



Why Should I Care?

- ✓ Opportunity to find, co-work and co-develop with the best academic and industry expertise. Contribute to future industry standards, certifications, regulation etc. Get <u>independently</u> <u>validated</u> in problem-solution and product-to-market-fit phases!
- ✓ Your competitors (even US Fortune 500 companies) are utilizing funding either directly or indirectly.
- ✓ Build international R&D <u>networks</u> and <u>commercial</u> channels.
- ✓ Get access to hard to find IP (e.g. patents, data, algorithms)
 and get new technology and IP licensing income (partners!).





SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

IA | EUR 7-8M | Opening 12 Mar 2020 | DL 27 Aug 2020 Specific Challenge: Recent events demonstrate the increase of combined physical and cyber-attacks due to their interdependencies. A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent installations, plants and systems. Scope: To forecast, assessment of physical and cyber risks, prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs), and fast recovery after incidents, achieving the security and resilience.



SU-Al01-2020: Developing a research roadmap regarding Artificial Intelligence in support of Law Enforcement

CSA | EUR 1.5M | Opening 12 Mar 2020 | DL 27 Aug 2020 Specific Challenge: To better understand AI: 1) proactive policing (from reactive to anticipative policing); 2) data analysis (e.g., connecting the dots, discovering criminal patterns); 3) identity checks (improving detection, targeting and interdiction). Scope: To provide an EU AI roadmap for LEAs, meeting their specific operational and cooperation needs, by identifying the key areas in which AI would be beneficial, where it could pose a threat to security, cybersecurity requirements for LEAs, as well as means of prevention and mitigation of malicious use of Al.



SU-Al02-2020: Secure and resilient Al technologies, tools and solutions in support of Law Enforcement and citizen protection against adversarial Al

IA | EUR 17M | Opening 12 Mar 2020 | DL 27 Aug 2020 Specific Challenge: How to mostly benefit from the AI based technologies in enhancing EU's resilience against newly emerging security threats (both "classical" and new AI supported) and in reinforcing the capacity of the Law Enforcement Agencies. Scope: To develop AI tools and solutions in support of LEAs daily work. This should include combined hardware and software solutions such as robotics or Natural Language Processing. To develop cybersecurity tools and solutions. To exploit Al technologies for cybersecurity operation purposes of LE.



SU-Al03-2020: Human factors, and ethical, societal, legal and organisational aspects of using Al in support of Law Enforcement

CSA | EUR 1.5M | Opening 12 Mar 2020 | DL 27 Aug 2020 | Specific Challenge: The lack of transparency of AI technologies and tools complicates their acceptance by users and citizens. Ethical and secure-by-design algorithms are necessary to build trust in this technology. To build a human-centred & socially driven AI.

<u>Scope</u>: An exhaustive analysis of human, social and organisational aspects related to the use of AI tools, including gender related aspects, in support of Law Enforcement, both for cybersecurity and the fight against crime, cybercrime, terrorism.



SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism

IA | EUR 8M | Opening 12 Mar 2020 | DL 27 Aug 2020

Specific Challenge: Large amounts of data and information from a variety of origins have become available to practitioners involved in fighting crime & terrorism. Lacks analysis capacities. Scope: The effectiveness of law enforcement action depends on capabilities to improve the quality of data, and to convert voluminous and heterogeneous data sets (images, videos, geospatial intelligence, communication data, traffic data, financial transactions related date, etc.) into actionable intelligence. E.g. darknets, IoT, wearable devices, 3D printers, autonomous cars...



SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches

IA | EUR 6-8M | Opening 12 Mar 2020 | DL 27 Aug 2020 | Specific Challenge: The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity.

<u>Scope</u>: The proposals should demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks and data breaches. E.g. (i) assessing vulnerabilities and threats, (ii) designing adequate security measures, (iii) implementing resilience tests, (iv) demonstrating the effectiveness of the measures with a cost-benefit analysis.





AI4EU

- ✓EUR 20 M, 87 participants, 22 countries, 36 mo project.
- ✓ AI4EU will distribute €3 million equity-free among individuals, start-ups and SMEs. Organizes <u>AI4EU Web Café Sessions</u>.
- ✓ <u>AI Prototypes</u>: AI4EU will select 25 individuals who could be researchers, students or developers per open call. Beneficiaries can receive to €30,000 and a 4-month support program to develop prototypes based on AI resources.
- ✓ <u>Tech Transfer program</u>: AI4EU will select 20 Scale-ups that
 could be financed up-to €180,000 in equity-free cash.



WORLD IDEAS

Pekka Rantala Senior Advisor Expert, National Contact Point (ICT, eHealth, Cyber) +358 50 396 2922 pekka.rantala@businessfinland.fi