EU Security Research in Fight against Crime and Terrorism

Call 2019

Policy context

The European Agenda on Security defines the priority actions at EU level to ensure an effective EU response to security threats over the period 2015-2020:

*(…)"**Terrorism, organised crime and cybercrime** are the three core priorities which are highlighted in this Agenda for immediate action. They are clearly interlinked and cross-border threats, and their multi-faceted and international dimension shows the need for an effective and coordinated response at EU level". (…)*

(…)"The response to cybercrime (e.g. phishing) must involve the entire chain: from Europol's European Cybercrime Centre, Computer Emergency Response Teams in the Member States concerned by the attack, to internet service providers that can warn end-users and provide technical protection. In short, cybercrime demands a new approach to law enforcement in the digital age." (…)

The 9th Security Union progress report

Based on a comprehensive assessment of EU security policy since 2001, the report highlights the remaining gaps and challenges to be addressed.

Incomplete implementation of existing policies remains a challenge, as do evolving threats such as radicalisation and cybercrime — which may require changes to existing instruments.

Policy context
Forensics

06/2016: Council Conclusions on the way forward in view of the creation of a European Forensic Science Area

- A detailed action plan with six specific areas:
  - Best Practice Manuals for forensic disciplines.
  - Stimulating exchange of forensic information from databases, for example in the area of weapons and ammunition, explosives and drugs.
  - Proficiency tests and collaborative exercises for forensic disciplines.
  - Forensic awareness and training for law enforcement and justice communities.
  - Stimulating accreditation of forensic service providers and competence of forensic personnel on a voluntary basis.
  - Stimulating exchange of forensic data via Prüm and improving quality.
- The Council noted that additional funding from the European Commission would be crucial for implementing the new action plan and developing the European Forensic Science Area, calling for support for forensic sciences via Horizon 2020 and Internal Security Funds

Policy context
Cybercrime

09/2017: Cybersecurity package (COM(2017)477)

- **A more effective law enforcement response focusing on detection, traceability and the prosecution of cyber criminals** is central to building an effective disincentive to commit such crimes. The Commission is therefore proposing to boost deterrence through new measures to combat fraud and the counterfeiting of non-cash means of payment.

- The proposed Directive will strengthen the ability of law enforcement authorities to tackle this form of crime by expanding the scope of the offences related to information systems to all payment transactions, including transactions through virtual currencies. The law will also introduce common rules on the level of penalties and clarify the scope of Member States' jurisdiction in such offences.

- Background: Recent figures show that digital threats are evolving fast and that the public perceives cyber-crime as an important threat: Whilst ransomware attacks have increased by 300% since 2015, the economic impact of cyber-crime rose fivefold from 2013 to 2017, and could further rise by a factor of four by 2019, studies suggests. **87% of Europeans regard cybercrime as an important challenge to the EU's internal security.**

Policy context
Child sexual abuse and exploitation

09/2017: Cybersecurity package (COM(2017)477)

- (12/2016) the Commission adopted two reports on the measures taken by MSs to combat the sexual abuse and sexual exploitation of children and child pornography:
  - One report covers the entire Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011/92/EU);
  - The other report focuses on the measures against websites containing or disseminating child pornography.
- The reports present a first overview of measures taken by Member States to transpose the Directive into national law. The reports show that, although the Directive has led to substantial progress, there is still considerable room for improvement, in particular with regard to **prevention and intervention programmes for offenders, the assistance, support and protection measures for child victims, the prompt removal of child sexual abuse material in Member States' territory** and the provision of adequate safeguards when the optional blocking measures are applied.

Policy context
Anti-terrorism, "soft targets" & abuse of encryption

The 11th Security Union progress report (10/2017): Commission presented **anti-terrorism package** to better protect EU citizens - a package of operational and practical anti-terrorism measures to be rolled out over the next 16 months. These measures will help MSs address vulnerabilities exposed by recent terrorist attacks and will make a real difference in enhancing security. The measures will, amongst other:

- Support Member States in protecting public spaces (and so-called "*soft target*" protection);
- Close the space in which terrorists can operate by further restricting access to explosive precursors and improving cross border access to financial information;
- Support law enforcement and judicial authorities that encounter encryption by criminals in criminal investigations;
- Set out the next steps on countering radicalisation;
- Reinforce the EU's external action on counter-terrorism.

WP 2018-2020: SEC Call – FCT
SU-FCT01-2018-2019-2020

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

- A specific sub-topic each year; in 2019:
  - Sub-topic 2: Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour
- 'Open' sub-topic

- **EU contribution of about 5 M€ per proposal**

WP 2018-2020: SEC Call – FCT
SU-FCT02-2018-2019-2020

- **Technologies to enhance the fight against crime and terrorism**

- A specific sub-topic each year; in 2019:
  - **Sub-topic 1:** Trace qualification
  - **Sub-topic 2:** Digital forensics in the context of criminal investigations (focus on CSE)
- 'Open' sub-topic

- **TRL 4-6**
- **EU contribution of about 5 M€ per proposal**

Eligibility criteria for SU-FCT01 and SU-FCT02

- **Predefined subtopics: at least 3 LEAs from at least 3 different EU or Associated countries**

- **Sub-topic: Open requires at least 5 LEAs from at least 5 different EU or Associated countries**

WP 2018-2020: SEC Call – FCT
SU-FCT03-2018-2019-2020

- **Information and data stream management to fight against (cyber)crime and terrorism**
- Open in 2018, 2019 and 2020
- Big Data analysis, AI, OSINT gathering, predictive analytics in fight against (cyber)crime and terrorism:
  a) to characterise trends in cybercrime and cybercriminal organisations, and
  b) to enhance citizens security against terrorist attacks in places considered as soft targets
- 'Open' sub-topic
- TRL 5-7
- EU contribution of about 8 M€ per proposal

Eligibility criteria for SU-FCT03

- Involvement of at least 3 LEAs from at least 3 different EU or Associated countries
- The duration of the proposed activities must not exceed 24 months

Budgetary overview

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 19 Mar 2019				
SU-FCT01-2018-2019-2020 (RIA)	**10**	**10**		22-Aug-19
SU-FCT02-2018-2019-2020 (RIA)	**21**	**28,16**		
SU-FCT03-2018-2019-2020 (IA)	**8**	**8**		

Thank you!

#InvestEUresearch

www.ec.europa.eu/research

Participant Portal www

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-su-sec-2018-2019-2020.html