensure adequate risk assessment, optimal risk management, and proper counter measures. Consequently, a determining factor is to bring a rapidly deployable diagnostic capacity as close as possible to the crisis area. Considering specific infectious diseases is of paramount importance as also is the possibility to develop scalable capacities for joint multinational intervention.

In the EU Civil Protection and Health policy framework, mobile laboratories are increasingly becoming part of crisis responses and recovery plans, and the COVID-19 illustrated the needs for further developments in this area. Pandemics risk mitigation comprises prevention, preparedness and post-crisis management, including networking, regional and international partnership, consolidating, coordinating and optimizing existing capabilities in terms of expertise, training, technical assistance and equipment. There is a need for building synergies among existing initiatives to develop an EU capacity building by strengthening the national and regional capacities and staff training for mobile laboratories operation, long-term sustainability culture of safety and security.

Topic DRS03-3.2021 (IA) – Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery –

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Identification and evaluation of existing technologies, highlighting their strengths and weaknesses.
- Testing and implementation of most promising user-centred technologies in real-worlds conditions.

Scope:

Supplying relief items to various demand spots in disaster-prone areas is a critical task due to last-kilometer logistics problems that hamper the process of and efficient transportation of first responders and their equipment. Blocked roads, heavy terrain and bad weather conditions are factors that are faced by first responders (e.g. fire brigade, emergency medical services) in the immediate response to disasters. Innovative technologies (e.g. drones, AI, sensors etc.) are considered to support emergency workers in overcoming the aforementioned challenges related to relief items delivery and can provide ability to obtain critical information remotely about the extent, perimeter, or interior of the incident as well as conduct on-scene operations remotely without endangering responders. For example, technology solutions for navigation in smoky environments in the case of wild fires can potentially increase the efficiency of search operations by fire fighters.

Topic DRS03-4.2021 (IA) Improved international cooperation addressing first responder capability gaps

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Improved real-time detection, tracking and analysis of different situations, incidents and risks (including the location and well-being of first responders)
- More targeted actionable intelligence and more efficient command operations due to the fast analysis of different information sources
- Enhanced European and global interoperability for different types of first responders (e.g. firefighters, medical responders, police, civil protection)
- Availability of first responder solutions that are oriented on internationally defined requirements, recognised practices and thus can be used with different national systems and equipment

Scope:

International cooperation is key to respond to different kind of natural and man-made disasters, as well as intentional security threats. Besides operational cooperation, there is a need to find a common understanding on what innovation is needed to able to respond to different challenges. The Sendai Framework for Disaster Risk Reduction 2015-2030 list the need *'to strengthen technical and logistical capacities to ensure better response to emergencies'*[19]as one priority for national and local levels. Such capacities depend to a large extent on the effectiveness and the specific capabilities of organisations responsible for first response to incidents.

In order to perform their dangerous tasks, First Responders require the best possible equipment that is tailor-made for extreme scenarios. As such, tools and gear need to be highly specialised and adapted to the different specific first responder needs. The market for such equipment is however fragmented, limiting the availability and affordability.

International cooperation to define common requirements has helped to create a clearer picture on what gaps remain and cannot be satisfied by existing solutions, thus requiring targeted research. Global capability gaps have been identified by international expert groups such as the UNDRR Scientific and Technical Advisory Group and the International Forum to Advance First Responder Innovation (IFAFRI), involving scientific experts, firefighters, medical responders and police officers from several EU and non-EU countries.

Proposals under this topic are invited to address one or several of the following capability gaps that were identified by national first responders within IFAFRI:

[19] https://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

- The ability to know the location of responders and their proximity to risks and hazard in real time
- The ability to detect, monitor, and analyse passive and active threats and hazards at incident scenes in real time
- The ability to monitor the physiological signs of emergency responders
- The ability to incorporate information from multiple and non-traditional sources into incident command operations
- The ability ty to create actionable intelligence based on data and information from multiple sources

Proposed solutions should take into account the different specifications as defined within IFAFRI, most notably the Gap Analysis, Statement of Objectives and Deep Dive Analysis[20] and propose solutions (to the extent possible) that are suitable for different types of responders.

Proposals can be submitted by any eligible organisation and do not necessarily require the cooperation with any co-applicant from an IFAFRI member country.[21] Participation from non-associated third countries (including the non-EU IFAFRI partners) is however encouraged.

[20] Resources: https://www.internationalresponderforum.org/resources

[21] List of IFAFRI members: https://www.internationalresponderforum.org/partners

CALL DRS 2022:

Area DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens

Topic DRS01-1.2022 (RIA) – Better understanding of citizens' behavioural and psychological reactions in the event of a disaster or crisis situation

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Qualitative and quantitative analyses on the behaviour of diverse society groups affected by a natural and man-made disaster or crisis situation, during and after an even occurs, based on real cases and testimonies, lessons learned from past disasters or crisis and recommendations from citizens and local authorities. Examine how this analysis could be integrated into preparedness plans and processes to include cultural, historical, and ethical perspectives on what defines disasters and how they are responded to.

- Analyses of human behaviour as triggering or cascading factors of disasters or crisis situations, and transformation of qualitative data into quantitative information to improve vulnerability and exposure analyses.

- Development of community-centred (vis-à-vis victim- or patient-centred) approaches and corresponding preparedness plans: in view of limited emergency response capacities and threat of systems collapses (e.g. health system, food distribution, supply chains) in large-scale disaster scenarios, analyse what community practices and communication strategies can help mitigate the latter and enable the public to be a capable partner in emergency planning and response.

- Specific measures to better address the needs and requirements of most vulnerable groups (chronic suffers, persons with disabilities, children, elderly persons, economically and social deprived persons, refugees and illegal migrants in emergency planning and recovery measures.

- Analyses of the nature and scope of mental health issues of the affected populations and of first-responders arising during and following natural or man-made disasters or crisis situations and their implications for response and recovery, and options to address these issues, including through social and health services such as emergency psycho-social support.

- Analyses of mechanisms and factors that can lead to false alarms and misdirected actions, and of the direct consequences on both population and decision-makers.

Scope:

Human actions and behaviour may strongly influence the effects and dynamics of a disaster or crisis situation and on the response, potentially modifying the vulnerability of the population.

For example, inadequate design of technological systems may favour cascading consequences due to limited consideration of human performance, and insufficient planning. Linked to this, due to extreme time pressure, crisis managers are often forced to make decisions on the basis of inadequate information. The behaviour of the general public, mostly influenced by demographic factors (e.g. gender, age, income, education, risk-tolerance, social connectivity etc.) and the perception of risks, depends on the availability, form and access to information about the crisis and management of trade-offs (e.g. efficiency and thoroughness trade-offs). Social media play an important role here being a means of disinformation and misinformation.

Recent disasters related either to natural causes (including climate-related and geological hazards), man-made causes (including industrial accidents or terrorist attacks) or the COVID-19 pandemic crisis have shown the lack of sufficient knowledge in the way citizens react in case of disasters or crisis situations, with implications on policy design and implementation for example in the form of preparedness plans. In this respect, taking into account the knowledge gathered by projects funded in Horizon 2020 and ensuring complementarity, behavioural and psychological research on how citizens behave in the event of a disaster or crisis situation is needed to better understand how to best raise awareness in the population and develop tools to facilitate this.

It is hence necessary to better investigate how historical, cultural and emotional factors (e.g. anxiety, panic etc.) during a disaster or a crisis influence rational actions, evaluations of options and information seeking. In addition, the impact of disasters on health also requires looking into the short and long-term consequences of exposure to high stress/threat levels bears, in particular for mental health.

Topic DRS01-2.2022 (RIA) - Enhanced preparedness and management of High-Impact Low-Probability or unexpected events

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

- Increased understanding of high impact low probability events in the short and medium term, both from natural and man-made hazards. These perspectives include cultural, societal, regional, ethical and historical contexts. This should capture new and emerging risks and develop end-user-friendly tools for risk assessors to conceptualise such risks.

- Improved methods/tools for decision-making under uncertainty to prepare for high-impact low-probability events. These methods could include the impact of past events, communication and linguistic components, and regional specificities. These should be developed in close cooperation with end users to maximise application of these tools in practice.

- Better preparedness for and management of high-impact low-probability risks that most, if not all, experts have difficulty conceptualising (the unexpected events), including by developing no-regret options that can address different kinds of impacts irrespective of the cause.

- Improved mapping of i) socioeconomic systems' interdependencies that can be negatively affected by high-impact low-probability events, and ii) which systems contribute to the materialisation of high-impact low-probability risks by increasing societal vulnerability. This would be supported by identification of interventions where resilience-building would be most effective. This identification could be based on an in-depth understanding of past events, a mapping of the current societies' cultural sensibilities in a geographical space / region context, and/or their ethical and legal contexts.

- Improved preparedness at an individual level, at local level and at the governmental level, including through clarifying roles and responsibilities around management of high-impact low-probability risks. An improved understanding of existing risk and resilience management capacities across Europe at national and regional levels for responding to high-impact low-probability risks that Europe may face.

- Development of appropriate simulation tools to identify areas under higher risk of occurrence of HILP events and development of preparedness plans and management mechanisms, including communication, to address the effects of such occurrence.

- Combination of qualitative and quantitative approach strategies, which encompass practical and probabilistic knowledge to increase the success rate of identifying and adequately monitoring fast developing risks into potential high-impact low-probability events

- Multi-disciplinary reference library around HILP events and their impacts would allow to build up a record of observations that can help quantify the impacts and, by analogy, similar risks that might arise in the future.

- Scenario-building exercises and stress-test risk-related practices in critical infrastructure sectors (e.g., transport, communications, energy) would enhance preparedness and help identify particularly affected social groups while enabling rapid financial and practical support where national organizations are unable to cope or where the consequences are cross-border in nature. Independent, high-quality hubs (national or regional) for up-to-date risk notification and provision of scientific information and communication in a crisis – supported by governments, businesses and industry associations

Scope:

The risk landscape has changed significantly over the last decades. With new and emerging risks and risk magnifiers such as climate change, cyber threats, infectious diseases and terrorism, countries need to anticipate and prepare for the unexpected and difficult to predict.

At European level, there is, however, no agreed definition nor methodology to characterise HILP and unexpected events, resulting in differing impact scales and a lack of comparability of risk ratings among National Risk Assessments. High-impact, low-probability risks (HILP/Hi-Lo) can be understood as "events or occurrences that cannot easily be anticipated, arise randomly and unexpectedly, and have immediate effects and significant impacts". They can manifest themselves not only as one-off high-profile crises and mega-disasters (e.g., Fukushima Daiichi Nuclear Accident, eruption of the Eyjafjallajökull volcano, 9/11 terrorist attack in the U.S. and COVID-19 pandemic) but also as lower-profile, persistent events with equally serious impacts such as flooding, droughts and cyclones which, owing to the low likelihood of occurrence or the high cost of mitigating action, remain un- or under-prepared for.

High-impact, low-probability events (HILP) and their cascading effects raise many challenges for governments, businesses and decision-makers, including defining where the responsibilities lie in preparing for both individual shocks and slow-motion trends (e.g. global warming, tipping points, sea level rise) that tend to increase their magnitude and frequency. A revision of Decision 1313/2013/EU on a Union Civil Protection Mechanism has brought attention to high impact low probability risks and events, now requiring Member States to take prevention and preparedness measures to address them where appropriate, and fully financing capacities through rescEU to respond to high impact low probability events.

To get the right balance between planning for specific 'known' events and creating generic responses for events that are rare or unexpected, research should support the anticipation and management of shock events through improving planning processes, establishing broader risk-uncertainty frameworks that capture such events, enhancing business resilience and responses to shocks, and stepping up communications in a crisis.

Preparing for and managing the consequences of a HILP event will benefit firstly from developing an increased understanding of new and emerging risks, besides the required risk understanding dealt with in topics DRS01-1.1.2021 and DRS02-2.1.2021, and in close connection to them. Improved methods should also be sought to support risk assessors and decision-makers in conceptualising these risks and developing no-regret options to manage them. A thorough understanding of existing risk management capacities across Europe at national and regional levels for responding to high-impact low-probability risks that Europe may face would contribute to improving preparedness at the European level to risks that can affect multiple countries at once and overwhelm national response capacities. Finally, enhancing preparedness for and management of high impact low-probability events cannot happen without an increased resilience of individuals. In close connection to topic DRS01-2.1.2021, research is also needed on how to prepare citizens for unfamiliar risks and what information to disseminate, and how to communicate, during the disaster or crisis-related emergency in order to manage panic, confusion and threats of disinformation.

Given the practical nature of this topic, co-design, co-development, co-dissemination and co-evaluation of the research outputs engaging the intended end users will be particularly important.

Topic DRS01-3.2022 (IA) – Better integration of citizen volunteers in field validation of risk management approaches

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Lessons learnt from near-to-real-cases exercises (demonstrations simulating real cases) involving citizen volunteers, local authorities and first responders, with recommendations to be delivered to Member States authorities in charge of management of different types of risks on how to integrate citizen volunteers in the disaster preparedness and response actions and how to coordinate them on site in the disaster area.

- Advisory dissemination materials, highlighting good practices of interactions among citizens, local authorities and first responders in the event of (natural or man-made) disasters, addressed to European public in different EU languages.

Scope:

Building a common culture for improving societal resilience closely relies not only on the understanding of risks by citizens but also on their engagement in preparatory actions and inclusion of their knowledge. Among them, demonstrations and field validation of risk management approaches, as well as training actions addressing first responders, may have a strong impact on the risk awareness and engagement of citizens in the case of disaster events, supporting citizens in acting efficiently by themselves. This engagement of citizens in disaster and crisis management will also benefit from their involvement in field validation of different approaches / methods used by local authorities and first responders, in representative urban and non-urban environments.

On the basis of past experiences built-up by large-scale demonstration projects in the field of natural hazards and CBRN sectors, near-to-real-cases exercises should involve citizen volunteers, local authorities and first responders to enhance the understanding of risks and the interactions among different actors (policy-makers and implementers, scientists, practitioners and citizens). Dissemination efforts should be ensured so that experiences with citizens can be widely shared in Europe via social networks and other means.

Area DRS02 - Improved Disaster Risk Management and Governance

Topic DRS02-1.2022 (RIA) - Hi-tech capacities for cross-border crisis response and recovery after a natural-technological (NaTech) disaster

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Development of a holistic vision of crisis management after telluric (e.g. volcanic, seismic, tsunami) or extreme climate events (e.g. floods, storms, storm surges, fires, droughts) producing impacts on critical assets (e.g. infrastructures, industries) and creation of new management framework for handling NaTech crises.

- Enhanced existing crisis management tools to develop a common platform (shared among public and private operators) allowing cross-border exchanges and decision-making, while respecting legal frameworks and responsibilities.

- Demonstrated operational protocols and development of standard operating procedures able to respond to NaTech crises in cross-border configurations, including comprehensive risk modelling of worst-case scenarios taking into account cascading effects and future impacts of climate change.

- Improvement of our understanding and capabilities to identify and mitigate risks associated with interdependencies across infrastructures and other human (social and economic) systems.

Scope:

The confluence of incidents in recent years has brought renewed concerns over our systemic resilience to external shocks arising from natural-technological (NaTech) disasters. This is particularly acute in the event of disruption in the transport, power, water supply and communication sectors in highly populated and industrialised areas, or when such events raise the likelihood of cascading effects with severe impacts on communities and the economy that are hard or impossible to predict. The main focus on NaTech risks lies on a thorough understanding of the vulnerability of industrial sites and critical infrastructure, and the potential impact natural hazards can have on such technological resources. This entails the identification of both physical (safety of building facilities and structures) and operational vulnerabilities, often addressing multi-hazard conditions. Innovative methods are required for analysing worst-case scenarios, and informing decision-makers about the crosscutting and shared responses to different crises given available resources.

Research involving multiple fields of expertise is also required to improve hi-tech capacities for operational response systems to better cope with natural and/or technological disasters occurring in Europe (and in oversea territories) in an integrated manner. This will rely on a knowledge sharing among natural and technological risks communities to develop a holistic vision for an integrated operational crisis management of NaTech disasters.

Topic DRS02-2.2022 (IA) - Improved impact forecasting and early warning systems supporting the rapid deployment of first responders in vulnerable areas

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Comparison of measures and technologies to enhance the response capacity to extreme weather and geological events (including local measures and warning systems) affecting the security of people and assets.

- Adjustments of warning and response systems in the light of cross-disciplinary cooperation, involving planning authorities and first responders, to better manage the rapid deployment of first responders and communication to citizens in vulnerable areas in the case of extreme climate events or geological disasters.

- Timely operational forecasts of severe (short-term focus) extreme weather events (e.g. floods, hot waves, storms, storm surges) or geological hazards (e.g. volcanic eruption, earthquake, tsunami) to aid planning authorities, civil protection agencies and first responders in their decision-making.

- European-scale multi-hazard platform to facilitate the identification of expected natural hazards with great specificity in time and space and improve science communication for boosting interactions between scientists, general media and the public.

- Methodologies to integrate innovative state-of-the art early warning systems into existing tools for decision-making and situation reporting already used by civil protection authorities from international to local level.

Scope:

Enhanced risk and crisis assessment and preparedness to natural hazards rely on tools using different types of data, information and forecasts (e.g. meteorological data, physical data related to geohazards and climate projections etc.) which may enable to anticipate the occurrence of disasters. Based on the legacy of existing solutions, in particular in the area of extreme weather events, further developments are required to compare impact forecasting and early warning approaches at international level. The aim of such comparisons would be to design EU-wide decision-support and information systems supporting planning authorities and civil protection agencies in the rapid deployment of first responders and communication to citizens in vulnerable areas in the case of extreme climate events or geological disasters. This platform development might be prone to international cooperation, hence supporting the implementation of both EU policies and the UN Sendai Framework for Action. Innovation actions should improve measures and technologies that are needed to better plan for extreme climate events and geological disasters, reduce risks, as well as manage the immediate consequences of natural disasters, in particular regarding emergency responses. This should lead to sound and timely operational forecasts of severe (short-term focus) extreme weather events or geological hazards to aid planning authorities, civil protection agencies and first responders in their decision-making. Built up on developments from relevant H2020 projects, a European-scale multi-hazard platform should be designed, taking into account existing developments at EU level, in order to facilitate the identification of expected natural hazards with great specificity in time and space. The aim is to utilize largely existing capabilities and combine them into a single, user-friendly platform.

Topic DRS02-3.2022 (RIA) - Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Development of prevention/preparedness actions based on the (existing) analysis of interdependencies between critical infrastructures and possible cascading effects;
- Analysis of existing communication systems and assessment/development of alternative communication tools for Civil Protection and Crisis Management security authorities, including the communication with private sector and actors responsible for critical infrastructures;

Scope:

The modern societies are highly dependent on the (unlimited) availability of electricity and digital infrastructures. A digital breakdown with loss of electricity and IT infrastructures would have severe impacts on various infrastructures and areas critical for the functioning of societies. Assessment of the consequences of possible digital breakdown (internet, electricity etc.) would require focused research in order to design appropriate crisis prevention and preparedness actions taking into account cascading effects. This includes analysis of interdependencies between different critical infrastructures, the assessment of different scenarios and conditions like duration and extent of the digital breakdown as well as possible cascading effects.

Assess also the advantage of using satellite broadcast in case of unavailable terrestrial systems (disseminate instructions and guidance to populations, to rescue teams, to authorities, etc)

Topic DRS02-4.2022 (IA) – Improved disaster risk pricing assessment

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Contribute to the public accessibility of fiscal data and information related to disaster risks, and available risk transfer mechanisms such as insurance in an easily available and understandable way.
- EU-wide or international standard or guidance on how to monetise and account intangible values from Climate Change Adaptation and Disaster Risk Reduction measures

- Innovative financial instruments and IT-solutions to reduce transaction costs for disaster risk finance and insurance products (e.g. earth observation data, artificial intelligence, financial technologies)

- Research and testing of novel European, cross-border, national and regional disaster risk financing frameworks. This needs to involve a wide range of stakeholders (e.g. disaster risk management, finance, communication) from public and private sectors.

- Risk model development for future natural catastrophe events, development of European stress-testing scenarios including vulnerable hotspots and uninsurable risks.

Scope:

Natural disasters (weather and climate related extremes and geological events) in the EU have cost on average EUR 17 billion per year the past ten years. Around 35 % of the total losses from climate and extreme and weather events are insured today in the EU, although the proportion of the insured losses ranges from 1 % in Romania and Lithuania to about 60 % in Belgium. In the near-term future, the European insurance industry and their regulators have warned that affordability and insurability are likely to become an increasing concern with climate change. Insurance, in combination with other risk transfer and financing mechanisms, is an important tool to achieve disaster risk reduction targets. Insurance plays an important role in financially supporting the recovery of individuals, organisations, businesses and communities affected by natural disasters. Large disaster losses in recent years have led insurance companies to re-examine their approach to increase the extent of insurance coverage and compensation for loss in vulnerable areas. This includes increasing their investment in assessing and modelling risk, developing advice on risk prevention and establishing new forms of coverage to support governments in managing the costs they face in post-disaster recovery. Questions remain about the limits of insurance in tackling fast-rising threats - not only how people at highest risk and with lower incomes can afford it, but whether insurance models can cope with much more frequent and destructive. Rethinking insurance pay-outs, giving homeowners clearer information on potential risks - using simple online tools, or providing data at the time of house purchases - may also be the way forward to more resilient communities.

Area DRS03.1 - Strengthened capacities of first responders

Topic DRS03-1.2022 (IA) - Enhanced situational awareness and preparedness of first responders and improved capacities to minimize time-to-react in urban areas in the case of CBRN-related events

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Development of tools and technologies, including novel multiplatform CBRNe systems, to enhance situational awareness to prepare for and rapidly react to CBRN events both for responders on the ground as well as for dispatch and crisis centres, especially in urban areas.

- Support of first responders' situational awareness via high level processing solution, e.g. based on dispersion modelling or threat recognition / prediction solution using sensor data fusion and algorithms that combine heterogeneous sensor data in order to reduce the likelihood of false alarms and contribute to an improved decision-making process for the responders.

- Development of fast, reliable and portable devices for responders to perform an in-situ provisional identification of CBRN suspicious samples, enabling to decide which personal protective equipment (PPE) is required for first responders, including smart wearable equipment.

- Solutions integrating different commercial and experimental sensors/platforms, which should improve the state-of-the-art products in terms of communication (e.g. by using novel and open communication protocols, pre-processing of data), power consumption (e.g. by offering supplemental power source to the existing sensors), interfacing capability (e.g. by proposing an open interface specification). The proposals should also cover the system transportability, online capability and continuous operation issues.

Scope:

Addressing first responders' needs requires innovative actions resulting in technological, institutional and capacity-building solutions that are tailored to the risks, affordable, accepted by citizens, and customized and implemented for the (cross-sectoral) needs of practitioners. Innovative solutions are required to enable first responders to get a faster overview of any disaster situation based on the knowledge of past events and prevention actions. Complementing this, novel technologies and tools are necessary to enhance situational awareness in the case of disaster-prone events or health-related crises, especially in the case of cross-border situations, in order for first responders to be better prepared in emergency operations. In this context, innovative technologies are required for first responders to rapidly identify hazardous agents and contaminants such as CBRN substances in case of an accident, outbreak/pandemics or terrorist attack and act more efficiently and rapidly regarding communication. This requires novel rapid and accurate detection of substances (possibly coupled with unmanned vehicles or drones) and on-line communication systems to support first responders' operations and to provide the ability to conduct on-scene operations remotely without endangering them. Needs cover a broad range of technologies on top of existing CBRN detectors, e.g. samplers, separation systems, dilution or sample pre-concentrators etc., multiplying their capabilities. Advancements should take into consideration power consumption of front-end technology, as well as, transportability, on-line, dynamic sampling, automation, smart samplers, sample preparation, integration with detectors, standardization. A focus should be made on experimental or commercial systems that are not optimized in terms of online, continuous measurements, power consumption and hyphenation. Other areas of research closely depending upon enhanced situational awareness and preparedness concern decisions related to the protection of first responders (e.g. advanced protective gear and smart wearable equipment), in particular in case of CBRN-related events (infectious diseases, accidental or linked to terrorism), and ways to minimise their time-to-react in urban areas or to conduct on-scene operations remotely without endangering responders (e.g. ways through traffic, UAVs etc.).

Topic DRS03-2.2022 (RIA) - Augmented reality solutions for improved situational awareness for public safety in case of cross-border emergency situations

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Innovative Artificial Intelligence tools to process large amounts of data (both operational and open sources) in real-time or near real-time patterns in audio or video streams, identifying abnormal or suspicious situations, people or behaviours, measuring and mitigating the lack of real data in sufficient volume and quality for the implementation of large-scale pilot projects to test the effectiveness of prototypes.

- Systems to identify relevant information (for missions) in open source analysis, with specific attention to fake news and correlation with field information filtered by Mission Critical Services platforms.

- Improved reporting tools to reduce repetitive and procedural activities.

- Location means for responders, vis-à-vis their proximity to threats and hazards in real time.

- Enhanced communication and cooperation between citizens, experts and practitioners.

Scope:

Public Safety end users are faced with large amounts of multimedia contents regarding any kind of events. These data can be aggregated and analysed to build and provide a rich common operational picture and enhanced situational awareness services to first responders. Nonetheless, the huge amounts of date produced, on the one hand, from the management control itself and, on the other hand, from multiple sources of data, cannot be processed by human beings, thus limiting the potential benefits for Public Safety users. Innovative solutions are therefore needed to use information from different sources for command operations, exploiting Artificial Intelligence to analyse various digital streams (real time audio / video or data) related to an incident or a mission in order to support Public Safety end users while respecting legal frameworks and responsibilities. As such, they can provide actionable intelligence that exploits different data sources and enhance their situational awareness while facilitating their mission management (e.g. mission workflow, reporting, inter-agencies and cross-border cooperation).

Topic DRS03-3.2022 (IA) - Enhanced capacities of first responders for more efficient rescue operations of victims and decontamination of infrastructures in the case of a CBRN event

Expected Outcomes: Projects’ results are expected to contribute to the following outcomes:

- Analysis on if and how the specific requirements of operating under CBRN conditions can be taken into consideration also for teams/capacities that are traditionally not operating under CBRN conditions (e. g. search and rescue, medical care, shelter, firefighting, flood rescue, etc.).

- Development of innovative technologies and/or operating procedures for emergency management units that might need to work under CBRN conditions such as search and rescue (including victim triage procedures), medical care, shelter, firefighting, flood rescue, etc. Develop innovative technology and procedures for mass decontamination but also for the decontamination of inanimate material (infrastructure, buildings, vehicles, equipment), including identifying standards for determining something as “decontaminated” in close collaboration with Topic DRS02-3.3.2021 (CSA)

Scope:

Chemical, biological, radiological and nuclear (CBRN) events increasingly target civilians, with first responders likely to be police officers, firefighters or paramedics. Based on the legacy of knowledge gathered in H2020 projects, innovative technologies and solutions are required for first responders to act more efficiently and rapidly in case of CBRN disaster events of any kinds. This includes the ability to rapidly identify hazardous agents and contaminants and to analyse threats and hazards in real time, the faster search and identification of victims enabling more efficient rescue operations, platforms for medical care and site management/shelter for a more efficient the triage of victims and their care, i.e. via appropriate decontamination chains of victims and infrastructures. Regarding this last point, links to standardization and Topic DRS02-3.3.2021 (CSA) are particularly important to be able to determine thresholds and identify people as well as objects as “decontaminated” or “free of decontamination”.

Destination – SSRI (Strengthened Security Research and Innovation)

Relevant Cluster 3 Expected Impact:

"Security threats are more effectively addressed thanks to better cross-cutting knowledge across different areas of security and diverse disciplines, included social sciences and humanities, enhanced implementation of the research and innovation cycle and improved uptake at all levels of society."

The EU-funded security research and innovation framework was launched with the Preparatory Action for Security Research[22]. Since then, the programme has contributed substantially to knowledge and value creation in the field of internal security and to the consolidation of an ecosystem better equipped to capitalise on research and innovation to support the EU security priorities.

While the success of the programme has materialised in relevant scientific findings, maturation of promising technology areas, operational validation of innovative concepts or support to policy implementation, a key challenge remains in improving the uptake of innovation.

The extent to which innovative technologies developed thanks to EU R&I investment are industrialised and commercialised by EU industry, and later acquired and deployed by end-users, thus contributing to the development of security capabilities[23], could give a valuable measure of the impact achieved with the programme. However, there are factors inherent to the EU security ecosystem (often attributed to the market) that hinder the full achievement of this impact. These include market fragmentation, cultural barriers, analytical weaknesses, programming weaknesses, ethical, legal and societal considerations or lack of synergies between funding instruments, among others.

It is worth noting that such factors affect all the security domains addressed in Cluster 3; that there is not one predominant factor with sufficient leverage by itself to change the overall innovation uptake dynamics; and that they exhibit complex relationships among them which are difficult to disentangle. It should also be noted that the innovation uptake process starts before the R&I cycle is triggered, and it is not finalised with the successful termination of a research project. Therefore, the uptake challenge extends beyond the realm of R&I. However, from within R&I it is possible, if not to materialise the uptake in every case, at least to pave the way towards its materialisation.

[22] COM(2004) 72

[23] For the purpose of this work programme, the terms "Capability" should be understood as "the ability to pursue a particular policy priority or achieve a desired operational effect". The term "capability" is often interchanged with the term "capacity", but this should be avoided. "Capacity" could refer to an amount or volume of which one organisation could have enough or not. On the other hand, "capability" refers to an ability, an aptitude or a process that can be developed or improved in consonance with the ultimate objective of the organisation.

To that aim, there is a need to create a favourable environment that is designed with the main purpose of increasing the impact of security R&I, that is visible and recognisable to those interested in contributing to this aim, and which provides bespoke tools that serve to tackle the factors that hinder innovation uptake.

The SSRI destination has therefore been designed with this purpose to serve equally to all the expected impacts of Cluster 3. Research applied in this domain will contribute to increasing the impact of the work carried out in the EU security Research and Innovation ecosystem as a whole and to contribute to its core values, namely: i) Ensuring that security R&I maintains the focus on the potential final use of its outcomes; ii) Contributing to a forward-looking planning of EU security capabilities; iii) Ensuring the development of security technologies that are socially acceptable; iv) Paving the way to the industrialisation, commercialisation, acquisition and deployment of successful R&I outcomes; v) Safeguarding the EU autonomy and technological sovereignty in critical security areas by contributing to a more competitive and resilient EU security technology and industrial base.

While the other destinations of the Horizon Europe Cluster 3 work programme offer research and innovation instruments to develop solutions to address specific security threats or capability needs, the SSRI destination will contribute with instruments that will help bringing these and other developments closer to the market. Such instruments will help developers (including industry, research organisations and academia) in better valorising their research investment. They will also support buyers and users in materialising the uptake of innovation and further develop their security capabilities.

In addition, the SSRI destination will offer an open environment to create knowledge and value through research in matters (including technology, but also social sciences and humanities) that are not exclusive of only one security area, but cross-cutting to the whole Cluster. This will contribute to reducing thematic fragmentation, bringing closer together the actors from different security domains, and expanding the market beyond traditional thematic silos.

Finally, SSRI will allow the allocation of resources to the development of tools and methods to reinforce the innovation cycle itself from a process standpoint, thus increasing its effectiveness, efficiency and impact. This destination will contribute to the development of an analytical capacity tailored to the specific needs of security stakeholders for the materialisation of a structured long-term capability based planning of research and innovation for security.

Expected impact

Proposals for topics under this Destination should set out a credible pathway to contributing to strengthen security research and innovation, more specifically to one or several of the following impacts:

- A more effective and efficient evidence-based development of EU civil security capabilities built on a stronger, more systematic and analysis-intensive security research and innovation cycle;

- Increased industrialisation, commercialisation, adoption and deployment of successful outcomes of security research reinforces the competitiveness and resilience of EU security technology and industrial base and safeguards the security of supply of EU-products in critical security areas.

- R&I-enabled knowledge and value in cross-cutting matters reduces sector specific bias and breaks thematic silos that impede the proliferation of common security solutions;

The following call(s) in this Work Programme contribute to this Destination:

CALL SSRI 2021:

Proposals are invited against the following topic(s):

Area SSRI 01 - Stronger pillars of security Research and Innovation

SSRI01-1.2021 (RIA) – A maturity assessment framework for security technologies

Expected Outcomes: Project results are expected to contribute to the following outcomes:

- Increased literacy on the value and efficient use of maturity assessment frameworks to communicate the readiness of technology, synchronise parallel developments, forecast implementation and support decision making in the planning of investment in the area of security;

- Improved cross-disciplinary assessment of the maturity of innovative technologies based on common harmonised frameworks for the security domain;

- Comprehensive and timely updated map of the maturity of the security solutions developed through EU-funded security research and innovation programmes enabled by widely accessible assessment tools and methods;

- Evidence-based programming of security research built on a more reliable assessment of the state of the art technologies in the field of security.

Scope:

Having awareness of the maturity of a system is an invaluable reference to understand how ready this system is to be deployed on a numeric scale. Given the challenge posed by the limited uptake of the outcomes of EU-funded security R&I, having the capacity to characterise the progress achieved by security systems under development basing on readiness characteristics, and not only from a purely technological perspective, can be a powerful tool to identify areas that require further work or to provide input to strategic investment decision making processes.

Scales using metrics such as the Technology Readiness Levels (TRL) are widely used and have been adapted to different domains. Other scales have been developed, including Integration Readiness Level (IRL), Commercialisation Readiness Level (CRL), Manufacturing Readiness Levels (MRL), Security, Privacy and Ethics Readiness Level (SPRL) or Societal Readiness Level (SRL), among others. These may have been defined for different purposes and often focusing on non-technological aspects of technology development. However, problems emerge when readiness levels proliferate and are used without a commonly agreed definition, when they are not duly adapted to the specific context of application[24] or when they are implemented without the support of adequate tools and methods to carry out a reliable assessment.

Applicants are invited to submit proposals for the development of a maturity assessment framework that serves as a reference for the development of civil security technology-based solutions. The framework should be cross-disciplinary and combine different readiness scales in an aggregated manner in order to be able to deliver holistic and quantitative maturity assessments agglutinating different perspectives (e.g. technological, systemic, societal, etc.). The scales proposed must be robust, repeatable and agile, so they can be trusted, replicated, and applied to different types of security solutions in the different domains covered by this work programme.

The scales proposed shall rely as much as possible in existing and recognised scales and methods that show the appropriate quality features to ensure their reliability. Such scales shall be tailored and adapted to the security context as required in a justified manner.[25]

Based on the maturity assessment framework proposed, the project shall deliver tools that allow the guided and/or the self-assessment of the maturity of concrete security solutions being developed under the frame of EU-funded security research work programmes. These tools shall allow an open access to those actors interested in assessing the readiness levels of concrete technologies, preferably through a web-based environment that allows for a high degree of automation. It is of particular relevance to allow open access to the online tools to actors participating in EU-funded security research projects so they are able to assess the progress in the maturation of their technologies throughout the project.

An extensive validation process for the developed assessment tools shall be conducted as part of the project. This validation shall be conducted by performing maturity assessments on different solutions recently delivered or currently under development in H2020 or Horizon Europe projects. The results of the maturity assessment shall be made available to the projects collaborating with the validation for their own use and in support to their activities. The results shall also be made available to other EC-chaired or funded initiatives for which this information

[24] "The TRL Scale as a Research & Innovation Policy Tool", European Association of Research and Technology Associations (EARTO), 30 April 2014

[25] Proposals willing to explore Societal Readiness Level scales shall avoid overlapping and possibly cooperate with actions funded under the topic SSRI03-1.2021

can be of added value, such as the Networks of Practitioners projects funded under H2020 Secure Societies work programme, to the European Networks for Security Research & Innovation funded under the Horizon Europe Cluster 3 work programme, to the Community of Users for Secure, Safe and Resilient Societies or to other security research and innovation working groups set-up by EC Agencies.

The project shall explore the options, also from a business perspective, for the exploitation of the results beyond the project lifetime, including the setting up of formal mechanisms for the certification of readiness of security solutions by entrusted bodies.

The project shall have a maximum estimated duration of 3 years.

SSRI01-2.2021 (CSA) – European Networks for Security Research & Innovation

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Enhanced analytical capacity to support the programming of EU-funded security research and capacity building funds through a periodic and timely evidence-based policy feedback ;
- Periodically aggregated and consolidated view of the capability needs and gaps in the thematic areas under consideration[26];
- Periodically aggregated and consolidated view of the state-of-the-art technologies, techniques, methods and tools that can contribute to fill the identified capability gaps;
- Periodically aggregated and consolidated view of outcomes (including on technological, industrial, legal and ethical issues), future trends, lessons learnt and best practices derived from past and current security research effort incurred in the thematic areas under consideration.
- More systematic assessment and validation of the outcomes of EU-funded security research projects with respect to identified capability gaps through harmonised support mechanisms;
- Common and updated map of opportunities and constraints for the industrialisation, commercialisation, adoption and deployment of innovative solutions in response to common capability gaps;

[26] The thematic areas under consideration are described in the topic and are different for each call. Only one network in each area can be funded.

- Common and updated map of areas requiring standardised solutions and/or certification schemes to foster innovation uptake and market creation, as well as options for the implementation of such schemes.
- Enhanced cooperation between research institutions, smaller private research agencies, security practitioners, SMEs and community representatives to support integrated participation in requirements determination and analysis, research and validation and evaluation of results.

Scope:

Innovation uptake is not a linear process, and even less a single-step process that happens only at the end of a research project and it is not automatically enabled by a successful research result. The innovation uptake process begins with the identification of a need and ends with an innovative solution deployed on the field of operations, being R&I only one of the many contributors to the overall process, but not the first and not the last. In other words, successful results of research projects are a necessary but not sufficient condition to guarantee the uptake of innovation.

Investment in security research needs to be designed taking into consideration how and when it can deliver outcomes that contribute to the development of security capabilities. Therefore, research shall be undertaken, from its very early stages, in a way that addresses real needs while guaranteeing the impact in the final solutions. It shall also ensure to identify and underpin the factors that could help in the implementation of its results. However, the programming of research is highly conditioned by the quality, reliability and timeliness of the evidence that supports its decision making process. This includes the identification and understanding of the contextual elements that can or will influence or be influenced by the research (process), the research team and the research projects themselves.

The European Commission and the Member States carry out this programming exercise periodically, taking into account a wide variety of inputs. The complexity of the challenge is notable, considering that the EU security landscape is volatile, uncertain, complex and ambiguous in what regards the security threats, the capabilities required to face them and the evolution of modern technologies. In order to carry out a sound programming exercise, the Commission and the Member States strive to consult and involve all actors. With that aim, experts are gathered in different configurations and their inputs are coordinated at EU and national levels to be factored in by the decision making bodies of EU-funded security research.

These experts require high quality, reliable and timely evidence to support their assessments, but information is often scattered, hardly visible and requires bespoke processing for the detection of patterns and for the generation of actionable intelligence. In other cases, it is simply not presented in the right format to unveil its value.

Applicants are invited to submit proposals for the establishment of European Networks for Security Research & Innovation. The role of these networks shall be to collect, aggregate, process, disseminate and exploit the existing knowledge to directly contribute to the expected outcomes of this topic.

Networks shall engage with the main sources of information in order to have a sound and updated picture of the aspects mentioned above. This includes interaction with security experts (beyond the members of the project consortium), organisations, projects or initiatives, but also an extensive review of available databases, studies, reports or literature (notably all information generated under the EU-funded security research programmes, and possibly under other EU or MS funding programmes).

The networks shall ensure the maximum outreach of their findings to the different communities of the security research ecosystem, including policy makers, security authorities, industry, researchers and citizens. Special emphasis shall be made on the contribution of these networks to the work of entities and initiatives established by the EC and the EU Agencies to contribute to the security research programming effort. In this regard, the networks shall contribute timely and intensively to the work of the Thematic Working Groups of the Community of Users for Secure, Safe and Resilient Societies and of other equivalent innovation labs/groups set-up by EU Agencies (e.g. Frontex). The networks shall contribute to these working groups with the quantitative and qualitative evidence required to carry out their activities in support to a more impactful EU-funded Security R&I and to a more frequent and systematic innovation uptake.

The networks shall be in a position to deliver findings on the abovementioned challenges starting from the month 6 of the project and periodically every 6 months or less, in accordance with the information needs of the entities and initiatives they are contributing to.

Proposals shall clearly describe the process and timing for the collection of inputs and the generation of outcomes. This plan shall go beyond the description of project deliverables and milestones, and describe in detail how and when the findings will be exploited during the project and in collaboration with the communities described above.

The applicants submitting the proposals shall ensure sufficient representativeness of the communities of interest and an adequate coverage in terms of knowledge and skills of the different knowledge domains required to face the challenge, including security operations, technologies, research & innovation, industry, market, etc. In this sense, the network may possibly expand beyond the project partners during its implementation, but the project beneficiaries shall be the core and the driver of the activities. The applying consortia need to demonstrate that the integrating partners guarantee the expertise required to steer the project activities in all the knowledge domains to ensure the success of the action. The work of the partners shall be supported by solid and recognised tools and methods, also accompanied by the required expertise to put them in practice.

The networks shall build to the extent possible on the work initiated by the Networks of Practitioners funded under the H2020 Secure Societies work programme. When such networks are still ongoing maximum cooperation and minimum overlapping must be ensured and demonstrated.

Under this call, the applicants are invited to propose networks on the thematic areas of:

i) Border Security

ii) Critical Infrastructure Protection.

Only one network in each area can be funded.

The project shall have an estimated duration of 3 years.

SSRI01-3.2021 (CSA) – PLACEHOLDER National Contact Points (NCPs) in the field of (cyber)security

Area SSRI 02 - Increased Innovation uptake

SSRI02-1.2021 (PCP) – Demand-led innovation for situation awareness in civil protection

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- An identifiable community of EU first responders with common user/functional needs for innovative technology solutions for situation awareness in the field of civil protection;

- Tested and validated capacity of EU technology and industrial base to develop and produce technology prototypes for situation awareness in the field of civil protection that meet the needs of the EU user community;

- Improved delineation of the EU market (including demand and supply) for situation awareness systems in the field of civil protection that can articulate alternative options for uptake in function of different industrialisation needs, commercialisation needs, acquisition needs, deployment needs and additional funding needs (beyond R&I funding).

Scope:

End-users and public procurers from several countries are invited to send proposals for launching a Pre-Commercial Procurement action for the acquisition of R&D services for the development of technology solutions for situation awareness in the field of civil protection.

The proposals shall build on the outcomes of the SAYSO project, which followed the call 2016 of H2020 Secure Societies work programme, under the topic *SEC-02-DRS-2016 - Situational awareness systems to support civil protection preparation and operational decision making*. Proposals shall therefore give continuity to the works initiated by the SAYSO project. The consortium members shall have the background and skills required to do so, as well as to conduct the activities required for the implementation of a PCP action.

Applicants shall note that this project responds not only to the needs of EU stakeholders and to the policy priorities of the Commission in the field of civil protection, but also to the capability needs and gaps identified by the International Forum to Advanced First Responders Innovation (IFAFRI). Therefore, applicants are encouraged to seek alignment with the needs of first responders as set out in the respective Gap Analysis, Statement of Objective and Deep Dive Analysis Documents which IFAFRI has produced[27].

The proposals are expected to provide clear evidence on a number of aspects in order to justify and de-risk the PCP action, including:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;
- That there is a consolidated group of end-users and procurers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint-procurement of innovative solutions;
- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who could be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;
- That the state of the art and the market (including research) has been explored and mapped to the needs, and that there are different technical alternatives to address the proposed challenge;
- That the PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready in due time in order to launch the call for R&D services according to the PCP rules.

[27] https://www.internationalresponderforum.org/resources

- That there is a commitment to pursue the exploitation of results beyond the end of the project through engagement with stakeholders and implementation of exploitation strategies towards future uptake.

The open market consultations required prior to launching the PCP call for tenders must have taken place in at least three EU Member States. Market consultations conducted during the SAYSO project can be used if this requirement is fulfilled, and if it is justified that: i) their purpose was enough to guarantee the viability of the procurement and; ii) that the state-of-the-art has not changed since they were conducted.

In relation with the PCP tendering process, the applicants shall guarantee that:

- The principles of the EU Directive for public procurement and in particular with the provisions related to PCP will be duly respected;
- The specific provisions and funding rates of PCP actions and the specific requirements for innovation procurement (PCP/PPI) supported by Horizon Europe grants, as stated in the General Annexes of the Horizon Europe Work Programme 21-22[28], will be duly respected;
- Conflict of interests will be avoided, including through the ineligibility of bids from technology providers who are also beneficiaries of the project or who have been beneficiaries of the previous SAYSO project;
- The confidentiality of the intellectual property of potential bidders will be protected;
- The technology developments to be conducted in the PCP will be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data;
- In developing technology solutions, societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) will be taken into account in a comprehensive and thorough manner;
- All participating public buyers commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular the principles of data protection by design and by default;
- The guidance for attracting innovators and innovation, as explained in the Commission Guidance on Innovation Procurement C(2018) 3051, will be duly taken

[28] Inspired on the text of H2020. To be tailored to the General Annexes of the HE WP.

into account, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

Applicants shall propose an implementation of the project that includes:

- A minimal preparation stage dedicated to finalise the tendering documents package for a PCP call for tenders based on the technical input resulting from project SAYSO, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.
- Launching the call for tenders for research and development services. The call for tenders should envisage a competitive development composed of different phases that would lead to at least 2 prototypes from 2 different providers to be validated in real operational environment at the end of the PCP cycle;
- Conducting the competitive development of the prototypes following the PCP principles including, at least, a design phase, an integration and technical verification phase and a validation in real operational environment phase. In evaluating the proposals and the results of the PCP phases, the applicants shall consider technical merit, feasibility and commercial potential of proposed research efforts.
- Consolidating the results of the evaluation of the developed prototypes, extracting conclusions and recommendations from the validation process, and defining a strategy for a potential uptake of solutions inspired in the PCP outcomes, including a complete technical specification of the envisaged solutions and standardisation needs and/or proposals. This strategy should consider joint-cross border procurement schemes and exploit synergies with other EU and national non-research funds.

The applicants shall maximise the visibility of the project outcomes to the wide community of potential EU public buyers. Liaison with other communities beyond civil protection is encouraged (e.g. Border Guard and Law Enforcement Agencies) in order to assess the reuse and extensibility of the results achieved in other security applications.

SSRI02-2.2021 (RIA) – Effective pathways towards standardisation and certification schemes for security

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Better understanding of the potential value of standardised solutions and certification schemes for the demand and supply actors in the security market taking into account the specificities of the different policy areas and priorities addressed by the Cluster 3 Work Programme[29] and in the light of the distinctive features of the EU Security market[30];

- Stronger capabilities for EU security practitioners to address security challenges[31] built on standardised solutions and certifications schemes that leverage the regulatory, policy, operational and market context of such areas;

- Plausible pathways to the development of standardised security solutions (including de-iure and de-facto approaches) that contemplate the different profiles and roles of actors that must intervene in the process as well as the different instruments available, such as the EU standardisation system, public procurement or security research, among others;

- More efficient, harmonised and EU-wide endorsed processes for the development and adoption of standardised security solutions and/or certification schemes by security technology developers and users in high priority security areas;

- Better understanding of the obstacles that impede the development and adoption of standards in the different areas of security as well as of the necessary measures to overcome these;

Scope:

Standardisation plays an important role in eliminating technical barriers to trade and facilitate market access. Standards also help to ensure that complementary products and services are interoperable, facilitate the introduction of innovative products and ultimately build trust in the quality of products and services[32].

In a complex, multidimensional and multinational environment, the impact of the actions taken to ensure the security of citizens are heavily conditioned by the availability and adequacy of the measures deployed (including technology-based measures) to prevent, prepare, react and recover from the occurrence of security threats. The quality, harmonisation, interoperability, innovation and trust brought by standardised solutions is therefore desirable in the field of civil

[29] Notably by those addressed by the new Security Union Strategy and the new Pact on Asylum and Migration.

[30] Some of these features are described in the Action Plan for an innovative and competitive security industry, COM(2012) 417

[31] Actions shall not focus on one concrete area of security, but cover the full landscape of security areas addressed under the destinations FCT, BM, INFRA and DRS. When touching upon Disaster Risk Management, actions funded under this topic shall avoid overlapping and build on the results, as needed, of actions funded under Topic DRS02-3.3.2021.

[32] COM(2018) 764

security in the sense that: i) It would increase the chances that the market is ready to offer security solutions when and where these are required; ii) It would increase the level of confidence in the quality and performance of such solutions.

Likewise, certification, understood as the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements[33], can be a useful tool to add credibility to the security equipment acquired by practitioners by demonstrating that it meets the quality and performance expectations. It also has a positive effect on the creation of a clearer European identity for these technologies[34] that should contribute to enhancing the global competitiveness of the EU companies with regards to third country competitors.

However, the definition and implementation of EU security standards and certification schemes has proven to be challenging. The obstacles found so far have their roots not only in the particular features of the security market[35] and the EU standardisation system[36], but also in diverging national interests, in how Member State authorities have traditionally built operational capacity or in highly competitive industrial dynamics. However, the underlying reasons for the lack of EU standards or common certification schemes for security technology are not easily identifiable. In order to fill this gap in our understanding of the phenomenon and to be in a position to propose measures to address this challenge, a serious and holistic analysis is required.

Applicants are invited to submit proposals to explore how the development and adoption of EU standardised security solutions and certification schemes would impact the effectiveness and efficiency of the measures put in place by the EU and the Member States to face current and future threats. In relation to common certification schemes, research should also address the possibility of defining and implementing unified methods for the verification and validation of measures of performance and effectiveness of security technologies under development, notably under the frame of EU-funded security research projects and with the aim of ensuring the wide acceptance of their outcomes by the end-user community. In addition, research should show how standardised security solutions and certification schemes can be utilised to give continuity to the results of EU-funded research onto other funding instruments oriented to the commercialisation (e.g. EIC Accelerator) and/or the deployment (e.g. ISF, IBMF) of innovative technologies.

The proposed research will need to take into consideration the EU security policy priorities addressed by the Cluster 3 Work Programme (including in the area of Infrastructure Protection,

[33] https://www.iso.org/conformity-assessment.html

[34] An "EU brand", as referred to in the Action Plan for an innovative and competitive security industry, COM(2012) 417

[35] Reference to Annex including the analytical paper in the Action Plan for Security R&I, when adopted

[36] COM(2018) 764

Disaster Resilience, Fight Against Crime and Terrorism and Border Management), the particular features of the EU security market, the relevant legal framework in place and the roles of the different stakeholders that could potentially steer and contribute to the development and adoption of EU standardised security solutions and certification schemes (e.g. policy makers, security authorities, end-users, public buyers, industry –including SMEs- and other organisations of interest –including European Standards Organisations-).

Research should not only shed light on the value of standards and certification, but also on the obstacles that impede their development and adoption, the challenges and opportunities to address those obstacles and practical pathways to follow in cases where their potential value justifies the action. The alternatives proposed should not only focus on formal *de-iure* standards, but also, and notably, on *de-facto* approaches that can rely on multilateral agreements, joint cross-border public procurement or research, among other instruments. Comparing the adequacy of each approach in different scenarios derived from the context mentioned above shall be the basis for the applicants to deliver concrete policy recommendations for the development and adoption of EU standardised solutions.

Proposals shall closely collaborate and interact with the EC-chaired or funded initiatives that hold the widest body of knowledge in the area of security research, such as the Networks of Practitioners funded under H2020 Secure Societies work programme, the European Networks for Security Research & Innovation funded under Horizon Europe Cluster 3 work programme, the Community of Users for Secure, Safe and Resilient Societies, or other security research and innovation working groups set-up by EU Agencies. The proposals shall also exploit the knowledge and build on the results of previous or current EU-funded security research projects with activities in the field of pre-normative research and standardisation, as well as on the achievements of ongoing policy-led initiatives for the development of mandatory or voluntary standardisation and certification schemes.

The project shall have a maximum estimated duration of 2 years.

Area SSRI 03 - Cross-cutting knowledge and value for common security solutions

SSRI03-1.2021 (RIA) - Societal Impact assessment and impact creation transdisciplinary methods for security research technologies driven by active civil society engagement

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Promotion of socially and environmentally sustainable products and services through stronger civil society engagement;
- Policy-makers, security practitioners and the research community implement security technological solutions and policies that fulfil both societal and legal requirements, such

as inclusiveness, accessibility, universal design, openness, legitimacy, proportionality, ethics;

- State and non-state actors base their decision-making on an assessment of any possible negative societal impacts of security research outputs, including human rights implications and risks of ill-intended use;
- Security practitioners and citizens are provided with technical solutions that are transparent, privacy-sensitive, open source, friendly and easy to use;
- Security practitioners and citizens have the necessary skills and knowledge on the use of the new technologies being produced, as well as their impact on the society;
- Security practitioners have a broader understanding of the new opportunities offered by technological developments, including accessibility and universal design aspect of technologies which goes beyond the mere response to security challenges to ensure that everyone is included;
- Security practitioners, the research community and policy-makers build upon existing knowledge on lessons learned and best practices, as well as recommendations and good examples of how the EU is using technology to combat risks to security while respecting and promoting fundamental rights.

Scope:

Applied research derives its meaning, and therefore, its financial justification from its relevance to society, to society's needs, to society's values, to its aims, needs or ambitions. Applied research presupposes that a distinct societal need is identified and that a programme of research is devised to provide the concrete knowledge required to meet that need as well as to better understand areas related to experience and requirements of technologies regarding vulnerable groups through universal design and common accessibility principles.

The finality and value of applied research is assessed on the grounds of this relevance, on the degree to which the results of the research can be applied to one or several problems beyond or after the research itself. The salience and value of any type of applied research – including security research – lies outside the research itself and in its impact on society.

In general, research can have an impact on society at two different points: at the level of the scientific methodology that employs and at the level of the scientific outputs that generates and communicates. Any action can have desirable and undesirable outcomes. Undesired results of security research can include both the results of research that does not reach its intended aims or research that does not reach its aims, but whose aims do not provide the security it originally set out to provide. Significantly, it can include particular measures that have as a secondary effect an increase in insecurity such as the development of technological solutions.

In innovation processes and advances of technological change, societal covers all those areas that influence the citizen, society and the state. This can be from privacy issues, confidentiality, the use of products and services, the potential for misuse of information and data, fake news, security marking, secure infrastructure etc.

Technological solutions in the area of civil security for society are often perceived as intrusive means to intensify and broaden surveillance and control of citizens in a top-down approach. Security technology is addressed with mistrust as regards to its detrimental effects on civil liberties and raises questions on fundamental rights and freedoms, privacy and data protection. Nevertheless, a wide variety of technological tools is available in different languages for different risk scenarios and with different functionalities. At the same time, technology can also be applied to increase societal resilience, improve and strengthen horizontal coordination, raise citizens' awareness and facilitate exchange of information among citizens in crisis' situations, disasters or pandemic risk incidents. Strengthening a co-productive use of technology to enhance societal resilience requires a better understanding of inclusive design, crowd-based, and Information and Communication Technologies (ICT)-enabling horizontal communication processes.

A systemic stock of such technologies, including an evidence-based assessment of the number of users in Europe and an evaluation of their impact in past human life disasters or crisis management incidents can help to improve the societal acceptability, directionality, desirability and ethicalness of security research and innovation. A societal development plan that examines the socio, economic, political context, which might have caused the security problems, can also help to learn from past-experiences. Demonstrating awareness of the risks that potentially build biases into automated systems would be important to identify best solutions for relevant functionalities and pave the way for a coordinated European approach, which strikes the right balance between practitioners' technology requirements and privacy-friendly tools and solutions for the citizens. Furthermore, improved knowledge of relevant human and societal factors in order to assist, supplement or override human misjudgement, lack of compliance or understanding through education and training modules can better achieve the desired impacts on attitude and behaviour change creating resilience to security threats.

In assessing the impact of security technologies, proposals are expected to examine methodologies that allow citizens genuine participation, including the vulnerable groups and people with disabilities in innovation processes. A socio-technical approach can enhance the ambition and effectiveness of innovations by inspiring socially acceptable design for systematic change and societal transformation. They should look into methodologies that measure the impact of technologies on society by addressing issues of: what can be measured (qualitative and quantitative measurements); why it is important to measure; what is important to measure both from policy and technology aspects and how societal impact can be measured (qualitative and quantitative measurements), including evidence about cognitive biases.

Proposals should also address mitigation measures that could be taken to reduce the impact on privacy, human rights and fundamental freedoms with the involvement of citizens as co-designers and beneficiaries in security research. When assessing impact, attention should also be paid to citizens' training for reducing negative effects, modelling and simulation of their behaviour in the event of security threats. This may include virtual assessment of different protection (prevention, preparedness and response) measures.

Proposals' consortia should comprehend security practitioners, system developers, public sector, technology and civil society organisations[37], communication specialists on security research, researchers and Social Sciences and Humanities Experts from a variety of European Member States and Associated Countries. In order to ensure a meaningful democratic oversight of the EU's security research programme, projects and policies at national and European level, proposals should ensure a multidisciplinary approach and have the appropriate balance of industry, citizens' representatives and social sciences and humanities experts.

Project proposals' consortia are encouraged to cooperate closely with the Networks of Practitioners funded under H2020 Secure Societies work programme if valuable results on impact can be obtained, as well as with the European Networks for Research and Innovation in Security funded under the Horizon Europe Cluster 3 work programme.

Proposals should also comply with the new contractual provision under article 33(2) of the MGA of Horizon Europe on the "The obligation to ensure effective SSH integration, where appropriate".

The project shall have a maximum estimated duration of 4 years.

As indicated in the introduction of this call, proposals should foresee resources for clustering activities with other projects funded in the same or other calls to identify synergies and best practices.

Proposals could also be linked to finished or ongoing projects such as the NewHoRRizon (under the H2020 Research and Innovation Programme) which have developed Societal Readiness Level Tools. They may also consider using their interactive web tools provided to help study the societal input and engagement as part of project proposal development and implementation.

This action also allows for the provision of financial support to third parties in line with the conditions set out in Part K of the General Annexes[38]. Due to the nature of the work to be supported under the call(s) supporting deployment of innovative solutions, the contribution to a third party may go beyond EUR 60 000. The selection of the third parties to be supported under the grant will be based on an external independent peer review of their proposed work.

The calls to be launched within the grant for the selection of third parties should respect the rules and conditions laid out in Annex K of the Work Programme[39], in particular as regard transparency, equal treatment, conflict of interest and confidentiality.

[37] A civil society organisation can be defined: "any legal entity that is non-governmental, non-profit, not representing commercial interests and pursuing a common purpose in the public interest". https://ec.europa.eu/research/participants/portal/desktop/en/support/reference_terms.html; Check also the study "Network Analysis of Civil Society Organisations' participation in the EU Framework Programmes", December 2016.

[38] The Annexes are currently being drafted.

[39] The Annexes are currently being drafted.

CALL SSRI 2022:

Proposals are invited against the following topic(s):

Area SSRI 01 - Stronger pillars of security Research and Innovation

SSRI01-1.2022 (CSA) – Increased foresight capacity for security

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- An increased knowledge base on technology foresight, more accessible to the security stakeholders, that supports the consolidation of a forward-looking culture in the planning and use of resources in the area of security.
- Anticipatory steering of the foreseeable evolution of security-relevant technologies and of the challenges and opportunities brought by such evolution on the industrialisation and use of future security technologies facilitated by a common foresight framework for EU civil security;
- An evidence-based identification, prioritisation and programming of security R&I and capacity building investment sustained on an anticipated and consolidated view of how future technology, research and industrial trends impact, influence and shape future threats and security capabilities;
- A recognised EU-wide definition of critical technological building blocks and components for the development of future high-priority capabilities;

Scope:

Anticipating the future, both in terms of threats and of opportunities offered by new emerging technologies is a real challenge. Having the capacity to depict plausible futures, to identify upcoming threats and to propose early responses can be of invaluable help to decision makers.

The sound programming of EU-funded security research can also be notably improved if the analytical capacity required to identify mid to long-term trends in the EU security context is in place and its outcomes are made available to decision makers through the right channels on a timely manner. This includes not only the identification of academic research, technology, innovation and industrial trends, but also of how these can be translated into early warning of threats and anticipated response. A common EU approach for civil security to address this need, properly covering the full range of security policy dimensions and acknowledging their particularities and distinctive features, is therefore needed.

Many organisations, including the European Commission, have developed instruments that provide timely assessment of technology trends on a regular basis. The broad technology landscape does not show frequent fluctuations, and a plethora of tools and ready-made information products unveiling trends in different time horizons are widely available. However, pure technology watch-based approaches are not helpful for civil security decision makers unless they are embedded in a qualitative assessment of threats and capabilities. Such assessment shifts the focus from a purely technological standpoint to the way in which these technologies are and will be used in a given policy, operational, industrial and societal context.

Therefore, building on existing technology and research landscaping mechanisms (and possibly tailoring them to the specificities of the civil security domain), applicants are invited to submit proposals for the development and operationalisation of a foresight framework for security including advanced tools, methods, techniques and processes. Such framework shall be accompanied by a solid scientific model that connects future technologies with their future use. This shall allow to identify how future civil security technology, research, innovation and industrial trends impact, influence and shape future threats and security capabilities, taking into account contextual aspects. These may include ethical, legal, societal, economic, geopolitical, environmental or industrial aspects, with particular emphasis on the capacity of the EU security technology and industrial base to achieve the desired technology development objectives, thus safeguarding the EU security technology sovereignty, if and when this is required. The proposed approach shall combine qualitative and quantitative methods, maximise their automation and allow for qualified inputs through distributed and collaborative environment/schemes in order to make the most efficient and effective use of the human and technical resources available.

The proposals shall take into account existing foresight approaches implemented by other EU and international organisations (e.g. JRC, EDA, INTERPOL, UNIDO, etc.). Should these be used as a reference, the newly proposed approaches should not just replicate the existing ones, but reference the source accordingly and adapt them to the context of EU civil security. Proposals shall also take into account previous EU-funded research projects addressing foresight and build strong synergies with ongoing projects, in particular with the Networks of Practitioners funded under H2020 Secure Societies work programmes and the new European Networks for Security Research & Innovation funded under Horizon Europe Cluster 3.

The proposed foresight framework must be operationalised since the early stages of the project and deliver information products until its finalisation and beyond. When operationalising the proposed approach, applicants shall consider that they must deliver tangible value to the programming of the Union´s investment for the development of security capabilities, including through research and capacity building funds. Therefore, the results shall be made available at least to all stakeholders involved in this task, both at EU and national level. In order to allow that the developed foresight framework works with and for this purpose, the applicants shall demonstrate that the working cycles proposed and the exchanges of information required are duly coordinated with the work of the Thematic Working Groups of the Community of Users for Secure, Safe and Resilient societies set-up by the European Commission and/or with equivalent innovation labs set-up by EU Agencies in the different thematic areas addressed (e.g. Frontex). Therefore, the thematic working groups shall not only be a source of information, but also a validator of the foresight approach proposed and a beneficiary of the information products delivered.

Applicants must show a good understanding of the context where security research and capacity building programming takes place (mostly at EU level), of who are the main actors involved and of what are their needs in terms of foresight. The proposal should pay special attention to the type and format of the outcomes to be delivered, their timeliness and to what audience these are addressed. In this sense, outcomes shall be delivered periodically every 6 months or less throughout the whole project starting from month 6.

The project shall identify and describe options for the exploitation of the foresight model proposed beyond the project lifetime, including the setting up of a permanent technology foresight capacity in support to EU-funded security research and innovation programming, i.e. under the Research-as-a-service approach.

The project shall have a maximum estimated duration of 3 years.

SSRI01-2.2022 (CSA) – European Networks for security Research & Innovation

<u>Expected Outcomes</u>: Projects' results are expected to contribute to the following outcomes:

- Enhanced analytical capacity to support the programming of EU-funded security research and capacity building funds through a periodic and timely evidence-based policy feedback ;
- Periodically aggregated and consolidated view of the capability needs and gaps in the thematic areas under consideration[40];
- Periodically aggregated and consolidated view of the state-of-the-art technologies, techniques, methods and tools that can contribute to fill the identified capability gaps;
- Periodically aggregated and consolidated view of outcomes (including on technological, industrial, legal and ethical issues), future trends, lessons learnt and best practices derived from past and current security research effort incurred in the thematic areas under consideration.

[40] The thematic areas under consideration are described in the topic and are different for each call. Only one network in each area can be funded.

- More systematic assessment and validation of the outcomes of EU-funded security research projects with respect to identified capability gaps through harmonised support mechanisms;

- Common and updated map of opportunities and constraints for the industrialisation, commercialisation, adoption and deployment of innovative solutions in response to common capability gaps;

- Common and updated map of areas requiring standardised solutions and/or certification schemes to foster innovation uptake and market creation, as well as options for the implementation of such schemes.

- Enhanced cooperation between research institutions, smaller private research agencies, security practitioners, SMEs and community representatives to support integrated participation in requirements determination and analysis, research and validation and evaluation of results.

Scope:

Innovation uptake is not a linear process, and even less a single-step process that happens only at the end of a research project and it is not automatically enabled by a successful research result. The innovation uptake process begins with the identification of a need and ends with an innovative solution deployed on the field of operations, being R&I only one of the many contributors to the overall process, but not the first and not the last. In other words, successful results of research projects are a necessary but not sufficient condition to guarantee the uptake of innovation.

Investment in security research needs to be designed taking into consideration how and when it can deliver outcomes that contribute to the development of security capabilities. Therefore, research shall be undertaken, from its very early stages, in a way that addresses real needs while guaranteeing the impact in the final solutions. It shall also ensure to identify and underpin the factors that could help in the implementation of its results. However, the programming of research is highly conditioned by the quality, reliability and timeliness of the evidence that supports its decision making process. This includes the identification and understanding of the contextual elements that can or will influence or be influenced by the research (process), the research team and the research projects themselves.

The European Commission and the Member States carry out this programming exercise periodically, taking into account a wide variety of inputs. The complexity of the challenge is notable, considering that the EU security landscape is volatile, uncertain, complex and ambiguous in what regards the security threats, the capabilities required to face them and the evolution of modern technologies. In order to carry out a sound programming exercise, the Commission and the Member States strive to consult and involve all actors. With that aim, experts are gathered in different configurations and their inputs are coordinated at EU and national levels to be factored in by the decision making bodies of EU-funded security research.

These experts require high quality, reliable and timely evidence to support their assessments, but information is often scattered, hardly visible and requires bespoke processing for the detection of patterns and for the generation of actionable intelligence. In other cases, it is simply not presented in the right format to unveil its value.

Applicants are invited to submit proposals for the establishment of European Networks for Security Research & Innovation. The role of these networks shall be to collect, aggregate, process, disseminate and exploit the existing knowledge to directly contribute to the expected outcomes of this topic.

Networks shall engage with the main sources of information in order to have a sound and updated picture of the aspects mentioned above. This includes interaction with security experts (beyond the members of the project consortium), organisations, projects or initiatives, but also an extensive review of available databases, studies, reports or literature (notably all information generated under the EU-funded security research programmes, and possibly under other EU or MS funding programmes).

The networks shall ensure the maximum outreach of their findings to the different communities of the security research ecosystem, including policy makers, security authorities, industry, researchers and citizens. Special emphasis shall be made on the contribution of these networks to the work of entities and initiatives established by the EC and the EU Agencies (e.g. Union Civil Protection Knowledge Network) to contribute to the security research programming effort. In this regard, the networks shall contribute timely and intensively to the work of the Thematic Working Groups of the Community of Users for Secure, Safe and Resilient Societies and of other equivalent innovation labs/groups set-up by EU Agencies (e.g. EUROPOL). The networks shall contribute to these working groups with the quantitative and qualitative evidence required to carry out their activities in support to a more impactful EU-funded Security R&I and to a more frequent and systematic innovation uptake.

The networks shall be in a position to deliver findings on the abovementioned challenges starting from the month 6 of the project and periodically every 6 months or less, in accordance with the information needs of the entities and initiatives they are contributing to.

Proposals shall clearly describe the process and timing for the collection of inputs and the generation of outcomes. This plan shall go beyond the description of project deliverables and milestones, and describe in detail how and when the findings will be exploited during the project and in collaboration with the communities described above.

The consortia submitting the proposals shall ensure sufficient representativeness of the communities of interest and an adequate coverage in terms of knowledge and skills of the different knowledge domains required to face the challenge, including security operations, technologies, research & innovation, industry, market, etc. In this sense, the network may possibly expand beyond the project partners during its implementation, but the project beneficiaries shall be the core and the driver of the activities. The applying consortia need to demonstrate that the integrating partners guarantee the expertise required to steer the project activities in all the knowledge domains to ensure the success of the action. The work of the partners shall be supported by solid and recognised tools and methods, also accompanied by the required expertise to put them in practice.

The networks shall build to the extent possible on the work initiated by the Networks of Practitioners funded under the H2020 Secure Societies work programme. When such networks are still ongoing maximum cooperation and minimum overlapping must be ensured and demonstrated.

Under this call, the applicants are invited to propose networks on the thematic areas of:

i) Disaster Resilience

ii) Fighting Crime and Terrorism.

Only one network in each area can be funded.

The project shall have an estimated duration of 3 years.

SSRI01-3.2022 (CSA) – Community building for Safe, Secure and Resilient Societies at local, regional and national level

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- An increased visibility of capability needs, gaps, and technology solutions expressed by national, regional and local communities;
- A more reliable measure of the impact of security research and innovation built on a better awareness of innovation-uptake success stories stemming from the participation of national players in EU-funded security research projects;
- Reduced geographical fragmentation of the security market through the establishment or up-scaling of National Communities of Users for Secure, Safe and Resilient Societies set up and running in the different Member States or Associated Countries;
- A seamless integration of the national, regional and local dimensions of security into the EU picture through the consolidation of a network of Contact Points for the National CoUs;

Scope:

Policy-makers, practitioners, industry, academia and citizens are the pillars on which to build a sound security research agenda. Notwithstanding the contribution of these stakeholders to the implementation of projects, the Commission ensures that their knowledge also feeds the programming of research.

The EU-funded security research ecosystem has changed the traditional relationship between end-users and solution providers. The awareness of security needs and solutions has been steadily growing at all levels during the last years, with EU funded security research and innovation projects playing a pivotal role. This awareness guarantees not only that research addresses critical needs, but also that the research investment will deliver tangible results.

The Community of Users for Safe, Secure and Resilient Societies (CoU), established by the Commission in 2014, has largely contributed to building this ecosystem. This an informal setting composed of more than 1500 members (policy-makers, practitioners, academia, industry and civil society) that regularly interact and meet in thematic sessions. The CoU is progressively consolidating and is expected to enable the capacity required to look into future challenges, anticipate research needs and propose innovative technology solutions and pathways for their uptake by security practitioners.

This set-up increases the visibility of the security challenge at EU level and across security areas. However, the security sector exhibits a remarkable geographic fragmentation, with actors operating at EU level, at national level, at regional level and even at local level. In order to acknowledge the different perspectives of all stakeholders and break geographical silos, there is a need to aggregate the knowledge existing in the EU Member States and regions and incorporate it to the European picture. With the push towards a "Place-based innovation and experimentation" brought by the New Industrial Strategy for Europe[41], the development and testing of new security solutions in European Regions, drawing on their local characteristics, strengths and specialisms, deserves reinforcement.

Setting up structures equivalent to the CoU at national level shall help to have a more comprehensive view of the common EU security needs and solutions and to better capitalise on pan-European cooperation opportunities.

Applicants are invited to submit proposals for setting up a pan-European network of National CoUs. The scope of this network will be to contribute to the foundations for the definition, implementation and roll-out of such communities, with the objective of keeping the national CoUs operational even beyond the duration of the project.

The proposals shall aim at defining common structures for the functioning of the national CoUs and establishing the necessary link to the governance structure and operation of the European CoU established by the Commission. In this regard, the members of the network shall act as Contact Points of the national CoUs and guarantee the integration of their activities at EU level. In order to do so, the applicants shall represent organisations with a demonstrated capacity to convene all relevant national actors (i.e. policy makers, users, industry, academia and civil society), and preferably representing their respective national administrations. In order to guarantee the EU-wide representativeness of the network, the participation of at least 8 EU Member States or Horizon Europe Associated Countries is required.

[41] COM(2020)102

Proposals shall contemplate a period no longer than 1 year from the beginning of the project for the establishment of at least 8 national CoUs. The rest of the project shall be dedicated to jointly launching and rolling-out their activities in close coordination with the European CoU. The activities of the national CoUs shall address at least the following challenges at national, regional and local level:

- Relay the information generated under the European CoU to national, regional and local players;
- Identify capability gaps, solutions to address those gaps, and research needs at local, regional and national level and integrate them in the EU picture through the European CoU;
- Share research opportunities coming from national research programmes and initiatives with the wider EU community;
- Improve the visibility of the results achieved by national players following their participation in research projects (national or EU-funded), and in particular those which have led to the deployment of solutions in the field of operations, or which have a strong potential for uptake as a result of the interest expressed by national buyers;
- Identify financial pathways and opportunities to enable the uptake of innovative solutions stemming from EU, national or regional capacity building funds, with special emphasis on the EU Home Affairs funds (both in the parts under shared management and those under direct management by the Commission) and on the European Regional Development Funds.

As an output of the action, the beneficiaries shall develop a model not based on EU security research funding for the sustainability and enlargement of the national CoUs beyond the lifetime of the project. The network of National CoUs shall ensure synergies with the networks of Horizon Europe Cluster 3 National Contact Points[42].

The project shall have a maximum estimated duration of 5 years.

Area SSRI 02 - Increased Innovation uptake

SSRI02-1.2022 (CSA) – Stronger grounds for pre-commercial procurement of innovative security technologies

[42] The Horizon Europe NCP model is under development by DG RTD. To be updated once more information is available.

Expected Outcomes: Projects' results are expected to contribute to the following outcomes:

- Consolidated demand for innovative security technologies built on the aggregation of public buyers with a common need expressed in functional and/or operational terms without prescribing technical solutions;
- Better informed decision-making related to investment in innovative security technologies based on a better understanding of the potential EU-based supply of technical alternatives that could address common needs of EU public buyers;
- Better informed decision-making related to investment in innovative security technologies based on an improved visibility of the potential demand in the EU market for common security technologies;
- Increased capacity of EU public procurers to align requirements with industry and future products and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement.

Increased innovation capacity of EU public procurers through the availability of innovative tendering guidance, commonly agreed validation strategies and evidence-based prospects of further joint procurement of common security solutions.

Scope:

End-users and public procurers from several countries are invited to submit proposals for a preparatory action that should build the grounds of a future Pre-Commercial Procurement action. Both this preparatory action and the future PCP action will be oriented to the acquisition of R&D services for the development of innovative technologies, systems, tools or techniques to enhance border security, to fight against crime and terrorism, to protect infrastructure and public spaces, or to make societies more resilient against natural or man-made disasters.

Projects funded under this topic will have the opportunity to submit a proposal for a follow-up PCP action that shall be included in the Horizon Europe Cluster 3 Work Programme 2024 (subject to budget allocation and priorities of the work programme 23-24). The applications to the follow-up PCP topic will follow the regular procedure for Horizon Europe calls for proposals.

The works to be done in relation to this topic shall take into account and/or ensure compliance with the following:

- The EU Directive for public procurement and in particular with the provisions related to PCP;
- The specific provisions and funding rates of PCP actions and the specific requirements for innovation procurement (PCP/PPI) supported by Horizon Europe

grants, as stated in the General Annexes of the Horizon Europe Work Programme 21-22[43];

- The guidance for attracting innovators and innovation, as explained in the Commission Guidance on Innovation Procurement C(2018) 3051, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

During the course of the project, the applicants are expected to deliver clear evidence on a number of aspects in order to justify and de-risk the follow-up PCP action, including:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;
- That there is a consolidated group of potential buyers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint-procurement of innovative solutions;
- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who could be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;
- That the state of the art and the market (including research) has been explored and mapped, and that there are different technical alternatives to address the proposed challenge;
- That the future PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready on due time in order to launch the call for the acquisition of R&D services according to the PCP rules.
- That the technology developments to be conducted in the future PCP can be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data.
- That in developing technology solutions, societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) can be taken into account in a comprehensive and thorough manner.

[43] Inspired on the text of H2020. To be tailored to the General Annexes of the HE WP.

Open market consultations carried out during this project shall take place in at least three EU Member States or Associated Countries.

Should the applicants intend to submit a proposal for the follow-up PCP foreseen for the 2014 call, the above evidence must be consolidated in project deliverables of this CSA and duly referenced in the proposal before its submission.

To ensure that the outputs of this action also becomes available for further procurement purposes to EU Member State national authorities as well as EU agencies that are not beneficiaries of this action, proposals must necessarily state:

(1). Agreement from the beneficiaries to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to procure a capability or a product fully or partly derived from this action, the use of the information required to run such a procurement process, and solely for that purpose.

(2). Commitment from the beneficiaries to consult with any legal entity generating information to be released for the purpose set out in paragraph (1), unless contrary to applicable legislation.

(3). Commitment from the beneficiaries to negotiate the use granted under paragraph (1) on Fair Reasonable and Non-Discriminatory (FRAND) terms.

The project shall have a maximum estimated duration of 1 year.

Area SSRI 03 - Cross-cutting knowledge and value for common security solutions

SSRI03-1.2022 (RIA) –Social innovations as enablers of security solutions and increased security perception

Expected Outcomes: Projects' results are expected to contribute to one or several of the following outcomes:

- Policy makers, security practitioners and researchers have increased understanding of the capabilities and capacities of local communities and citizens to contribute to developing security solutions;
- Policy makers, researchers and system developers increase the orientation of security solution development towards socially innovative and Responsible Research and Innovation approaches;
- The notions of 'smart citizens' and 'smart local communities' empowered by Responsible Research and Innovation and social innovation, where the general public co-control safety and security of their environments, are more widely adopted by decision makers;

- New benchmarks, standards or other quality criteria are established for developing security solutions through Responsible Research and Innovation[44];
- Increased collaboration across all parts of the quadruple helix (academia/research, public authorities, industry/SMEs, civil society/citizens/local communities) to develop innovations in line with the needs, values and expectations of society;
- Innovative, transferable and potentially scalable technological solutions co-created with citizens and local communities in social labs and innovation living hubs, and citizens empowered to act as generators, validators and end-users of the new horizontal technologies;
- Societal trust in security research products, their desired usefulness and social acceptability[45];

Scope:

Citizens and local communities are insufficiently involved in the co-creation of socially innovative processes to develop security solutions and thus conceptions of what citizens and local communities know and think about security could be predominantly shaped by media coverage. This might result in bias in the assessment of the seriousness and probability of different security threats. Nevertheless, social acceptance of security technology depends on understanding citizens' awareness of security problems and threats. Comprehensive discussion that involves citizens from all parts of society directly in co-design such as through Responsible Research and Innovation and social innovation, alongside other security technology actors, would integrate public concerns beyond incident-based interpretations of security threats, thereby increasing social acceptance of security technology and subjective feelings and perceptions of personal security in daily life. At the same time, industry would be in a position to identify new business opportunities in producing and delivering security products and

[44] Responsible research and innovation is a process for better aligning research and innovation with the values, needs and expectations of society. It implies close cooperation between all stakeholders in various strands comprising science education, definition of research agendas, access to research results and the application of new knowledge in full compliance with gender and ethics considerations. Outcome of the Council Meeting 3353rd Council meeting Competitiveness (Internal Market, Industry, Research and Space) Brussels, 4 and 5 December 2014, p. 13.

[45] Social acceptance is seen as the process by which innovation becomes embedded in everyday practices, that needs to be supported by good design and creative, inclusive design methods. It enables a focus on enhancing the *acceptability* of solutions. This may imply careful attention to usability and the context of appropriation as it may require wider systemic change and will often depend on stakeholder value chain mapping, and methods of collaborative design and responsible research and innovation to which reference is made.

services which are in line with needs, values and expectations of citizens and local communities and support their well-being.

Social innovations[46] for increasing security and security perception can be manifold and the scope of application of social innovation is potentially wide-ranging and can address diverse aspects. For example, apps that help citizens to prevent, detect and respond with first responders in disaster and crisis situation and to access real-time information about adequate responses; the formation of networks of parents of children who are considered susceptible to extreme ideologies to establish early warning and early-intervention mechanisms. What these examples have in common is that they give citizens an active role in co-creation and produce a practical use value.

Giving more emphasis on a co-creation procedure from the design phase could also overcome the corresponding lack of knowledge about how socially innovative solutions can contribute to increased security and security perception. Although citizens and local communities can successfully support as co-designers and beneficiaries to replicate and upscale best practices as well as systemic and cross-sectorial solutions that combine technological, digital, social and nature-based innovation, existing knowledge of such contributions is limited. Therefore, proposals should develop a societal development plan that builds upon a people-centred approach and examines how social innovations on security are organised, how they work, how and why they are adopted or rejected, their direct and indirect benefits and costs, including in vulnerability assessments, how they sustain, and which interfaces with other more formal security agents are established.

Proposals should map and analyse a social innovation in one or more distinct social spheres, in areas such as:

(a) Security disturbance at large (pop-) cultural and sports events;

(b) Security and security behaviour in public places, public transport or mobility;

(c) Radicalisation, dis-integration in local communities and social media;

(d) Digital identity, data portability and data minimisation with an attribute based society in control;

[46] "Social innovation can be defined as innovations that are social both as to their means and in particular those which relate to the development and implementation of new ideas (concerning products, services and models), that simultaneously meet social needs and create new social collaborations, thereby benefiting society and boosting its capacity to act"; (European Commission Bureau of European Policy Advisors (BEPA, 2011, p. 9). The co-legislators adopted the BEPA definition two years later in the Regulation (EU) No 1296/2013 of the European Parliament and of the Council of 11 December 2013 on a European Union Programme for Employment and Social Innovation ("EaSI"); Regulation (EU) No 1296/2013 of the European Parliament and of the Council of 11 December 2013 on a European Union Programme for Employment and Social Innovation ("EaSI") and amending Decision No 283/2010/EU establishing a European Progress Microfinance Facility for employment and social inclusion, Article 2, paragraph 5).

(e) Safety and security in remote communication, command and control of operation in risk scenarios;

(f) Mobilisation on human trafficking;

(g) Automatic detections' use.

Proposals should consider the social relevance of research, social marketing, transferability and scaling of such social innovations as this is an area where there is limited research and experimentation, which could help to spread the use of such solutions. They should also consider education, training and change individual behavioural and social practices by involving citizens and local communities as generators, validators and end-users of the new horizontal/advanced technologies.

Proposals which have developed innovative ideas on societal resilience under the destination area of Disaster-Resilient Societies and which can transform them into social innovations for disaster crisis situations engaging citizens and local communities are not pre-empted to participate in this topic.

Consortia should give meaningful roles to all research and innovation actors, including security practitioners, system developers, the public sector, technology development organisations, civil society organisations[47], communication specialists on security research, researchers and Social Sciences and Humanities Experts from a variety of European Member States and Associated Countries. In order to ensure a meaningful democratic oversight of the EU's security research programme, projects and policies at national and European level, proposals should establish a multidisciplinary approach and have the appropriate balance of industry, representatives of citizens and local communities and social sciences and humanities experts.

Proposals should comply with the new contractual provision under article 33(2) of the MGA of Horizon Europe on the "The obligation to ensure effective SSH integration, where appropriate".

The project shall have a maximum estimated duration of 4 years.

As indicated in the introduction of this call, project proposals should foresee resources for clustering activities with other projects funded in the same or other calls, to find synergies, and identify best practices, and to develop close working relationships with other Programmes (e.g.

[47] A civil society organisation can be defined: "any legal entity that is non-governmental, non-profit, not representing commercial interests and pursuing a common purpose in the public interest". https://ec.europa.eu/research/participants/portal/desktop/en/support/reference_terms.html; Check also the study "Network Analysis of Civil Society Organisations' participation in the EU Framework Programmes", December 2016.

the Civil Society Empowerment Programme (CSEP-ISF), Science with and for Society (SwafS), the Digital Europe Programme).

This action also allows for the provision of financial support to third parties in line with the conditions set out in Part K of the General Annexes[48]. Due to the nature of the work to be supported under the call(s) supporting deployment of innovative solutions, the contribution to a third party may go beyond EUR 60 000. The selection of the third parties to be supported under the grant will be based on an external independent peer review of their proposed work.

The calls to be launched within the grant for the selection of third parties should respect the rules and conditions laid out in Annex K of the Work Programme[49], in particular as regard transparency, equal treatment, conflict of interest and confidentiality.

[48] The Annexes are currently being drafted.
[49] The Annexes are currently being drafted.