Horizon EUROPE - Specific Programme

proposal for a Decision of the Council [ST_8550/19_INIT]

PILLAR II - Global Challenges and European Industrial Competitiveness

CLUSTER III – CIVIL SECURITY FOR SOCIETY

The EU is confronted by many challenges, some of which are also global challenges. The scale and complexity of the problems are vast, need to be tackled jointly and matched by adequate, properly trained and skilled human resources, by the appropriate amount of financial resources and a proportionate effort in order to find solutions. These are precisely the areas where the EU must work together; smart, flexible and joined-up for the benefit and well-being of all our citizens.

Greater impact can be obtained through aligning actions with other nations and regions of the world within international cooperation along the lines indicated by the United Nations 2030 Agenda for Sustainable Development and the Sustainable Development Goals and the Paris climate agreement. Based on mutual benefit, partners from across the world will be invited to join EU efforts as an integral part of research and innovation for sustainable development.

Research and innovation are key drivers of sustainable and inclusive growth and technological and industrial competitiveness. They will contribute to finding solutions to today's problems, and the problems of tomorrow, in order to reverse as quickly as possible, the negative and dangerous trend that currently links economic development with the growing use of natural resources and growing social challenges. This will turn the challenges into new business opportunities and into rapid benefits for society.

The EU will benefit as user and producer of knowledge, technologies and industries showcasing how modern industrialised, sustainable, inclusive, creative, resilient, open and democratic society and economy can function and develop. The growing economic-environmental-social examples of the sustainable economy of the future will be fostered and boosted, be they for: health and well-being for all; or resilient, creative and inclusive societies; or societies strengthened by civil security; or available clean energy and mobility; or a digitised economy and society; or a transdisciplinary and creative industry; or space-related, marine or land-based solutions; or a well-functioning bioeconomy, including food and nutrition solutions; sustainable use of natural resources, protection of the environment, climate change mitigation and adaptation, all generating wealth in Europe and offering higher quality jobs. Industrial transformation will be crucial, as well as developing EU innovative industrial value chains.

New technologies affect virtually all policy areas. For each separate technology there is often a combination of social and economic opportunities, opportunities for efficiency and quality and improvement of the government, consequences for employment and education, but also possible risks for safety, privacy and ethics. Technology policy therefore necessarily requires an integral weighing of interests, and cross-sectoral cooperation and strategy formulation.

Research and innovation under this pillar of Horizon Europe is grouped into integrated, non-siloed broad clusters of activities. Rather than addressing sectors, the investments aim at systemic changes for our society and economy along a sustainability vector. These will only be achieved if all actors, both private and public, engage in co-designing and co-creating research and innovation; bringing together end-users, scientists, technologists, producers, innovators, businesses, educators, policy-makers, citizens and civil society organisations. Therefore, none of the clusters is intended for only one set of actors and all activities will be implemented primarily by collaborative research and innovation projects selected on the basis of competitive calls for proposals.

In addition to addressing global challenges, activities in the clusters will also develop and apply, key enabling and emerging technologies (either or not digital-based) as part of a common strategy to promote the EU's industrial and social leadership. Where appropriate this will use EU space-enabled data and services. All TRL levels up to 8 will be covered in this pillar of Horizon Europe without prejudice to Union competition law.

Actions will generate new knowledge and develop technological and non-technological solutions, bring technology from lab to market and to develop applications including pilot lines and demonstrators, and include measures to stimulate market uptake and to boost private sector commitment and incentives to standardisation activities within the Union. Technologies require critical mass of European researchers and industry to establish world leading eco-systems, that include state of the art technology infrastructures e.g. for testing. Synergies with other parts of Horizon Europe and the EIT, as well as other programmes will be maximised.

The clusters will boost the quick introduction of first-of-its-kind innovation in the EU through a broad range of embedded activities, including communication, dissemination and exploitation, standardisation as well as support to non-technological innovation and innovative delivery mechanisms, helping create innovation friendly societal, regulatory and market conditions such as the innovation deals. Pipelines of innovative solutions originating from research and innovation actions will be established and targeted to public and private investors as well as other relevant EU and national or regional programmes. Synergies will be developed with the third pillar of Horizon Europe in that perspective.

Gender equality is a crucial factor in order to obtain sustainable economic growth. It is therefore important to integrate a gender perspective in all global challenges.

Cluster 2: 'Civil Security for Society'

3.1 Rationale

European cooperation has contributed to an era of unprecedented peace, stability and prosperity on the European continent. However, Europe has to respond to the challenges arising from persistent threats to the security of our increasingly complex and digitalised society. Terrorist attacks and radicalisation, as well as cyber-attacks and hybrid threats, raise major security concerns and put particular strain on societies. New, emerging security threats caused by new technologies in the near future, also require attention. Future security and prosperity depend on improving the abilities to protect Europe against such threats. These cannot be dealt with purely by technological means but require knowledge about people, their history, culture and behaviour, and include ethical considerations regarding the balance between security and freedom. Moreover, Europe has to ensure its non-dependence on security-critical technologies and support the development of breakthrough security technologies.

European citizens, state institutions, EU bodies and the economy need to be protected from the continued threats of terrorism and organised crime, including firearms trafficking, drug trafficking and trafficking in human beings and trafficking of cultural goods. Human and social dimensions of criminality and violent radicalisation require better understanding so as to improve public policies in terms of security. Strengthening protection and security through better border management, including maritime and land borders, is also key. Cybercrime is on the increase and related risks are diversifying as the economy and society digitalise. Europe needs to continue its efforts to improve cybersecurity, digital privacy, personal data protection and combat the spread of false and harmful information in order to safeguard democratic, social and economic stability. Further efforts are required to limit the effects on lives and livelihoods of extreme weather events which are intensifying due to climate change, such as floods, storms, heat waves or droughts leading to forest fires, land degradation and other natural disasters, e.g. earthquakes. Disasters, whether natural or human-made, can put at risk important societal functions and critical infrastructures, such as communication, health, food, drinking water, energy supply, transport, security and government.

This requires both technical research and research into the human factors involved to improve disaster resilience, including, where appropriate, testing applications, training and cyber hygiene and education. More efforts are needed to evaluate the results of security research and promote their uptake.

This cluster will seek synergies, in particular with the following Programmes: Internal Security Fund, Integrated Border Management Fund and Digital Europe as well as improved research and innovation cooperation between intergovernmental agencies and organisations including through exchange and consultation mechanisms for example in the intervention area 'Protection and Security'.

Security research is part of the wider comprehensive EU response to security threats. It contributes to the capability development process by enabling the future availability of technologies, techniques and applications to fill capability gaps identified by policy-makers and practitioners and civil society organisations. Already, funding to research through the EU's framework programme has represented around 50% of total public funding for security research in the EU. Full use will be made of available

instruments, including the European space programme (Galileo and EGNOS, Copernicus, Space Situational Awareness and Governmental Satellite Communications). Whereas research and innovation activities under this Programme will have an exclusive focus on civil applications, coordination with EU-funded defence research will be sought in order to strengthen synergies, recognizing that there are areas of dual-use technology. Duplication of funding is avoided. Cross-border collaboration contributes to developing a European single security market and improving industrial performance, underpinning the EU's autonomy. Due attention will be given to the human understanding and perception of security.

Security research responds to the commitment of the Rome Agenda to work towards "a safe and secure Europe", contributing to a genuine and effective Security Union.

Activities will contribute directly to the following Sustainable Development Goals (SDGs) in particular: SDG 16 – Peace, Justice and Strong Institutions.

3.2 Areas of Intervention

3.2.1 Disaster-Resilient Societies

Disasters may arise from multiple sources, whether natural or human-made, including those from terrorist attacks, climate-related and other extreme events (including from sea level rises), from forest fires, heat waves, floods, droughts, desertification, earthquakes, tsunamis and volcanic events, from water crises, from space weather events, from industrial and transport disasters, from CBRN events, as well as those from resulting cascading risks. The aim is to prevent and reduce the loss of life, harm to health and the environment, trauma as well as economic and material damage from disasters, ensure food, medicine supply and services and water security as well as to improve the understanding and reduction of disaster risks and enhance post-disaster recovery. This implies covering the full spectrum of crisis management: from prevention and training, to crisis management and post-crisis management and resilience.

BROAD LINES:

- Technologies, capabilities and governance for first responders for emergency operations in crisis, disaster and post-disaster situations and the initial phase of recovery;
- The capacities of society to better prevent, manage and reduce disaster risk, including through nature-based solutions, by enhancing forecasting capabilities, prevention, preparedness and response to existing and new risks and domino effects, impact assessment and a better understanding of the human factor in risk management and risk communication strategies;
- More effectively support the build-back-better philosophy of the Sendai Framework through better understanding of post-disaster recovery and research into more effective post-disaster risk assessment;
- Interoperability of equipment and procedures to facilitate cross-border operational cooperation and an integrated EU market.

3.2.2 Protection and Security

There is a need to protect citizens from and to respond to security threats from criminal including terrorist activities and hybrid threats; to protect people, public spaces and critical infrastructure, from both physical (including CBRN-E) attacks and cyber-attacks; to fight terrorism and violent radicalisation, including understanding and tackling terrorist ideas and beliefs; to prevent and fight serious crime, including cybercrime, and organised crime (such as piracy and counterfeiting of products); to support victims; to trace criminal financial flows; to develop new forensic capabilities; to support the use of data for law enforcement and to ensure the protection of personal data in law enforcement activities; to strengthen border protection capabilities, to support air, land and sea EU border management, for flows of people and goods and to understand the human factor in all these security threats and in their prevention and mitigation. It is essential to maintain flexibility to rapidly address new and unforeseen security challenges that may arise.

BROAD LINES:

- Innovative approaches and technologies for security practitioners (such as police forces, fire brigades, medical services, border and coast guards, customs offices), in particular in the context

of, digital transformation and interoperability of security forces, operators of infrastructure, civil society organisations, and those managing open spaces;

- Analysis of cross-border crime phenomena, advanced methods of fast, reliable, standardised and privacy enhanced data sharing and collection as well as best practices;
- Human and socio-economic dimensions of criminality and violent radicalisation, in relation to those engaged or potentially engaged in such behaviour as well as to those affected or potentially affected, including understanding and tackling terrorist ideas and beliefs and crimes based on gender, sexual orientation or racial discrimination;
- Analysis of security aspects of new technologies such as DNA-sequencing, genome editing, nanomaterials and functional materials, Artificial Intelligence, autonomous systems, drones, robotics, quantum computing, cryptocurrencies, 3D printing and wearables, blockchain, as well as improving awareness of citizens, public authorities and industry to prevent the creation of new security risks and to reduce existing risks, including from those new technologies;
- Improved foresight and analysis capabilities for policy making and at strategic level on security threats;
- Protection of critical infrastructures as well as open and public spaces from physical, digital and hybrid threats, including the effects of climate change;
- Monitoring and combatting disinformation and fake news with implications for security, including developing capabilities to detect the sources of manipulation;
- Technological development for civil applications with the scope to enhance, where appropriate, interoperability between civil protection and military forces;
- Interoperability of equipment and procedures to facilitate cross-border, intergovernmental and inter-agency operational cooperation, and develop an integrated EU market;
- Developing tools and methods for an effective and efficient Integrated Border Management, in particular to increase reaction capability and improved capacity to monitor movements across external borders to enhance risk detection, incident responding and crime prevention;
- Detection of fraudulent activities at border crossing points and throughout the supply chain, including identifying forged or otherwise manipulated documents and detecting trafficking in human beings and illicit goods;
- Ensuring the protection of personal data in law enforcement activities, in particular in view of rapid technological developments, including confidentiality and integrity of information and traceability and processing of all transactions;
- Developing techniques for identifying counterfeit products, for enhancing protection of original parts and goods and for controlling transported products.

3.2.3 Cybersecurity

Malicious cyber activities not only threaten our economies but also the very functioning of our democracies, our freedoms and our values. Cyber threats are often criminal, motivated by profit, but they can also be political and strategic. Our future security, freedom, democracy and prosperity depend on improving our ability to protect the EU against cyber threats. The digital transformation requires improving cybersecurity substantially, to ensure the protection of the huge number of IoT devices expected to be connected to the internet, and the safe operation of network and information systems, including for power grids, drinking water supply and distribution, vehicles and transport

systems, hospitals, finances, public institutions, factories, homes. Europe must build resilience to cyber-attacks and create effective cyber deterrence, while making sure that data protection and the freedom of citizens are strengthened. It is in the Union's interest to ensure that it develops and retains essential cybersecurity strategic capacities in order to secure the Digital Single Market, and, in particular, to ensure the protection of critical networks and of information systems and to provide key cybersecurity services. The Union must be in a position to autonomously secure its digital assets and to compete on the global cybersecurity market.

BROAD LINES:

- Technologies across the digital value chain (from secure components and quantum-resistant cryptography to self-healing software and networks);
- Technologies, methods, standards and best practices to address cybersecurity threats, anticipating future needs, and sustaining a competitive European industry, including tools for electronic identification, threat detection, cyber hygiene, as well as training and education resources;
- An open collaboration for European cybersecurity competence network and competence centre.