


Technologies to enhance the fight against crime and terrorism

There is a growing need to focus on technology opportunities provided by new and emerging technologies. To this end, it is necessary to identify new knowledge and targeted technologies for fighting old, new and evolving forms of criminal and terrorist behaviour supported by advanced technologies. Challenges are numerous. In conventional investigations, rapid and near real-time forensics is often crucial for preventing subsequent attacks or crimes. A consequence of the increasing digitisation of society and ever increasing adoption levels is that virtually any type of crime has a digital forensics component, which is a challenge in itself. Money-flow tracking represents yet another challenge. The issues of location and jurisdiction need to be addressed, taking into account highly probable cross-border nature of such crimes.

Proposals should be submitted under only one of the following sub-topics:

- Sub-topic 1: [2019] Trace qualification

Forensic analysis of trace material can be extremely helpful in the initial phase of investigation, if the answers are rapid (near real-time), at an acceptable cost and compliant with criminal justice. Novel robotized or automated tools for forensic analysis should be developed. There is a need for a better knowledge and interpretation of: trace composition, time when they were left, cause of their origin (crime-related or inoffensive), etc.

Proposers are encouraged to address how they contribute to the European Forensic Science Area. [[The Council Conclusions and the related Action Plan on the way forward in view of the creation of an European Forensic Science Area (EFSA) adopted on 9 June 2016: <http://data.consilium.europa.eu/doc/document/ST-10128-2016-INIT/en/pdf> .]]

- Sub-topic 2: [2018-2019] Digital forensics in the context of criminal investigations

New forensic tools, techniques and methodologies are needed, based on common practices, standards, protocols and/or interoperability requirements that allow for rapid retrieval, storage, analysis and validation of digital evidence (including the one stored in the cloud) that upholds in court, and enables investigations to identify perpetrators as well as victims, in particular in cases of child sexual abuses. They should focus on data gathering, data exploitation, and speedy exchange of information. All types of crime, terrorist activities and propaganda, and malicious acts by foreign-state perpetrators are concerned. Research in this domain should take into account new and emerging trends (for instance, abuse of encryption for criminal or terrorist purposes), while fully respecting fundamental rights such as the right to privacy and the right to protection of personal data.

In 2019, proposals should focus on data gathering, classification and exploitation, as well as speedy exchange of information in the context of child sexual abuses investigations, taking into account main and emerging trends (for instance, intensive use of Peer to Peer network, anonymous activity on the Dark Web and abuse of encryption).

- Sub-topic 3: [2020] Money flows tracking

Organized crime increasingly adopts technology (for example, pseudo-legal sales, shadow economy, internet/Darknet as well as cryptocurrencies) as a facilitator for preparation, organisation and execution of various physical/traditional criminal activities (e.g. child sexual abuse, trafficking of organs or human embryos, trafficking of human beings, trafficking of firearms, drug trafficking, money laundering and terrorism) and/or as a tool for online criminal activities (e.g. ransomware, domain-name piracy, phishing). Furthermore, there is a need for governing and detecting cross-border money flows with the potential to support terrorism, for reinforcing effective and legitimate public-private cooperation for the sharing of financial data, and for strengthening the effectiveness of current methods of countering terrorism financing and of modelling abnormal transactions in the fight against terrorism.

Research should address the following issues: approaches to identify new developments (new markets and networks; new modi operandi); tools for tracing money flows as well as those engaged in criminal activities online whilst ensuring privacy and protection of personal data; Darknet marketplace analysis and mobility; tools for locating and mapping hidden service directories; tools for forensic analysis of digital media in order to identify digital currency datasets; data provenance models (providing evidence that is admissible in court), including the relationship between algorithmic proof artefacts and legal evidence.

- Sub-topic 4: [2020] Development and deployment of technologies, tools and relevant infrastructure to identify speedily terrorist content online, and prevent its re-upload

To address the threat of terrorist content online, the Commission has adopted a proposal for a Regulation on 12 September 2018.[[COM(2018) 640 final]] Under the proposal a number of measures would be required to be taken by Member States (in particular law enforcement authorities)/Europol and hosting service providers. Hosting service providers from around the world (covering social media, cloud services, file sharing, etc.) offering their services to EU citizens would be required to put in place a certain number of measures, ranging from speedy reactive ones e.g. one hour deadline to remove or disable terrorist contents following a removal order from a Member State authority (considering that terrorist content is most harmful in the first hours of its appearance online) to proactive measures, including automated detection, in order effectively and swiftly to remove or to disable terrorist content and to stop it from reappearing and being disseminated once it has been removed.

Under the proposal, these measures would need to be implemented not only by large companies, but also by micro enterprises and SMEs, irrespective of size or turnover, albeit remaining proportionate. Putting in place such proactive/automated means is likely to create a burden on resources, hence mitigating measures for the benefit of smaller companies should be envisaged. Research should therefore be leveraged to support the development and deployment of technologies, tools and relevant infrastructure to identify speedily terrorist content online, and to prevent its re-upload. The media content analysis could play a relevant role in the development of tools for the active detection of harmful online behaviour (e.g. with natural language processing or image/video content analysis). The beneficiaries of such projects should include SMEs so as to ensure that the technology developed would be of direct relevance to their platforms. A further global take-up and dissemination of these technologies, tools and infrastructure where relevant should also be encouraged.

- Sub-topic: [2018-2019-2020] Open

Proposals addressing other issues relevant to this challenge (for instance: technologies to improve LEAs capabilities (including augmented reality); autonomous systems to improve the fight against crime and terrorism; technologies to support better protection of public figures; tracking and monitoring technologies, including automated prevention of uploading terrorism-related content; capabilities to detect the widest possible range of threats and concealments (including complex concealed weapons)) and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions).

In all sub-topics and in order to facilitate the EU-wide take-up of new technologies, proposers are encouraged to include the design of innovative curricula for LEAs training and (joint) exercises, and of information packages for the wider public and civil society organisations.

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

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Organized crime and terrorist organisations are often at the forefront of technological innovation in planning, executing and concealing their criminal activities and the revenues stemming from them. Law Enforcement Agencies (LEAs) are often lagging behind when tackling criminal activities supported by advanced technologies.

Medium term:

- novel, user-friendly technologies, tools and/or systems, addressing traditional or emerging forms of crime and terrorism at acceptable costs;
- improved investigation capabilities, especially regarding quality and speed;
- increased efficiency and effectiveness of the information sharing among EU LEAs.

Long term:

- prevention/reduction of criminal and terrorist threats;
- harmonisation of information formats at international level, improved cross-border acceptance and exchange of court-proof evidence, standardised evidence collection and harmonised procedures in the investigation of trans-border crimes in full compliance with applicable legislation on protection of personal data.

Letzte Aktualisierung: 12 April 2024

Permalink: https://cordis.europa.eu/programme/id/H2020_SU-FCT02-2018-2019-2020/de

