ANNEX 3 - HORIZON EUROPE CLUSTER 3

CIVIL SECURITY FOR SOCIETY

1. Global Challenges and their Drivers

Security is one of the main concerns for the EU's citizens and is therefore among the top priorities for the Commission. While the threats of terrorism and crime against the EU remain serious, challenges like cyber-attacks are requiring coordinated responses and novel concepts. Illegal migration caused by ongoing insecurity and economic instability in the EU's neighbourhood as well as an increase of legal movements of persons and goods are requiring new technological solutions to allow for more efficient and better integrated border management. Disasters, whether natural or man-made, can put at risk important societal functions, such as health, energy supply and government. The aim is to prevent and reduce the loss of life, harm to health and the environment, economic and material damage from disasters, ensure food security as well as to improve the understanding and reduction of disaster risks and post-disaster lesson learning. Research can play an active role in this respect by supporting the development of innovative and collaborative solutions.

This cluster has as its vision to support wider EU responses to security challenges i.e. to support 'a resilient and more stable Europe that protects' as well as for this purpose supporting a competitive European civil security industry sector. It will address the challenges arising from persistent security threats like terrorism and crime, including cybercrime, as well as natural and man-made disasters.

As these challenges are rapidly evolving and technological progress is making a response increasingly complex, security research can serve as a tool to move from a reactive approach to security to a proactive approach based on foresight and anticipation. Among other, EU security research is a cornerstone of the Security Union enabling innovation in technologies and knowledge and furthermore contributes to a more competitive and, when necessary, autonomous European security industry. Research will enable opportunities that will be offered by emerging technologies such as e.g. Artificial Intelligence while at the same time preventing the malicious use of such same technologies.

2. EU Policy Objectives

This cluster will support implementation of EU policy priorities relating to security, including cybersecurity, and disaster risk management. In order to ensure a best possible impact, the activities under the cluster are aiming at supporting concrete EU policy as defined for each area of intervention:

- R&I activities in relation to disaster risk management will support implementation of the Union Civil Protection Mechanism, the EU Adaptation Strategy as well as of the Sendai Framework for Disaster Risk Reduction (2015-2030) and the Paris Agreement, and

related international processes such as IPCC and IPBES. In relation to CBRN-E incidents, R&I will support implementation of the EU CBRN and Explosives Action Plans.

- As regards protection and security, R&I activities will support implementation of relevant EU policies including those developed under the framework of the European Agenda on Security and the development of a Security Union. These include policies on integrated border management, the EU Action Plan on the protection of public spaces, policies and instruments on protecting critical infrastructure, as well as on fighting crime, including cybercrime and terrorism.

- R&I activities will help to put into practice the EU Maritime Security Strategy and, as concerns EU maritime borders, take in role in developing integrated border management.

- Cybersecurity, as addressed by the digital and privacy policy of the Union, in particular the NIS Directive, the GDPR, the EU Cybersecurity Act, and the future e-Privacy Regulation will benefit from R&I activities so as to keep up with rapid technological developments and the understanding of emerging trends in the cyber-domain.

As an overarching priority, effective support will be provided to practitioners, law enforcement agencies, first responders and other public authorities or private entities which are ensuring the security of European citizens, infrastructures and assets in general.

Alongside supporting EU policy responses to security challenges, R&I within this cluster will boost the competitiveness of companies and research organisations in the EU civil security sector and thereby strengthen the EU's technology and industrial base in this sector By doing so, it will also support European strategic autonomy in critical security areas such as cybersecurity; cloud services; artificial intelligence; critical raw materials and components; EU space technologies, systems and the EU Space Programme and its components (e.g. Copernicus, Galileo and EGNOS, SSA and GOVSATCOM).

All these activities will help to achieve SDG 16 (peace, justice, rule of law) and other relevant SDGs.

3. Targeted impacts
The main impacts sought are to support implementation of EU policy priorities relating to security, including cybersecurity, and disaster risk management:

- improved disaster risk management and societal resilience, leading to reduced losses from man-made and natural disasters;

- improved management of air, land and sea EU external borders, leading to better monitoring of movements across external borders and reduction of illegal movements of people and goods across those borders;

- 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;

- improved security and resilience of infrastructure and vital societal functions, such as healthcare, law enforcement, energy, mobility, public services, financial services, communication and logistics infrastructures/networks, so as to minimise disruptions including from hybrid threats;

- improved maritime security, including from man-made and natural disasters and from security challenges such as trafficking, piracy and potential terrorist attacks, cyber and hybrid threats, notably through better maritime surveillance and capability development;

- fighting crime and terrorism more effectively, particularly through better prevention of criminal acts and enhanced investigation capabilities notably as concerns cybercrime;

- cybersecurity and a secure online environment, with citizens, public bodies and companies empowered to protect their data and online activities.

Those desired impacts are further specified in the following section in relation to each priority.

4. Key R&I Orientations

Within this cluster, civil security research will be progressively framed under the wider umbrella of a capability-based approach to capacity building in the security sector. This approach focuses R&I activities as a contribution (notably, but not exclusively, through technology) to fill gaps in capabilities. It is for policy-makers and practitioners to identify those gaps and resulting requirements, and in such a way that ensures they reflect national and the shared needs at EU level. The process for defining and implementing R&I activities in this cluster needs to recognise that Member States have the front line responsibility for security but cannot address transnational threats in an optimal way when acting on their own. R&I can support this process, including by improving cooperation and exchange of information, and by increasing knowledge about relevant human and societal factors. EU-level R&I to fill capability gaps reduces risks of fragmented approaches and promotes better use of standards and resources, thus increasing the impact of EU responses.

An integrated approach is needed so as to take into account short-term needs stemming from fast-changing security threats but also to promote a proactive anticipatory culture to address longer-term scenarios of future threats and mega trends.

In the field of security research it is particularly important to take into account human factors and the societal context, and to ensure the respect of fundamental rights, including privacy and protection of personal data and to engage citizens and communities in the process of making society more resilient via R&I-enabled technological, non-technological and social innovation.. Furthermore, improved knowledge of relevant human and societal factors can better achieve the desired impacts. In this context, the Commission intends to continue to require that applicants complete a 'Societal Impact Table' as part of the submission process.

Account will be taken of the gender dimension, notably as part of R&I relating to the human and societal context of security and of disaster resilience and response.

Availability of and access to threats, risk and resilience knowledge, preparedness scenarios

and data, needs to be enhanced to strengthen capacities to forecast and to respond, and with practitioners' involvement (e.g. knowledge centres and networks). This includes data sets representing simulated scenarios. If possible, specific European research infrastructures, including those of the European Strategy Forum on Research Infrastructures (ESFRI), contributing to the identified challenges will be harnessed and new capabilities will be developed as needed.

4.1 Disaster-resilient societies
This priority aims to allow for reduced losses from disasters, both in terms of impact on citizens and of environmental, economic, material and immaterial damage, in particular in vulnerable groups and areas, including heritage sites.

Disaster risk management can be improved through related R&I activities. This includes a better understanding of the disaster management cycle for incidents with a high impact but a low probability of occurrence ("Lo-Hi/HILP"events). In this context research will enhance societal risk awareness, prevention and preparedness, including through early warning and alert systems and a capacity to be better prepared and able to respond to natural and man-made disasters

With the help of enhanced technological solutions and concepts, relevant communities can be better involved in the development and implementation of plans supporting cost-effective risk reduction and societal resilience, including for the evacuation of vulnerable populations.

An improved response to disasters requires better tools and procedures for the coordination of cross-border incidents, more integrated and interoperable technologies, tools and methods to support emergency procedures which are developed with all relevant actors. Finally, research can lead to the creation of standards on the EU-level for response and emergency planning.

Targeted R&I tackles cross-sectoral and multilevel governance on disaster risk management at EU level which manages also trade-offs in policy-making. This includes not only civil protection as such but related areas such as land management, agriculture and rural development, as well as environment, climate and energy. It will further contribute to the creation of methodologies to be defined for 'resilient by design' infrastructure. As a result of improved knowledge of human and societal factors, post-disaster recovery will respect local communities' aesthetic-historical-social values as well as quality standards for cultural heritage sites.

More specifically, there are four areas within the priority 'Disaster-resilient societies' which require more targeted R&I:

 a) chemical, biological, radiological, nuclear and explosive (CBRN-E) incidents
There is need for a deeper understanding of CBRN-E risks as well as for the creation of specific measurements, including standards and certification for detection equipment, better comparability of data, both within EU and beyond.

CBRN-E incidents create unique risks also for first responders. Security research can help mitigate such risks by identifying and filling gaps in capabilities for response, mission critical communication and protection equipment for first responders. In addition projects

will focus on capabilities for detecting and evaluating threats and incidents, or detection and triage of victims lead to an enhanced preparedness for and response to incidents.

R&I should further explore methods for seamless cooperation between relevant actors (e.g. law enforcement and civil protection authorities, health), including strengthening internal-external links (EU CBRN Centres of Excellence Initiative) and with key international partners (NATO, OPCW, Interpol).

b) climate-related risks and extreme events, such as fires, droughts, floods, heatwaves and storms

A consequent improvement in climate risk management will rely on more exact forecasting and understanding of climate change related risks and vulnerabilities, including their application within emergency planning. This is to be explored in connection with a generally more flexible adaptation to climate change impacts, including cascading and spill-over effects and improved cross-border management, both within the EU and at wider transboundary levels, of new and emerging climate change induced risks and impacts.

This includes science-to-practice knowledge exchange and use of sustainable, cost-effective and inclusive approaches, like nature-based solutions.

c) geological disasters, such as earthquakes, volcanic eruptions and tsunamis

Given the devastating potential of such disasters, R&I needs to support better preparedness for and response after such events. This includes better and technologically advanced civil protection capacities, notably faster detection and evacuation of victims.

d) pandemics and emerging infectious diseases[1]

The most critical part in fighting pandemics and infectious diseases is earlier detection of outbreaks. Here exists a big potential for improvement via targeted R&I. Besides the detection, projects can explore ways to better respond, for example by European Pandemic Preparedness Plans[2] informed by scenario development, enhanced capabilities in case of cross-border events through validating operational strategies and technologies in real-case scenarios.

---

[1]   Activities in relation to pandemics and emerging infectious diseases will complement those undertaken under the cluster 'Health'.
[2]   See the requirement for Preparedness Plans in Decision No 1082/2013/EU on serious cross-border threats to health, as well as the link with the International Health Regulations (2005).

4.2 Protection and Security

4.2.1 EU external borders
This priority aims to support air, land and sea EU border management and is expected to allow for more effective implementation as a result of improved knowledge about human and societal factors underlying cross-border threats. The European Border and Coast Guard Agency (Frontex) will be closely associated with relevant R&I activities, taking into account its central role – proposed by the Commission (COM(2018) 631) – in defining capability requirements for the European Border and Coast Guard.

An effective border management relies on comprehensive information and its exchange between Member States and EU Agencies. R&I will therefore enhance the interoperability and performance of relevant EU information systems, leading to better and faster exchange as well as analysis.

With specific reference to movement of persons, whether crossing borders legally or illegally, the contribution of the European Border and Coast Guard Agency in identifying the relevant research requirements will be crucial. This should lead to the development of tools and methods for Integrated Border Management, in particular to increase reaction capability and capacity for monitoring movements across external borders. This will allow for better risk-detection, incident response and crime prevention.

Concerning the flow of goods, projects are expected to address requirements identified by EU customs authorities, most notably improved detection of fraudulent activities at border crossing points and throughout the supply chain.

4.2.2 Protection of public spaces[3]
The core target of this priority is improved security and public safety, while at the same time preserving the open nature of urban public spaces. All measures to be explored by R&I in this area should ensure that citizens can continue their daily lives without major intrusions.

To achieve higher security for public space, research 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 increase the capacity to detect explosives, firearms and other weapons, as well as CBRN-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 potential targets have the potential to reduce the potential impacts of such attacks.

---

[3]   This priority also relates to the intervention area 4.1 Disaster-resilient societies.

4.2.3 Security and resilience of infrastructure and vital societal functions[4]
Activities conducted under the umbrella of this priority will ensure security and resilience of basic societal functions such as healthcare, law enforcement, energy, mobility, public services, financial services, communication and logistics infrastructures and networks (both physical, on ground and in space, and digital), so as to minimise societal disruptions.

In order to allow for effective countermeasures, there is a need for better risk assessments, especially taking into account interdependencies between different critical infrastructures and cascading risks arising from their disruption.

To better prevent and detect attacks (including cyber and hybrid attacks) or natural hazards as well as to allow for quick response, R&I will bring new tools for security actors (police, relief workers, disaster managers, crisis managers) notably in the fields of communication, surveillance and advanced robotics.

Technologies and also new concepts and cooperation instruments will help mitigation of consequences and allow for faster recovery of service performance levels, including leveraging the potentials of big data and artificial intelligence.

4.2.4 Maritime security
This priority addresses capability requirements identified by the EU Maritime Security Action Plan. Research activities will therefore enable better maritime surveillance, risk awareness and management of EU critical maritime infrastructure border protection and coast guard functions. The scope of maritime security in this regard includes man-made and natural disasters, accidents, climate change as well as security threats such as terrorism and piracy, cyber, hybrid and CBRN threats.

The EU Maritime Security Research Agenda lays down in this regard specific areas to be addressed, including cybersecurity, interoperability and information sharing, autonomous systems, networking and communication systems and multi-purpose platforms.

4.2.5 Fighting crime and terrorism
This priority aims to bring improved prevention, investigation and mitigation of impacts of criminal acts, including of new/emerging types (such as those resulting from digitisation). This needs to be based on a deeper knowledge of human and social aspects of relevant societal challenges, such as violent radicalisation, child sexual exploitation, trafficking of

---

[4] This priority also relates to the intervention area 4.3 Cybersecurity.

human beings and cybercriminality, including support to victims.[5] Research can further help to transpose such knowledge into the operational activities of EU law enforcement agencies and civil society organisations.

R&I will support law enforcement agencies in better tackling crime, including cybercrime and terrorism as well as the different forms of serious and organised crime (such as smuggling, money laundering, counterfeiting of products, drugs trafficking, environmental crime or illicit trafficking of cultural goods[6]) by developing new technologies, tools and systems (including digital tools, e.g. artificial intelligence). This refers especially to capabilities to analyse in near-real-time large volumes of data to forestall criminal events, or to combat disinformation and fake news with implications for security.

In addition to improved knowledge and prevention, projects will deliver operational tools for enhanced criminal investigation capabilities for law enforcement agencies. 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, R&I allows to generate knowledge for counter-terrorism on the continuously evolving methods related to dangerous chemicals, and the development of technologies to counter and respond to related incidents.

4.3 Cybersecurity
Supported by R&I under this priority, citizens, public authorities and companies, including SMEs, will be empowered to protect their data and online activities notably when using social media. Research will be aligned with the activities of the Cybersecurity Competence Centre and Network of National Coordination Centres (Commission proposal COM(2018) 630)[7] will take into account activities of the pilot networks of cyber competence networks and will be coordinated with the Digital Europe Programme.

This requires a resilient critical digital infrastructure, both private and public, that better protects the Digital Single Market and the digital life of citizens against malicious cyber activities, including via non-digital fall-back technology and appropriate levels of systemic redundancy. Research should strengthen European cybersecurity industrial capacities and thus increase the strategic autonomy vis-à-vis foreign technologies.

R&I will support in this regard use of innovative digital technologies, including self-healing, artificial intelligence, cryptography, massively distributed computing and storage, as well as

---

[5]   Activities in relation to smuggling and trafficking of persons will complement those undertaken in relation to migration under the 'Social and Economic Transformations' priority of the cluster 'Culture, Creativity and Inclusive Society'.

[6]   Activities in relation to trafficking of cultural goods will complement those undertaken under the 'Cultural Heritage' priority of the cluster 'Culture, Creativity and Inclusive Society'.

[7]   The proposed Regulation is still under discussion.

quantum to increase data security and augment cybersecurity. It will further allow for security-relevant innovations in the area of governance of algorithms, coding architecture and programming languages. All these measures are aiming at defending the EUs high standards concerning right to privacy, protection of personal data, and the protection of fundamental right in the digital age on the global stage.

The frequency and complexity of cyber-attacks from state and/or criminal actors is increasing rapidly. R&I will therefore need to support the effectiveness and coordination of measures to respond to them.

An emerging threats in the cyber-area are attacks against democracy and European societies, including electoral meddling, fake news, and online forgeries and manipulation. In order to allow for an adequate response for the coming years, research is necessary to better understand the nature and source of such attacks as well as technologies and strategies to counter them.

For all activities against cyber-threats, the architectural principles of 'security-by-design' and 'privacy-by-design' will be implemented in digital technologies and their applications, such as 5G, industry 4.0, artificial intelligence, Internet of Things, blockchain, quantum key distribution, mobile devices and connected cooperative and autonomous mobility and energy.

5. European Partnerships
No new partnerships are currently suggested under this cluster.

6. Missions

One of the main novelties of Horizon Europe is the introduction of missions; high-ambition, high-profile initiatives which will put forward concrete solutions to challenges facing European citizens and societies. Missions are currently in the process of being defined within five areas;

- adaptation to climate change including societal transformation
- cancer
- healthy oceans, seas, coastal and inland waters
- climate-neutral and smart cities
- soil health and food

Accomplishing missions will require a cross-cutting approach, drawing on research and innovation activities defined not only through individual Clusters, but across Horizon Europe and beyond. Research and innovation activities within this Cluster thus have the potential to support missions in all of the above-mentioned areas. The synergies between each mission and cluster will be further explored as possible missions take shape.