Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism

The Lisbon Treaty enables the EU to act to develop itself as an area of freedom, security and justice. The EU Security Union is now in the building, and requires an EU-wide approach to security that integrates prevention, investigation and mitigation capabilities in the area of the fight against crime.

The globalisation of communications and finance infrastructure allows crime to develop and take new forms. Trafficking in human beings for all forms of exploitation purposes is a serious and organised crime often with cross-border dimension, violating fundamental rights of the individuals and creating a security challenge. Prevention of child sexual abuse and exploitation is another area where research is acutely needed. The use of the internet as a platform for child sex offenders to communicate, store and share child sexual exploitation material and to hunt for new victims continues to be one of the internet’s most abhorrent aspects. Cybercriminality, as a whole, is not satisfactorily understood nor properly addressed; the constantly expanding attack surface combined with the ever increasing number of attack vectors requires a more structured approach. Radicalisation is yet another challenge of our society that requires a multi-disciplinary approach, with policy recommendations and practical solutions to be implemented by a variety of policy-makers and practitioners.

Proposed approaches need to rely on existing knowledge and to exclude approaches that have previously failed. The societal dimension of fight against crime and terrorism should be at the core of the proposed activities. Proposals should be
submitted by consortia involving relevant security practitioners and civil society organisations, each under only one of the following sub-topics:

- **Sub-topic 1: [2018] New methods to prevent, investigate and mitigate trafficking of human beings and child sexual exploitation – and on the protection of victims**

Globalisation and technological developments facilitate trafficking in human beings and child sexual exploitation. A variety of preventive measures, as well as measures to ensure adequate victim protection and assistance are needed, that build upon advances in social sciences and humanities.

Proposals in this subtopic should address both phenomena in a balanced way. They should ensure that the research focuses on prevention, investigation and/or assistance related to all victims of trafficking and not only addressing child trafficking. In the same way, the proposals should cover any area concerning prevention, investigation and/or assistance to victims of child sexual exploitation, not only the assistance to victims of child sexual exploitation resulting from trafficking.

With respect to the trafficking of human beings, research should bear on:

- preventing the phenomenon and to reduce the demand for all forms of exploitation in the trafficking chain and its legal and illegal sectors. The analysis of possible involvement of organized crime groups implicated in trafficking of human beings in other crimes as well (e.g. financial crimes) is recommended;
- new approaches to investigate cases involving the trafficking of human beings;
- new approaches to mitigate the impact on victims in the short and long term.

Regarding child sexual exploitation:

- how to address new threats, such as live-streaming of child abuse and coercion and extortion of victims that have escalated in the last years;
- how to provide law enforcement with effective means to detect, investigate and bring down the many peer-to-peer networks and the growing number of forums on the darknet that facilitate the exchange of child sexual exploitation material and support offenders;
- how to help victims of abuse during criminal investigations and court procedures;
- how to help the victims in the long term, to help them deal with the effects;
- how to reduce risks of (re-)offending by better understanding the behaviour of abusers and potential abusers.

**Sub-topic 2: [2019] Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour**

The Internet of Things, the ever increasing number of internet-connected devices, may pose substantial threats to (cyber)security since this fully connected world as well as the network itself have become a target for cybercriminals. The key challenge
in this respect is to determine what the drivers of new forms of cyber criminality are and how they might be prevented and mitigated. The dissemination of "cybercrime-as-a-service" business models is an important enabler for crime and poses significant challenges to security. The increasing variety of such services, the modalities through which they are offered and the connections with different criminal activities need to be investigated to understand their trends and thus to allow for prevention and law enforcement.

Human factors determining online behaviour as described for instance by the online disinhibition effect (individuals acting more boldly online, being less inhibited and with their judgment impaired) are drivers for cybercrime as individuals feel disconnected from the actual crime or do not even perceive it as a crime. Recent trends also indicate a growth in cyber juvenile delinquency and a rise in adolescent hacking.

These developments call for further research in domains such as psychology, criminology, anthropology, neurobiology and cyber psychology to understand better the factors contributing to it and to devise preventive and deterrence measures, including providing alternatives to harness the potential of these young talents for cybersecurity and technologies.

- Sub-topic 3: [2020] Developing comprehensive multi-disciplinary and multi-agency approaches to prevent and counter violent radicalisation and terrorism in the EU
- Sub-topic: [2018-2019] Open

Proposals analysing and recommending other ways to solve human, social, and societal issues in fighting against crime and terrorism, and supported by large numbers of practitioners, are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of privacy, protection of personal data and free movement of persons. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience, gender-related behaviours) have to be addressed in a comprehensive and thorough manner.

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately through multidisciplinary projects confronting different schools of thought. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

The free and democratic EU society, based on the rule of law, mobility across national borders, globalised communication and finance infrastructure, provides
many opportunities to its people. However, the benefits come along with risks related to crime and terrorism, a significant number of which have cross-border impacts within the EU. Security is a key factor to ensure a high quality of life and to protect our infrastructure through preventing and tackling common threats. The EU must play its part to help prevent, investigate and/or mitigate the impact of criminal acts, whilst protecting fundamental rights. The consistent efforts made by EU Member States and the EU to that effect are not enough, especially when criminal groups and their activities extend far beyond national borders.

Medium term:

- improved and consolidated knowledge among EU Law Enforcement Agencies officers on the issues addressed in this topic;
- exchange of experiences among EU Law Enforcement Agencies about human, social and societal aspects of security problems and their remedies;
- policy-making toolkits for security policy-makers, to support the establishment of a European Security Model;
- toolkits for EU Law Enforcement Agencies and/or civil society organisations, validated against practitioners' needs and requirements to facilitate their daily operations.

Long term:

- European common approaches for assessing risks/threats, and identifying and deploying relevant security measures, which take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as the rights to privacy, to protection of personal data and the free movement of persons;
- support towards the implementation of the European Security Union by strengthening the perception by citizens of the EU as an area of freedom, justice and security;
- advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals.

Last update: 16 April 2019


European Union, 2024